

INSTITUT D'ESTUDIS CATALANS
SECCIÓ DE CIÈNCIES I TECNOLOGIA

PILAR BAYER
JORDI GUÀRDIA
ARTUR TRAVESA

ARRELS GERMÀNIQUES DE LA MATEMÀTICA CONTEMPORÀNIA

Amb una antologia de textos matemàtics de 1850 a 1950

BARCELONA
2012

INSTITUT D'ESTUDIS CATALANS
SECCIÓ DE CIÈNCIES I TECNOLOGIA

PILAR BAYER
JORDI GUÀRDIA
ARTUR TRAVESA

ARRELS GERMÀNIQUES DE LA MATEMÀTICA CONTEMPORÀNIA

Amb una antologia de textos matemàtics de 1850 a 1950

BARCELONA
2012

Biblioteca de Catalunya. Dades CIP

Bayer i Isant, Pilar, 1946-

Arrels germàniques de la matemàtica contemporània : amb una antologia de textos matemàtics de 1850 a 1950

Bibliografia. Índex

ISBN 9788499651194

I. Guàrdia, Jordi II. Travesa i Grau, Artur

III. Institut d'Estudis Catalans. Secció de Ciències i Tecnologia

1. Matemàtica – Alemanya – Història – S. XIX 2. Matemàtica – Alemanya – Història – S. XX
51(430)''18/19''

DIRECCIÓ

Pilar Bayer Isant. Institut d'Estudis Catalans

AUTORIA

Pilar Bayer Isant. Facultat de Matemàtiques. Universitat de Barcelona

Jordi Guàrdia Rúbies. Escola Politècnica Superior d'Enginyeria de Vilanova i la Geltrú. Universitat Politècnica de Catalunya

Artur Travesa Grau. Facultat de Matemàtiques. Universitat de Barcelona

PERSONAL TÈCNIC

Maria Teresa Sucarrats Pous. Assessora lingüística

Dionís Remón Adell. Facultat de Matemàtiques. Universitat de Barcelona

Classificació AMS: Primària: 01A75, 00B50. Secundària: 01A45, 01A50, 01A55, 01A60, 01A61, 01A65, 01A72, 01A73, 01A74, 01A75, 11-03, 30-03, 33-03, 34-03, 49-03

Amb suport parcial de MTM2006-04895, MTM2009-07024, MTM2009-13060-C02-02 i de Caixa de Terrassa

© dels seus textos i de la traducció, Pilar Bayer Isant, Jordi Guàrdia Rúbies i Artur Travesa Grau

© 2012, Institut d'Estudis Catalans, per a aquesta edició
Carrer del Carme, 47. 08001 Barcelona

Primera edició: juny del 2012

Tiratge: 200 exemplars

Imprès a Service Point FMI, SA

ISBN: 978-84-9965-119-4

Dipòsit Legal: B-19051-2012

Són rigorosament prohibides, sense l'autorització escrita dels titulars del copyright, la reproducció total o parcial d'aquesta obra per qualsevol procediment i suport, incloent-hi la reprografia i el tractament informàtic, la distribució d'exemplars mitjançant lloguer o préstec comercial, la inclusió total o parcial en bases de dades i la consulta a través de xarxa telemàtica o d'Internet. Les infraccions d'aquests drets estan sotmeses a les sancions establertes per les lleis.

Irrtum verlässt uns nie; doch ziehet ein höher Bedürfnis
immer den strebenden Geist leise zur Wahrheit hinan.

J. W. Goethe

Vier Jahreszeiten, Herbst

Prefaci

Reproduir una visió sistemàtica i unificadora de la història de les idees matemàtiques dels darrers segles és una feina ingent que caldria, però, plantejar-se algun dia. Comporta fer un estudi acurat de l'evolució dels diferents conceptes matemàtics i de com aquests s'han anat fertilitzant per la interacció de diferents escoles.

De manera molt més modesta, aquesta obra ofereix un apropament a un recull de treballs de matemàtiques que, desenvolupats a Alemanya entre 1850 i 1950, han tingut una forta repercussió en algunes de les fites assolides per la matemàtica contemporània.

Si bé l'avenç de les matemàtiques no és pas privatiu de cap nació ni de cap època, la història posa de manifest que, en determinats llocs i en determinats moments, circumstàncies excepcionals han derivat cap a una creació matemàtica remarcable, tant per la seva originalitat i la seva profunditat com pel seu impacte posterior. L'escola matemàtica d'Alexandria i la transmissió dels seus resultats a Occident ofereixen un exemple paradigmàtic d'aquest fet.

Un segon exemple, potser menys popular, és el de la matemàtica que es desenvolupà a Alemanya en el decurs del segle XIX i el primer terç del segle XX. A partir de 1930, però, gran part dels científics alemanys hagueren d'emigrar cap als Estats Units i la Unió Soviètica, ja fos per causa del seu origen o per motius polítics. Es pot dir que el règim nazi aconseguí destruir, en poc més d'una dècada, l'emplaçament d'una tradició secular de pensament matemàtic, al mateix temps que es produïa la desintegració d'unes escoles que, com les de Berlín i de Göttingen, eren pols d'atracció d'estudiants i d'investigadors d'arreu del món.

La matemàtica creada a Alemanya esdevingué en certa manera universal perquè, un cop acabada la Segona Guerra Mundial, se'n començaren a difondre i a treballar els resultats. Massa sovint, però, els textos moderns s'han escrit d'una manera asèptica; n'ha interessat el vessant formal i, en pro d'una pretesa *neutralitat de la ciència*, no s'hi han esmentat ni els antecedents, ni la procedència de les idees. Durant molts anys, l'evolució matemàtica ha operat en contradicció flagrant amb l'axioma *Natura non facit saltus* —admès des d'Aristòtil i fins a l'adveniment de la mecànica quàntica.

Un cop assolida la globalització actual de la matemàtica, aquesta ha deixat d'expressar-se en alemany, francès, suec, noruec, italià, rus, japonès o xinès (dissortadament, no ha parlat mai gaire cap de les llengües peninsulars) per a passar a fer-ho en anglès, *en benefici de tothom*.

D'entrada, el fet de disposar d'una *lingua franca* per a difondre el pensament científic —com ho fou en el seu moment el llatí— és bo, però es pot confondre amb un mètode de democratització de la ciència. Cal no oblidar que, en els

segles en què el llatí fou d'ús científic universal, aquest ja no era l'idioma privatiu de cap país, per la qual cosa el seu sentit anivellador i unificador era indiscutible. Cap científic no gaudia de l'immens privilegi de poder expressar-se i de poder formar-se amb l'ús *exclusiu* de la seva pròpia llengua. A l'extrem contrari ens trobem els matemàtics de parla catalana, perquè només ocasionalment podem accedir a la lectura de textos de recerca escrits en català.

Les obres d'aquesta antologia han estat escollides pel desig de fer abastables uns desenvolupaments matemàtics que es troben en l'origen de sofisticades tècniques actuals. Se n'ofereix una mostra, petita però representativa, traduïda al català, a fi que es puguin apreciar —esperem que amb tota comoditat— els seus infinits matisos.

Els articles seleccionats en aquesta ocasió han estat els deu següents:

RIEMANN, B.: Über die Anzahl der Primzahlen unter einer gegebenen Grösse. *Monatsberichte der Berliner Akademie* (November, 1859), p. 145–153. Reproduït a *Gesammelte mathematische Werke*, editat per H. Weber, Teubner, Leipzig 1892, p. 671–680.

KRONECKER, L.: Über die auflösung der Pellschen Gleichung mittels elliptischer Functionen. *Monatsberichte der Königlich Preussischen Akademie der Wissenschaften zu Berlin* (1863), p. 44–50.

THOMAE, C. J.: Beitrag zur Bestimmung von $\vartheta(0, 0, \dots, 0)$ durch die Klassenmoduln algebraischer Functionen. *J. reine u. angew. Math.* **71** (1870), p. 201–222.

DEDEKIND, R.: Schreiben an Herrn *Borchardt* über die Theorie der elliptischen Modul-Functionen. *J. reine u. angew. Math.* **83** (1877), p. 265–292.

FUCHS, L.: Über eine Klasse von Functionen mehrerer Variabeln, welche durch Umkehrung der Integrale von Lösungen der linearen Differentialgleichungen mit rationalen Coefficienten entstehen. *J. reine u. angew. Math.* **89** (1880), p. 151–169.

FROBENIUS, G.: Über die constanten Factoren der Thetareihen. *J. reine u. angew. Math.* **98** (1885), p. 244–263. Reproduit a *Gesammelte Abhandlungen* II, p. 241–260.

NOETHER, E.: Invariante Variationsprobleme. *Nachr. v. d. Ges. d. Wiss. zu Göttingen* (1918), p. 235–257.

DEURING, M.: Die Typen der Multiplikatorenringe elliptischer Functionenkörper. *Abh. Math. Sem. Hansischen Univ.* (després, *Abh. Math. Sem. Hamburg*) **14** (1941), p. 197–272.

SPRAGUE, R.: Über Zerlegungen in ungleiche Quadratzahlen. *Math. Z.* **51** (1948), p. 289–290.

RICHERT, H.: Über Zerfällungen in ungleiche Primzahlen. *Math. Z.* **52** (1949), p. 342–343.

Tant les obres seleccionades com els autors s'han contextualitzat. Això ha comportat, d'una banda, la redacció d'una primera part dedicada a la gènesi i el desenvolupament de les matèries tractades, així com també a la seva ubicació en les dues escoles més representatives de la matemàtica alemanya d'abans de la Segona Guerra Mundial: l'escola de Berlín i l'escola de Göttingen. D'altra banda, ha comportat la recerca d'apunts biogràfics de les figures

estudiades i, també, d'alguns dels seus predecessors i coetanis. Alhora, no ens hem abstingut de remarcar aquells trets històrics que, al nostre entendre, tingueren repercussions rellevants en l'assoliment d'una recerca i una docència universitàries excel·lents.

Agraïments

La realització d'aquesta obra ha estat possible gràcies als projectes *Matemàtiques a l'abast: de l'alemany al català* (I i II), de l'Institut d'Estudis Catalans que, en particular, ens permeteren disposar de la senyora Maria Teresa Sucarrats en qualitat d'assessora lingüística; al projecte ministerial MTM2006–04895, del qual en foren investigadors Pilar Bayer i Artur Travesa i que, amb el cofinançament de la Caixa de Terrassa, ens permeté disposar del senyor Dionís Remón en qualitat de tècnic; al projecte ministerial MTM2009–07024, del qual en són investigadors Pilar Bayer i Artur Travesa; i al projecte ministerial MTM2009–13060–C02–02, del qual n'és investigador Jordi Guàrdia.

Expressem el nostre agraïment a la Universitat de Barcelona i a la Facultat de Matemàtiques i Estadística de la Universitat Politècnica de Catalunya per haver possibilitat la reproducció parcial dels textos de Pilar Bayer [17], [18], i [19].

Contingut

I	Arrels històriques	1
1	L'inici de la matemàtica a Alemanya	3
1.1	Les primeres càtedres	6
1.2	Les Corts germàniques	7
1.3	La Universitat de Leipzig	11
1.4	Leibniz	12
1.5	La Universitat de Göttingen	19
1.6	Gauss	21
1.7	<i>Disquisicions aritmètiques</i>	28
1.8	La Universitat de Berlín	33
1.9	La Universitat de Königsberg	34
1.10	Jacobi	35
1.11	Integrals el·líptiques i funcions theta	38

2	L'escola de Berlín	47
2.1	Dirichlet	50
2.2	Kummer	52
2.3	Enters algebraics	55
2.4	Weierstrass	60
2.5	Funcions el·líptiques	62
2.6	Kronecker	65
2.7	El <i>Somni de Joventut</i>	68
2.8	Fuchs	71
2.9	Thomae	77
2.10	Frobenius	81
2.11	Sprague	107
3	L'escola de Göttingen	109
3.1	Riemann	112
3.2	Funcions abelianes	115
3.3	Dedekind	127
3.4	Funcions zeta	131
3.5	Klein	133
3.6	Hilbert	138
3.7	Els 23 problemes de Hilbert	142
3.8	Àlgebres no commutatives	153

3.9	Teoria de cossos de classes	160
3.10	Emmy Noether	166
3.11	Deuring	187
3.12	Funcions L de corbes el·líptiques	191
3.13	Richert	198
4	Impacte del nacionalsocialisme	201
4.1	Irrupció del règim nazi a la vida cultural i científica	201
4.2	Impacte a l'escola matemàtica de Berlín . .	204
4.3	Impacte a l'escola matemàtica de Göttingen	205
II	Antologia	209
5	Riemann	211
5.1	1859: La memòria sobre els nombres primers	211
5.2	<i>Sobre la quantitat de nombres primers per sota d'una quantitat donada</i>	227
6	Kronecker	241
6.1	1863: El treball sobre l'equació de Pell . . .	242
6.2	<i>Sobre la resolució de l'equació de Pell mit- jançant funcions el·líptiques</i>	249

7	Thomae	257
7.1	1870: La fórmula de Thomae	258
7.2	<i>Contribució a la determinació de $\vartheta(0, \dots, 0)$ per mitjà dels mòduls de classes de funcions algebraïques</i>	263
8	Dedekind	301
8.1	1877: La funció <i>valència</i>	303
8.2	<i>Escrit al Sr. Borchardt sobre la teoria de les funcions modulars el·líptiques</i>	313
9	Fuchs	357
9.1	1880: El problema de la inversió d'integrals	357
9.2	<i>Sobre una classe de funcions de més d'una variable que s'originen per la inversió d'in- tegrals de solucions d'equacions diferencials lineals de coeficients racionals</i>	363
10	Frobenius	395
10.1	1885: Constants theta jacobianes	395
10.2	<i>Sobre els factors constants de les sèries theta</i>	405
11	Emmy Noether	439
11.1	1918: Simetries i lleis de conservació	440
11.2	<i>Problemes de variació invariants</i>	445

12 Deuring	481
12.1 El concepte de multiplicador	482
12.2 1941: Aportacions a la teoria de la multiplicació complexa	487
12.3 <i>Els tipus d'anells de multiplicadors dels cosos de funcions el·líptiques</i>	505
13 Sprague i Richert	621
13.1 1948–1949: Aportació a la teoria additiva de nombres	622
13.2 <i>Sobre descomposicions en nombres quadrats diferents</i>	627
13.3 <i>Sobre descomposicions en nombres primers diferents</i>	631
III Referències	635
Cronologia	637
Perfil biogràfic dels autors	689
Bibliografia	693

IV Índexs 749**Índex de figures 751****Índex de taules 753****Índex antroponímic 755**

Part I

Arrels històriques

Capítol 1

L'inici de la matemàtica a Alemanya

A fi de poder-nos situar en el context històric i polític, no necessàriament vinculat a la vida acadèmica, i conèixer millor alguns dels esdeveniments que feren possible el desenvolupament a Alemanya d'una etapa esplendorosa per a la matemàtica, ens ha semblat oportú incloure de bon començament un resum de la història d'aquest país.

L'Imperi Germànic sorgí de la part més oriental de l'Imperi Carolingi, segons la divisió acordada en el Tractat de Verdun de l'any 843. Des d'aleshores, a la història d'Alemanya podem distingir-hi set grans etapes, de les quals detallem tot seguit alguns fets remarcables.

• El Primer Reich o Sacre Imperi Romanogermànic (962–1806)

1158. Creació de la Lliga Hanseàtica

1517. Inici de la Reforma Luterana

1545–1555. Contrareforma. Pau d'Augsburg

1618–1648. Guerra dels Trenta Anys. Pau de Westfàlia

1701. Creació del Regne de Prússia amb Frederic I de Prússia

1756–1763. Guerra dels Set Anys

1806. Batalles de Jena i d'Auerstedt contra les tropes de Napoleó I

● **La Restauració (1806–1871)**

1806–1815. Confederació del Rin, amb Napoleó I

1815. Creació de la Confederació Germànica

1866. Guerra de les Set Setmanes

1867. Creació de la Confederació de l'Alemanya del Nord

1870–1871. Guerra Francoprussiana, amb la victòria dels estats germànics sobre les tropes de Napoleó III

● **El Segon Reich o l'Imperi Alemany (1871–1919)**

1871. Creació de l'Imperi Alemany, amb l'annexió d'Alsàcia i Lorena a la Confederació de l'Alemanya del Nord. Bismarck n'és nomenat canceller

1898. Desacord entre Bismarck i el Kàiser Guillem II.
Caiguda de Bismarck

1914–1918. Primera Guerra Mundial. Tractat de Versalles

- **La República de Weimar (1919–1933)**

1921. Davallada del valor del marc i hiperinflació

1929. Gran Depressió mundial

1932. Celebració d'eleccions i arribada al poder del Partit Nacional Socialista Alemany dels Treballadors

- **El Tercer Reich (1933–1945)**

1933. Nomenament d'Adolf Hitler com a Cap d'Estat

1939. Inici de la Segona Guerra Mundial

1939–1941. Invasió alemanya de França, Bèlgica, Holanda, Dinamarca, Luxemburg, els Balcans, Grècia, Noruega, Tunísia i Líbia

1941. Invasió alemanya de Rússia

1945. Ocupació d'Alemanya i capitulació

- **Les dues Alemanyas (1945–1990)**

1945. Conferència de Potsdam. Redefinició del mapa d'Europa

1947. Inici de la Guerra Freda

1949. Proclamació de la República Federal Alemanya

1949. Proclamació de la República Democràtica Alemanya

1954. Sobirania de la República Democràtica Alemanya

1955. Sobirania de la República Federal Alemanya

• La unificació alemanya (1990–)

1990. Caiguda del Mur de Berlín i Tractat d'Estat sobre la Unificació

1.1 Les primeres càtedres

L'interès per l'ensenyament de la matemàtica ve de lluny. En les universitats medievals, les matemàtiques formaven part de les set arts liberals. L'estudi del *trivium*, integrat per la gramàtica, la lògica i la retòrica, era seguit pel del *quadrivium*, integrat per l'aritmètica, la geometria, l'astronomia i la música. Els matemàtics islàmics es dedicaren en cos i ànima a la recuperació i a la traducció —a l'àrab i a l'hebreu— de textos matemàtics de l'antiguitat grega, alhora que avançaven en la confecció de taules trigonomètriques i en l'estudi de l'astronomia i creaven l'àlgebra.

En el Renaixement, els estudis de matemàtiques prengueren un altre caire: els coneixements de càlcul necessaris per a l'art de navegar i per a la pràctica del comerç eren

impartits regularment per mestres fora dels àmbits universitaris. El gran nombre d'aritmètiques mercantils impreses els segles XV i XVI són una prova fefaent d'aquesta situació. Un bon exemple de casa nostra és la *Suma de la art de Arismetica* de Francesc Santcliment, un incunable imprès a Barcelona per Pere Posa l'any 1482. Es tracta del segon llibre de matemàtiques imprès a Europa; el primer fou un llibre de característiques similars imprès a Treviso, prop de Venècia, l'any 1478. El mateix Santcliment adaptà l'obra al castellà i l'edità a Saragossa, també al Regne d'Aragó, l'any 1487.

El *trivium* i el *quadrivium* medievals derivaren en el Renaixement en les facultats d'arts i de filosofia; i és a redós d'aquestes on sorgiren les primeres càtedres universitàries europees de matemàtiques. Entre les més antigues figuren la càtedra de matemàtiques de la Universitat d'Aberdeen, a Escòcia (1505), la de la Universitat de Bolonya (1555), la càtedra de matemàtiques i astronomia de la Universitat de Barcelona (1576), la càtedra de geometria de la Universitat d'Oxford (1619) i la càtedra lucasiana de matemàtiques de la Universitat de Cambridge (1663), el segon titular de la qual fou Sir Isaac Newton, que l'ocupà l'any 1669. A Alemanya, cal arribar fins a l'any 1735, en què tingué lloc la fundació de la càtedra de matemàtiques de la Universitat de Göttingen.

1.2 Les Corts germàniques

La família dels Brunsvic es remunta a l'any 1235 i formà diverses branques a Europa. Una d'elles és la dels Electors

d'Hannover, d'on procedeix la família reial anglesa actual. Es convertí en una de les famílies més insignes de la reialesa alemanya protestant; en canvi, els Habsburg (o Àustria) eren coneguts pel seu catolicisme a ultrança.

La Guerra dels Trenta Anys (1618–1648), iniciada com a conflicte religiós dins del Sacre Imperi Romanogermànic entre estats partidaris de la Reforma i estats partidaris de la Contrareforma, acabà per convertir-se en una guerra europea. La Pau de Westfàlia i el Tractat dels Pirineus, amb els quals finalitzà, suposaren el punt més àlgid d'aquell segle de la rivalitat per l'hegemonia a Europa entre França i els territoris dels Habsburg: l'Imperi Espanyol i el Sacre Imperi Romanogermànic. La guerra assolà molt especialment els estats germànics, en què s'estima que hi provocà una disminució de la població d'entre un quinze i un trenta per cent.

En el segle XVIII, l'Alemanya actual estava constituïda per petits estats, els uns catòlics i els altres protestants, regits per governants absoluts. En els estats catòlics, l'ensenyament depenia de l'Església; en els estats protestants, l'ensenyament era públic. En aquests darrers, el naixement de noves universitats està íntimament lligat al mecenatge de certes famílies.

Un dels membres de la família dels Brunsvic del qual ens interessa parlar és Carles Guillem Ferran (1735–1806), Duc de Brunsvic i Lüneburg, i Príncep de Brunsvic, Lüneburg i Bevern des de l'any 1780. Es tracta d'un mariscal prussià que s'havia distingit a la Guerra dels Set Anys (1756–1763). El seu pare havia fundat, l'any 1745, el *Collegium Carolinum*, un institut d'educació superior que es convertí més endavant en la Universitat Tècnica de Brunsvic. Carles

Guillem Ferran era nebot de Frederic II el Gran, Rei de Prússia des de l'any 1740. Les Corts germàniques no tenien la pompa de les Corts franceses de la mateixa època; en canvi, s'esmerçaven a protegir filòsofs, músics i científics. El Príncep intentava traslladar a la seva Cort l'ambient culte que havia aconseguit el seu oncle.

A la fi del segle XVIII, l'ambient intel·lectual respirava una barreja de racionalisme i de romanticisme. D'una banda, es tenia la mirada posada en els cànons clàssics; de l'altra, es parlava de l'alliberament de l'esperit i del seu retorn a la natura. És el temps del moviment literari *Sturm und Drang* (1765–1785), que preconitzava la glorificació del geni (*Geniezeit*). Segons aquest corrent de pensament, les persones extraordinàriament dotades només han d'obeir els impulsos que els permeten la seva realització plena. La Revolució Francesa, l'any 1789, i les guerres napoleòniques, que s'estengueren entre 1799 i 1815, són esdeveniments que repercutiren en la vida científica de l'època.

La família dels Brunsvic està vinculada amb Barcelona a través de la figura d'Elisabet Cristina de Brunsvic Wolfenbüttel (1691–1750). Elisabet Cristina es casà a Barcelona amb l'Arxiduc Carles, el qual després esdevindria l'Emperador Carles VI, en la numeració dels Àustria. Fou així Emperadriu d'Àustria i Reina de Catalunya i Aragó a partir de l'any 1708. Fou la mare de Maria Teresa d'Àustria (1717–1780) i l'àvia, per tant, de Maria Antonieta (1755–1793). Elisabet Cristina i Carles són els Àustria que es retiren de Barcelona, l'any 1714, quan Catalunya passa a mans dels Borbó. No solament l'expulsió dels àrabs i dels jueus fou perjudicial per al desenvolupament de la ciència en el nostre país, sinó també aquest altre moment, en el

qual persones interessades en les arts i les ciències abandonen Catalunya. L'any 1717, Felip V clausurà les vuit universitats catalanes existents aleshores, i concentrà els estudis universitaris en la Reial i Pontificia Universitat de Cervera. La Universitat de Barcelona romangué tancada 120 anys, fins a la seva restauració, l'any 1837.

D'altra banda, Frederic II nomenà Alexander Georg von Humboldt camarlenc d'Elisabeth Cristina de Charlottenburg (o de Brunsvic-Lüneburg), primera esposa del seu nebot i hereu al tron de Prússia, Frederic Guillem II. El seu pare havia estat oficial de l'exèrcit prussià i ascendit a la noblesa. Alexander Georg es casà amb Elisabeth von Holwede, nascuda Colomb, una vídua rica amb la qual tingué dos fills, Wilhelm von Humboldt i Alexander von Humboldt, l'educació dels quals transcorregué entre el palau que la mare tenia a les seves possessions de Tegel i a la ciutat de Berlín. Com a supervisor dels seus preceptors tingueren a Gottlob Johann Christian Kunth, que els procurà una educació exquisida, que incloïa macroeconomia, estadística, dret natural, filosofia, i llengües clàssiques i modernes. L'objectiu d'aquesta educació era preparar els germans per al desenvolupament de càrrecs importants de govern. Després d'un semestre a la Universitat de Frankfurt de l'Oder, Wilhelm es matriculà a la Universitat de Göttingen l'any 1788. A principis del segle XIX, els germans von Humboldt tindrien un paper sobresortint en el ressorgiment de l'Estat Prussià, que, com la resta, estava arruïnat després de les guerres amb Napoleó. Una de les fites que aconseguiren fou la fundació de la Universitat de Berlín, l'any 1810. Hi ha constància que, prèviament a la fundació d'aquesta, els dos germans Humboldt havien viatjat al nostre país, amb

estades al Monestir de Montserrat. Alexander ho feu l'any 1799 i Wilhelm, l'any 1800.

1.3 La Universitat de Leipzig

Una de les universitats més antigues d'Europa és la Universitat de Leipzig, localitzada a l'antic Regne de Saxònia. Fou fundada l'any 1409 per Frederic I, Elector de Saxònia, i pel seu germà Guillem II, d'acord amb una butlla papal emesa pel Papa Alexandre V. Al principi constà de quatre facultats: Filosofia i Lletres, Teologia, Medicina, i Lleis.

En aquesta universitat, l'evolució del pensament filosòfic vers el pensament matemàtic es produí dos segles i mig més tard per mitjà de les figures de Mencke i de Leibniz.

Mencke fou un filòsof i científic del segle XVII que obtingué el seu doctorat l'any 1665 a la Universitat de Leipzig amb una tesi sobre teologia natural. La teologia natural era una branca de la metafísica que després de Leibniz es conegué amb el nom de teodicea; el seu objectiu principal és arribar al coneixement de Déu per mitjà de la raó, sense implicar-hi la revelació. No és estrany que els filòsofs que s'hi dedicaren fossin també persones amb vocació científica. Mencke, juntament amb Leibniz, fou el fundador, l'any 1682, de la primera revista científica alemanya, anomenada *Acta Eruditorum*, i amb ell s'inaugurà una dinastia matemàtica que comptaria amb les remarcables figures de Gauss i de Hilbert.

1.4 Leibniz

Gottfried Wilhelm von Leibniz (Leipzig, 1 de juliol de 1646; Hannover, 14 de novembre de 1716)

Leibniz, juntament amb Newton, fou un dels científics més importants de l'Europa del seu temps. Nasqué dos anys abans del final de la Guerra dels Trenta Anys. Fou fill de Friedrich Leibniz, jurista i professor de filosofia moral de la Universitat de Leipzig, i de Catherina Schmuck, filla d'un professor de lleis. L'any 1661, a l'edat de 14 anys, ingressà a la Universitat de Leipzig, on completà els seus estudis als 20 anys, després d'haver-se especialitzat en lleis i haver adquirit un domini dels clàssics, de lògica i de filosofia escolàstica. Això no obstant, la seva educació en matemàtiques no estava a l'altura de la que podien adquirir els estudiants francesos o els britànics. L'any 1666 publicà el seu primer llibre, *Sobre l'art de les combinacions*, la primera part del qual, *Disputatio arithmetica de complexionibus*, constituí la seva tesi d'habilitació en filosofia. Després que la Universitat de Leipzig declinés assegurar-li una plaça docent en lleis, Leibniz optà, el mateix any 1666, per lliurar la seva tesi en lleis, *Disputatio Inauguralis De Casibus Perplexis In Jure*, a la Universitat d'Altdorf. Tot seguit declinà l'oferiment d'un lloc acadèmic a Altdorf per a dedicar la resta de la seva vida al servei de famílies preeminents de la noblesa alemanya. L'any 1676 encara presentaria una tercera tesi, aquesta a la Reial Acadèmia de Ciències de París (*Académie Royale des Sciences de Paris*), sota la direcció de Christiaan Huygens.

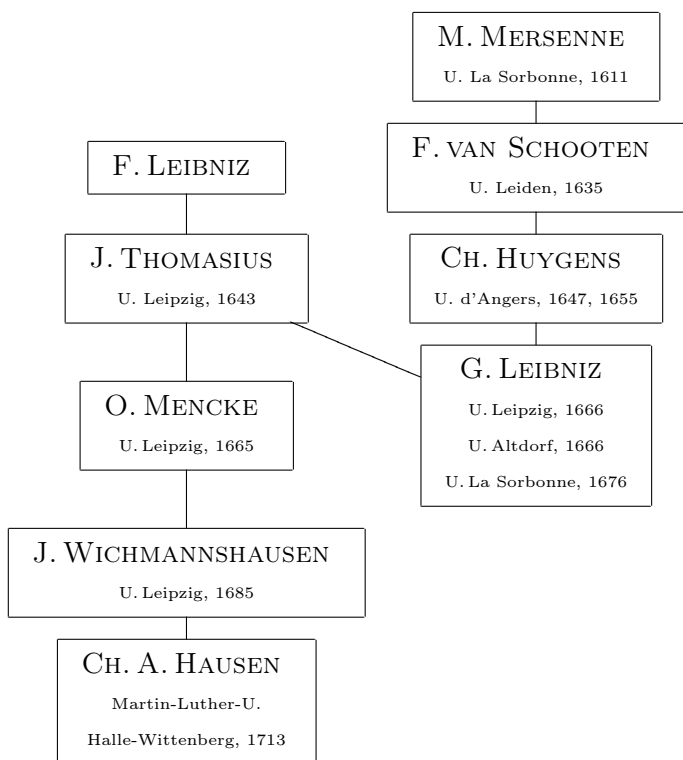
Diverses missions diplomàtiques que li foren encomanades el portaren a viatjar en el decurs de tota la seva vida.

Leibniz, doctorat ja en lleis i a fi de protegir els estats alemanys, proposà distreure Lluís XIV oferint-li que França envaís Egipte com a primer pas vers la conquesta de les Índies Orientals Holandeses. A canvi, França s'havia de comprometre a no pertorbar ni Alemanya ni Holanda. L'any 1672, el Govern francès invità Leibniz a París per a la negociació d'aquella iniciativa. Però l'inici de la guerra entre França i Holanda avortà la iniciativa en aquells moments. (De fet, la idea s'implementà més d'un segle més tard en la invasió d'Egipte per les tropes de Napoleó.)

D'aquesta manera, Leibniz inicià una estada a París d'uns quants anys, durant els quals incrementà els seus coneixements de matemàtiques i de física fins al punt de realitzar-hi contribucions originals. Conegué Nicolas Malebranche i Antoine Arnauld, filòsofs francesos de l'època; estudià els escrits de Descartes i de Pascal, i inicià una llarga amistat amb el matemàtic alemany Ehrenfried Walther von Tschirnhaus, amb qui mantingué correspondència fins al final dels seus dies. Especialment important fou la seva relació amb el matemàtic i físic holandès Christiaan Huygens, qui aleshores també es trobava a París i que li féu de mentor en diverses ocasions.

A principis de 1673, i quan es féu patent que França no portaria a terme el seu pla egipci, Leibniz fou enviat a una missió diplomàtica a Londres. Davant de la Reial Societat Britànica (*British Royal Society*), mostrà una màquina calculadora que havia estat dissenyant i construïnt des de 1670. Es tractava de la primera màquina que podia executar les quatre operacions aritmètiques bàsiques; ja apuntava cap a nocions de maquinari i de programari que després serien treballades per Charles Babbage i Ada

Lovelace. Es deu a Leibniz la descoberta del sistema binari, que constitueix el fonament de la pràctica totalitat de les arquitectures dels computadors actuals.



Taula 1: Els precursors

L'any 1677 Leibniz fou promogut, per voluntat pròpia, a Conseller Privat de Justícia, càrrec que mantingué la resta de la seva vida. Estigué al servei de tres governants consecutius de la Casa de Brunsvic com a historiador, com a conseller polític i com a bibliotecari de la Biblioteca Du-

cal. Des d'aleshores es dedicà a escriure documents polítics, històrics i teològics relatius a la Casa de Brunsvic.

Sortosament, els Brunsvic toleraren el gran esforç que Leibniz dedicava, al marge dels seus deures vers aquesta família, als seus propis projectes intel·lectuals, com ara el perfeccionament del càlcul, els escrits de matemàtiques, de lògica, de física o de filosofia, així com també al manteniment d'una vasta correspondència.

Leibniz advocà per la creació de societats científiques a Dresden, Sant Petersburg, Viena i Berlín que seguissin el model de la Reial Societat Britànica i de la Reial Acadèmia de Ciències de París, de les quals era membre corresponent. L'any 1700 aconseguí que es creés l'Acadèmia de Ciències de Berlín, de la qual en redactà els estatuts i en fou President fins a la fi dels seus dies. Aquesta institució portà inicialment el nom de *Societat de Ciències de l'Electorat de Brandenburg* (*Kurfürstlich-Brandenburgische Societät der Wissenschaften*) i després el de *Reial Acadèmia Prussiana de Ciències* (*Königlich-Preußische Akademie der Wissenschaften*).

La formació de Leibniz tingué un fort component escolàstic i aristotèlic, adquirit per la influència d'un dels seus professors a Leipzig, Jakob Thomasius, que fou el supervisor de la seva primera tesi. Els estudiosos també han detectat en la seva primera obra la influència de Ramon Llull i de Francisco Suárez, jesuïta espanyol conegut com a Doctor Eximius. Leibniz mostrà un profund interès pels mètodes nous de la seva època; esdevingué un bon coneixedor de l'obra de Descartes, Huygens, Newton i Boyle. És remarcable la seva influència posterior i com els seus mètodes i raonaments anticiparen el desenvolupament de la

lògica, de la filosofia analítica i de la lingüística del segle XX.

Leibniz començà a treballar en el càlcul l'any 1674. Les seves contribucions matemàtiques més importants foren publicades entre 1682 i 1692. Generalment aparegueren a *Acta Eruditorum*, revista que jugà un paper clau en la seva reputació com a matemàtic i contribuï a la seva rellevància com a diplomàtic, historiador, teòleg i filòsof.

Si bé trobem implícita la noció matemàtica de funció en la trigonometria i en les taules de logaritmes, existents en el temps de Leibniz, aquest fou el primer, entre 1692 i 1694, que les emprà explícitament per a denotar alguns conceptes geomètrics derivats del de corba, com per exemple els d'abscissa, d'ordenada, de tangent, de corda i de perpendicular o normal. Posteriorment, en el segle XVIII, el concepte de funció es deslligaria d'associacions geomètriques. Leibniz s'avançà també a la consideració de sistemes d'equacions lineals i al seu tractament pel mètode que després serà conegut com a eliminació gaussiana.

D'acord amb els quaderns de Leibniz, el dia 11 de novembre de 1675 tingué lloc per primera vegada l'ús del càlcul integral per a l'obtenció de l'àrea limitada per la corba definida per una funció, $y = f(x)$. En relació amb aquest fet, Leibniz introduí diverses notacions que encara són emprades en l'actualitat: el signe d'integració, $\int$, representat mitjançant una *S* allargada (la inicial llatina de *summa*), i el signe de diferencial, *d* (la inicial llatina de *differentia*). A més, Leibniz fou el primer a utilitzar el terme *analysis situs*, que en el segle XVIII seria emprat per Euler, en el seu famós treball de 1736 en què resol el problema dels ponts de Königsberg, i a finals del XIX per Poincaré, en un no

menys famós treball de 1895 al qual donava títol i que fou iniciador de la branca matemàtica coneguda avui amb el nom de topologia.

En els seus escrits, Leibniz concedí una gran importància a la notació. Per influència de Llull, creia que la simbologia era fonamental per a la transcripció del pensament humà. Avui se li reconeix el paper que tingué en el naixement de la lògica simbòlica. La seva aspiració de tenir un sistema universal de caràcters que permetés als humans transcriure els seus pensaments el dugué a definir la noció de *caràcter real* com aquell que *representa* directament una idea i no la paraula que la designa. Així, en el cas que es pogués portar a terme aquest programa, es podria manipular amb les idees tal com es fa amb els nombres en aritmètica o amb les figures en geometria.

Inspirat en el comportament dels nombres primers respecte a la resta dels nombres naturals, la lògica de Leibniz es basava en dos principis:

1. Totes les nostres idees es componen a partir d'un nombre d'idees *simples*, que constitueixen l'alfabet del pensament humà.

2. Les idees complexes s'obtenen a partir de les idees simples per mitjà d'una combinació *uniforme* i *simètrica* semblant a la de la multiplicació.

Aquest plantejament influí en l'evolució del pensament matemàtic que cercà en contextos diversos la noció d'objecte simple, de semisimple, o bé de compost, amb graus diferents de complexitat.

Leibniz escriví principalment en tres idiomes: llatí escolàstic, francès i alemany. De fet, lliçons universitàries en llengua alemanya es començaren a impartir per primera vegada a la Martin Luther Universität Halle Wittenberg per Christian Thomasius, a qui també havia dirigit la tesi el seu pare, Jakob Thomasius.

El pensament de Leibniz es troba dispers en multitud de cartes, en molts articles acadèmics, i en dos tractats filosòfics publicats en vida de l'autor: *De Ars combinatoria* i *Theodice*, de l'any 1710. La publicació crítica de la seva obra se subdivideix en set sèries d'escrits. Endegada per l'Acadèmia de Ciències de Berlín l'any 1923, compta amb 25 volums editats i encara no ha pogut ésser completada. Remarquem l'interès de les obres següents, relatives a la seva correspondència amb matemàtics i als seus textos matemàtics en general:

Der Briefwechsel von Gottfried Wilhelm Leibniz mit Mathematikern. Ed. C.I. Gerhardt. Berlín, 1899; reimpressió: Hildesheim, Georg Olms, 1962.

Leibniz' Mathematische Schriften. Ed. C.I. Gerhardt, 7 volums, Berlín, 1849–1863.

A la *Theodice*, Leibniz intenta justificar les imperfeccions del món físic; hi afirma que és el millor dels mons possibles i que cal que sigui així, atès que fou creat per un Déu perfecte. El seu és un Déu amb capacitat ordenadora, no moralment sinó matemàticament. Dels infinits mons possibles, Déu hauria trobat la variant més estable i homogènia, tot minimitzant-ne el mal. Tot i que l'afirmació segons la qual vivim en el millor dels mons possibles fou mal interpretada per alguns dels seus coetanis i filòsofs

posteriors, com ara Voltaire, els historiadors de la matemàtica no han passat per alt la influència directa del seu pensament en la gestació del càlcul de variacions per part d'Euler. En els dos segles posteriors a la seva mort, una defensa de la seva visió optimista de la creació conduiria a l'enunciat de principis científics avui fermament establerts en el camp de la física: el principi de la mínima acció i els de la conservació de la massa i de l'energia, per no parlar del principi antropomòrfic, segons el qual la realitat física està basada en el valor numèric de certes constants que determinen les lleis físiques, l'estructura de l'univers i, en última instància, fan possible l'existència de vida i d'intel·ligència en el nostre planeta.

1.5 La Universitat de Göttingen

Entre els anys 1734 i 1736 tingué lloc l'etapa fundacional de la *George Augustus Universität*, a la petita ciutat alemanya de Göttingen, per part de l'Electeur Georg August de Hannover, que era, al mateix temps, el Rei George II de Gran Bretanya i Irlanda. Aquesta universitat nasqué amb el nou esperit de la Il·lustració, de la mà de Gerlach Adolph, Baró de Münchhausen i Ministre de Hannover. Seguia el model de les universitats angleses d'Oxford i de Cambridge, i tenia fama per la seva independència respecte de l'Església i del Govern. La recerca científica s'hi portava a terme amb tota llibertat. Es concedí una importància primordial a la docència. I les biblioteques, que foren dotades econòmicament i desenvolupades sistemàticament, s'obriren per primera vegada als estudiants. A fi de potenciar les disciplines científiques emergents, Münchhausen creà noves càtedres,

que cobrí habitualment amb figures destacades en el seu àmbit.

Des de 1735, la Universitat comptà amb una càtedra de matemàtiques. El primer titular en fou Johann Andreas Segner, qui, alhora, s'encarregà de la construcció de l'Observatori astronòmic de la Universitat, obra que s'acabà l'any 1751. L'any 1755, amb l'ajut d'Euler, Segner es traslladà a Halle, on també construï un observatori, i fou professor a la *Martin Luther Universität* de Halle Wittenberg.

L'Acadèmia de Ciències de Göttingen fou fundada l'any 1751 i, pel seu treball conjunt amb la Universitat, jugà un paper decisiu a l'hora de convertir la ciutat en un centre científic europeu d'importància cabdal. Aquesta interacció trencà l'esquema, existent a l'època, que entenia les universitats com a centres exclusivament docents i les acadèmies com a centres exclusivament de recerca.

Des de molt al començament, la Universitat de Göttingen atragué nombrosos estudiants i científics d'Alemanya, d'Europa i de la resta del món.

Un d'aquests fou Kästner, que havia estudiat lleis, filosofia, física, matemàtiques i metafísica a la Universitat de Leipzig, en la qual s'habilità l'any 1739. L'any 1756 esdevingué professor de filosofia natural i de geometria a la Universitat de Göttingen i l'any 1763 fou nomenat director de l'Observatori astronòmic d'aquesta ciutat. Conegut també com a poeta d'una certa fama, els seus escrits matemàtics comprenen les obres *Fonaments de la matemàtica* (*Anfangsgründe der Mathematik*, Göttingen 1758–1769, 4 volums; 6a. edició de 1800) i *Història de la Matemàti-*

ca (*Geschichte der Mathematik*, Göttingen 1796–1800, 4 volums). L'any 1751 havia estat escollit membre de la Reial Acadèmia de Ciències de Suècia (*Kungliga svenska Vetenskapsakademien*), on fou traductor a l'alemany de diversos volums de les seves actes, incloent-hi tots els publicats entre 1784 i 1792. Entre els deixebles de Kästner hi ha Johann Pfaff, que seria posteriorment el director de la tesi de Gauss, i Farkas Bolyai, amic de Gauss en la seva època d'estudiant a Göttingen i pare de János Bolyai, un dels matemàtics implicats en el descobriment de les geometries no euclidianes.

1.6 Gauss

Johann Carl Friedrich Gauss (Brunsvic, 30 d'abril de 1777; Göttingen, 23 de febrer de 1855)

La vida de Gauss transcorregué entre dues ciutats pertanyents a dos estats protestants: Brunsvic, que era la capital del Ducat de Brunsvic-Lüneburg, i Göttingen, a l'Estat de Hannover. L'educació de Gauss fou finançada per Carles Guillem Ferran de Brunsvic. Entre els coetanis de Gauss, hi ha: Goethe (1749–1832) i von Schiller (1759–1805), en literatura; Kant (1724–1804) i Hegel (1770–1831), en filosofia; Mozart (1756–1791) i Beethoven (1770–1827), en música.

Pel que fa a les matemàtiques, Euler (1707–1783) morí quan Gauss comptava 6 anys. Legendre (1752–1833), Poisson (1761–1840) i Galois (1811–1832) són contemporanis seus, a França; Jacobi (1804–1851) i Dirichlet (1805–1859) ho són a Alemanya; i Abel (1802–1829) ho és a Noruega.

Als 15 anys, Gauss havia ingressat en el *Collegium Carolinum*, una institució acadèmica estatal, moderna, orientada cap als estudis científics. El centre comptava amb una biblioteca excel·lent, on Gauss es pogué familiaritzar amb obres de Newton, d'Euler i de Lagrange.

Als 18 anys, Gauss es traslladà a la Universitat de Göttingen. Per a Gauss, anar a estudiar a Göttingen implicava anar-se'n a l'estranger, car aquesta ciutat pertanyia a l'Estat de Hannover, diferent doncs de Lüneburg. El Príncep hauria preferit que Gauss estudiés a la Universitat de Helmstedt, fundada l'any 1569 i situada en el seu propi estat, però Gauss no ho volgué adduint l'excel·lència de la Biblioteca de la Universitat de Göttingen. Quan Gauss estudiava, aquesta estava ubicada a l'església de Sant Pau (*Paulinerkirche*). Encara avui, l'edifici és seu d'una biblioteca i sala d'exposicions.

L'eclosió del talent matemàtic de Gauss tingué lloc en el decurs dels seus anys d'estudiant a la Universitat de Göttingen. Quan comptava 19 anys, aquell jove estudiant descobrí que el polígon regular de 17 costats és construïble amb regla i compàs i, segons ell mateix explica, s'adonà dels principis generals que permeten la caracterització dels polígons regulars construïbles amb aquests instruments. Exposà els seus resultats a Kästner, que no se'n féu ressò. Però el goig d'aquella descoberta decantà Gauss definitivament pels estudis de ciències, per davant dels de llengües clàssiques.

En finalitzar els seus estudis a Göttingen, Gauss presentà una versió preliminar de les *Disquisitiones arithmeticae* al Príncep Carles Guillem Ferran. Aquest, però, considerà que el text no era suficient per a justificar la beca que li ha-

via proporcionat durant tots aquells anys. Gauss hagué de presentar una tesi doctoral a la Universitat de Helmstedt, a l'estat del Príncep. El tema de la tesi de Gauss fou la demostració del teorema fonamental de l'àlgebra. Tal com hem dit més amunt, el seu director fou Pfaff, professor a Helmstedt i deixeble de Kästner. Gauss presentà la tesi l'any 1799. El grau de doctor li fou concedit *in absentia* i se'l lliurà de l'examen oral habitual, o defensa de la tesi. Finalment, les *Disquisitiones arithmeticae* veieren la llum a Leipzig l'any 1801.

El 14 d'octubre de 1806 tingueren lloc les batalles de Jena i d'Auerstädt contra les tropes napoleòniques. En aquesta última, el Príncep protector de Gauss, que comandava les tropes, fou ferit de mort. L'any 1807, Gauss retornà a Göttingen com a director de l'Observatori, però desproveït de la protecció del Príncep, i l'any 1809 publicà el seu segon tractat, en dos volums, *Theoria motus corporum coelestium in sectionibus conicis Solem ambientium*.

En els decurs dels anys següents publicà les *Disquisitiones generales circa seriem infinitam*; *Methodus nova integralium valores per approximationem inveniendi*; *Bestimmung der Genauigkeit der Beobachtungen*, i *Theoria attractionis corporum sphaeroidicorum ellipticorum homogeneorum methodus nova tractata*. En aquestes obres hi ha un tractat sobre sèries que inclou una introducció a les funcions hipergeomètriques; un assaig sobre integració numèrica; una discussió d'estimadors estadístics, i un tractat de teoria del potencial inspirat per problemes geodèsics.

L'any 1820, Gauss acceptà l'encàrrec, de 1818, de l'Estat de Hannover de fer-se càrrec d'un estudi geodèsic del territori que prolongués la xarxa danesa ja existent aleshor-

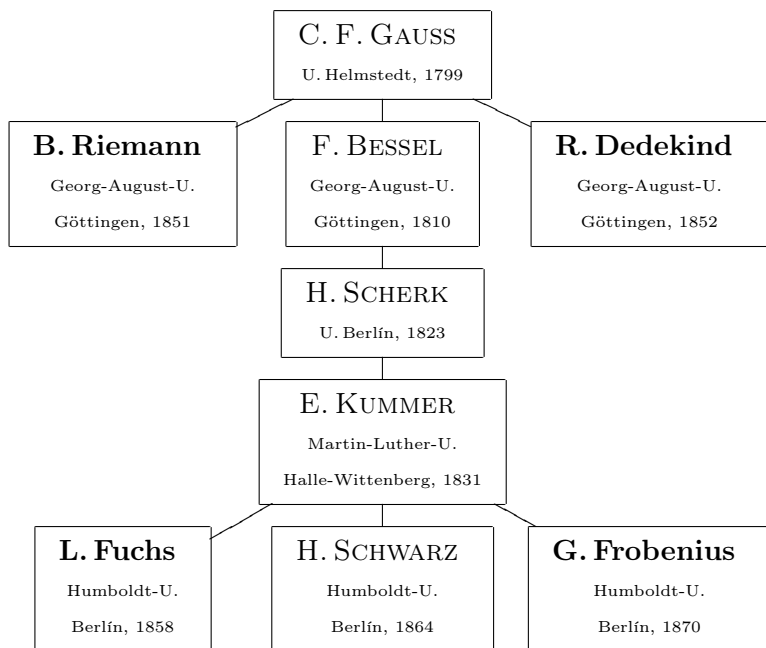
res. Ell mateix es féu càrrec dels mesuraments, durant el dia, i dels càlculs associats, durant els vespres. Per a tal fi, inventà l'heliotropi, un instrument geodèsic usat per a fer observacions a llarga distància mitjançant un raig de sol reflectit per un mirall. Sobre els seus progressos mantingué contactes epistolars amb Schumacher, Olbers i Bessel. Entre 1820 i 1830 publicà una setantena de treballs, entre els quals hi ha *Untersuchungen über Gegenstände der Höheren Geodäsie*; *Theoria combinationis observationum erroribus minimis obnoxiae*; *Disquisitiones generales circa superficies curvas*; *Über ein neues allgemeines Grundgesetz der Mechanik*, i *Principia generalia theoriae figurae fluidorum in statu aequilibrii*. En aquest període rebutjà l'ofertament d'una plaça a la Universitat de Berlín per a quedar-se a Göttingen.

L'any 1831 Gauss recolzà que Wilhelm Eduard Weber ocupés la càtedra de física que havia estat de Tobias Mayer, pare del matemàtic Johann Tobias Mayer. L'any 1832, Gauss i Weber iniciaren la investigació necessària a fi d'atendre la petició d'Alexander von Humboldt de fer un mapa del magnetisme terrestre. Per a tal fi es construí un observatori magnètic, que es completà l'any 1833. Entre 1832 i 1840, Gauss publicà *Intensitas vis magneticae terrestres ad mensuram absolutam revocata*; *Allgemeine Theorie des Erdmagnetismus*, i *Allgemeine Lehrsätze in Beziehung auf die im verkehrten Verhältnisse des Quadrats der Entfernung wirkenden Anziehungs und Abstossungskräfte*.

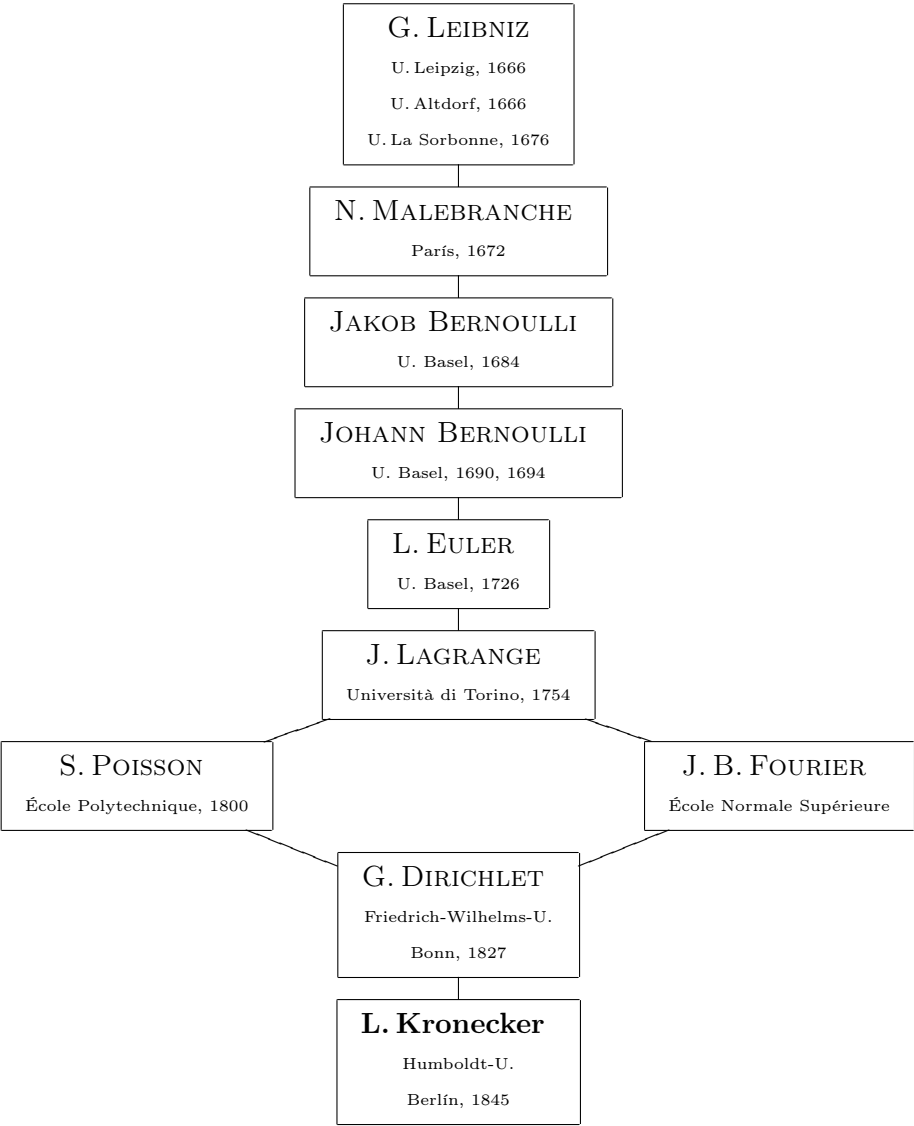
En sis anys de col·laboració, Gauss i Weber construïren el primer aparell de telègraf, que transmetia els seus senyals a la distància d'1,5 km que separa l'església de Sant Pau de l'Observatori astronòmic. El primer a fer-ne un ús pràctic

fou l'aprenent de banquer Israel Bere Josafat; aquest era fill d'un rabí, adoptà posteriorment el nom de Paul Julius Reuter i, anys després del seu contacte amb Gauss, crearia la primera agència de transmissió mundial de notícies. De 1845 a 1851, Gauss es dedicà a les finances, a partir de l'experiència obtinguda amb la posada al dia dels fons de viduitat de la Universitat de Göttingen. L'any 1849, i amb la presència a l'aula de Dirichlet i Jacobi, Gauss impartí la lliçó de celebració del cinquantenari de la lectura de la seva tesi amb una variació d'aquesta.

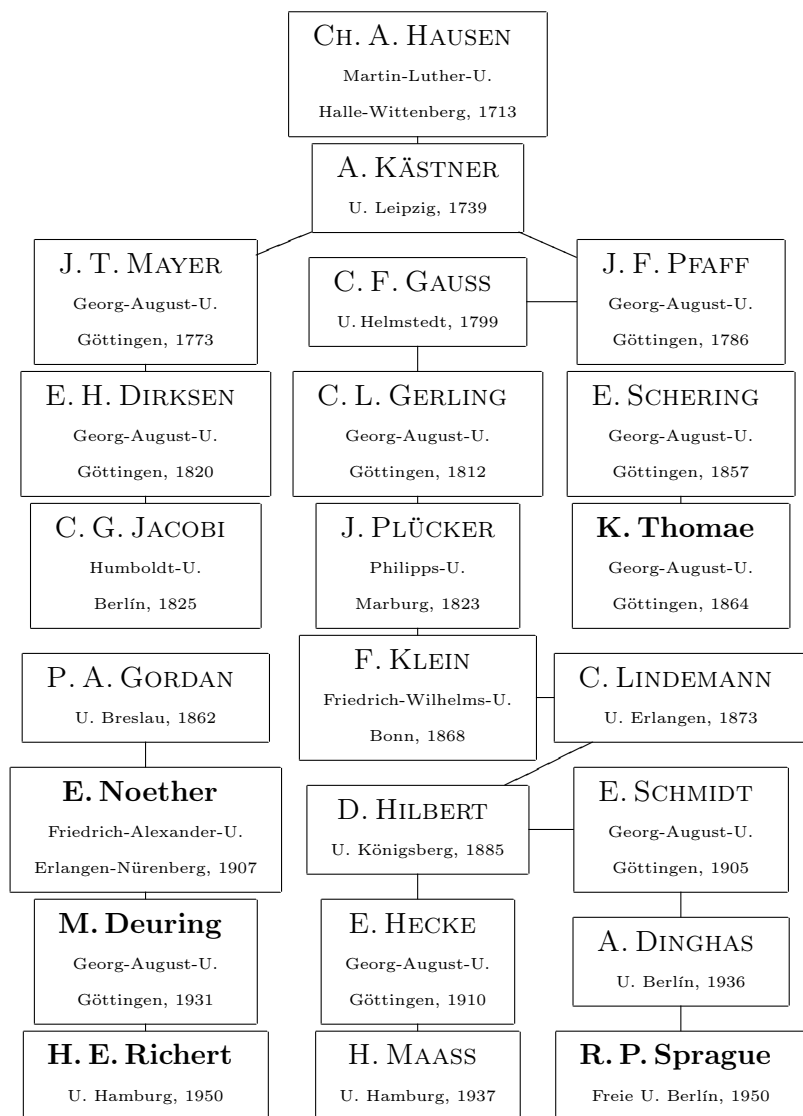
Entre els estudiants de doctorat de Gauss hi ha Bessel, Gerling, Listing, Gudermann, Encke, Riemann, Dedekind i l'historiador de la matemàtica Moritz Cantor.



Taula 2: Orígens de les escoles de Göttingen i de Berlín



Taula 3: Arbre genealògic (1666–1845)



Taula 4: Arbres genealògics (1713–1950)

L'any 1863 Schering inicià l'edició de l'obra de Gauss. Des de l'any 1863 al 1933 se n'editaren 12 volums (dos d'ells dobles) per l'Acadèmia de Ciències de Göttingen, l'editorial Teubner, a Leipzig, i per Julius Springer, a Berlín. Avui es poden consultar en línia al *Göttinger Digitalisierungs Zentrum*.

1.7 *Disquisitiones arithmetiques*

Com ja hem apuntat més amunt, Gauss publicà les *Disquisitiones arithmeticae* l'any 1801, quan tenia tan sols 23 anys. L'obra representa el naixement de la teoria de nombres moderna. El terme aritmètica deixa de tenir el sentit exclusivament utilitari atorgat pels mestres del Renaixement i esdevé la denominació d'una disciplina matemàtica especialitzada en l'estudi de les propietats intrínseques dels nombres. En certa manera, aquest punt de vista recupera el de la matemàtica grega del segle IV, en què Diofant d'Alexandria recopilà els coneixements aritmètics del seu temps.

Disquisitiones arithmeticae és una obra de joventut, que conté prop de 700 pàgines; el seu format és l'usual avui: teoremes, demostracions, corollaris, etcètera, però tot això il·lustrat amb nombrosos exemples.

Després de la primera edició de les *Disquisitiones arithmeticae* l'editor, que suposadament havia de distribuir l'obra, es declarà en fallida. Moltes còpies es perderen i, posteriorment, els deixebles de Gauss hagueren de copiar a mà els seus passatges. La situació començà a canviar només a partir de 1840, quan Dirichlet n'emprengué l'es-

tudi i començà a impartir classes sobre el text. A partir d'aleshores, la influència del seu contingut ja no s'aturaria.

L'obra ha estat traduïda al francès, l'any 1807; a l'alemany, l'any 1889; al rus, l'any 1959; a l'anglès, l'any 1965; al castellà, l'any 1995; i al català, l'any 1996. La traducció castellana fou publicada per l'Academia Colombiana de Ciencias Exactas, Físicas y Naturales. La traducció catalana és deguda a la matemàtica Griselda Pascual i Xufré i fou publicada per la Societat Catalana de Matemàtiques.

El nucli central de les *Disquisicions aritmètiques* està format per la secció cinquena; titulada *De les formes i equacions indeterminades de segon grau*, ocupa més de 350 pàgines. En ella, la força creativa de Gauss es manifesta en tota la seva potència, en tant que els resultats que ell obté ultrapassen resultats familiars a Fermat, Euler, Lagrange i Legendre.

Gauss hi estudia les formes quadràtiques binàries i els enters que representen; és a dir, les equacions $ax^2 + 2bxy + cy^2 = d$, en què a, b, c, d són nombres enters, i de les quals se cerquen solucions enteres x, y . El nombre $b^2 - ac = D$ és anomenat el determinant de la forma. En relació amb aquest problema, Gauss coneixia els resultats d'Euler i de Fermat relatius a l'estudi de les sumes de dos quadrats ($a = c = 1, b = 0$), i altres casos particulars tractats per Legendre.

Gauss comença la secció classificant les formes quadràtiques binàries per mitjà de canvis lineals invertibles. En el llenguatge actual, es tracta de canvis de base definits per matrius del grup especial lineal $SL(2, \mathbb{Z})$, o bé del grup lineal $GL(2, \mathbb{Z})$. En el primer cas, Gauss parla d'equivalència

pròpia. A continuació, Gauss dóna un criteri per a escollir representants senzills dins de cada classe de formes. D'aquesta manera obté les anomenades formes reduïdes. El procés de reducció de formes és diferent segons que el determinant D sigui positiu o negatiu. En el cas $D < 0$, cada classe dóna lloc a un únic representant reduït. En el cas $D > 0$, no quadrat, hi pot haver formes reduïdes equivalents, que s'agrupen en cicles. Per completesa, Gauss també estudia els casos en què D és un quadrat no nul i en què $D = 0$. En aquestes situacions, les formes descomponen en producte de formes lineals i Gauss remet la representació d'enters al seu estudi previ de les equacions diofantines lineals en dues incògnites. Per mitjà de la consideració de les formes reduïdes, Gauss demostra que el nombre de classes de formes d'un determinant donat és finit. Tot seguit resol el problema de la representabilitat dels enters per formes de determinant prefixat: donats un enter i un determinant, Gauss pot dir si l'enter és representat o no per alguna de les classes de formes d'aquell determinant. En particular, recupera els teoremes clàssics sobre els enters expressables com a suma de dos quadrats perquè en aquest cas el nombre de classes és igual a 1.

Després de classificar les formes, Gauss distribueix les classes en ordres i en gèneres. Els ordres consten de classes de formes del mateix determinant i amb el mateix màxim comú divisor, $\text{mcd}(a, b, c)$, de les formes. Quan aquest màxim comú divisor és igual a 1, l'ordre s'anomena primitiu. El concepte de gènere sorgeix en Gauss arran del fet següent. En tenir present que la classificació de les formes es fa per mitjà de matrius invertibles de coeficients enters, és evident que formes equivalents representen els mateixos nombres. Però Gauss s'adona que formes del mateix de-

terminant que representin els mateixos nombres no han de ser necessàriament equivalents. Les classes de formes de determinant donat que representen els mateixos nombres formen un gènere. Tot seguit considera una composició de classes de formes, que fa extensiva a una composició d'ordres i una de gèneres. La composició es fa de manera que si una classe de formes representa un nombre i una altra, un altre nombre, la composició representa el producte. Per composició de classes de formes de determinant donat, arriba a l'estructura algebraica d'un grup abelià finit. Especialment important és el grup abelià que sorgeix de les classes de formes pròpiament primitives; és a dir, aquelles en què $\text{mcd}(a, 2b, c) = 1$.

En la mateixa secció, inicia un estudi de les formes quadràtiques ternàries, però només en aquells aspectes que li proporcionen informació addicional sobre les formes quadràtiques binàries. En representar formes binàries per la ternària especial $x^2 - 2yz$, Gauss demostra l'existència de gèneres per a exactament la meitat dels caràcters totals associats a un discriminant. Aquests es calculen per mitjà de la llei de reciprocitat quadràtica, que ha demostrat en la secció quarta. Els diferents gèneres es caracteritzen per la igualtat dels símbols anteriors, calculats sobre els nombres representats per la forma. Gauss demostra que tots els gèneres d'un mateix ordre contenen el mateix nombre de classes, i calcula el nombre de classes ambigües de determinant donat, que són els elements d'ordre 2 del grup de classes. La distinció que obté dels diferents gèneres per mitjà de caràcters originarà més endavant la definició de l'anomenat caràcter de Kronecker.

Aquesta classificació de les formes tan ben organitzada evoca els rangs taxonòmics de Carl von Linné, naturalista suec que havia aplicat les categories aristotèliques a la classificació dels éssers vius.

Expressat en el llenguatge d'avui, donada una classe de formes, Gauss considera el seu grup d'isotropia, que, en el cas binari, només depèn del determinant. Veu que la solució general per a representar un nombre per una classe prové d'una solució particular modificada amb les que resulten de l'acció del grup d'isotropia. Alhora, el grup d'isotropia de la forma es calcula resolent una equació de Pell. Descriu un mètode per a obtenir la solució particular més petita de l'equació de Pell i, en tenir en compte l'estructura general de les solucions d'aquesta equació, n'obté la solució general.

Si bé Gauss no dóna fórmules generals per al nombre de classes, es dedica a estudiar-ne molts exemples. Ell mateix ens diu que quan el llibre s'imprimí havia calculat el nombre de classes fins a $D = -3000$.

Observem que, tres quarts de segle abans de la creació de la primera teoria de conjunts, per part de Dedekind i Cantor, Gauss, abans dels 24 anys, ja treballa amb els conceptes de conjunt, relació d'equivalència, classe d'equivalència, conjunt quocient, grup abelià, grup abelià quocient, grup de transformacions, operació de grups en conjunts, representació de grups i caràcters de grups abelians, entre d'altres.

Anys després, Gauss empraria de nou les formes quadràtiques binàries, en el seu estudi de la curvatura de les superfícies.

1.8 La Universitat de Berlín

Al final de la primera dècada del segle XIX, Wilhelm von Humboldt fou nomenat responsable d'educació de l'Estat Prussià, càrrec que estava directament vinculat al Ministeri de l'Interior i des del qual inicià una important reforma educativa a tots els nivells, des de primària fins a les universitats, incloent-hi la formació del professorat. Punt àlgid d'aquesta reforma educativa fou la fundació de la Universitat de Berlín, l'any 1810.

Segons Wilhelm von Humboldt, la universitat havia d'estar integrada per unitats docents i d'investigació que fossin punt de trobada d'alumnes i professors. Tant els uns com els altres havien de restar lliures d'exigències i de limitacions per part de l'Estat. Humboldt era del parer que les universitats podien cobrir les necessitats educatives de l'Estat per mitjà de l'exercici de la seva pròpia responsabilitat. En certa manera, la visió de Humboldt definí el concepte d'universitat literària moderna, el qual seria copiat en el decurs dels 150 anys posteriors.

Els ideals de Humboldt per a la universitat es resumeixen de la manera següent: unitat d'ensenyament i d'investigació; investigació basada en la curiositat; llibertat d'ensenyament, i llibertat d'aprenentatge.

Al començament, la Universitat de Berlín comptà amb les quatre facultats clàssiques: Dret, Medicina, Filosofia i Teologia.

Després de Napoleó, els estudis de matemàtiques foren valorats des d'un punt de vista militar. És d'aquests cercles d'on sorgí la idea de fundar a la Universitat de Berlín un

institut politècnic d'acord amb el model de l'*École Polytechnique* de París. El naturalista Alexander von Humboldt, germà de Wilhelm, intentà guanyar-ne Gauss com a possible director. Les seves obligacions s'havien de limitar a la instrucció dels alumnes que ell mateix sol·licités; l'institut coordinaria la resta d'institucions científiques de l'Estat, amb inclusió dels observatoris, i havia de tenir certa influència en el desenvolupament general de l'ensenyament a Prússia. L'ofertament fou rebutjat per Gauss, l'any 1824. L'any 1829, un càrrec semblant fou ofert al matemàtic noruec Niels Abel, però el nomenament no arribà a temps a causa de la mort prematura d'aquest.

Per influència d'Alexander von Humboldt, la Universitat de Berlín fou una de les pioneres en la introducció de les disciplines científiques química, física i matemàtiques. Ell mateix hi inaugurà les primeres lliçons sobre ciències naturals amb una sèrie de classes sobre el cosmos, impartides l'hivern del curs 1827–1828, que després redactaria en la seva magna obra *Kosmos*, en cinc volums.

En el camp de les matemàtiques sobresortiria més endavant l'anomenada “triple estrella”, formada per Kummer, Weierstrass i Kronecker.

1.9 La Universitat de Königsberg

La Universitat Albertina de Königsberg fou fundada l'any 1544 pel Duc Albrecht von Brandenburg-Ansbach; fou la segona universitat que es fundà a Prússia —la primera després de l'Acadèmia Catòlica de Cracòvia (*Jagiellonian Universität*), que ho havia estat l'any 1364—; també fou la se-

gona universitat protestant (luterana) que es fundà arreu —la primera després de la de Marburg, a Hesse, l'any 1527.

L'inici de la recerca matemàtica a la Universitat de Königsberg es remunta al segle XVIII amb la figura de Goldbach, natural d'aquesta ciutat i en la universitat de la qual es formà en matemàtiques i lleis. Més tard, gran part de la seva vida transcorregué a l'Acadèmia de Ciències de Sant Petersburg, on arribà a ser tutor del Tsar Pere II, l'únic nét masculí directe de Pere I el Gran.

La ciutat es féu famosa per la solució negativa donada per Euler al popular problema, ja mencionat a la pàgina 16, dels seus set ponts sobre el riu Pregel. També Kant s'hi ocupà de problemes de física matemàtica i d'astronomia.

Bessel, Jacobi i el físic Franz Ernst Neumann dotaren la Universitat de Königsberg d'una tradició en matemàtiques i física per la qual seria coneguda en el decurs dels segles XIX i XX. L'any 1868, els matemàtics de Königsberg Alfred Clebsch i Carl Gottfried Neumann, tots dos estudiants d'Otto Hesse, crearen la revista *Mathematische Annalen*.

La tradició matemàtica iniciada per Jacobi seria continuada posteriorment per figures tan rellevants com les de Lindemann, Hurwitz, Hilbert i Minkowski.

1.10 Jacobi

Carl Gustav Jacob Jacobi (Potsdam, 10 de desembre de 1804; Berlín, 18 de febrer de 1851)

Jacobi, fill d'un banquer jueu, féu els seus primers estudis de filosofia, llengües clàssiques i matemàtiques a la Universitat de Berlín. Des dels seus anys a la secundària, havia estudiat matemàtiques pel seu compte, interessant-se de manera especial per les obres d'Euler i de Lagrange. L'any 1825, després d'haver sotmès una tesi dirigida per Dirksen a la Universitat de Berlín, titulada *Disquisitiones Analyticae de Fractionibus Simplicibus*, li fou oferta una plaça per a ensenyar matemàtiques en el *Joachimsthalsche Gymnasium*. A fi de poder esdevenir professor universitari, Jacobi es convertí al cristianisme i així pogué exercir la docència a la Universitat de Berlín durant el curs 1825–1826. Cal notar que l'edecte de Prússia de 1812, tot i que havia declarat els jueus com a ciutadans, encara els exclouïa del funcionariat.

L'any 1826 es traslladà a la Universitat de Königsberg, on coincidí amb Franz Neumann, també doctorat a Berlín, i Bessel, que s'havia doctorat a Göttingen sota la direcció de Gauss. Abans de la seva arribada a Königsberg, Jacobi ja havia portat a terme descobertes importants en teoria de nombres, com ara les relatives als residus cúbics, i les havia comunicades a Gauss. Però les contribucions més notables de Jacobi es troben en el context de la teoria de les funcions el·líptiques. L'any 1827 inicià una extensa correspondència sobre aquest tema amb Legendre, que n'era el màxim expert; podem dir que la teoria de les funcions el·líptiques rep el seu màxim impuls de la mà de tres matemàtics: Legendre, Abel i Jacobi. El treball bàsic de Jacobi en funcions el·líptiques es basa en la introducció de les quatre funcions theta que porten el seu nom i la seva publicació més destacada és la memòria de l'any 1829 titulada *Fundamenta nova theoria functionum ellipticarum*. L'any 1834, Jacobi

demostrà el notable resultat que si una funció d'una variable complexa és doblement periòdica, aleshores el quocient entre els dos períodes no és real.

La fama de Jacobi atragué molts estudiants a la Universitat de Königsberg, on introduí el sistema de seminaris per a ensenyar els darrers avenços en matemàtiques. Borchardt, Heine, Hesse, Richelot, Rosenhain, i Seidel, pertanyeren al seu cercle.

La molt important depressió econòmica que vivia Prússia en aquella època ocasionà que Jacobi perdés la fortuna que havia heretat de la seva família. Per causa de problemes de salut, l'any 1843 li fou recomanat que es traslladés a Itàlia per una temporada. Ho pogué fer gràcies a un ajut econòmic que li fou concedit per Friedrich Wilhelm IV, a instàncies d'Alexander von Humboldt i de Dirichlet. Humboldt i Jacobi també mantingueren una extensa correspondència, de la qual han sobreviscut 44 cartes. En el viatge a Itàlia, l'acompanyaren Borchardt i Dirichlet i, a Roma, Jacobi pogué satisfer la seva curiositat per la història de la matemàtica a la Biblioteca Vaticana, on consultà manuscrits de l'*Arithmetica* de Diofant.

De retorn a Alemanya, l'any 1844, li fou oferta una plaça purament acadèmica a la Universitat de Berlín, sense obligacions docents, ja que hom considerà que el clima de Königsberg era poc adequat per a la seva salut. Els seus darrers anys es veieren pertorbats per raons polítiques relacionades amb la gènesi del procés d'unificació alemanya.

Entre els estudiants de doctorat de Jacobi hi ha Hesse i Richelot. Algunes fonts citen Gordan com a estudiant de doctorat de Jacobi, la qual cosa no pot ésser per im-

pediment de dates i de llocs. Podria ésser que, a Breslau, Gordan hagués estat deixeble de Schröter, que alhora fou deixeble de Richelot, o bé de Joachimsthal, que alhora sembla que podria ésser el primer deixeble de Kummer.

L'obra de Jacobi ha estat editada en vuit volums per la Reial Acadèmia Prussiana de Ciències, entre els anys 1881 i 1891, i reeditada per Chelsea l'any 1969. Els editors foren: Borchardt, del primer volum; Weierstrass, dels volums segon al setè, i Clebsch, del vuitè.

1.11 Integrals el·líptiques i funcions theta

Jacobi situà la data del naixement de les funcions el·líptiques el 23 de desembre de 1751, el dia en què Euler rebé l'obra de Fagnano. A la sessió de l'Acadèmia del 27 de gener de 1752, Euler exposà un treball sobre la comparació dels arcs d'una corba no rectificable on demostrà una sèrie de teoremes sobre arcs d'el·lipse, d'hipèrbola i de lemniscata, les coordenades dels quals són la suma o la diferència de valors d'una funció algebraica; i sobre arcs que són múltiples els uns dels altres. Euler hi afirmà, sense demostració, resultats sobre la divisió amb regla i compàs dels arcs de lemniscata.

En la terminologia clàssica, una integral el·líptica és una integral de la forma

$$\int_c^x R(t, P(t))dt,$$

on R és una funció racional de dues variables, $P(t)$ és l'arrel quadrada d'un polinomi de grau 3, o bé de grau 4, sense arrels múltiples, i c és una constant.

Més endavant, les investigacions de Legendre sobre les integrals el·líptiques s'estengueren durant un període de més de 40 anys. Els seus resultats sobre el tema aparegueren publicats en tres volums amb el nom *Exercices du Calcul Intégral* (1811, 1817, 1819). Legendre en preparà una segona edició amb el nom *Traité des Fonctions Elliptiques*, reorganitzada de nou en tres volums (1821, 1826, 1830). Legendre aplicà les integrals el·líptiques a l'estudi de la rotació de la Terra, a la determinació de l'atracció exercida per un el·lipsoide, i a la resolució de múltiples problemes de mecànica, cosa que requerí la confecció de nombroses taules.

Legendre reduí les integrals el·líptiques a tres formes canòniques, anomenades de primera, de segona i de tercera espècie, respectivament:

$$F(\varphi, k) = \int_0^\varphi \frac{d\theta}{\sqrt{1 - k^2 \sin^2 \theta}},$$

$$E(\varphi, k) = \int_0^\varphi \sqrt{1 - k^2 \sin^2 \theta} \, d\theta,$$

$$P(\varphi, k, n) = \int_0^\varphi \frac{d\theta}{(1 + n \sin^2 \theta) \sqrt{1 - k^2 \sin^2 \theta}}.$$

Legendre anomenà φ l'amplitud de la integral; k , el mòdul; i n , el paràmetre, en el cas de la integral de tercera espècie. Quan l'amplitud és igual a $\pi/2$, parla de la integral completa.

El valor de la integral completa de primera espècie fou obtingut per Gauss com a resultat de les seves investigacions arran de la mitjana aritmètico-geomètrica i de les sèries hipergeomètriques:

$$\begin{aligned} K(k) &= F\left(\frac{\pi}{2}, k\right) = \int_0^{\pi/2} \frac{1}{\sqrt{1 - k^2 \sin^2 \theta}} d\theta = \\ &= \frac{\pi}{2} \sum_{n=0}^{\infty} \left(\frac{(2n-1)!!}{(2n)!!} \right)^2 k^{2n}. \end{aligned}$$

El valor de la integral completa de segona espècie es calcula de manera anàloga:

$$\begin{aligned} E(k) &= E\left(\frac{\pi}{2}, k\right) = \int_0^{\pi/2} \sqrt{1 - k^2 \sin^2 \theta} d\theta = \\ &= \frac{\pi}{2} \left(1 - \sum_{n=1}^{\infty} \left(\frac{(2n-1)!!}{(2n)!!} \right)^2 \frac{k^{2n}}{2n-1} \right). \end{aligned}$$

La integral el·líptica de primera espècie apareix en el càlcul del període del pèndol. Legendre demostrà que, com a funció del mòdul, aquesta integral satisfà l'equació diferencial de segon ordre:

$$k(k^2 - 1) \frac{d^2 F}{dk^2} + (3k^2 - 1) \frac{dF}{dk} + kF = 0.$$

La integral el·líptica de segona espècie proporciona la longitud d'un arc d'el·lipse d'excentricitat igual al mòdul. Alhora, Euler coneixia que aquesta integral satisfà l'equació diferencial de segon ordre:

$$k(k^2 - 1) \frac{d^2 E}{dk^2} + (k^2 - 1) \frac{dE}{dk} - kE = 0.$$

Ambdues equacions diferencials són casos particulars d'equacions diferencials de tipus fuchsà.

Segons Abel, la primera idea relativa a les funcions el·líptiques es deu a Euler, que demostrà que l'equació diferencial de variables separades

$$\frac{dx}{\sqrt{\alpha + \beta x + \gamma x^2 + \delta x^3 + \epsilon x^4}} = - \frac{dy}{\sqrt{\alpha + \beta y + \gamma y^2 + \delta y^3 + \epsilon y^4}}$$

podia ésser integrada algebraicament. En les seves dues memòries sobre les funcions el·líptiques, de 1827 i 1828, Abel escriu les integrals el·líptiques de primera espècie en la forma

$$\alpha = \int_0^x \frac{dx}{\sqrt{(1 - c^2 x^2)(1 + e^2 x^2)}}.$$

Per la seva inversió, obté les funcions

$$\varphi(\alpha; c, e) = x,$$

a les quals associa dues funcions més de α :

$$f(\alpha; c) = \sqrt{1 - c^2 \varphi^2(\alpha)}, \quad F(\alpha; e) = \sqrt{1 + e^2 \varphi^2(\alpha)}.$$

Demuestra que φ és una funció doblement periòdica i que els valors de φ obtinguts per multiplicació i per divisió per nombres enters dels arguments,

$$\varphi(N\alpha), \quad \varphi\left(\frac{\alpha}{N}\right),$$

s'expressen algebraicament en funció de $\varphi(\alpha)$. Abel redueix la resolució de l'equació de divisió $P_N = 0$, en principi de grau N^2 , a la resolució d'una equació de grau $N + 1$; fa notar que aquesta equació no sembla, en general, que sigui resoluble algebraicament; és a dir, d'acord amb la

terminologia actual, per radicals; i prova que es pot resoldre en molts casos particulars, per exemple, quan $e = c$, $e = c\sqrt{3}$, $e = c(2 \pm \sqrt{3})$, etcètera.

En estudiar el cas $e = c = 1$, Abel obté el notable resultat pel qual la lemniscata és divisible en N parts iguals mitjançant el regle i el compàs si N és el producte d'una potència de 2 per nombres primers diferents de Fermat. És a dir, Abel obté els mateixos valors que, en el seu dia, obtingué Gauss per a la divisió de la circumferència.

En el seu estudi de les relacions més generals entre una quantitat arbitrària de funcions el·líptiques, Abel ha de caracteritzar els casos en què l'equació diferencial de variables separades

$$\frac{dy}{\sqrt{(1-y^2)(1+\mu y^2)}} = a \frac{dx}{\sqrt{(1-x^2)(1+\mu x^2)}}$$

pot ésser integrada algebraicament. En el supòsit que el multiplicador a sigui un nombre real, descobreix que a ha d'ésser un nombre racional. En el supòsit que a sigui imaginari no real, llavors a ha d'ésser un irracional quadràtic $a = m + i\sqrt{n}$, $m, n \in \mathbb{Q}$, i en aquest cas el mòdul μ està sotmès a restriccions.

Poc temps després de la publicació del monumental tractat de Legendre sobre les integrals el·líptiques, el 5 d'agost de 1827 Jacobi li comunicà en una carta els seus propis resultats arran de la multiplicació d'aquestes integrals. Jacobi comparava integrals el·líptiques associades tant al mateix mòdul com a mòduls diferents.

En una segona carta, el 29 de novembre de 1827, Jacobi informà Legendre dels treballs d'Abel sobre aquest tema:

“es tracta de la primera part d’una memòria del Sr. Abel, a Cristiania, que m’ha dit que va ésser a París fa dos o tres anys, i que ha estat inserida en el número dos del segon volum del *Journal für die reine und angewandte Mathematik*, publicada a Berlín pel Sr. Crelle”. Jacobi explica a Legendre els resultats d’Abel utilitzant la seva pròpia notació. En particular, descriu una sèrie de fórmules de les quals dedueix la doble periodicitat. Per inversió de la integral el·líptica de primera espècie

$$(u \mid k)(\theta) = \int_0^\theta \frac{d\varphi}{\sqrt{1 - k^2 \sin^2 \varphi}},$$

defineix $(\theta \mid k)(u) = \text{am}(u \mid k)$, i demostra la doble periodicitat de la funció $\sin(\text{am}(u \mid k))$:

$$\sin \text{am}(u + 4mK + 2m'iK' \mid k) = \sin \text{am}(u \mid k),$$

on $K = K(k)$, $K' = K'(k) = K(k')$, $k^2 + k'^2 = 1$.

Jacobi posa de manifest que les arrels de l’equació de grau N^2 que proporciona la divisió de la integral el·líptica u en N parts iguals són de la forma

$$\sin \text{am} \left(\frac{u + 4mK + 2m'iK'}{N} \mid k \right), \quad 0 \leq m, m' \leq N - 1.$$

Jacobi també comunicà a Legendre que certes integrals el·líptiques admeten multiplicacions per nombres complexos $a \pm bi$ d’una certa forma. Advertí que això ocorre, per exemple, per a tots els mòduls que estan lligats per una escala qualsevol amb $k = \frac{1}{\sqrt{2}}$, i afegí que és un tipus de multiplicació que no té anàleg en el cas dels arcs del cercle.

Legendre, Jacobi i Abel, que estaven totalment familiaritzats amb el tractat d'Euler *Introductio in analysin infinitorum*, en el qual es consideren les fórmules d'addició, de multiplicació i de divisió de les funcions circulars, s'adonaren de seguida que estaven davant d'una nova teoria que presentava notables semblances, alhora que notables diferències, amb la teoria de les funcions circulars. Així, mentre que $\sin(iu) = \sinh(u)$, $\cos(iu) = \cosh(u)$, es té que

$$\operatorname{sl}(iu) = i \operatorname{sl}(u), \quad \operatorname{cl}(iu) = 1/\operatorname{cl}(u).$$

Gudermann, un dels primers matemàtics que impartiren lliçons sobre funcions el·líptiques, simplificà una mica la notació utilitzada per Jacobi, en introduir les funcions sn , cn , dn , donades per

$$\begin{aligned} \operatorname{sn}(u \mid k) &= \sin \operatorname{am}(u \mid k), \\ \operatorname{cn}(u \mid k) &= \cos \operatorname{am}(u \mid k), \\ \operatorname{dn}(u \mid k) &= \Delta \operatorname{am}(u \mid k) = \sqrt{1 - k^2 \sin^2 \operatorname{am}(u \mid k)}. \end{aligned}$$

En particular, es té que

$$(u \mid k) = \int_0^\theta \frac{d\varphi}{\sqrt{1 - k^2 \sin^2 \varphi}} = \int_0^{\operatorname{sn}(u \mid k)} \frac{dt}{\sqrt{(1 - t^2)(1 - k^2 t^2)}}.$$

Gudermann s'havia doctorat l'any 1841 a la Georg August Universität de Göttingen, sota la direcció de Gauss, amb la memòria de tesi *Sobre el desenvolupament de les funcions modulars* (*Über die Entwicklung der Modularfunctionen*). Pel que fa a Gudermann, aquest fou el director de tesi de Weierstrass.

Una altra de les aportacions de Jacobi, que no hem d'ometre, és la seva expressió de les funcions el·líptiques com a quocients de funcions theta.

Les funcions theta ja havien estat utilitzades per matemàtics francesos; per exemple, per Fourier, en el seu estudi de l'equació de la calor. Més endavant, ho serien en la tesi de Bachelier, llegida i publicada l'any 1900 i reconeguda avui com un antecedent de la matemàtica financera.

Es defineix la funció theta bàsica com

$$\theta(z, \tau) := \sum_{n \in \mathbb{Z}} e^{2\pi i n z + \pi i n^2 \tau},$$

on $z, \tau \in \mathbb{C}$ i $\Im(\tau) > 0$. Es tracta d'una funció semiperiòdica, perquè

$$\theta(z + 1, \tau) = \theta(z, \tau), \quad \theta(z + \tau, \tau) = e^{-\pi i \tau - 2\pi i z} \theta(z, \tau).$$

Les funcions theta amb característiques són funcions analítiques en dues variables que es defineixen a partir de la funció theta bàsica:

$$\theta_{a,b}(z, \tau) := e^{\pi i a^2 \tau + 2\pi i a(z+b)} \theta(z + b + a\tau, \tau), \quad a, b \in \mathbb{Q}.$$

Les funcions

$$\theta_1 = \theta_{\frac{1}{2}, \frac{1}{2}}, \quad \theta_2 = \theta_{\frac{1}{2}, 0}, \quad \theta_3 = \theta_{0,0} = \theta, \quad \theta_4 = \theta_{0, \frac{1}{2}}$$

són les anomenades funcions theta de Jacobi. En particular, es té que $\theta_3 = \theta$.

En tenir en compte els zeros i els pols de les funcions sn , cn , dn , Jacobi n'obté expressions en forma de quocients

de funcions theta:

$$\operatorname{sn}(u \mid k) = \frac{\theta_3(0)}{\theta_2(0)} \cdot \frac{\theta_1(z)}{\theta_4(z)},$$

$$\operatorname{cn}(u \mid k) = \frac{\theta_4(0)}{\theta_2(0)} \cdot \frac{\theta_2(z)}{\theta_4(z)},$$

$$\operatorname{dn}(u \mid k) = \frac{\theta_4(0)}{\theta_3(0)} \cdot \frac{\theta_3(z)}{\theta_4(z)},$$

on

$$z = \frac{u}{\pi\theta_3^2(0)}, \quad k^2 = \frac{\theta_2^4(0)}{\theta_3^4(0)}, \quad \theta_i(z) = \theta_i(z, \tau),$$

per a $\tau = iK'/K$, i on $4K$, $2iK'$ són els períodes de la funció $\operatorname{sn}(u \mid k)$.

Al llarg del segle XIX i bona part del XX, les funcions theta de Jacobi i les seves generalitzacions donaren lloc a una extensa literatura.

Capítol 2

L'escola de Berlín

A la fi de l'etapa fundacional de la Universitat de Berlín, la matemàtica hi començà a fer acte de presència. Així, trobem que Dirksen, després d'haver defensat una tesi a Göttingen l'any 1820, s'habilità aquell mateix any a la Universitat de Berlín i el Ministre de Prússia l'en nomenà professor extraordinari (*ausserordentlicher Professor*); aquesta denominació és equivalent a la nostra de professor titular. L'any 1824, esdevingué catedràtic d'aquesta institució. L'any 1823, Scherk hi defensà la tesi sota la direcció de Bessel; i Jacobi la hi defensà l'any 1825 sota la direcció de Dirksen.

Però, probablement, podríem situar la gènesi de l'escola matemàtica de Berlín a partir de l'arribada de Dirichlet, l'any 1828. Aquesta arribada acomplia el vell somni d'Alexander von Humboldt, que no havia pogut satisfer amb Gauss, d'incorporar primeres figures a la matemàtica berlinesa. Dirichlet hi portà de París els aires de la Il·lustració, sorgits paral·lelament amb la Revolució Francesa.

L'escola de Berlín començà a adquirir forma pròpia sota la iniciativa de Kummer i Weierstrass. Amb la jugada política de recomanar el seu primer alumne, Joachimsthal, a la plaça que ell mateix ocupava a Breslau, Kummer aconseguí que Weierstrass, que a priori era el candidat més ben situat per a aquella plaça, pogués anar a Berlín l'any 1856.

Per adaptació del sistema de seminaris iniciat prèviament a Königsberg i a Göttingen, el seminari de Berlín començà la seva trajectòria l'any 1861. Dedicat únicament i exclusivament a les matemàtiques, tenia el nombre de participants limitat a 12, i els seus integrants eren escollits mitjançant un procés rigorós de selecció en el qual l'aspirant havia de sotmetre a aprovació un treball o bé superar un examen. Kummer i Weierstrass dirigiren aquest seminari durant dues dècades, i en ell es formaren nombrosos futurs professors universitaris. El mateix any, es creà la Societat matemàtica berlinesa (*Berliner mathematischer Verein*) que, en aquella època, ja comptà amb una mitjana de 50 membres.

Un altre dels aspectes que sobresurten de l'escola matemàtica berlinesa des dels seus inicis és l'interès per la publicació de textos matemàtics i, en especial, per la creació i el suport de publicacions periòdiques.

El *Journal für die reine und angewandte Mathematik* (*Revista per a la matemàtica pura i aplicada*), una de les revistes matemàtiques més prestigioses i que encara es publica avui, fou fundada per l'enginyer berlinès A. L. Crelle, l'any 1826. Des dels seus inicis es coneix popularment com la *Revista de Crelle* (amb un petit parèntesi en què ho fou com a *Revista de Borchardt*). Inicialment pensada per a la matemàtica de caràcter pur i aplicat, la revista s'allunyà

lentament del vessant aplicat previst. El seu to el proporcionaren ja els primers volums, en què s'hi publicaren treballs d'Abel, Jacobi i Steiner, entre altres. Això féu que els crítics al corrent purista de l'època diguessin jocosament que *Journal für die reine, unangewandte Mathematik* hauria estat un nom més escaient per a la publicació. Paradoxalment, seria en aquesta revista on es desenvoluparien, al llarg de molts anys, les eines i el llenguatge que han esdevingut imprescindibles en la física matemàtica actual.

Berlín fou també la seu de la primera revista matemàtica dedicada a la revisió d'articles, l'*Anuari sobre els progressos de la matemàtica* (*Jahrbuch für die Fortschritte der Mathematik*), fundada l'any 1870 i que derivaria, en els anys 1940, en el popular *Zentralblatt*. El primer volum d'aquesta revista revisà 500 documents, corresponents a la literatura matemàtica publicada durant l'any 1868. La gran quantitat d'articles de matemàtiques que es publicaven cada any fou causa que, amb el transcurs del temps, la revista s'anés endarrerint en la publicació de les revisions. Per exemple, les revisions dels articles publicats l'any 1925 no aparegueren fins al volum de l'any 1932. A partir de 1922 la revista fou editada per l'editorial Walter de Gruyter; actualment ho és per l'editorial Springer.

Entre les revistes fundades a Berlín abans de 1950 també hi ha les *Sitzungsberichte der berliner mathematischen Gesellschaft* (1901); *Mathematische Zeitschrift* (1918); *Zeitschrift für angewandte Mathematik und Mechanik* (1921); *Deutsche Mathematik* (1936–1943), i *Mathematische Nachrichten* (1948).

2.1 Dirichlet

Johann Peter Gustav Lejeune Dirichlet (Düren, 13 de febrer de 1805; Göttingen, 5 de maig de 1859)

La família de Dirichlet procedia de Bèlgica. L'any 1822, un cop completats els seus estudis secundaris a Bonn, i per causa del poc nivell que en aquell temps tenien les universitats alemanyes, Dirichlet havia marxat a estudiar matemàtiques al *Collège de France* i a la Facultat de Ciències de la Universitat de París, amb les *Disquisitiones arithmeticae* sota el braç. Allà estudià amb Biot, Fourier, Laplace, Legendre i Poisson, entre altres.

El primer treball de Dirichlet, de l'any 1825 i que li donà una certa fama, fou relatiu a la resolució del Teorema de Fermat en el cas d'exponent $n = 5$. Els casos $n = 4$ i $n = 3$ havien estat resolts prèviament per Fermat i per Euler, respectivament.

Recomanat per Alexander von Humboldt, Dirichlet optà per ésser professor en alguna universitat alemanya. De totes maneres, el nomenament no podia ésser directe, atès que ni era doctor, ni tenia l'habilitació per a la universitat alemanya, ni parlava llatí, condició indispensable a l'època per a ésser professor universitari. El problema es resolgué per mitjà d'un doctorat honorífic que li concedí la Universitat de Colònia, la qual cosa li permeté sotmetre a la Universitat de Breslau una tesi d'habilitació, que versà sobre un tema de polinomis amb una classe especial de divisors primers. L'any 1827 fou nomenat professor a la Universitat de Breslau, i després d'un any, i de nou per influència de von Humboldt, del Col·legi Militar i de la

Universitat de Berlín, on romangué fins l'any 1855. Amb Dirichlet, començà l'època daurada de les matemàtiques a Berlín. Després de la mort de Gauss, aquell any 1855, se li oferí una càtedra a la Universitat de Göttingen, que acabà acceptant en no sortir-se'n de fer-la servir per a obtenir millors condicions a Berlín.

A Berlín, von Humboldt introduí Dirichlet en el cercle de la família Mendelssohn. Moses Mendelssohn havia estat un filòsof jueu impulsor, juntament amb Lessing, del moviment *Haskalah*, d'emancipació jueva. Els seus fills Joseph i Abraham foren els fundadors, l'any 1795, de la Bankhaus Mendelssohn, una banca privada que fou liquidada l'any 1939 pel Deutsche Bank. L'any 1831, Dirichlet accedí a l'Acadèmia de Berlín, fet que li provocà una millora del salari. Poc després es casà amb Rebecka Mendelssohn, filla d'Abraham i germana dels compositors Felix i Fanny Mendelssohn, un cop Rebecka s'havia convertit al cristianisme.

L'amistat de tota la vida de Dirichlet amb Jacobi afavorí el desenvolupament de la teoria de nombres. Entre els resultats més remarcables provats per Dirichlet en aquest camp sobresurt el teorema de 1837, anomenat de la progressió aritmètica, segons el qual en tota progressió aritmètica en què el primer terme i la diferència són coprimers, hi ha una infinitat de nombres primers. El resultat havia estat emprat sense demostració per Legendre i conjecturat per Gauss, i es considera el punt d'inici de la teoria analítica de nombres.

Una de les preocupacions constants de Dirichlet fou l'estudi i la difusió del contingut de les *Disquisitiones arithmeticae* de Gauss. En aquesta direcció, esmentem els seus resultats de 1838 i 1839 relatius a les avui anomenades sè-

ries de Dirichlet i a la fórmula analítica per al nombre de classes de formes quadràtiques binàries.

Les seves lliçons sobre teoria de nombres foren publicades pòstumament per Dedekind l'any 1863 amb el títol *Vorlesungen über Zahlentheorie* i constitueixen un primer tractat de la teoria algebraica de nombres. El text conté el desenvolupament de la teoria d'ideals en els anells d'enters dels cossos de nombres i s'hi demostra, entre d'altres, el teorema de les unitats, provat per Dirichlet l'any 1846, segons el qual les unitats de l'anell dels enters algebraics d'un cos de nombres formen un grup abelià finitament generat i de rang igual a $\nu - 1$, on ν és la suma dels nombres d'immersions reals i de parelles d'immersions complexes conjugades no reals del cos.

A més de les aportacions de Dirichlet a la teoria de nombres, les seves aportacions fundacionals a l'anàlisi i el seu estudi sobre la convergència de les sèries de Fourier constitueixen un altre dels valors de la matemàtica del segle XIX. Part dels seus treballs foren publicats a la *Revista de Crelle*. Fem notar que Riemann fou un estudiant de Dirichlet. Entre els estudiants de doctorat de Dirichlet hi ha Eisenstein, Kronecker i Lipschitz.

2.2 Kummer

Ernst Eduard Kummer (Sorau, Brandenburg, 29 de gener de 1810; Berlín, 14 de maig de 1893)

Kummer, fill d'un metge, inicià els seus estudis de matemàtiques a la Universitat de Halle, l'any 1828, com a pas

previ als seus estudis de filosofia. L'any 1831 rebé el doctorat sota la direcció de Scherk. El curs 1831–1832 ensenyà a l'Institut de Sorau en què ell s'havia format; i, després d'un any, esdevingué professor a l'Institut de Liegnitz, a Silèsia, on romangué 10 anys. Els seus dos alumnes més famosos foren Kronecker i Joachimsthal, els quals, sota el mestratge de Kummer, iniciaren treballs de recerca matemàtica mentre eren a l'escola.

Kummer mateix emprengué la seva pròpia recerca matemàtica mentre ensenyava a Liegnitz. L'any 1836, publicà a la *Revista de Crelle* un article sobre sèries hipergeomètriques que cridà l'atenció primerament de Jacobi i després de Dirichlet. L'any 1839 fou nomenat membre de l'Acadèmia de Berlín, per recomanació de Dirichlet. Jacobi s'adonà que calia trobar-li una plaça de professor universitari. L'any 1840, Kummer es casà en primeres núpcies amb Ottilie Ernestine Mendelssohn, una cosina de Rebecka, l'esposa de Dirichlet.

L'any 1842, i per recomanació de Jacobi, Kummer obtingué la seva primera plaça de professor universitari a la Universitat de Breslau, a Silèsia. L'any 1855, quan Dirichlet deixà Berlín a fi de succeir Gauss a Göttingen, Dirichlet recomanà Kummer per a succeir-lo a ell a Berlín. Per la seva part, Kummer recolzà Joachimsthal per a substituir-lo a Breslau i, d'aquesta manera, un any més tard, Weierstrass pogué tenir una plaça a la Universitat de Berlín, tal com desitjava Kummer. Tal com hem esmentat més amunt, Kummer i Weierstrass establiren el primer seminari de matemàtiques pures a Berlín l'any 1861. Les lliçons de Kummer a Berlín versaren sobre geometria analítica, mecànica, teoria de superfícies i teoria de nombres.

A Berlín, Kummer dirigí un gran nombre d'estudiants de doctorat, entre els quals hi ha Cantor, Frobenius, Prym, Schönflies i Schwarz. Kummer també recolzà el nomenament de lector per a molts joves estudiants, com ara Clebsch, Christoffel i Fuchs. De fet, quan Kummer es retirà l'any 1883, Fuchs el succeí a la càtedra de Berlín.

Kummer començà les seves recerques matemàtiques en el camp de la teoria de funcions. Estengué el treball de Gauss sobre les sèries hipergeomètriques, calculant-ne el grup de monodromia, amb un tractament que fou útil en l'estudi de les equacions diferencials.

L'any 1843, i després d'adonar-se que els fracassos en la demostració del Teorema de Fermat eren ocasionats per la manca de factorització única en els enters ciclotòmics, hi creà la noció de *nombre ideal*. Aquest concepte evolucionaria a partir de Dedekind cap a la noció d'ideal, bàsica en el desenvolupament posterior de l'àlgebra commutativa i de la geometria algebraica. La resta de la seva producció matemàtica estigué orientada a la demostració del Teorema de Fermat.

L'any 1857, li fou donat el Gran Premi de l'Acadèmia de Ciències de París destinat a la demostració del Teorema de Fermat, tot i no haver-la aconseguit íntegrament i malgrat no haver-s'hi presentat.

L'obra de Kummer fou editada per Weil l'any 1975, en dos volums publicats per Springer.

2.3 Enters algebraics

El pas inicial de l'estudi aritmètic dels cossos de nombres fou la construcció per Kummer de la seva teoria dels nombres ideals, adreçada als anells d'enters $\mathbb{Z}[\zeta_N]$ dels cossos ciclotòmics $\mathbb{Q}(\zeta_N)$. L'estudi de Kummer fou motivat pel de la divisibilitat en $\mathbb{Z}[\zeta_N]$ arran de les seves investigacions sobre l'equació de Fermat $X^N + Y^N = Z^N$. Els conceptes més importants elaborats per Kummer són, a més de la seva definició de nombres ideals, l'estudi de les unitats ciclotòmiques; la classificació dels nombres primers en regulars i en irregulars; la caracterització d'aquests en termes de nombres de Bernoulli; l'estudi de les lleis de reciprocitat dels cossos ciclotòmics, així com també la seva demostració del Teorema de Fermat per a tots els exponents primers regulars, a més de les seves múltiples aportacions al cas irregular.

Al voltant de 1840, i quasi simultàniament, Eisenstein, Dirichlet i Hermite havien arribat a la noció d'element enter algebraic: un element $\alpha \in \overline{\mathbb{Q}}$ es diu que és un enter algebraic si és solució d'una equació de la forma

$$X^n + a_{n-1}X^{n-1} + \cdots + a_n = 0, \quad a_i \in \mathbb{Z}.$$

El conjunt $\mathcal{O}_K$ dels enters algebraics inclosos en un cos de nombres K constitueix un anell; els ideals d'aquest anell i les seves unitats es designen amb el nom d'ideals i unitats, respectivament, del cos K . Els primers exemples d'anells d'enters són el propi $\mathbb{Z}$, l'anell $\mathbb{Z}[\zeta_4]$ dels enters de Gauss i l'anell $\mathbb{Z}[\zeta_3]$ dels enters d'Eisenstein.

La teoria de la divisibilitat creada per Kummer en els cossos ciclotòmics fou estesa per Dedekind i per Kronecker

a qualsevol cos de nombres. Dedekind demostrà que tot ideal no nul de l'anell d'enters $\mathcal{O}_K$ d'un cos de nombres K descompon de manera única com a producte d'una quantitat finita d'ideals primers d'aquest anell. Els ideals primers $(0) \neq \mathfrak{p} \subseteq \mathcal{O}_K$ són maximals, cosa per la qual els anells de classes residuals $\mathcal{O}_K/\mathfrak{p}$ són cossos. Com que $\mathcal{O}_K$ és un grup abelià finitament generat, aquests cossos residuals són finits. Amb la introducció de la noció d'ideal fraccionari de K , el conjunt de tots els ideals (enters i fraccionaris) s'organitza com un grup multiplicatiu, I_K , que posseeix com a subgrup el grup P_K format pels ideals fraccionaris principals. Per un teorema de Minkowski, el grup de classes d'ideals $\text{Cl}_K := I_K/P_K$ és un grup abelià finit; el seu cardinal h_K és l'anomenat nombre de classes de K i mesura com de lluny és l'anell $\mathcal{O}_K$ d'ésser un domini d'ideals principals.

Un nombre enter primer p es diu que ramifica en K quan en la descomposició de l'ideal $p\mathcal{O}_K$ apareixen factors múltiples. El discriminant del cos K és un ideal de $\mathbb{Z}$ divisible únicament pels ideals primers ramificats (afectats d'exponents convenients).

Quan el cos K és quadràtic de discriminant D , el grup de classes d'ideals de K recupera el grup de classes de formes quadràtiques binàries de discriminant fonamental D introduït per Gauss.

En el cas dels cossos ciclotòmics, els primers regulars en el sentit de Kummer són aquells per als quals p no divideix el nombre de classes $h_{\mathbb{Q}(\zeta_p)}$.

Un primer pas per a comprendre l'aritmètica dels anells d'enters és la determinació del grup multiplicatiu $\mathcal{O}_K^*$ de les unitats (o elements invertibles) de $\mathcal{O}_K$. Aquest grup conté

el subgrup $\mu(K)$ de les arrels de la unitat contingudes en K . Però en K hi pot haver unitats d'ordre infinit, com és el cas dels cossos quadràtics reals $\mathbb{Q}(\sqrt{D})$, $D > 0$, les unitats dels quals es determinen mitjançant la resolució de l'equació de Pell $X^2 - DY^2 = \pm 1$. En general, les unitats ε d'un cos de nombres K són els elements de $\mathcal{O}_K$ que satisfan l'equació nòrmica $N_{K|\mathbb{Q}}(\varepsilon) = \pm 1$, de grau $n = [K : \mathbb{Q}]$.

L'any 1844, Eisenstein obtingué una descripció del grup de les unitats dels cossos cúbics. En la seva tesi de 1845, Kronecker estudià les unitats dels cossos ciclotòmics. Ambdós resultats foren generalitzats l'any 1846 per Dirichlet a qualsevol cos de nombres mitjançant el seu teorema d'estructura de les unitats.

El teorema de Dirichlet de les unitats afirma que el grup multiplicatiu $\mathcal{O}_K^*$ és un grup abelià finitament generat, del qual en determina el rang; el seu subgrup de torsió és òbviament $\mu(K)$. Per mitjà de la immersió logarítmica de K^* , Dirichlet identifica el grup quocient $\mathcal{O}_K^*/\mu(K)$ amb un reticle d'un espai euclidià del qual demostra que és de dimensió $r := r_1 + r_2 - 1$, on $n = r_1 + 2r_2$ és la descomposició del grau de K proporcionada pel nombre r_1 de les seves immersions reals i el nombre r_2 de les seves parelles d'immersions complexes conjugades no reals. El punt clau per a la determinació de r es troba en el fet que un determinant, R_K , format amb logaritmes d'un cert sistema d'unitats, és no nul; R_K s'anomena el regulador del cos K . D'aquesta manera, Dirichlet demostra l'existència d'unitats fonamentals $\varepsilon_i \in \mathcal{O}_K^*$, tals que tota unitat ε de $\mathcal{O}_K$ s'escriu de manera única en la forma

$$\varepsilon = \zeta \varepsilon_1^{n_1} \cdots \varepsilon_r^{n_r}, \quad \zeta \in \mu(K), \quad n_i \in \mathbb{Z}.$$

Un caràcter de Dirichlet χ mòdul un nombre enter $N \geq 1$ és un homomorfisme de grups

$$\chi : (\mathbb{Z}/N\mathbb{Z})^* \longrightarrow \mathbb{C}^*.$$

A tot caràcter de Dirichlet χ se li pot associar una funció L definida per

$$L(\chi, s) := \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}, \quad \Re(s) > 1.$$

El símbol de Legendre es pot interpretar com un caràcter de Dirichlet. Donat un discriminant fonamental D , definim

$$\chi_D(p) := \left(\frac{D}{p} \right), \quad \text{si } p \neq 2 \text{ és un nombre primer,}$$

$$\chi_D(2) := \begin{cases} 0, & \text{si } D \equiv 0 \pmod{4}, \\ 1, & \text{si } D \equiv 1 \pmod{8}, \\ -1, & \text{si } D \equiv 5 \pmod{8}, \end{cases}$$

$$\chi_D(p_1^{n_1} \cdots p_s^{n_s}) := \chi_D(p_1)^{n_1} \cdots \chi_D(p_s)^{n_s}.$$

A més,

$$\chi_D(-1) := \begin{cases} 1 & \text{si } D > 0, \\ -1 & \text{si } D < 0. \end{cases}$$

La llei de reciprocitat quadràtica implica que χ_D és un caràcter de Dirichlet mòdul $|D|$.

Si K és un cos quadràtic de discriminant D , se satisfà que

$$\zeta(K, s) = \zeta(s) \cdot L(\chi_D, s);$$

així, aquesta descomposició proporciona una interpretació analítica de la llei de reciprocitat quadràtica. El caràcter χ_D se sol anomenar el caràcter de Kronecker del cos quadràtic.

Més generalment, avancem que les lleis de reciprocitat pròpies de les extensions abelianes $K|\mathbb{Q}$ permeten descompondre la funció zeta de Dedekind $\zeta(K, s)$ com a producte de n funcions $L(\chi, s)$, on $n = [K : \mathbb{Q}]$.

Euler, Legendre i Gauss eren conscients que tota progressió aritmètica $\{a + tN : t \geq 0\}$ en la qual $\text{mcd}(a, N) = 1$ havia de contenir una infinitat de nombres primers. La demostració d'aquest fet, conegut com a teorema de la progressió aritmètica, és deguda a Dirichlet.

Donat un discriminant fonamental D , mitjançant un ús adequat del càlcul integral, Dirichlet determinà el valor de la funció $L(\chi_D, s)$ en $s = 1$. Per a això, féu ús de la teoria de Gauss de la reducció de les formes quadràtiques binàries. El seu resultat constitueix la denominada fórmula analítica del nombre de classes, en el cas quadràtic:

$$h(D) = \begin{cases} \frac{w \sqrt{|D|}}{2\pi} L(\chi_D, 1), & \text{si } D < 0, \\ \frac{\sqrt{D}}{\log \varepsilon_0} L(\chi_D, 1), & \text{si } D > 0, \end{cases}$$

on w denota el nombre d'arrels de la unitat incloses en el cos quadràtic imaginari i ε_0 , la unitat fonamental del cos quadràtic real.

En particular, de la fórmula analítica per al nombre de classes es dedueix que

$$L(\chi_D, 1) \neq 0, \quad \text{per a tot } D.$$

A partir d'aquest fet, Dirichlet demostrà que el conjunt de nombres primers inclosos en una progressió aritmètica de mòdul N té una densitat en el conjunt de tots els nombres primers igual a $1/\varphi(N)$, on $\varphi(N) := \#(\mathbb{Z}/N\mathbb{Z})^*$ és la funció d'Euler. És a dir, els nombres primers que no divideixen N es reparteixen per igual entre les $\varphi(N)$ classes de residus del grup multiplicatiu $(\mathbb{Z}/N\mathbb{Z})^*$; en particular, cada classe conté una infinitat de primers.

2.4 Weierstrass

Karl Theodor Wilhelm Weierstrass (Ostenfelde, 31 d'octubre de 1815; Berlín, 19 de febrer de 1897)

Weierstrass era fill d'un secretari d'ajuntament i inspector d'impostos; cursà els estudis de secundària a l'Institut de Paderborn i l'any 1834 entrà a la Universitat de Berlín per a estudiar lleis, economia i administració. Però en lloc de seguir els estudis reglats, estudià matemàtiques pel seu compte, dedicant-se especialment a la lectura de la *Mécanique céleste* de Laplace, treballs de Jacobi sobre funcions el·líptiques i apunts de les classes de Gudermann. L'any 1838 estudià a la Universitat de Bonn, i l'any després ho féu a l'Acadèmia de Teologia i Filosofia de Münster a fi d'esdevenir professor de secundària. A Münster assistí a les classes que hi impartia Gudermann sobre funcions el·líptiques, i aquest l'encoratjà a continuar els estudis de

matemàtiques. Weierstrass fou professor de secundària a l'Institut de Münster, l'any 1841; al *Deutsch Krone* a la Prússia occidental, actualment Polònia, de 1842 a 1848; i al *Collegium Hoseanum* de Braunsberg, de 1848 a 1854. L'any 1854 obtingué un doctorat honorari a la Universitat de Königsberg i l'any 1856 fou nomenat professor a l'Institut d'Indústria, posteriorment Escola Tècnica Superior (*Technische Hochschule*) de Berlín.

Weierstrass es relacionà amb Kummer i Kronecker, i plegats aconseguiren que la Universitat de Berlín fos un centre de gran prestigi per als estudis de matemàtiques. Entre els estudiants que es beneficiaren dels ensenyaments de Weierstrass hi ha Cantor, Frobenius, Fuchs, Killing, Sofia Kovalevskaya, Lerch, Mangoldt, Runge, Schottky i Schwarz.

L'any 1854, Weierstrass publicà l'article *Zur Theorie der Abelschen Functionen* a la *Revista de Crelle*, que incloïa una descripció preliminar del seu mètode per a la representació de funcions abelianes per mitjà de sèries convergents. En l'article *Theorie der Abel'schen Functionen*, publicat l'any 1856 també per Crelle, hi desenvolupà la seva teoria d'inversió d'integrals hiperel·líptiques.

A Berlín, Weierstrass impartí nombrosos cursos, que versaren sobre funcions analítiques, funcions el·líptiques, funcions abelianes, càlcul de variacions, aplicacions de les funcions el·líptiques, i aplicacions de les sèries de Fourier a la física matemàtica.

A més, fou l'editor de les obres de Jacobi i supervisà l'edició dels primers volums de les seves pròpies. L'obra de Weierstrass fou editada per la Reial Acadèmia de Ciències

de Prússia entre els anys 1894 i 1927. L'edició de la resta de volums estigué a càrrec de Knoblauch i de Rothe.

2.5 Funcions el·líptiques

Les funcions meromorfs doblement periòdiques s'anomenen funcions el·líptiques. Sigui $\Lambda = \mathbb{Z}\lambda_1 \oplus \mathbb{Z}\lambda_2$ un $\mathbb{Z}$ -mòdul lliure de rang 2, $\lambda_i \in \mathbb{C}$; escriurem $\Lambda' := \Lambda \setminus \{(0, 0)\}$. El conjunt de totes les funcions el·líptiques de reticle de períodes Λ constitueix un cos, que denotarem per $\mathbb{C}(\Lambda)$.

Weierstrass construí la funció el·líptica que duu el seu nom com a solució de l'equació diferencial

$$\left(\frac{d\wp}{du}\right)^2 = 4\wp^3 - g_2\wp - g_3, \quad \Delta := g_2^3 - 27g_3^2 \neq 0,$$

amb un pol en $u = 0$. Les funcions de Weierstrass

$$\wp(u, \Lambda) = \frac{1}{u^2} + \sum_{\lambda \in \Lambda'} \left(\frac{1}{(u - \lambda)^2} - \frac{1}{\lambda^2} \right),$$

$$\wp'(u, \Lambda) = -2 \sum_{\lambda \in \Lambda} \frac{1}{(u - \lambda)^3}$$

proporcionen un sistema de generadors del cos $\mathbb{C}(\Lambda)$.

Com que la funció $\wp$ i la seva derivada $\wp'$ estan lligades per una relació algebraica, el grau de transcendència del cos $\mathbb{C}(\Lambda) = \mathbb{C}(\wp, \wp')$ és igual a 1. Per tant, les funcions de Weierstrass proporcionen una parametrització meromorfa de la corba el·líptica d'equació

$$E : Y^2 = 4X^3 - g_2X - g_3, \quad \Delta \neq 0.$$

Els coeficients g_2 i g_3 s'obtenen a partir de les anomenades sèries d'Eisenstein de pesos 4 i 6 respectivament, en ésser avaluades en el reticle de períodes:

$$g_2(\Lambda) = 60 \sum_{\lambda \in \Lambda'} \lambda^{-4}, \quad g_3(\Lambda) = 140 \sum_{\lambda \in \Lambda'} \lambda^{-6}.$$

El problema clàssic de la uniformització euclidiana de les corbes el·líptiques consisteix a saber si tota corba el·líptica complexa

$$Y^2 = 4X^3 - AX - B, \quad A^3 - 27B^2 \neq 0, \quad A, B \in \mathbb{C}$$

admet una parametrització per funcions de Weierstrass. La resposta és afirmativa i la seva demostració s'obté a partir de les propietats de la funció modular j , de la qual parlarem més endavant.

Un cop parametritzada una corba el·líptica per mitjà de les funcions de Weierstrass corresponents, el mètode de la secant i de la tangent proporciona les fórmules d'addició i de duplicació:

$$\wp(u+v) = \frac{1}{4} \left(\frac{\wp'(u) - \wp'(v)}{\wp(u) - \wp(v)} \right)^2 - \wp(u) - \wp(v), \quad u \neq v,$$

$$\wp(2u) = \frac{1}{4} \left(\frac{\wp''(u)}{\wp'(u)} \right)^2 - 2\wp(u).$$

En altres paraules, les funcions de Weierstrass $\wp$, $\wp'$ estableixen un isomorfisme additiu entre els punts d'un tor complex amb reticle de períodes $\Lambda = \langle \lambda_1, \lambda_2 \rangle$ i el grup abelià $E(\mathbb{C})$ dels punts complexos de la corba el·líptica corresponent.

La funció σ de Weierstrass es defineix per mitjà d'un producte convergent que proporciona zeros simples en tots els punts $\lambda \in \Lambda'$:

$$\sigma(u) = u \prod_{\lambda \in \Lambda'} \left(1 - \frac{u}{\lambda}\right) e^{\frac{u}{\lambda} + \frac{1}{2}\left(\frac{u}{\lambda}\right)^2}.$$

Se satisfà que

$$\wp(u) = -\frac{d^2(\log(\sigma(u)))}{du^2}.$$

El teorema d'Abel proporciona una manera eficient per a construir funcions el·líptiques amb zeros i pols donats prèviament. Donat un divisor $D = \sum_{j=1}^r m_j(u_j) - \sum_{j=1}^s n_j(v_j)$ en $\mathbb{C}/\Lambda$, la condició d'Abel afirma que D és principal si, i només si, $\text{gr}(D) = 0$ i

$$\sum_{j=1}^r m_j u_j \equiv \sum_{j=1}^s n_j v_j \pmod{\Lambda}.$$

En aquest cas, D es pot representar en la forma

$$D = \sum_{j=1}^n a_j(u_j) - \sum_{j=1}^n b_j(v_j), \quad \sum_{j=1}^n a_j - \sum_{j=1}^n b_j = 0,$$

i n'hi ha prou de prendre

$$\frac{\prod_{j=1}^n \sigma(u - a_j)}{\prod_{j=1}^n \sigma(u - b_j)}$$

per a tenir una funció el divisor de la qual és D . El teorema d'Abel es generalitza a tota superfície de Riemann, sigui quin sigui el seu gènere.

En general, donada una corba el·líptica E definida sobre un subcòs $K \subseteq \mathbb{C}$, la seva llei d'addició determina que el conjunt $E(K)$ dels seus punts K -racionals té estructura de grup abelià. Els punts de N -divisió de E , és a dir, els punts P que satisfan $NP = 0_E$, són racionals sobre la clausura algebraica $\overline{K}$ de K . El seu conjunt $E[N]$ és un subgrup de $E(\overline{K})$ de N^2 elements, isomorf a $\mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$.

L'any 1901, Poincaré s'ocupà de la determinació de l'estructura del grup dels punts de coordenades racionals d'una corba el·líptica definida sobre el cos $\mathbb{Q}$ dels nombres racionals. Les seves investigacions donaren lloc a l'anomenada conjectura de Poincaré per a corbes el·líptiques, segons la qual, donada una corba el·líptica E definida sobre $\mathbb{Q}$,

$$E: \quad Y^2 = X^3 + a_4X + a_6, \quad a_i \in \mathbb{Q},$$

el grup abelià $E(\mathbb{Q})$ és finitament generat.

2.6 Kronecker

Leopold Kronecker (Liegnitz, 7 de desembre de 1823; Berlín, 29 de desembre de 1891)

Kronecker nasqué en el si d'una família jueva i molt rica. Fou educat per tutors privats fins que entrà al *Gymnasium* de Liegnitz, on tingué Kummer com a professor de matemàtiques; ell li despertà l'interès per la matèria, en incitar-lo a la recerca.

A partir de 1841, Kronecker estudià a la Universitat de Berlín, amb Dirichlet i Steiner; l'estiu de 1843, a Bonn; el curs 1843–1844, a Breslau, on hi havia com a catedràtic de la Universitat el seu antic professor, Kummer; i el curs 1844–1845, de nou a Berlín, on l'estiu de 1845 llegí la tesi, dirigida per Dirichlet. En aquella època, Jacobi i Eisenstein eren professors a Berlín; Kronecker els conegué i, més endavant, es notaria la seva influència.

Un cop llegida la tesi, Kronecker es retirà a les propietats de la seva família per a dedicar-se a algunes qüestions relacionades amb els negocis del seu oncle, es casà amb la seva cosina, i només es dedicà a la recerca en matemàtiques per al seu propi gaudi.

Quan, l'any 1855, Kummer arribà a Berlín per a cobrir la plaça deixada vacant per l'anada de Dirichlet a Göttingen, Kronecker retornà a Berlín i, com que no ho necessitava per a viure, no hi va voler cap tipus de treball remunerat. Cap a la fi d'aquell any, Borchardt, que feia classes a la Universitat de Berlín des de 1848, es convertí en l'editor de la *Revista de Crelle*. I, un any més tard, també Weierstrass arribà a la Universitat de Berlín. Així, en poc menys d'un any, es trobaren a la ciutat de Berlín els matemàtics Borchardt, Kummer, Kronecker i Weierstrass.

A partir d'aquest punt, Kronecker gaudí d'un període de recerca i de producció molt actiu; i el mes de gener de 1861 entrà a l'Acadèmia de Berlín, a instàncies de Kummer i amb el recolzament de Borchardt i de Weierstrass. A partir de finals de 1862, i de nou per la influència de Kummer sobre ell, Kronecker exercí el dret que tenia com a acadèmic de poder ensenyar a la Universitat. Ho féu sobre els temes de la seva pròpia recerca: teoria algebraica de

nombres, teoria d'equacions algebraiques, teoria de determinants, funcions el·líptiques, i teoria d'integració; i també intentant millorar, simplificar i presentar des de nous punts de vista els coneixements que se'n tenia.

Kronecker només volia estar a Berlín; fins al punt que, l'any 1868, renuncià a l'oferiment de la càtedra de matemàtiques de Göttingen; en canvi, acceptà ésser nomenat membre de l'Acadèmia de París, aquell mateix any; més endavant, l'any 1884, encara seria nomenat membre corresponent de la Reial Societat de Londres.

L'any 1880, quan Borchardt morí, Kronecker el rellevà com a editor de la *Revista de Crelle*; aquest fet féu augmentar la influència de Kronecker a Berlín. Aquesta influència encara es faria més gran quan Kummer es retirà l'any 1883. Llavors, Kronecker el substituï en la codirecció del seminari de matemàtiques de Berlín, que Kummer havia fundat juntament amb Weierstrass l'any 1861, i amb qui el codirigia.

L'any 1890 es creà la Societat Matemàtica Alemanya i preparà la primera reunió per al setembre de 1891. Cantor, com a senyal de respecte i malgrat les profundes diferències de caire matemàtic que tenia amb Kronecker, el convidà a pronunciar-hi el discurs d'obertura. Però Kronecker no ho arribà a fer per la mort de la seva esposa, ocorreguda el 23 d'agost a causa d'un accident. Kronecker mateix moriria pocs mesos després.

En teoria de nombres, el nom de Kronecker s'associa indefectiblement al seu *Somni de Joventut* (*Jugendtraum*). Aquest somni no s'ha de confondre amb el *Somni del Jovent* (*Traum der Jugend*) que expressà la compositora Fanny

Mendelssohn en una de les seves *Romances sense paraules* (*Lieder ohne Worte*) que, alhora, no s'han de confondre amb les *Romances sense paraules* (*Lieder ohne Worte*) del seu germà Fèlix.

Entre els deu estudiants de doctorat de Kronecker, dels quals set ho foren en el període 1883–1885, destaquem Hensel, l'introduïdor dels nombres p -àdics i, alhora, el director de tesi de Hasse. D'altra banda, podem esmentar que Hensel era nét de Fanny Mendelssohn.

L'obra de Kronecker fou editada per Hensel i impresa a Leipzig, entre els anys 1895 i 1931, en cinc volums, el tercer en dues parts, i reeditada l'any 1968 per Chelsea.

2.7 El *Somni de Joventut*

En un article publicat l'any 1853, Kronecker manifestà haver obtingut el notable resultat que les solucions de qualsevol equació polinòmica de coeficients enters i grup de Galois abelià són expressables com a funcions racionals d'arrels de la unitat.

La intuïció de Kronecker resultà ésser correcta. Però el camí fins a obtenir una primera demostració del fet que tota extensió abeliana del cos racional és ciclotòmica fou laboriós. Aquesta afirmació es coneix avui amb el nom de teorema de Kronecker–Weber. Weber n'assolí diverses demostracions, no exemptes de crítiques. L'any 1896, Hilbert en donà la primera prova acceptada, que inclogué en el seu *Zahlbericht* un any després ([205], [206]).

Els intents posteriors relatius a la generalització del teorema de Kronecker–Weber donaren lloc al naixement de la teoria de la multiplicació complexa. A partir d'uns quants exemples en què se sabia que els valors de divisió $\text{sl}(\varpi/4)$, $f(\varpi/4)$, $F(\varpi/4)$ generaven extensions abelianes de $\mathbb{Q}(i)$, Kronecker afirmà que *totes* les extensions abelianes de $\mathbb{Q}(i)$ s'haurien de poder obtenir adjuntant valors de divisió $\text{sl}(\varpi/N)$, $N \in \mathbb{N}$. No content amb això, pensà en una possibilitat semblant quan el cos base és un cos quadràtic imaginari qualsevol.

En una carta dirigida a Dedekind, datada el 15 de març de 1880, Kronecker (que en aquells moments tenia 57 anys) li comunicà la seva satisfacció perquè creia haver culminat, després d'una recerca represa més a fons en els darrers mesos, l'última d'una sèrie de dificultats que encara restaven pendents relatives al seu *Somni de Joventut*:

Moltíssimes gràcies per la seva amable carta del 12 del corrent. Crec que és una bona ocasió per a comunicar-li que avui crec haver vençut la darrera d'una sèrie de dificultats que encara romanien per a la finalització d'una recerca en la qual m'he tornat a implicar intensivament en els darrers mesos. Es tracta del meu estimat Somni de Joventut, a saber, la demostració que les equacions abelianes en [coeficients/arrels quadrades de nombres racionals s'esgoten per mitjà de les equacions de transformació de les funcions el·líptiques de mòduls singulars, de la mateixa manera que les equacions abelianes

en [coeficients] enters [ho fan] amb equacions d'arrels de la unitat.

Kronecker [244]

La interpretació d'aquestes paraules no estigué exempta de controvèrsia. Certament, en un altre passatge clau de 1877, en el qual havia alludit al seu Somni de Joventut, Kronecker ens parla de dos tipus de nombres algebraics per a generar les extensions abelianes dels cossos quadràtics imaginaris: els mòduls singulars, corresponents a valors especials de funcions modulars el·líptiques, i els valors de divisió, donats per funcions el·líptiques de mòdul singular avaluades en arguments relacionats racionalment amb els períodes.

L'afirmació que tota extensió abeliana d'un cos quadràtic imaginari es genera mitjançant mòduls singulars i valors de divisió de funcions el·líptiques de mòdul singular és correcta. La seva demostració constitueix el teorema de completesa de la teoria de la multiplicació complexa en el cas quadràtic imaginari.

El mateix Kronecker no arribà a demostrar el teorema de completesa. Weber, tampoc, tot i que hi féu notables avenços. L'any 1901, Takagi demostrà aquest teorema quan el cos base és el cos $\mathbb{Q}(i)$ dels nombres racionals de Gauss. Per a això, utilitzà les senzilles propietats de divisibilitat de l'anell dels nombres enters de Gauss i un coneixement explícit de les equacions de divisió de les funcions lemniscàtiques.

Les primeres demostracions del teorema de completesa es gestaren en una sèrie d'articles de Fueter, publicats entre 1905 i 1927, en què hi ha una multitud d'afirmaci-

ons incorrectes que el mateix autor va corregint en treballs successius. Takagi aconseguí donar una demostració del teorema de completesa l'any 1920.

El desenvolupament de la teoria de la multiplicació complexa en el cas quadràtic imaginari corregué paral·lel al descobriment de la teoria de cossos de classes. Després de l'etapa inicial protagonitzada per Fueter i Takagi, la teoria de la multiplicació complexa en el cas quadràtic imaginari assolí la seva formulació actual entre els anys 1940 i 1950. En aquest període, Hasse i Deuring aconseguiren expressar els seus resultats en termes de les funcions L de les corbes el·líptiques dotades de multiplicació complexa.

2.8 Fuchs

Lazarus Immanuel Fuchs (Moschin, Posen, ara Poznań, Polònia, 5 de maig de 1833; Berlín, 26 d'abril de 1902)

Fuchs, juntament amb Frobenius i Schwarz, forma part de la segona generació de matemàtics de l'escola de Berlín. Nascut a Prússia i fill d'un professor, la seva educació tingué lloc a Berlín, on, després de cursar els estudis de secundària al *Friedrich Wilhelm Gymnasium*, estudià a la seva Universitat. Entre els seus professors hi ha Kummer i Weierstrass. Aquest li dirigí la tesi, que, amb el nom *Sobre les línies de curvatura de les superfícies* (*De Superficierum lineis curvaturae*), defensà l'any 1858. Notem que a mitjan segle XIX encara era habitual presentar els treballs científics en llatí.

Després d'exercir uns quants anys de professor de secundària, Fuchs entrà com a encarregat de curs (*Privatdozent*) a la Universitat de Berlín l'any 1865; aquest càrrec permetia impartir docència a l'alumnat que ho sol·licités. A partir de l'any següent i fins al 1869 en seria professor extraordinari. Des de 1867 fins a 1869, simultaniejà les seves tasques a la universitat amb les de professor de matemàtiques a l'Escola d'Artilleria i Enginyeria de la mateixa ciutat. Entre 1869 i 1874 fou professor de la Universitat de Greifswald. Finalment, després d'un any a Göttingen (1874–1875) i nou anys més a Heidelberg (1875–1884), tornà a la Universitat de Berlín com a successor de Kummer a la càtedra, quan aquest es retirà. En morir Kronecker, l'any 1891, Fuchs el substituï com a editor de la *Revista de Crelle*, fins a la seva pròpia mort, esdevinguda l'any 1902.

Fuchs treballà principalment en equacions diferencials i teoria de funcions. Després dels resultats fonamentals de Gauss, Abel, Riemann i Cauchy en aquests camps, els seus treballs serviren de pont a desenvolupaments posteriors de Poincaré, Painlevé i Picard, i influïren en l'obra de Dedekind i de Jordan.

L'obra de Fuchs en equacions diferencials s'emmarca en l'intent de traslladar a aquest terreny els resultats emergents de la teoria de funcions de variable complexa. El seu interès per les equacions diferencials sorgí com a conseqüència de les lliçons que rebé de Weierstrass sobre funcions abelianes i teoria d'equacions diferencials lineals.

En aquella època, Riemann ja havia portat a terme l'estudi de l'equació hipergeomètrica des del punt de vista de la variable complexa, i havia introduït, en generalitzar aquella, les seves funcions P , que són funcions definides a

l'esfera de Riemann amb tres punts de ramificació donats per endavant, no necessàriament $0, 1, \infty$.

L'any 1857, Riemann havia desenvolupat una teoria de funcions algebraiques i les seves integrals en el treball *Teoria de funcions abelianes* (*Theorie der Abel'schen Functionen*). Per extensió d'un treball previ de Weierstrass per al cas d'integrals hiperel·líptiques, Riemann es plantejà l'existència de funcions amb zeros i pols donats per endavant i que fossin solució d'un sistema d'equacions diferencials lineals. La resposta a aquesta pregunta donaria lloc més endavant al teorema de Riemann–Roch.

Al mateix temps, l'escola francesa, amb Cauchy, Briot i Bouquet, es preocupava d'investigar les singularitats de funcions de variable complexa definides per equacions diferencials.

En un treball primerenc de l'any 1865, que constituí la seva tesi d'habilitació, que publicà en forma revisada l'any 1866 (cf. [156]), i que amplià l'any 1868, Fuchs considerà equacions diferencials lineals ordinàries d'ordre n ,

$$\frac{d^n y}{dx^n} = p_1 \frac{d^{n-1} y}{dx^{n-1}} + \cdots + p_n y,$$

en què els coeficients són funcions racionals de x . Demostrà que, fora dels pols dels coeficients, l'equació posseeix una base de n solucions linealment independents que queda determinada per l'elecció de valors inicials de $y, \frac{dy}{dx}, \dots, \frac{d^{n-1} y}{dx^{n-1}}$ en un punt no singular. Aquest fet seria reconsiderat posteriorment per Frobenius.

Fuchs s'adonà que els punts singulars de les solucions es troben entre els punts singulars dels coeficients i, per tant,

pertanyen a un conjunt fix, independent de les condicions inicials. Tot seguit es preocupà de saber quines restriccions han de satisfer els coeficients de l'equació diferencial a fi que les singularitats de les solucions siguin únicament pols o punts de ramificació logarítmics; en aquest cas, es diu que les singularitats de l'equació diferencial de partida són punts singulars regulars. Fuchs obtingué una resposta a aquest problema seguint els mètodes de Riemann. Si $\mathbf{y} = (y_1, \dots, y_n)$ és un sistema de n solucions independents que és vàlid a l'entorn d'un punt singular a de l'equació, aleshores per continuació analítica de $\mathbf{y}$ al voltant de a es produeix un altre sistema de solucions independents $\tilde{\mathbf{y}} = (\tilde{y}_1, \dots, \tilde{y}_n)$ i se satisfà que $\tilde{\mathbf{y}} = R\mathbf{y}$, on R és una matriu invertible $n \times n$ de nombres complexos, que més endavant seria anomenada matriu de monodromia. En tenir en compte els ρ punts singulars de l'equació diferencial i descriure un camí contràctil orientat a l'esfera de Riemann llevat d'aquests punts, s'obté una relació de la forma

$$R_1 B_2 R_2 B_2^{-1} \cdots B_{\rho+1} R_{\rho+1} B_{\rho+1}^{-1} = \text{Id},$$

d'on $\det(R_1 R_2 \cdots R_{\rho+1}) = 1$.

De manera innovadora, Fuchs es fixà en els valors propis de cadascuna de les matrius R_i , als quals anomenà arrels de l'equació fonamental determinadora. Si $w_{i,j}$ és un valor propi al qual li correspon una solució $\mathbf{y}_i$, aleshores $\tilde{y}_{i,j} = w_{i,j} y_{i,j}$. La solució $y_{i,j}$ és de la forma

$$y_{i,j} = x^{r_{i,j}} \sum_{n=-m_{i,j}}^{\infty} a_n(i, j) x^n,$$

on $w_{i,j} = e^{2\pi i r_{i,j}}$. Si les matrius R_i són diagonalitzables, aleshores les solucions no tenen termes logarítmics; si, a

més, els valors propis són diferents, aleshores els corresponents $r_{i,j}$ no difereixen en un nombre enter. En canvi, quan les matrius R_i no són diagonalitzables, són d'esperar termes logarítmics.

Observem que, en aquella època, Jordan encara no havia publicat els seus resultats sobre les formes canòniques de les matrius. Aquests apareixerien l'any 1870 en el seu *Tractat de les substitucions* (*Traité des substitutions*). Un treball pioner a aplicar les formes de Jordan a l'estudi de les equacions diferencials fou [179] (cf. [168]).

Fuchs deduí una equació per al càlcul directe dels exponents $r_{i,j}$; ell l'anomenà equació fonamental, i Cayley, l'any 1883, equació indicial. El punt culminant d'aquesta recerca de Fuchs fou el teorema segons el qual les singularitats de l'equació diferencial són totes regulars si, i només si, aquesta és de la forma

$$\frac{d^n y}{dx^n} = \frac{F_{\rho-1}}{\psi} \frac{d^{n-1} y}{dx^{n-1}} + \frac{F_{2(\rho-1)}}{\psi^2} \frac{d^{n-2} y}{dx^{n-2}} + \cdots + \frac{F_{n(\rho-1)}}{\psi^n} y,$$

on $\psi = (x - a_1)(x - a_2) \cdots (x - a_\rho)$ i F_k és un polinomi en x de grau com a molt k . L'equació té $\rho + 1$ punts singulars, $a_1, a_2, \dots, a_\rho$, i $a_{\rho+1} = \infty$. A més, el comportament previst de les solucions obliga que per als índexs $r_{i,j}$ se satisfaci la igualtat

$$\sum_{i=1}^n \sum_{j=1}^{\rho+1} r_{i,j} = (\rho - 1) \frac{n(n-1)}{2}.$$

Les equacions diferencials de la forma anterior s'han anomenat posteriorment equacions diferencials fuchsianes.

Llevat dels casos $n = 1$, ρ qualsevol, i $n = \rho = 2$, les equacions diferencials fuchsianes no són unívocament

determinades per les seves solucions. La determinació dels coeficients dels polinomis F_k implica més graus de llibertat que la quantitat de nombres $r_{i,j}$ disponibles. Els coeficients extrems s'anomenen paràmetres accessoris.

La presència de paràmetres accessoris per a les equacions diferencials de tipus fuchsianà s'ha revelat una de les dificultats principals a l'hora de procedir a la uniformització efectiva de corbes algebraïques. Els paràmetres accessoris només es poden determinar en casos en què es disposa d'informació addicional; per exemple, de condicions de simetria inherents a la natura del problema (cf. [16], [35], [36], [37]).

Era ben sabut que els períodes de les integrals el·líptiques, com a funció del mòdul, satisfan una equació diferencial de Legendre, que és un cas particular d'equació fuchsiana. A partir d'aquest resultat, Fuchs investigà els períodes de les integrals hiperel·líptiques i arribà a la conclusió que, com a funció dels mòduls, satisfan una equació diferencial fuchsiana. Més endavant, també fou capaç de reconèixer que els períodes de les integrals abelianes interpretats com a funcions dels mòduls, i les constants theta, interpretades com a funcions dels mòduls, també satisfan equacions diferencials fuchsianes.

Fuchs s'interessà, també, per la caracterització dels casos en què les solucions de les equacions diferencials fuchsianes són algebraïques. L'any 1872, Schwarz determinà els 14 casos, a més dels de la família diedral, en els quals totes les solucions de l'equació diferencial hipergeomètrica són algebraïques (cf. [338]). Schwarz arribà a aquest resultat per un estudi previ d'una equació diferencial de tercer ordre que és satisfeta pel quocient de dues solucions independents de l'equació hipergeomètrica. L'equació de tercer

ordre de què es tracta es coneix avui amb el nom de derivada schwarziana, tot i que, tal com el mateix Schwarz sabia molt bé, havia estat emprada prèviament, l'any 1834, pel seu sogre (cf. [248]). De fet, l'any 1779 ja l'havia usada Lagrange en un treball de geodèsia (cf. [251]) publicat a l'Acadèmia Prussiana de Ciències de Berlín.

Fou en aquest treball que Schwarz considerà l'aplicació conforme sobre el disc unitat de triangles curvilinis; les funcions així obtingudes es coneixerien més endavant com les funcions triangulars de Schwarz. Les que corresponen als quinze casos anteriors proporcionaren els primers exemples de funcions automorfes; en aquest cas, respecte de subgrups finits del grup $\mathrm{PSL}(2, \mathbb{C})$.

Entre 1871 i 1901, Fuchs dirigí 26 estudiants de doctorat, entre els quals hi ha Schlesinger, l'any 1887, i Zermelo, l'any 1894. Les obres de Fuchs foren editades en tres volums entre els anys 1904 i 1909 per Schlesinger, i el propi fill de Fuchs, Richard.

2.9 Thomae

Carl Johannes Thomae (Laucha, Unstrut, 11 de desembre de 1840; Jena, 1 d'abril de 1921)

Thomae inicià els seus estudis a la Universitat de Halle Wittenberg l'any 1861. Hi rebé lliçons de Carl Neumann i Eduard Heine, matemàtics que procedien de Königsberg, de l'entorn de Jacobi. Thomae adquirí de Neumann la seva disposició per a la matemàtica aplicada, i de Heine, la seva afició per la teoria de funcions.

Un any després, i d'acord amb la tendència dels estudiants alemanys, es desplaçà a Göttingen amb la intenció d'assistir als cursos de Riemann; però l'inici de la greu malaltia d'aquest li ho impedí. En substitució d'això, Thomae i Gordan decidiren treballar junts les lliçons de Riemann. Thomae assistí a les classes del substitut de Riemann, Schering, qui, l'any 1864, acabaria per supervisar-li la tesi doctoral.

Un cop llegida la tesi, es desplaçà a Berlín, on estudià funcions el·líptiques amb Weierstrass; i poc després inicià la preparació de treballs i la seva publicació. Tot i que l'any 1866 Thomae s'habilità a Göttingen —amb un treball introductori sobre els nombres ideals— i que mai no tingué cap plaça a Berlín, la seva obra s'emmarca dins d'aquesta escola per les seves característiques de contingut i de metodologia.

El mateix any 1866, Thomae prengué part en la Guerra Austroprussiana de les Set Setmanes, un conflicte iniciat per Bismarck. La guerra finalitzà amb la victòria de Prússia i, com a conseqüència d'això, es creà la Confederació de l'Alemanya del Nord, amb 21 estats, i de la qual Àustria fou exclosa, tal com pretenia Bismarck. Un cop acabada la guerra, Thomae retornà a Göttingen, on impartí lliçons sobre càlcul diferencial i integral.

L'any 1867 Thomae fou nomenat encarregat de curs a Halle, on esdevingué company de Heine i de Cantor. Alhora, presentà una altra tesi d'habilitació, que consistí en dos treballs seus d'anàlisi. L'any 1872 fou nomenat professor extraordinari a Halle, i l'any 1874, professor ordinari (*ordentlicher Professor*) a Freiburg; aquesta denominació és equivalent a la nostra de catedràtic. L'any 1879 se n'anà

a Jena, on coincidí amb Frege. La seva relació amb Frege fou intensa, tot i que científicament ambdós eren oposats. Tots dos romandrien a la Universitat de Jena fins a la fi de les seves carreres.

Thomae mantingué una intensa activitat en la direcció d'estudiants, que fructificà en la direcció de 47 tesis doctorals, les cinc primeres de les quals es defensaren a Freiburg, i la resta, a Jena. També desenvolupà diversos càrrecs de gestió; fou degà de la Facultat de Filosofia de Jena en quatre ocasions, i arribà a ésser Rector de la Universitat en dues, els anys 1888 i 1901.

Si bé Thomae compta amb una extensa producció científica de més de 100 treballs, no sembla que s'hagi editat la seva obra completa. És un analista típic del segle XIX; entre els seus temes preferents en matemàtica fonamental hi ha l'estudi de les funcions theta, les funcions abelianes, les sèries hipergeomètriques, les equacions diferencials, i alguns aspectes de geometria projectiva. En matemàtica aplicada, té treballs d'astronomia, de teoria de l'elasticitat i de teoria del potencial.

L'obra de Thomae en teoria de funcions fou fortament influenciada per les de Riemann i Weierstrass. La contribució més important es troba en els seus treballs sobre funcions theta. En ells es demostra la coneguda com a fórmula de Thomae, que expressa els punts de ramificació de les corbes hiperel·líptiques en termes de constants theta hiperel·líptiques. En un altre d'aquests mateixos treballs, Thomae prova que les arrels dels polinomis són expressables en termes de funcions theta hiperel·líptiques. L'any 1880, aparegué la primera edició del seu llibre *Teoria elemental de les funcions analítiques d'una variable complexa* (*Elemen-*

tare Theorie der analytischen Functionen einer complexen Veränderlichen). El volum s'inicia amb un tractament dels nombres; Thomae, després d'introduir els nombres enters i els nombres racionals, construeix els nombres irracionals per mitjà de successions, d'acord amb el mètode publicat prèviament per Cantor i Heine, per a finalitzar el capítol amb els nombres complexos. El llibre continua amb capítols dedicats a successions, sèries i productes; funcions d'una i de dues variables i el concepte de continuïtat; funcions enteres —polinòmiques en la terminologia actual— i la fórmula del binomi per a potències d'exponent enter; sèries de potències; la funció exponencial i les sèries trigonomètriques; la funció logaritme i les sèries logarítmiques; potències de base i exponent general; funcions racionals i productes infinits; funcions algebraïques, inversió de sèries i funcions ciclomètriques —inverses de les funcions trigonomètriques—; ordres de creixement; funcions theta; i funcions el·líptiques. (Aquest contingut, doncs, no és el del llibre d'Henri Cartan de l'any 1961 que, amb un títol gairebé idèntic, molts encara tenim a les nostres lleixes.)

La teoria de les funcions theta i de les funcions el·líptiques que presenta Thomae en el seu tractat és la de Jacobi, amb la novetat de fer incursions en les superfícies de Riemann corresponents. Pel fet que calia establir molta nomenclatura nova, Thomae es troba amb problemes a l'hora d'anomenar els objectes d'estudi del llibre; per exemple, parla de logaritmes artificials, en contraposició als logaritmes naturals, per a anomenar els logaritmes en base diferent del nombre e .

El tractament de les funcions theta que Thomae fa en aquest llibre seria àmpliament superat vint-i-tres anys més

tard pel de Krazer en l'impactant *Tractat de les funcions theta* (*Lehrbuch der Thetafunktionen*), de l'any 1903 [238]. Traces d'aquestes obres es poden detectar en la producció posterior de Poincaré, Weil o Mumford, per exemple.

A l'època de Thomae hi havia força reticències per a assimilar la teoria de conjunts de Cantor. Així, en una carta a Dedekind, i en relació amb el fet que hi ha el mateix nombre de punts en un espai de dimensió qualsevol que en una recta, Thomae comenta que “tot i que ho veu, no s'ho creu”. D'altra banda, ell fou pioner a intentar demostrar el teorema d'invariància de la dimensió, però no se'n sortí atesa la manca d'eines que encara patia la topologia.

Tot i que, avui, l'obra de Thomae és força desconeguda, la seva influència —com la d'altres matemàtics de l'època— és implícita en moltes de les construccions abstractes de la matemàtica del segle XX. Així, per exemple, l'estudi de les funcions theta i de les funcions abelianes ha influït en el desenvolupament de les teories geomètriques de fibrats i de varietats abelianes, respectivament.

2.10 Frobenius

Ferdinand Georg Frobenius (Berlín–Charlottenburg, 26 d'octubre de 1849; Berlín, 3 d'agost de 1917)

Frobenius nasqué a Charlottenburg, actualment un districte de Berlín, el 26 d'octubre de 1849. Estudià al *Joaachimsthal Gymnasium* des dels 11 anys fins als 18. La seva carrera universitària s'inicià l'any 1867 amb un breu període de sis mesos a la Universitat de Göttingen, però és a Ber-

lín on es formà, sota la influència de les tres grans figures de la universitat berlinesa: Kummer, Kronecker i Weierstrass. Només tres anys més tard, l'any 1870, ja presentà la seva tesi doctoral, *Sobre la representació per sèries infinites de funcions analítiques d'una variable* (*De functionum analyticarum unis variabilis per series infinitas representatione*), dirigida per Weierstrass. Quatre anys de docència a l'institut on s'havia format foren el preàmbul d'una carrera acadèmica brillant, que es desenvolupà a l'Escola Tècnica Superior Federal (*Eidgenössische Technische Hochschule*) (ETH) de Zuric i a la Universitat de Berlín, on exercí de catedràtic des de 1892 fins a la seva mort, el 3 d'agost de 1917.

Dirichlet, Eisenstein i Jacobi havien fet de la Universitat de Berlín un dels principals centres d'investigació europeus, i Kronecker, Kummer i Weierstrass n'eren les estrelles quan Frobenius hi anà a estudiar. La influència de Weierstrass tingué un paper important en la seva carrera, començant per la codirecció de la seva tesi, presentada l'any 1870.

Després d'uns anys a l'ensenyament secundari, Frobenius fou nomenat professor extraordinari de la Universitat de Berlín, i s'estalvià el període pertinent d'encarregat de curs, gràcies al recolzament de Weierstrass. Un any després, seguint el camí d'altres berlinesos il·lustres, com Prym, Schwarz o Schottky, fou nomenat professor ordinari a l'ETH de Zuric, on passà els disset anys següents. En el període transcorregut des de la presentació de la seva tesi, Frobenius publicà fins a trenta-set treballs a la *Revista de Crelle*.

La mort de Kronecker, l'any 1891, deixà una plaça vacant a la Universitat de Berlín i a la Reial Acadèmia de Ciències de Prússia. Weierstrass veia en Frobenius la persona que havia de mantenir aquesta darrera institució en l'avantguarda matemàtica. En un escrit de recomanació elaborat per a l'ocasió, Weierstrass i Fuchs enumeraren fins a quinze camps diversos en els quals Frobenius sobresortia. El text acabava així:

Tots els seus treballs demostren un gran domini de la matèria; tots ells contenen o bé resultats nous o bé resultats coneguts presentats en una forma nova. A més, Frobenius té un estil de primera línia, i escriu de forma clara i comprensible, evitant sempre de confondre el lector amb frases buides.

Creiem, després de tot això, que l'Acadèmia engrandirà el seu propi prestigi amb la seva elecció com a membre ordinari.

Weierstrass i Fuchs

L'amplitud i la vàlua dels treballs de Frobenius queden reflectits en el comentari següent de Fuchs i de Helmholtz, en una addenda a l'escrit de recomanació anterior:

Seria inútil incloure aquí la llista de títols dels seus nombrosos treballs; n'hi ha prou d'indicar els camps que deuen a la seva creativitat nous fonaments o l'enriquiment d'alguna disciplina particular. Són la teoria d'equacions diferencials, la teoria de nombres, l'àlgebra, la teoria de grups, la teoria de les funcions el·líptiques i

abelianes, i la teoria de les equacions en derivades parcials. En tots els temes que ha tractat, ha reconstruït els fonaments i, en molts dels seus treballs, a partir d'aquests fonaments, ha construït de nou una disciplina completa en una forma original i des d'un punt de vista unificat. Ha aconseguit mostrar els resultats existents de la disciplina amb una perspectiva nova, ha completat els buits que hi ha trobat, i ha creat una base que proporciona una oportunitat excel·lent per a la recerca futura. Cadascun dels seus treballs més llargs es pot prendre ben bé com un petit compendi de la disciplina considerada.

Fuchs i Helmholtz

Com hem dit més amunt, Frobenius ocupà la càtedra de la Universitat de Berlín des de l'any 1892 fins a la seva mort l'any 1917. La seva producció científica en aquest període avala la confiança que li féu Weierstrass: introduí els caràcters dels grups i creà la teoria de representacions dels grups, eines que esdevindrien cabdals per al desenvolupament de la matemàtica en el segle XX.

Malauradament, el temperament i les idees de Frobenius no l'ajudaren gaire. Haubrich ens ofereix una semblança del seu entorn ([193]):

[Els professors de la Universitat de Berlín] se sentien tots obligats a perpetuar la tradició neoclàssica prussiana d'ensenyament i de recerca universitàries tal com ells mateixos havien experimentat com a estudiants. Això és especialment palès en Frobenius. Es considerava un

erudit amb el deure de contribuir al coneixement de la matemàtica pura. La matemàtica aplicada, segons la seva opinió, corresponia a les escoles tècniques.

El mètode de treball de Frobenius confirma aquesta manera seva de pensar ([193]):

L'aspecte més sorprenent de la seva pràctica matemàtica és la seva habilitat extraordinària per als càlculs. De fet, Frobenius intentava resoldre problemes matemàtics bàsicament a través d'una aproximació algebraica calculística. Fins i tot en el seu treball analític el guiaven els mètodes algebraics i d'àlgebra lineal. Per a Frobenius, l'argumentació conceptual jugava un paper una mica secundari. Per bé que ell raonava en un marc relativament abstracte, l'abstracció no és un objectiu per si mateixa; per a ell, els seus avantatges recauen més que res en el fet que permet molta més claredat i precisió.

Frobenius hagué d'assumir l'ascens de la Universitat de Göttingen, que aportà un canvi d'estil a la tradició alemanya. En una carta a Hurwitz, que era originari de Göttingen, escriu:

Si vostè se n'estigués anant d'una escola en la qual hom es diverteix més amb imatges prometedores que amb idees sòlides, i si, per a la meua alegria, vostè també se n'està emancipant a poc

a poc, llavors... amor antic no es rovella (“alte Liebe rostet nicht”). *Si us plau, prengui's aquest acudit de broma.*

Frobenius

Efectivament, Göttingen anà guanyant pes. En canvi, el nombre de doctorats i d'habilitacions a la Universitat de Berlín minvava, per bé que el nombre d'estudiants augmentava considerablement. Les classes de Frobenius eren excel·lents (hi assistien fins a 250 estudiants) i cobrien un espectre molt ampli: teoria de nombres, àlgebra, geometria, teoria de grups, etcètera. Hi ha dos mèrits que llueixen especialment en el seu historial com a professor: la descoberta de Schur i la captació de Siegel per a les matemàtiques. Siegel arribà a la Universitat de Berlín l'any 1915 amb la idea d'estudiar astronomia, però després d'assistir a les primeres lliçons del curs de Frobenius sobre teoria de nombres, quedà fascinat per aquella matèria, de la qual no coneixia res, i ja no l'abandonà mai més. En paraules d'ell mateix, “després d'anys d'escolaritat depriment amb mestres mediocres o maliciosos, les classes de Frobenius foren una experiència nova i alliberadora”. Frobenius morí dos anys després, així que no tingueren oportunitat de col·laborar, per bé que sembla que Frobenius aconseguí que fos atorgada a Siegel una beca de la fundació Eisenstein. Molt més significativa fou la tasca realitzada amb Schur, a qui dirigí la tesi i amb qui col·laborà llargament per a desenvolupar la teoria de representacions de grups, que ell mateix havia iniciat. L'impacte de Schur en les matemàtiques del segle XX també fou de gran rellevància.

La vida acadèmica de Frobenius girà entorn de la Universitat de Berlín; Kronecker, Kummer i Weierstrass tin-

gueren una forta influència en la seva obra. Kummer i Weierstrass foren els seus directors de tesi. El resultat que es coneix avui com a teorema de Txebotarev naixé, de fet, de les idees de Kronecker, concretades per Frobenius.

Al llarg de la seva carrera, Frobenius col·laborà amb Stickelberger, també format a Berlín, amb qui publicà tres treballs sobre funcions el·líptiques i un sobre grups abeliàns. Mantingué correspondència amb Dedekind en el període anterior a la descoberta dels caràcters dels grups. No és agosarat pensar que l'interès de Frobenius pels grups tingué el seu origen en la teoria de nombres i que, probablement, el seu anhel fos la prova del teorema de Txebotarev. En la darrera etapa de la seva vida, Frobenius treballà amb Schur en el desenvolupament de la teoria de representacions de grups. Entre els descendents directes de Frobenius sobresurten Landau i, especialment, Schur. El seu arbre genealògic en matemàtiques comprèn altres grans noms com ara Brauer, Hopf, Heilbronn o Siegel.

La producció científica de Frobenius segueix una evolució marcada per la influència dels seus mestres —Weierstrass primer i Kronecker posteriorment— i del seu coetani Dedekind. Aquesta evolució es fonamenta en la descoberta de les aplicacions de l'àlgebra lineal, que el porta des del camp de les equacions en derivades parcials a la teoria de nombres i a la representació de grups; també ocasiona que la seva obra deixi empremta en àrees molt diverses de la matemàtica actual.

A grans trets, la recerca de Frobenius es divideix en quatre períodes, que desglossarem a continuació. Els primers treballs se centren en les sèries de potències i la seva aplicabilitat a la resolució d'equacions diferencials. Al

començament de la seva estada a Zuric, Frobenius s'ocupa de les funcions el·líptiques i de les funcions theta, amb algun treball ocasional de temàtica geomètrica. Un problema aritmètic li servirà de pont cap a la recerca en teoria de grups, a la qual es dedica intensament a partir de l'any 1896. L'àlgebra lineal, que ha anat fent acte de presència en els seus treballs, li ocuparà els darrers anys de la seva vida.

Equacions diferencials. L'aportació més rellevant de Frobenius en el camp de les equacions diferencials és el mètode que avui porta el seu nom per a la resolució de les equacions diferencials lineals, presentat l'any 1873 en el seu treball [132]. El mètode consisteix a escriure les solucions com a sèries de potències de coeficients indeterminats i, per substitució de les sèries en les equacions diferencials, deduir recurrències que permetin determinar-ne els coeficients. El treball de Frobenius és acurat, atès que inclou la discussió de la convergència uniforme de les sèries proposades com a solució. Es pot trobar una descripció del mètode en llenguatge actual en [170].

Funcions el·líptiques. El resultat més conegut de Frobenius en l'àmbit de les funcions el·líptiques és el que avui coneixem com a fórmula determinantal de Frobenius i Stickelberger, [155], que involucra les funcions $\wp$ i σ de Weierstrass, definides a la secció 2.5. La fórmula s'aplica en l'estudi de diversos problemes físics i matemàtics; és clau, per exemple, en la prova de la integrabilitat completa del sistema el·líptic Calogero i Moser [240]. Recentment, ha estat generalitzada per a funcions hiperel·líptiques i en altres contextos ([292], [293], [115]).

Funcions theta. De manera natural, l'interès de Frobenius per les funcions el·líptiques evolucionà cap a les funcions theta. Durant el quinquenni 1880–1885, publicà vuit articles sobre aquest tema, que, en aquell moment, després dels treballs de Riemann, era de gran actualitat. En aquests articles trobem l'estudi del comportament per isogènies de les funcions theta ([136], [138]) i l'estudi sistemàtic de les thetacaracterístiques, que el portaren a introduir els *sistemes fonamentals de thetacaracterístiques* ([137], [139]). Els resultats principals, però, aparegueren en els darrers treballs del quinquenni. Per bé que Riemann ja coneixia les relacions entre els períodes de les integrals abelianes (cf. [352, p. 242]), Frobenius ([140], [141], [142]) demostrà que aquestes relacions són condicions necessàries i suficients per a la convergència de les sèries theta. En el llenguatge actual, Frobenius proporciona les condicions que ha de satisfer un tor complex per a admetre una estructura de varietat algebraica projectiva. Malauradament, sovint s'atribueixen aquestes condicions només a Riemann. Finalment, el treball [143], una traducció del qual s'inclou en aquesta antologia, se centra en les identitats satisfetes per les funcions theta i les seves derivades. Els resultats obtinguts tindran transcendència històrica; els descriurem amb més detall a la secció 10.1.

Equacions en derivades parcials. L'any 1877, Frobenius publicà l'article [133], que suposà un punt d'inflexió en la seva carrera. El treball recull les seves aportacions a les equacions en derivades parcials i la seva influència és palesa en els treballs seminals d'Élie Cartan sobre el càlcul exterior. Però, sobretot, marcà l'inici de les recerques de Frobenius en el camp de l'àlgebra lineal, una disciplina que, amb el seu impuls, adquiriria carta de natura pròpia.

Atès que una anàlisi històrica d'aquest article ja es troba en [196], aquí ens limitarem a fer-ne un resum breu.

El problema de Pfaff s'origina en la teoria d'equacions en derivades parcials de primer ordre que s'estableix a partir dels treballs de Lagrange. El mateix Lagrange resolgué el cas lineal, però només pogué resoldre el cas general per a funcions de dues variables. Pfaff interpretà el problema en termes de formes diferencials: traduí la resolució d'una equació en derivades parcials en la *integració* d'una forma diferencial:

$$\omega = a_1(x)dx_1 + \cdots + a_n(x)dx_n = 0;$$

és a dir, en l'obtenció de les varietats sobre les quals la forma ω és idènticament nul·la. La generalització d'aquest problema es coneix actualment com el problema de Pfaff: donat un conjunt de formes diferencials en una varietat diferenciable, cal determinar totes les subvarietats sobre les quals les formes en qüestió són idènticament nul·les. Aquesta idea de Pfaff establí un pont ferm entre la teoria d'equacions en derivades parcials i la geometria diferencial, lligam que ha estat molt beneficiós per a ambdues.

En els temps de Frobenius, l'interès pel problema de Pfaff se centrava en la determinació de la dimensió màxima de les subvarietats solució. Jacobi i Clebsch havien treballat a bastament en el problema i havien establert condicions d'integrabilitat per a sistemes d'equacions pfaffianes, però fou Frobenius qui establí rigorosament les condicions. L'article de Frobenius conté una part significativa dedicada exclusivament a les formes lineals, en la qual prova, entre altres coses, que el rang de qualsevol matriu antisimètrica és parell, i on estableix la classificació de certes formes

bilineals alternades. Aquests resultats inspiren la segona part del treball, de caire analític, en la qual, per generalització dels resultats de Clebsch, estableix la classificació dels sistemes pfaffians i el criteri d'integrabilitat completa que avui porta el seu nom. Aquest criteri s'aplica a sistemes lineals homogenis d'equacions en derivades parcials de primer ordre, per a establir-ne l'existència de solucions de dimensió màxima. Val a dir, però, que el resultat és, bàsicament, una versió dual d'un resultat previ de Jacobi i Clebsch, i que la demostració que en fa Frobenius és, en les seves pròpies paraules, una versió més algebraica i simètrica d'una demostració deguda a Deahna [68]. Fou Cartan qui atribuï el resultat únicament a Frobenius en el seu llibre sobre invariants integrals [53].

Àlgebra lineal. L'àlgebra lineal és un exemple magnífic de com un llenguatge escaient pot alterar la natura pròpia d'una disciplina. L'àlgebra lineal començà a adquirir protagonisme com a eina matemàtica a principis del segle XIX. En aquest període, Cauchy i Jacobi desenvoluparen extensivament l'ús dels determinants. Si bé els sistemes d'equacions lineals i les formes bilineals ja copsaven l'atenció dels matemàtics, els conceptes propis de l'àlgebra matricial o dels espais vectorials encara no s'havien formalitzat. Els determinants s'estudiaven sovint amb tècniques analítiques; per exemple, mitjançant desenvolupaments en sèrie.

Kronecker i Weierstrass, des de Berlín, foren els precursors del desenvolupament d'aquesta disciplina. La teoria de Weierstrass dels divisors elementals per a la classificació de formes bilineals, basada en la teoria de determinants, també suposà un canvi d'estil en la manera de fer mate-

màtiques: des d'aleshores, l'estudi rigorós i sistemàtic esdevindria imprescindible. Frobenius fou un dels primers seguidors, i un dels més importants, d'aquest nou corrent.

La idea de treballar en abstracte amb les matrius, tot prescindint de la seva relació amb els sistemes d'equacions o amb les formes lineals, es desenvolupà durant la segona meitat del segle XIX a Anglaterra, França i Alemanya, gràcies a Cayley [56], Laguerre [252] i Frobenius [134]. En un moment en el qual la comunicació científica no tenia ni de bon tros la immediatesa actual, es fa difícil atribuir amb certesa l'autoria d'alguns resultats, però la importància de Frobenius en el desenvolupament de la disciplina no admet cap dubte: a més d'aportar el rigor en la presentació i en la demostració dels resultats, a ell es deu l'aplicació de l'àlgebra matricial a la resolució de problemes en camps diversos. Aquest fet fou un pas definitiu per a la consolidació de l'àlgebra lineal com a disciplina matemàtica.

En el seu treball de 1858, Cayley mostrà com operar amb matrius i les denotà per mitjà d'un únic símbol, tractant-les com a variables; aquesta notació innovadora en canviaria la percepció. El mateix Cayley féu palesa l'analogia de les matrius amb les quantitats algebraïques ordinàries [56]. En particular, Cayley plantejà la possibilitat de considerar funcions algebraïques matricials. En aquesta línia, Cayley es proposà provar que qualsevol polinomi en una indeterminada matricial pot ésser reduït a un polinomi de grau menor que la dimensió de la matriu. D'aquesta manera arribà a la formulació de l'anomenat teorema de Cayley–Hamilton. Cayley el comprovà per a les dimensions 2 i 3, però considerà innecessària la seva demostració

en el cas general. Fou Frobenius qui en donà la primera prova vint anys més tard.

Després que Frobenius ja havia començat a aplicar l'àlgebra lineal en el seu treball sobre el problema de Pfaff, s'ocupà d'un problema plantejat per Hermite: la determinació de les matrius que deixen invariant una forma quadràtica. Aquest fou l'origen del treball *Sobre les substitucions lineals i les formes bilineals* (*Über lineare Substitutionen und bilineare Formen*) [134]. S'hi introdueixen formalment els conceptes de matrius similars i de matrius còngrues; a saber, dues matrius A , B són similars si existeix una matriu invertible P tal que $B = P^{-1}AP$, i són còngrues si existeix una matriu invertible P tal que $B = P^tAP$. Frobenius demostrà que si dues matrius simètriques són similars, aleshores es pot trobar una matriu de canvi P que sigui ortogonal; és a dir, per a la qual se satisfaci la igualtat $P^{-1} = P^t$. Això el portà a l'estudi de les matrius ortogonals reals, per a les quals demostrà que els seus valors propis són nombres complexos de mòdul 1. Però, sens dubte, l'aportació més valuosa de l'article és la definició del polinomi mínim d'una matriu i l'enunciat i la demostració rigorosos de l'anomenat avui, potser injustament, teorema de Cayley–Hamilton. També s'hi fa palesa la relació entre els polinomis mínim i característic d'una matriu. En el treball ja s'apliquen aquests avenços; per exemple, en la determinació de les matrius que commuten amb una matriu donada, la qual cosa revisa i estén resultats de Cayley. La darrera perla del treball és la demostració que les úniques àlgebres de divisió sobre el cos dels nombres reals són, a més del propi cos real, el cos dels nombres complexos i el cos —no commutatiu— dels quaternions de Hamilton, que hi apareix representat, per primera vegada, com a àlgebra

de matrius 2×2 . Aquest treball pioner dóna una idea del potencial de Frobenius i de les eines que proposà, però les seves aportacions a l'àlgebra lineal no s'acabaren pas aquí.

L'estudi dels sistemes d'equacions lineals era un tema candent a la segona meitat del segle XIX. El paper dels determinants era prou conegut, i les nocions d'independència lineal i de rang estaven a l'ambient, per bé que, encara, no prou fixades. Charles L. Dogson, a més de jugar amb l'Alícia, publicà l'any 1837 el *Tractat elemental sobre determinants* (*Elementary treatise on determinants*), en el qual s'apropà molt al resultat general. Però novament fou Frobenius qui, en lligar caps i endreçar la teoria, la deixà ordenada com la coneixem avui. En el treball [135] definí el concepte de rang d'una matriu mitjançant els menors, s'adonà de la dualitat entre equacions i solucions, i introduí la noció d'independència lineal, no només per a equacions, sinó també per a les n -ples que les representen. Això li permeté establir la relació entre el rang d'un sistema i la dimensió de l'espai de les seves solucions.

Malgrat tots aquests avenços, l'àlgebra matricial no fou acceptada plenament entre els matemàtics fins a principis del segle XX, en el moment en què aplicacions potents com ara la representació de grups, deguda novament a Frobenius, s'escamparen entre la comunitat matemàtica.

Després dels dos treballs esmentats, l'atenció de Frobenius es començà a centrar en l'estudi dels grups i entrà en un període que seria de gran transcendència per a la teoria de grups. Cap al final de la seva carrera, però, retornà a l'àlgebra lineal per a demostrar un altre resultat d'importància cabdal avui, el teorema de Perron i Frobenius.

Un capítol de l'àlgebra lineal important per les seves aplicacions l'ofereix la teoria de matrius positives. A més de les aplicacions estrictament matemàtiques, teoria de grafs, anàlisi numèrica, probabilitat, etcètera, aquesta teoria juga un paper decisiu en l'estudi de les cadenes de Markov, les quals apareixen recurrentment en economia, demografia o telecomunicacions, per exemple.

Sorprenentment, l'origen de la teoria de matrius positives es troba en un problema estrictament aritmètic. Jacobi [218] s'havia inspirat en les fraccions continuades per a descriure un algorisme per al càlcul del màxim comú divisor de més de dos nombres enters. L'algorisme origina certes fraccions continuades generalitzades periòdiques. Cap a finals del segle XIX, la convergència de les fraccions continuades generalitzades era un dels temes d'estudi a la Universitat de Munic. Perron [297] tingué l'encert d'introduir els determinants per a l'estudi de la convergència d'aquestes fraccions continuades. Aquests determinants són, bàsicament, els polinomis característics de certes matrius associades al problema. En alguns casos, les matrius són positives; és a dir, tots els seus elements són positius; i, en d'altres, no més són regulars; és a dir, una potència seva és positiva. Per a establir la convergència de les fraccions continuades, Perron provà que les matrius quadrades positives tenen un valor propi de mòdul màxim; aquest valor propi és real, positiu, de multiplicitat 1, i admet un vector propi positiu. També demostrà que una matriu no negativa regular satisfà la mateixa propietat. Malgrat la transcendència que havien de tenir aquests resultats, Perron no estigué del tot satisfet perquè no fou capaç de donar-ne una demostració purament algebraica. Aquest fet atragué l'atenció de Frobenius, que l'any 1908 ja en publicà una prova en aquesta

direcció [151]. Aquest fou l'inici del viatge que emprengué Frobenius en el camp de les matrius positives. El viatge culminà l'any 1912 en el treball [152]. Aquí ja considera matrius no negatives, introdueix el concepte de matriu irreductible i demostra el resultat de Perron per a matrius no negatives, irreductibles, no necessàriament regulars.

Val a dir que la importància del teorema de Perron i Frobenius tardà a ésser reconeguda. Markov [270] tot just havia introduït les matrius estocàstiques l'any 1908 i encara haurien de passar vint anys més perquè aquestes adquirissin la rellevància que tenen actualment. Com ja s'ha esmentat, el teorema de Perron i Frobenius té un gran impacte en nombroses disciplines. Fins i tot en treu profit l'algoritme de cerca emprat per Google (cf. [163]).

El teorema de Rouché-Frobenius (*que ni és únicament de Frobenius, ni de Rouché*). Malgrat que en l'àmbit científic Frobenius potser no és un dels matemàtics de més anomenada, probablement és un dels més coneguts entre l'estudiantat d'àlgebra lineal, gràcies al teorema de Rouché-Frobenius sobre la resolubilitat dels sistemes d'equacions lineals. Però Frobenius no és pas el descobridor d'aquest teorema. En el treball [150], ell mateix afirma:

Les condicions per a la resolubilitat d'un sistema no homogeni d'equacions lineals foren publicades primer per Fontené (Théorème pour la discussion d'un système de n equations du premier degré à n inconnues, Nouv. Ann. (2) volume 14, 1875) i per Rouché (Sur la discussion des équations du premier degré. Comptes Rendus, volum 81, 1875), poc abans que jo (Über

das Pfaffsche Problem. Aquesta revista, volum 92, al final de §3, 1876).

Frobenius

Si hem de fer cas a Frobenius, sembla que fou Fontené el primer a demostrar el teorema, per bé que el primer a publicar-lo fou Rouché. L'aportació de Frobenius consistí a presentar-lo d'una forma més senzilla, gràcies al concepte de rang que ell mateix havia introduït [135]. Qui atribueix el teorema a Frobenius és Rey Pastor, i a través d'ell la comunitat matemàtica iberoamericana passà a identificar el resultat com a teorema de Rouché-Frobenius. Però el teorema s'associa a altres noms en altres parts del món: el més habitual és l'atribució a Rouché-Capelli, però a França l'atribució és a Rouché-Fontené, i en els països d'influència soviètica es batejà com a teorema de Kronecker-Capelli, la qual cosa provocà un “canvi de nom” a Cuba!

Teoria de nombres. Entre els objectes matemàtics que porten el nom de Frobenius, segurament el més conegut és l'automorfisme de Frobenius. El seu origen és estrictament aritmètic, per bé que ha inspirat generalitzacions diverses, especialment en el camp de la geometria. Més enllà de l'anècdota, els treballs de Frobenius en l'àmbit de la teoria de nombres constitueixen una etapa important en el camí cap al seu descobriment de les representacions de grups. De fet, Frobenius atribueix el seu interès per la teoria de grups a Kronecker. El seu segon treball sobre grups [145] comença amb la declaració següent:

Vaig ésser atret cap a les investigacions en la teoria dels grups, que formen el contingut d'aquest treball, a través de l'estudi del remarcable

tractat de Herrn Kronecker Sobre la irreductibilitat de les equacions (Über die Irreductibilität von Gleichungen, Monatsber. Berl. Akad. 1880, p. 155), particularment per l'intent de trobar les relacions indicades al final de la pàgina 157.

Frobenius

El treball mencionat de Kronecker estudia un problema aparentment innocent: donat un polinomi $F(x)$ de coeficients enters es tracta d'estudiar la factorització de $F(x)$ mòdul diferents nombres primers p . Per exemple, Kronecker prova que, denotant per ν_p el nombre de solucions de la congruència $F(x) \equiv 0 \pmod{p}$, es té la relació asimptòtica:

$$\sum_p \frac{\nu_p}{p^s} \sim r \log \frac{1}{s-1},$$

on r és el nombre de factors irreductibles de $F(x)$. Com a conseqüència d'aquest resultat, es demostra fàcilment que si K és un cos de nombres galoisià, la proporció de primers p que descomponen completament en K és $1/[K : \mathbb{Q}]$. A partir d'aquí, Kronecker estudia la proporció de primers per als quals un polinomi enter té un nombre fixat d'arrels mòdul p , però no pot provar l'existència d'aquestes densitats. És Frobenius qui completa i estén el treball de Kronecker.

Els resultats de Frobenius aparegueren l'any 1896 en l'article [147], per bé que s'havien obtingut molt abans. Això féu que alguns autors atribuïssin el descobriment de l'automorfisme de Frobenius a Dedekind, en basar-se en una carta del 8 de juny de 1882 en què Frobenius havia

exposat a Dedekind els seus avenços. Tal com ell mateix explica a la introducció de l'article:

Vaig escriure el treball següent el mes de novembre de 1880 i vaig comunicar els resultats que s'hi desenvolupen als meus amics STICKELBERGER i DEDEKIND. Les seves bases estan estretament relacionades amb les lleis segons les quals els primers racionals descomponen en factors ideals primers en un cos algebraic i, especialment, en un de normal. Per uns comentaris en els treballs de DEDEKIND, vaig haver d'assumir que ell s'havia ocupat molt de temps en la recerca d'aquestes lleis i, de fet, a demanda meua, el 8 de juny de 1882 em va enviar l'esquelet d'aquesta teoria, que ell ha publicat el 10 de setembre de 1894 en el Göttinger Nachrichten amb el títol Sobre la teoria d'ideals (Zur Theorie der Ideale). Jo sempre havia desitjat que aquest resum aparegués abans que el meu propi treball, i aquesta és la raó per la qual no m'he decidit fins ara sobre la seva publicació.

Frobenius

La contribució de més transcendència d'aquest treball és la definició de l'automorfisme anomenat de Frobenius. Juntament amb l'article de Kronecker esmentat, el treball també inicia el camí cap a les sèries d'Artin, una eina molt potent de la teoria de cossos de classes.

El grup de Galois d'un polinomi està format per les permutacions de les seves arrels que respecten els lligams algebraics que hi ha entre elles. Situem-nos en el cos K

generat per les arrels d'un polinomi mònic i irreductible $F(x)$, de coeficients enters; d'aquesta manera, els elements del grup de Galois de $F(x)$ s'interpreten com els automorfismes de K que deixen invariants els nombres racionals. Frobenius demostra que per a cada ideal primer $\mathfrak{p}$ de l'anell d'enters $\mathcal{O}_K$ de K que divideix un nombre primer p coprimer amb el discriminant de $F(x)$, existeix un element $\sigma_{\mathfrak{p}}$ del grup de Galois per al qual se satisfà que

$$\sigma_{\mathfrak{p}}(x) \equiv x^p \pmod{\mathfrak{p}}, \text{ per a tot } x \in \mathcal{O}_K.$$

Aquest element s'anomena l'automorfisme de Frobenius associat a $\mathfrak{p}$. Frobenius s'adona que si canviem l'ideal primer $\mathfrak{p}$ per un altre ideal primer $\mathfrak{p}'$ que també divideix p , l'automorfisme $\sigma_{\mathfrak{p}'}$ és conjugat de $\sigma_{\mathfrak{p}}$. D'aquesta manera, Frobenius associa a cada nombre primer p una classe de conjugació en el grup de Galois del polinomi. D'altra banda, cada element $\sigma_{\mathfrak{p}}$ ha de permutar les solucions de la congruència $F(x) \equiv 0 \pmod{p}$ en $\mathcal{O}_K/\mathfrak{p}$ i, en mirar-les així, $\sigma_{\mathfrak{p}}$ s'expressa com un producte de cicles disjunts. El punt clau que permet resoldre el problema plantejat per Kronecker és la coincidència entre les longituds dels cicles disjunts en què descompon $\sigma_{\mathfrak{p}}$ i els graus dels factors irreductibles de la descomposició de $F(x)$ mòdul p .

Un cop establert aquest lligam, Frobenius determina la proporció dels primers que donen lloc, via aquesta relació, a certs conjunts de classes de conjugació (els que contenen la classe de l'automorfisme de Frobenius i les de les seves potències), i conjectura quina ha d'ésser la proporció de primers als quals correspon, via l'automorfisme de Frobenius, una classe de conjugació donada. Aquesta conjectura es coneix avui dia com a teorema de densitat de Txebot-

rev, ja que fou aquest matemàtic ucraïnès qui la demostrà vint-i-cinc anys més tard ([58], [59]).

Teoria de grups. La consolidació del concepte de grup abstracte tingué lloc durant la segona meitat del segle XIX. Fins aleshores, havia fet acte de presència implícita mitjançant transformacions geomètriques o bé permutacions, com ara les de les arrels dels polinomis. Els grups abeliàns apareixien implícitament, ja des de Gauss, en diverses construccions de la teoria de nombres, en els anomenats grups de classes. Tot i no disposar d'una definició formal del concepte de grup, ja se n'estudiaven les propietats i les aplicacions. Cauchy havia demostrat que si p^ν és la màxima potència d'un nombre primer p que divideix $n!$, aleshores el grup de totes les permutacions de n elements posseeix subgrups d'ordre p^ν . L'any 1872, Sylow emprà aquest resultat per a deduir que la mateixa afirmació és certa per a qualsevol grup finit d'ordre n múltiple de p ; aquest resultat s'anomena avui el primer teorema de Sylow. D'altra banda, el mateix any 1872, Klein presentava el seu programa d'Erlangen.

L'abstracció del concepte de grup fou un procés lent i dificultós, que implicà matemàtics d'altura, com Galois, Cauchy, Cayley, Kronecker, Jordan, von Dyck, Weber o Burnside. Els primers llibres sobre teoria de grups foren *Tractat de les substitucions* (*Traité des substitutions*) de Jordan (1870) i *Teoria de substitucions i la seva aplicació a l'àlgebra* (*Substitutionentheorie und Ihre Anwendungen auf die Algebra*) de Netto (1882). Fins aleshores, el terme grup de substitucions es referia, bàsicament, als grups de permutacions. Caldria esperar al *Tractat d'àlgebra* (*Lehrbuch der Algebra*) de Weber ([390]) per a trobar l'estructura

algebraica abstracta de grup en un llibre. Hölder inicià la tradició d'escriure treballs en teoria de grups en què l'anàlisi de les propietats es presenta per mitjà de casuístiques extensíssimes, o sigui, cas per cas. Això comportava que, sovint, s'oblidés algun cas i, a vegades, se'n consideressin de més. Per exemple, el mateix Cayley [57] presentà una llista de *tres* grups d'ordre 6.

Cayley, a partir dels treballs de Galois, intentà abstréure l'estructura dels grups de permutacions, i establí formalment algunes de les propietats elementals dels grups. Kronecker, inspirant-se en la composició de formes quadràtiques de Gauss i en la teoria dels ideals de Kummer, introduí els grups abelians finits en abstracte, i arribà a provar-ne el teorema d'estructura.

En [154], Frobenius i Stickelberger treballen amb enters modulars sense utilitzar les propietats especials d'aquests elements i donen una definició primitiva de grup. En aquest treball apareix una prova del teorema de classificació dels grups abelians finitament generats. Cinc anys més tard, en [144], Frobenius donà una demostració per a grups finits dels resultats després anomenats teoremes de Sylow. Aquesta demostració, que és bàsicament la que inclouen els textos actuals, fa un ús molt acurat de les classes de conjugació. En aquest treball, Frobenius inclou els axiomes de l'estructura de grup (finit), atribuint-los a Kronecker i Weber. L'estudi sistemàtic de les classes de conjugació serà clau per a les seves recerques posteriors en teoria de nombres i, especialment, per al naixement de les representacions lineals dels grups finits.

El segon article de Frobenius sobre teoria de grups [145] conté les bases teòriques que li permetran endinsar-se en

la teoria de nombres. Se centra en l'estudi de les classes laterals dobles, introduïdes en certs casos particulars per Cauchy i Sylow. Frobenius les defineix en general i les usa per a donar una nova demostració del segon teorema de Sylow. El treball conté també la fórmula de les òrbites, resultat també anomenat lema de Burnside, usat a bastament en combinatòria. En realitat, el propi Burnside atribueix el resultat a Frobenius, però sembla que Cauchy, cap a l'any 1845, ja en tenia una idea més o menys clara en un cas particular. Actualment, el resultat també s'anomena lema de Cauchy i Frobenius o fórmula de Cauchy-Frobenius-Burnside.

Representació de grups. Una representació lineal (de dimensió finita) d'un grup és una aplicació que assigna una transformació lineal (matriu) a cada element del grup, de manera que aquestes transformacions satisfan les relacions algebraïques dels elements del grup dels quals provenen. Les representacions ens permeten interpretar els grups geomètricament, com a grups de transformacions d'espais vectorials. La interpretació per transformacions lineals és més interessant que la donada per matrius, atès que és independent de qualsevol referència de l'espai vectorial, i ens fa adonar, d'entrada, que cal mirar les representacions llevat de conjugació (canvi de base). En particular, els invariants habituals dels automorfismes dels espais vectorials es poden associar a les representacions de grups. Per exemple, podem considerar l'aplicació que a cada element d'un grup li assigna la traça de la matriu que li correspon en una representació matricial. Les aplicacions construïdes així s'anomenen caràcters i són una eina bàsica per a l'estudi dels grups. Tal com els hem presentat, sembla difícil imaginar que aquests conceptes no apareguessin de manera natural a

l'entorn del concepte de grup. Res més enllà de la realitat. Tots dos conceptes són deguts a Frobenius, però cal cercar el seu origen en els determinants dels grups, estudiats a bastament per Dedekind. Sorprenentment, Frobenius es trobà abans amb els caràcters (com Gauss ho féu en el seu moment en l'estudi del gènere de les formes quadràtiques binàries); les representacions aparegueren més tard.

Cal situar el naixement de la teoria de les representacions de grups l'abril de 1896, en la correspondència entre Dedekind i Frobenius. Les cartes, que es trobaren l'any 1968 per un caprici del destí, es conserven a la Universitat de Brunsvic (cf. <http://faculty.evansville.edu/ck6/bstud/dedek.html>).

En les seves recerques sobre bases normals de cossos de nombres galoisians, Dedekind es trobà amb un objecte sorprenent: els determinants de grups. Els determinants circulants, obtinguts per permutacions cícliques dels elements de la primera fila, eren ben coneguts a l'època, i Dedekind veié la possibilitat de generalitzar-los a permutacions associades a grups abelians. Dedekind definí el determinant d'un grup G de la forma següent: es pren un conjunt de $\#G$ indeterminades $\{X_g\}_{g \in G}$ indexades pels elements del grup, i es forma la matriu $(X_{gh^{-1}})_{g,h}$; per definició, el seu determinant és el determinant del grup G , $\det(G)$. En un apèndix a la seva tercera edició de les *Lliçons sobre teoria de nombres* (*Vorlesungen über Zahlentheorie*) de Dirichlet–Dedekind [107], Dedekind ja havia definit els caràcters irreductibles dels grups abelians com a homomorfismes del grup en el grup multiplicatiu dels nombres complexos no nuls i no tingué cap dificultat a aplicar les tècniques dels circulants per a obtenir la factorització del determinant

d'un grup abelià:

$$\det(G) = \prod_{\chi} \left(\sum_{g \in G} \chi(g) X_g \right),$$

en la qual χ recorre tots els caràcters del grup. Dedekind es plantejà trobar un resultat anàleg per al determinant dels grups no abelians. En els primers exemples que calculà, els determinants del grup simètric d'ordre 6 i del grup dels quaternions d'ordre 8, es trobà amb la sorpresa desagradable que el determinant té factors irreductibles no lineals. Dedekind cregué (com, més endavant, faria Dirac en un altre context) que la descomposició en factors lineals podria tenir lloc en algun sistema de nombres hipercomplexos, que és com es coneixien en aquell moment les $\mathbb{R}$ -àlgebres associatives. Però l'enfocament no fou encertat. El 25 de març de 1896 escriví una primera carta a Frobenius plantejant-li el problema. El problema despertà un gran interès en Frobenius; per bé que no havia sentit a parlar dels determinants dels grups, estava ben preparat per a assumir el repte: ja havia treballat amb grups abstractes i havia adquirit un domini important dels determinants en els seus treballs sobre funcions theta. En una segona carta, del 6 d'abril, Dedekind exposà a Frobenius els exemples que havia calculat i alguns resultats parcials sobre la possible factorització del determinant dels grups no abelians. Frobenius adoptà un enfocament diferent al de Dedekind: cercà directament els factors complexos irreductibles. Els dies 6, 12 i 17 d'abril, Frobenius escriví tres cartes a Dedekind en les quals resolía el problema. Roma no s'havia fet en tres dies, però els caràcters dels grups foren construïts en tres setmanes. Els continguts d'aquestes cartes aparegueren el mateix any en els articles [146], [148] i [149]. El mèrit de

Frobenius és extraordinari perquè creà les eines que li convenien per a resoldre el problema: en llenguatge actual, la representació del centre de l'àlgebra de grup i la descomposició d'aquesta àlgebra com a producte d'àlgebres simples centrals, que llavors era desconeguda. També definí els caràcters irreductibles dels grups no abelians a partir dels valors propis de les representacions corresponents a les àlgebres simples, en provà les propietats bàsiques —incloses les relacions d'ortogonalitat—, i els utilitzà per a descriure la factorització del determinant d'un grup no abelià. Els treballs han estat analitzats acuradament en [66] i [62].

Fou només després d'aquest *tour de force* que Frobenius descobrí els treballs de Molien sobre l'estructura de les àlgebres associatives semisimples, treball que li permetria reconèixer els caràcters dels grups finits com a traces de matrius, i arribar a definir les seves representacions lineals tal com les coneixem avui. En els quatre anys següents, entre 1897 i 1901, desenvoluparia la teoria general de les representacions de grups, introduiria els caràcters induïts i el producte tensorial de caràcters, descriuria els caràcters dels grups simètrics i alternats i aplicaria la teoria de caràcters a l'estudi de l'estructura dels grups que avui coneixem com a grups de Frobenius. Aquests són els grups que actuen sobre un conjunt de manera que l'acció dels elements no trivials té, com a màxim, un punt fix. La història és certament capriciosa: els caràcters dels grups feren caure en l'oblit els determinants dels grups, però aquests se serviren una venjança ben freda un segle més tard. És ben conegut que grups no isomorfs poden tenir la mateixa taula de caràcters; per tant, els caràcters no *caracteritzen* el grup; en canvi, el determinant el *determina* unívocament (cf. [127]).

Altres contribucions. A les seves classes, Frobenius acostumava a plantejar el problema següent: donats n nombres enters positius coprimers, trobeu el major enter que no n'és combinació lineal positiva. Els enters solució s'anomenen justament nombres de Frobenius. Aquest problema d'aparença innocent ha perdurat al llarg dels anys. Si bé sembla que l'any 1882 Sylvester ja el sabia resoldre per a $n = 2$, el pas del temps ens ha fet veure que el problema general és difícil; de fet, és un problema NP (cf. [308]). I no és estrany, vistes les seves nombroses aplicacions: algoritmes d'ordenació, teoria d'autòmats, codis algebraics geomètrics, generació de vectors aleatoris, entre d'altres.

2.11 Sprague

Roland Percival Sprague (Unterliederbach, Hoechst, 11 de juliol de 1894; 1967)

Sprague és un descendent familiar per línia directa de Kummer. Kummer s'havia casat en primeres núpcies amb Ottilie Ernestine Mendelssohn, que era cosina de Rebecka Mendelssohn, germana de Felix Mendelssohn i esposa de Dirichlet. Una filla d'aquest matrimoni de Kummer, Marie Elisabeth Kummer, es convertí en Marie Elisabeth Schwarz en contreure matrimoni amb el matemàtic Karl Hermann Amandus Schwarz. Una de les seves filles, Ottilie Bertha Augusta Schwarz, fou la mare de Roland Percival Sprague. Així, doncs, la mare de Sprague era filla de Schwarz i néta (filla d'una filla) de Kummer.

Es té molt poca informació sobre la biografia de Sprague. Se sap, però, que llegí una tesi a la *Freie Universität*

Berlin, l'any 1950, sota la direcció d'Alexander Dinghas, titulada *Sobre la determinabilitat unívoca dels elements d'un conjunt finit per partició doble* (*Über die eindeutige Bestimmbarkeit der Elemente einer endlichen Menge durch zweifache Einteilung*).

Sprague s'havia dedicat inicialment a l'estudi de problemes de teoria additiva de nombres i, també, a la teoria de jocs combinatoris; en particular, a l'estudi d'aquells jocs que, com el nim, posseeixen una estratègia guanyadora. En aquest context, els seus resultats s'inclouen en l'anomenada teoria de Sprague i Grundy, que desenvoluparen, independentment, Sprague l'any 1936 i Grundy, l'any 1939.

Observem que la carrera de Sprague, vinculat a la Universitat de Berlín, es desenvolupa en el període de la Segona Guerra Mundial i pot reflectir-ne molt bé les conseqüències. Probablement fou un dels molts que pagaren un preu elevat per la seva ascendència jueva.

Capítol 3

L'escola de Göttingen

L'escola matemàtica de Göttingen compta amb la figura de Gauss, que fonamentà no solament el progrés científic de la institució sinó també el de la matemàtica dels segles posteriors. El desenvolupament de l'escola matemàtica de Göttingen pròpiament dita es pot considerar posterior al de l'escola matemàtica de Berlín. Si, com a dates límit per a aquesta, fixem els anys 1828 —any de l'arribada de Dirichlet a Berlín— i 1917 —any de la mort de Frobenius—, com a dates per al desenvolupament de l'escola matemàtica de Göttingen podem prendre el període comprès entre els anys posteriors a la mort de Gauss i els anys en què té lloc la Segona Guerra Mundial. En els primers anys, hi trobem també Dirichlet, com a successor de Gauss en la càtedra, i Riemann, com a successor de Dirichlet.

La matemàtica de Göttingen compta, a més de Gauss, amb Dirichlet, Riemann, Dedekind, Klein, Hilbert, Emmy Noether, i Hasse com a figures més rellevants. En els anys esmentats, es pot dir que els matemàtics de Göttingen con-

tribuïren d'una manera especial a forjar moltes actituds i maneres de procedir que han esdevingut naturals —o desitjables— en el desenvolupament de la nostra professió. Posaren èmfasi en la investigació i en la publicació dels resultats; concediren a la docència de l'alumnat dotat tota la seva importància. Les biblioteques foren fonamentals en la posada al dia dels coneixements de l'època. Eren matemàtics estudiosos i cultes. Establiren contactes sòlids amb físics i, fins i tot, promogueren els primers contactes amb el món industrial.

Però, valorat amb el tarannà d'avui, potser la característica més important de Göttingen fou que els seus membres saberen establir contactes enriquidors amb els matemàtics d'altres cultures. Així, investigadors i estudiants d'arreu viatjaren a Göttingen per a rebre els ensenyaments d'uns matemàtics que estaven dotats d'una innegable generositat. Foren matemàtics genials, amb una capacitat de treball increïble, i que no dubtaren en cap moment a compartir el seu saber amb qui ho desitgés. Una mesura objectiva d'aquestes afirmacions és constituïda pels avenços matemàtics que s'hi produïren —molts dels quals, trencadors amb un passat no gaire llunyà—, i per l'ingent nombre de tesis que s'hi defensaren.

Al voltant de l'any 1930, la quantitat de literatura matemàtica que es publicava anualment era de l'ordre de 5.000 documents. Aquest fet, juntament amb l'endarreriment que patia la revisió d'articles a l'*Anuari sobre els progressos de la Matemàtica*, editat per part de matemàtics de Berlín, produí que matemàtics de Göttingen, especialment Courant i Neugebauer, juntament amb l'editorial Springer, fundessin la revista *Full central per a la matemàtica*

i les seves fronteres (*Zentralblatt für Mathematik und ihre Grenzgebiete*), amb l'esperit de fer la revisió dels articles al cap de poques setmanes de la seva aparició. Neugebauer en fou l'editor en cap fins l'any 1938, en què, fugint del nazisme, emigrà als Estats Units. Allà, l'any 1940, hi fundaria la revista *Recensions mathématiques* (*Mathematical Reviews*); editada per la Societat Matemàtica Americana (*American Mathematical Society*), aquesta és actualment la revista de recensions matemàtiques més coneguda arreu del món.

Neugebauer és conegut com a historiador de la matemàtica i, especialment, per la seva contribució a l'estudi de les tauletes matemàtiques d'argila de la cultura babilònica; per exemple, pel seu estudi de la tauleta Plimpton 322, datada al voltant de l'any 1800 a. de la n. e., que conté quinze ternes pitagòriques.

Les dificultats en la revisió d'articles a partir de l'inici de la Segona Guerra Mundial foren la causa que, l'any 1940, els editors del *Jahrbuch über die Fortschritten der Mathematik* i els del *Zentralblatt für Mathematik und ihre Grenzgebiete* s'unissin amb l'Acadèmia prussiana de Ciències i l'editorial Springer per a fer una sola publicació per a la revisió d'articles, mantenint el nom *Zentralblatt für Mathematik und ihre Grenzgebiete*. Aquesta, encara s'edita actualment; d'altra banda, la Biblioteca estatal de la Universitat de Göttingen i la Universitat Tècnica de Berlín han creat la base de dades matemàtica ERAM (*Electronic Research Archive for Mathematics*), coneguda també amb el nom de *Jahrbuch Project*, de consulta lliure.

3.1 Riemann

Georg Friedrich Bernhard Riemann (Breselenz, Hannover, 17 de setembre de 1826; Selasca, Itàlia, 20 de juliol de 1866)

El pare de Riemann era un pastor luterà pobre que havia lluitat a les guerres napoleòniques. L'any 1842, Riemann pogué entrar al *Johanneum Gymnasium* de Lüneburg, i l'any 1846 començà a estudiar filologia i teologia; però aviat es decidí, amb el permís previ del seu pare, per la matemàtica. Entrà a la Universitat de Göttingen, on rebé les seves primeres lliçons de Gauss, sobre el mètode dels mínims quadrats, i de Stern. Cal dir que, en aquella època, Göttingen no tenia encara la solvència que adquiriria pocs anys després com a centre reconegut per a l'estudi de la matemàtica. Els estudis de matemàtica estaven sota la direcció de Stern i Ulrich; i, encara que Gauss hi exercia la docència, aquesta es limitava als cursos de nivell més elemental.

L'any 1847, Riemann marxà a la Universitat de Berlín, on estudià amb Steiner, Jacobi, Dirichlet i Eisenstein. Tot i que aprengué molt d'Eisenstein, fou influenciat molt poderosament per Dirichlet, de qui adoptà els mètodes de treball.

L'any 1849, Riemann tornà a Göttingen, on, l'any 1851, presentà una tesi dirigida per Gauss. Allà rebé influències de dos col·laboradors de Gauss: de Wilhelm Eduard Weber, en física, i de Listing, en física i topologia.

En la tesi, titulada *Fonaments per a una teoria general de funcions d'una variable complexa* (*Grundlagen für eine allgemeine Theorie der Functionen einer veränderli-*

chen complexen Grösse), Riemann desenvolupà una teoria de funcions de variable complexa i, en particular, introduí les anomenades avui superfícies de Riemann. Per tant, es pot dir que fou l'introduïdor dels mètodes topològics en l'estudi de la variable complexa en tant que proporcionà un tractament geomètric de les funcions analítiques i de les representacions conformes, la qual cosa permeté avançar en les investigacions prèvies de Gauss, de Cauchy i de Puiseux.

Per recomanació de Gauss, Riemann obtingué una plaça a Göttingen i començà a treballar en la tesi per a la seva habilitació sobre la representabilitat de funcions en sèries trigonomètriques; presentà la seva memòria i impartí la lliçó corresponent l'any 1854 amb el títol *Sobre les hipòtesis en què es basa la geometria* (*Über die Hypothesen welche der Geometrie zu Grunde liegen*). Aquesta lliçó posà les bases de les anomenades actualment varietats de Riemann. D'una banda, en ella hi ha la definició de tensor de curvatura; de l'altra, Riemann es demana per la dimensió del món real i per quina geometria el descriu.

L'any 1857, Riemann publicà una altra de les seves obres més reconegudes i, alhora, més qüestionades, l'article *Teoria de funcions Abelianes* (*Theorie der Abel'schen Functionen*), basat en un curs impartit l'any anterior a tres estudiants, un dels quals fou Dedekind. Atesa la seva rellevància, comentarem aquest article en la secció següent.

Riemann exercí també una notable influència en Betti, entre els anys 1858, en què Betti visità Göttingen, i 1863, en què Riemann visità Betti en el seu viatge a Itàlia.

L'any 1859, Riemann ocupà la càtedra de Göttingen que havia quedat lliure pel decés de Dirichlet. Pocs dies després, fou elegit membre de l'Acadèmia de Ciències de Berlín, a instàncies de Kummer, Borchardt i Weierstrass. Com a memòria d'ingrés, presentà el seu estudi *Sobre la quantitat de nombres primers per sota d'una quantitat donada* (*Über die Anzahl der Primzahlen unter einer gegebenen Grösse*), que tractem més avall. És en aquesta memòria on Riemann presentà el comentari sobre la situació dels zeros no trivials de la funció zeta, comentari que donaria lloc a l'anomenada hipòtesi de Riemann, un dels problemes encara oberts i del qual en depenen més resultats matemàtics.

En la darrera part de la seva vida, Riemann viatjà diverses vegades entre Göttingen i Itàlia, per motius de salut.

La seva obra fou editada per Weber i Dedekind, i impresa a Leipzig per Teubner, l'any 1892, en un sol volum.

L'obra matemàtica de Riemann no és gaire extensa, però ofereix un exemple paradigmàtic de producció altament impactant. Els seus articles serviren per a consolidar l'ús de les funcions de variable complexa —que trobem incipient en Gauss— i exerciren una influència notable en el desenvolupament posterior de l'anàlisi, la topologia, la teoria d'invariants, la geometria algebraica, la geometria diferencial, la teoria de nombres i, fins i tot, la teoria de la relativitat. En molt pocs anys —atès que morí quan en comptava 39—, Riemann fou capaç de precisar el concepte d'integral, de forjar el concepte de superfície de Riemann, de matrius de períodes, de funcions theta en gènere superior, de treballar amb equacions diferencials de variable complexa, de generalitzar les sèries hipergeomètriques,

d'unificar les geometries de l'època dins del context del que s'anomenarien les geometries riemannianes, i de copsar la importància de la funció zeta per a l'estudi dels nombres primers —en la que seria la seva única publicació dedicada expressament a la teoria de nombres.

3.2 Funcions abelianes

L'article de Riemann [320] sobre funcions abelianes, publicat en el número 54 de la *Revista de Crelle*, l'any 1857, anava precedit en el mateix número de la revista per tres articles breus del mateix Riemann (a vegades se citen tots quatre com un sol article). En aquesta terna preliminar, Riemann fixa els conceptes bàsics que emprarà en l'article general, molts dels quals es troben ja en la seva tesi [316], de l'any 1851.

En el primer article [317], Riemann precisa que treballarà amb funcions analítiques d'una variable complexa definides en regions del pla; Riemann no empra, però, ni els termes analític, ni holomorf. Es limita a dir que considera funcions w de $x + iy$, contínues a l'entorn d'un cert punt a , i que satisfan l'equació diferencial

$$i \frac{\partial w}{\partial x} = \frac{\partial w}{\partial y},$$

la qual, com sabem, proporciona les avui conegudes com a relacions de Cauchy-Riemann. Per integració d'aquesta equació diferencial, dedueix el desenvolupament de la funció w en sèrie de potències de $z - a$, la seva determinació unívoca a partir dels valors que pren sobre un segment petit

qualsevol que parteixi del punt a , i explica com es fa la prolongació analítica de la funció fins a trobar una singularitat. Per prolongació analítica distingeix entre funcions univaluades i funcions multivaluades, les quals presenten una línia de discontinuïtat, com és el cas de la funció $\log(z - a)$, que difereix en $2\pi i$ al llarg de qualsevol línia que parteixi de a segons que aquesta es recorri en sentit positiu o negatiu. En honor de Gauss que fixà el sentit de $+i$, diu, Riemann considera positiu el recorregut en la direcció de $+i$ a 1. En general, Riemann treballa únicament amb funcions que presenten com a punts singulars pols o bé singularitats logarítmiques, i situats en posició general. També considera punts de ramificació a , d'ordre finit, a l'entorn dels quals les funcions són desenvolupables en sèries de potències de $(z - a)^{\frac{m}{n}}$.

En el segon article [318], Riemann introdueix el concepte de superfície $(2p+1)$ -múltiplement connexa. Es tracta de superfícies T que es transformen en superfícies T' simplement connexes després de fer-hi $2p$ talls escaients; en aquestes, qualsevol corba tancada divideix la superfície necessàriament en dues parts. El seu estudi, diu, és independent de mesures i forma part de l'*analysis situs*. Alhora, pensa T com un recobriment ramificat del pla complex unió amb el punt de l'infinit; és a dir, de l'esfera de Riemann. Aquesta interpretació de les superfícies li serà especialment útil per al tractament de les funcions multivaluades, atès que li proporcionaran branques univaluades en cada full de la superfície. Riemann acompanya l'article d'unes il·lustracions molt útils, que reproduïm a les pàgines següents, perquè posen de manifest la senzillesa del seu raonament.

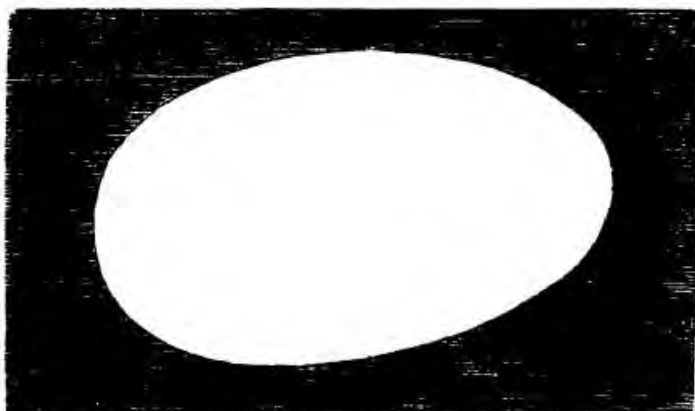


Figura 1. Superfícies simplement connexes

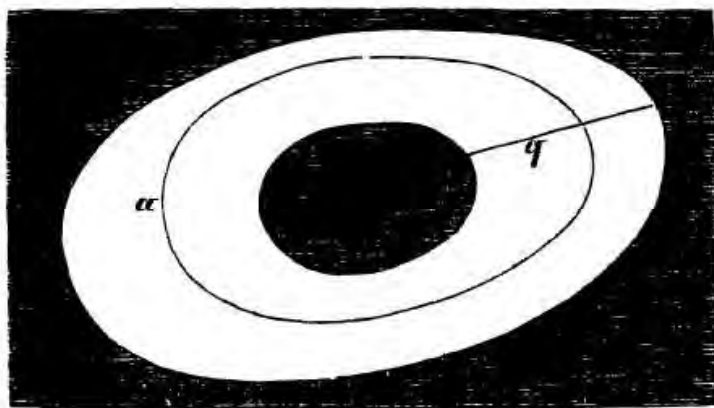


Figura 2. Superfícies 2-múltiplement connexes

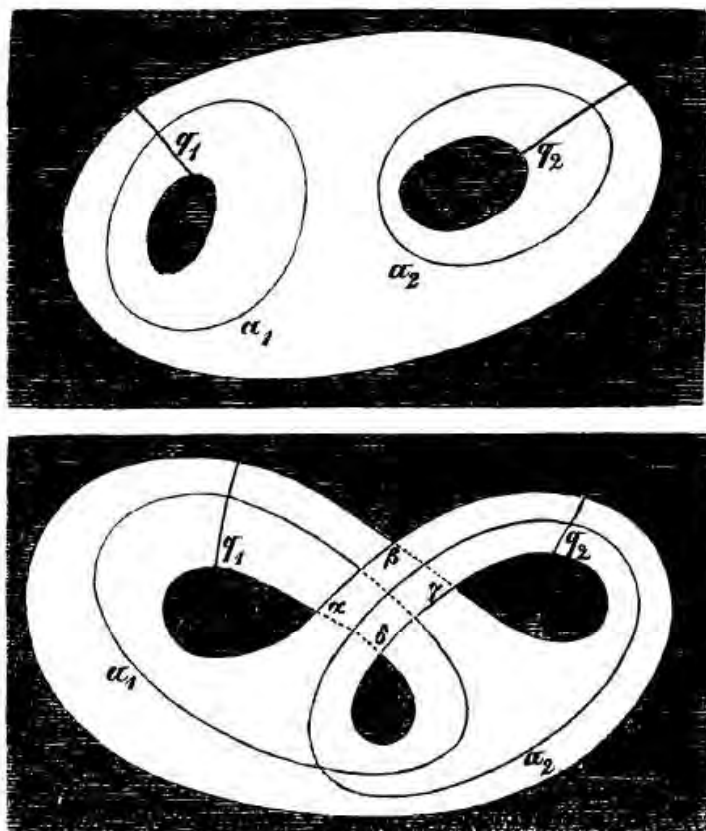


Figura 3. Superfícies 3-múltiplement connexes

En el tercer article [319], Riemann exposa la seva versió del principi de Dirichlet, una tècnica que, originada per problemes de la física, provenia de la teoria del potencial i del càlcul de variacions. Es tracta de provar l'existència de funcions que, amb valors prèviament donats a la frontera d'un domini, minimitzen un cert funcional al seu interior. El nom de principi de Dirichlet és degut a Riemann. Com ell mateix explica, respon a un tipus de raonament

que havia estat emprat per Dirichlet, en la resolució d'una equació de Laplace, $\Delta f = 0$, i per Gauss, en les seves lliçons sobre mínims quadrats impartides al llarg de molts anys a Göttingen. Riemann, però, ha de modificar el procedir d'aquests dos matemàtics en tant que ell necessita poder construir funcions amb tipus específics de discontinuïtats en els talls de les superfícies. L'ús d'aquest principi per part de Riemann —que és constant al llarg de tota la memòria— i la justificació que en fa suscitar en els anys següents una allau de crítiques aferrissades (cf., per exemple, [275]).

A la memòria principal [320], Riemann parteix d'una superfície sense vora T , $(2p + 1)$ -múltiplement connexa, en la qual considera donades p funcions

$$w_\pi, \quad 1 \leq \pi \leq p,$$

univaluades, finites, i contínues en T' , de les quals suposa que als dos costats dels p talls difereixen cadascuna en unes quantitats constants. Les funcions són anomenades integrals de primera espècie, i les constants, mòduls de periodicitat. Demostra que aquests poden ésser modificats de manera que les p funcions siguin linealment independents.

Tot seguit considera integrals de segona espècie i integrals de tercera espècie. Les integrals de segona espècie són com les de primera, llevat que esdevenen infinites, amb un pol simple, en un punt ε de T . Representa per $t^0(\varepsilon)$ una integral qualsevol de segona espècie. Les integrals de tercera espècie, $\tilde{\omega}(\varepsilon_1, \varepsilon_2)$, presenten singularitats logarítmiques en dos punts arbitraris ε_i de T .

A continuació, Riemann escull m punts ε_i en T , i es preocupa per l'existència de funcions definides en T amb,

com a màxim, pols simples en els punts triats. La forma més general d'aquestes funcions és

$$s = \beta_1 t_1 + \beta_2 t_2 + \cdots + \beta_m t_m + \alpha_1 w_1 + \alpha_2 w_2 + \cdots + \alpha_p w_p + \text{const.}$$

L'expressió que en resulta és una funció que depèn de $p + m + 1$ constants. Així, en principi, els mòduls de periodicitat que intervenen en l'expressió de s passen a dependre de $p + m + 1$ constants. En considerar els $2p$ talls i imposar que els mòduls hi siguin nuls, a fi que la funció s sigui univaluada arreu, Riemann es troba amb un sistema homogeni de $2p$ equacions lineals i $p + m + 1$ incògnites. Per tant, hi haurà funcions no constants com les que desitja sempre que

$$p + m + 1 - 2p \geq 2;$$

és a dir, sempre que sigui $m > p$. Aquesta desigualtat esdevindria coneguda com a desigualtat de Riemann.

Riemann demostra que, donada una funció s com la d'abans, existeix un polinomi irreductible $F(\sigma, z)$ tal que

$$F(s, z) = 0.$$

La notació expressa que el polinomi F és de grau n en s i de grau m en z . És a dir, la funció s és una funció algebraica de z . A més, se satisfà que

$$w + 2r = 2m(n - 1),$$

on r denota el nombre de punts de ramificació $(\gamma_\rho, \delta_\rho)$ per als quals

$$F = \frac{\partial F}{\partial s} = \frac{\partial^2 F}{\partial s^2} = 0, \quad \frac{\partial^2 F}{\partial z^2} \frac{\partial^2 F}{\partial s^2} - \left(\frac{\partial^2 F}{\partial s \partial z} \right)^2 \neq 0,$$

i w , el nombre de punts de ramificació per als quals

$$F = \frac{\partial F}{\partial s} = 0, \quad \frac{\partial F}{\partial z} \neq 0, \quad \frac{\partial^2 F}{\partial s^2} \neq 0.$$

Un càlcul de residus li permet deduir que

$$p = (n-1)(m-1) - r,$$

relació que donaria lloc a la fórmula de Riemann-Hurwitz.

A la memòria [48] de Brill i de Max Noether, de l'any 1894, es comenta que la igualtat anterior, en què una funció algebraica es veu representada com a suma de funcions transcendents, proporciona un dels trets característics de la teoria de Riemann; a saber, “invertir el sentit que fins aleshores anava del que és fàcil al que és difícil” —quelcom, afegim nosaltres, que únicament als genis sol donar bon resultat.

Riemann raona que les funcions w , que proporcionen les integrals de primera espècie, s'expressen en la forma

$$w = \int \frac{\varphi\left(\begin{smallmatrix} n-2 \\ s \end{smallmatrix}, \begin{smallmatrix} m-2 \\ z \end{smallmatrix}\right) \partial z}{\frac{\partial F}{\partial s}} = - \int \frac{\varphi\left(\begin{smallmatrix} n-2 \\ s \end{smallmatrix}, \begin{smallmatrix} m-2 \\ z \end{smallmatrix}\right) \partial s}{\frac{\partial F}{\partial z}},$$

on $\varphi(s, z)$ són funcions polinòmiques que s'anul·len en els r punts de ramificació $(\gamma_\rho, \delta_\rho)$ considerats abans. Un càlcul de constants li proporciona l'existència de les funcions φ , a partir de l'equació definidora F , i la independència lineal de p d'aquestes funcions. En la notació de Riemann, la integral s'estén al llarg d'un camí qualsevol contingut a T' , que parteix d'un punt fix, i la funció $w = w(x + iy)$ ho és de l'extrem superior. Comenta que es poden donar expressions semblants per a les integrals de segona espècie

i per a les de tercera, però que no ho detalla perquè ja ho farà per mitjà de funcions theta.

Per mitjà de combinacions lineals $\varphi^{(i)}$ de les funcions φ anteriors, demostra l'existència de funcions $\frac{\varphi^{(2)}}{\varphi^{(1)}}$ amb pols simples, com a màxim, en p punts de la superfície, i que totes les funcions amb aquesta propietat es poden escriure d'aquesta manera.

Riemann necessita, i demostra en el mateix treball, que dues funcions meromorfes qualssevol sobre la mateixa superfície són algebraicament dependents. Amb això, les superfícies de Riemann donen lloc a corbes algebraiques amb models plans, però Riemann no utilitza aquest llenguatge; es limita a treballar amb els polinomis esmentats, de dues indeterminades, $F(\sigma, z)$. Donat p , precisa quins són els graus mínims de F en σ i en z que li proporcionen el lligam entre les funcions corresponents i expressa el resultat en una taula com la següent:

p	(n, m)	r
1	$(2, 2)$	0
2	$(2, 3)$	0
$2\mu - 3$	(μ, μ)	$(\mu - 2)^2$
$2\mu - 2$	(μ, μ)	$(\mu - 1)(\mu - 3)$

Riemann passa a analitzar el comportament de les funcions per transformacions racionals de les variables. Conclou que, de fet, a T pot associar-li una classe biracional de funcions $F(s, z)$. Val la pena fer notar la importància històrica d'aquest punt de vista, en tant que canvia la consideració clàssica de les propietats d'una funció determinada per les d'una família de funcions i les relacions entre elles. Brill i M. Noether [48] remarquen que una classe de

funcions determinada per lligams biracionals esdevé així un “cos” (“*Körper*”) —i ho escriuen entre cometes. Ignorem si aquesta fou la situació que motivà el concepte matemàtic de cos; en tot cas, en el domini de l’aritmètica, la paraula cos de nombres (*Zahlenkörper*) no apareix fins a unes lliçons impartides per Dirichlet a Göttingen, l’any 1858; és a dir, un any després de la publicació d’aquest treball de Riemann.

La recerca d’invariants biracionals per als cossos de funcions motivaria una part important de l’estudi de la teoria d’invariants que tingué lloc en les dècades següents.

En una segona part de la memòria, Riemann generalitza en el seu context, és a dir, en una superfície $(2p + 1)$ -múltiplement connexa, els teoremes d’addició d’Abel i d’inversió de Jacobi, que són els que li proporcionen les funcions abelianes.

Per a tractar aquest darrer, introdueix la funció theta θ ,

$$\theta(v_1, v_2, \dots, v_p) = \left(\sum_{-\infty}^{+\infty} \right)^p e^{(\sum_1^p)^2 a_{\mu\mu'} \cdot m_\mu m_{\mu'} + 2 \sum_1^p v_\mu m_\mu},$$

on els sumatoris en els exponents són respecte de μ i μ' , i els sumatoris exteriors, de $m_1, m_2, \dots, m_p$. La funció θ s’avalua en p integrals algebraïques finites arreu i depèn de les matrius de períodes $(a_{\mu\mu'})$. Les matrius de períodes no són arbitràries, sinó que cal que satisfacin les relacions que avui coneixem com a relacions de Riemann, a fi que les sèries convergeixin. Riemann hi arriba per mitjà de la consideració de les actualment anomenades bases simplèctiques de l’homologia.

En la nostra notació, Riemann determina el comportament de la funció θ en $\mathbb{C}^p/\Lambda$, on Λ denota la xarxa generada pels mòduls de periodicitat de les integrals de primera espècie.

Per a les integrals de tercera espècie, obté expressions de la forma

$$\pi(\varepsilon_1, \varepsilon_2) = \frac{1}{p} (\log \theta(u_1^{(2)} - pu_1, \dots) - \log \theta(u_1^{(1)} - pu_1, \dots))$$

i, per a les de segona espècie,

$$t(\varepsilon_1) = \frac{1}{p} \frac{\partial \log \theta(u_1^{(2)} - pu_1, \dots)}{\partial z_1}.$$

En fer ús de l'aparellament d'intersecció en homologia, dedueix que la dimensió de l'espai de moduli de les superfícies de gènere p és $3p - 3$, si $p > 1$, i 1, altrament.

Deixa indicat que també es pot portar a terme la determinació del logaritme de les constants theta,

$$\log \theta(0, 0, \dots, 0),$$

en funció dels $3p - 3$ mòduls que determinen la superfície. L'any 1870, aquesta tasca seria empresa per Thomae en el cas particular en què $n = 2$, a l'article [382] del qual n'oferim una traducció.

Més endavant, en el llibre de Clebsch i Gordan *Teoria de funcions abelianes* (*Theorie der Abel'schen Functionen*), publicat l'any 1866 —amb el mateix títol que les memòries de Weierstrass [393] i de Riemann [320]—, la constant p passà a denominar-se el gènere de la superfície. Clebsch fou el successor de Riemann a la càtedra de Göttingen.

A fi de descriure amb més comoditat la contribució de Roch a la desigualtat de Riemann que hem explicat més amunt, emprarem una notació i una terminologia una mica més avançades. Donades una superfície de Riemann compacta i un divisor $D = \sum n_P P$ d'aquesta superfície, el conjunt de les funcions meromorfes definides sobre la superfície amb pols d'ordre, com a màxim, l'ordre dels pols de D i zeros d'ordre, com a mínim, l'ordre dels zeros de D , constitueix un espai vectorial complex $L(D)$ de dimensió finita $\ell(D)$. Les recerques de Riemann que hem esmentat proporcionen una fita inferior per a $\ell(D)$, en funció del gènere g ($= p$) de la superfície. El resultat de Riemann completat per Roch, l'any 1865, proporciona la igualtat

$$l(D) - l(K - D) = \deg(D) - g + 1,$$

on K denota el divisor canònic, definit per les diferencials regulars. A partir de l'any 1874, i després de treballs de Brill i de M. Noether, la igualtat anterior es conegué com a teorema de Riemann–Roch.

Diguem, de passada, que l'any 1861 i per consell de Möbius, Roch havia anat a estudiar a Göttingen, on assistí a les lliçons impartides per Weber i a les impartides per Riemann. L'any 1862 es traslladà a Berlín, on prosseguí la seva formació sota la direcció de Kronecker i de Weierstrass. El mateix any 1862, es doctorà a Leipzig —que era la seva universitat d'origen— sota la direcció de Drobisch —un descendent de Kästner. Roch morí a Venècia, l'any 1866, quan comptava 27 anys. Riemann i Roch moriren de la mateixa malaltia pulmonar, el mateix any, i en el mateix país —la qual cosa no ens ha d'estranyar, perquè tots dos s'havien traslladat a Itàlia per recomanació mèdica.

De les moltes versions i generalitzacions que s'han fet del teorema de Riemann–Roch, n'esmentarem només unes quantes. Una de les primeres, si no la primera, degué ésser la versió per a superfícies que en donà M. Noether, l'any 1871, i que es coneix avui com la fórmula d'intersecció de Noether. El seu refinament conduí a la teoria de Brill–Noether, que pren el nom d'un article publicat per aquests autors l'any 1874 i que exerciria una gran influència en els geomètres italians. Brill i M. Noether intentaren donar demostracions més geomètriques del teorema de Riemann–Roch, la qual cosa comportà haver de parlar de corbes i de les seves singularitats. El seu article, titulat *Sobre les funcions algebraïques i la seva aplicació a la geometria* (*Über die algebraischen Functionen und ihre Anwendung in der Geometrie*), obtingué un ressò molt més ampli a Itàlia que a Alemanya. Versions del teorema de Riemann–Roch foren donades per part de Castelnuovo l'any 1896, Enriques l'any 1893 i, posteriorment, per Zariski (cf. [169]).

Intents per a relacionar el teorema de Riemann–Roch amb el teorema d'uniformització, és a dir, per a incloure'l en el context de les funcions i de les formes automorfes, foren fets per Ritter, l'any 1894; Fricke i Klein, l'any 1912; Weyl, l'any 1913; Osgood, l'any 1929, així com també per Shimura, ja en els nostres dies (cf. [355]).

L'any 1936, F. K. Schmidt donà una versió del teorema de Riemann–Roch per a cossos de funcions algebraïques d'una variable sobre un cos algebraicament tancat de característica qualsevol necessària per a l'estudi de les funcions zeta congruencials (cf. secció 3.12); concretament, per a demostrar-ne el caràcter racional. L'any 1962, Hirzebruch en donà una formulació per a varietats complexes, que re-

cupera la fórmula de Noether en el cas de superfícies. En la dècada 1960–1970, tots aquests resultats quedarien inclosos en el teorema de Riemann–Roch–Grothendieck de la teoria d'esquemes.

Del mateix treball de Riemann de l'any 1857 sobre les funcions abelianes, en sorgiria el problema de les matrius de Riemann, dels multiplicadors d'aquestes i, més endavant, el concepte de varietat abeliana i el problema de la determinació de les seves àlgebres i anells d'endomorfismes, que tractarem a la secció 12.1.

3.3 Dedekind

Julius Wilhelm Richard Dedekind (Brunsvic, 6 d'octubre de 1831; Brunsvic, 12 de febrer de 1916)

A l'edat de 16 anys, Dedekind ingressà en el *Collegium Carolinum* de Brunsvic, la institució en què s'havia format Gauss i en la qual el seu pare i el seu avi matern hi exerciren com a professors. Dos anys després, l'any 1850, ingressà a la Universitat de Göttingen. Allí, Dedekind formà part del seminari conjunt, recentment creat, de física i matemàtica. En aquell moment, el departament de física estava dirigit per Listing i Wilhelm Eduard Weber. L'any 1850 assistí a les lliçons de Gauss sobre el mètode dels mínims quadrats, que li causaren una profunda impressió i que recordà tota la seva vida.

L'any 1852, Dedekind presentà la seva tesi doctoral amb la supervisió de Gauss. El treball versà sobre la teoria de les integrals eulerianes, és a dir, les integrals que defineixen les

funcions gamma i beta d'Euler. Ben aviat, però, Dedekind s'adonà que la seva formació matemàtica tenia mancances greus. En aquells moments, els estudis de matemàtica de Göttingen estaven més orientats a la preparació de futurs professors de secundària que a la d'investigadors, i el nivell dels seus cursos era inferior al dels impartits a Berlín.

Dedekind emprà els dos anys posteriors al seu doctorat en l'estudi dels darrers desenvolupaments matemàtics i en la preparació de la seva habilitació. L'any 1854, i amb poques setmanes de diferència, ell i Riemann s'habilitaren a Göttingen i, tot seguit, Dedekind hi començà a impartir classes de probabilitat i de geometria.

A partir de 1855, quan Dirichlet succeí Gauss en la seva càtedra de Göttingen, s'inicià una fructífera relació entre Dirichlet i Dedekind, com a mestre i alumne, primer, i com a col·laboradors, després. D'aquesta col·laboració naixeria, anys més tard, el text de Dirichlet–Dedekind *Lliçons sobre teoria de nombres* (*Vorlesungen über Zahlentheorie*), editat i completat per Dedekind sobre les lliçons de teoria de nombres que rebé de Dirichlet. Aquest és el primer llibre de teoria de nombres que es publicà després de les *Disquisitiones arithmeticae* de Gauss. A més de trobar-hi la teoria de les formes quadràtiques binàries enteres de Gauss, el text conté les fórmules analítiques per al nombre de classes d'aquestes de discriminant donat, el teorema de la progressió aritmètica, i resultats sobre l'aritmètica dels anells d'enters dels cossos de nombres que inclouen la factorització única d'ideals i el teorema de les unitats.

Al mateix temps, Dedekind assistí als cursos de Riemann sobre funcions abelianes i funcions el·líptiques, i es-

tudià els treballs de Galois. Dedekind fou el primer, a Göttingen, a impartir un curs sobre teoria de Galois.

L'any 1858, Dedekind fou nomenat catedràtic de l'Escola Politècnica de Zuric, on impartiria lliçons de càlcul diferencial i de càlcul integral. D'aquesta època data la seva coneguda construcció dels nombres reals pel mètode dels talls. En el seu viatge a Berlín, l'any 1859, amb motiu de l'ingrés de Riemann a l'Acadèmia de Ciències, Dedekind es relacionà amb Weierstrass, Kummer, Borchardt i Kronecker. L'any 1862 tornà a casa seva, en ésser nomenat professor de la Universitat Tècnica de Brunsvic, després de la conversió del *Collegium Carolinum* en aquesta institució. Hi romangué fins a la seva jubilació, l'any 1894.

En les edicions tercera i quarta de les *Lliçons sobre teoria de nombres*, publicades els anys 1879 i 1894, Dedekind introduí el concepte d'ideal i hi formulà la seva teoria de la divisibilitat en els ordres dels cossos de nombres. Amb tot, el terme anell no s'empraria fins que aquest fos introduït, més endavant, per Hilbert.

En un treball conjunt amb Heinrich Weber, publicat l'any 1882, Dedekind traslladà la seva teoria d'ideals a l'estudi de les superfícies de Riemann. En aquest context, els ideals són substituïts per polígons i, en particular, aquests autors proporcionaren una demostració algebraica del teorema de Riemann–Roch. Aquesta demostració fou essencialment reproduïda en el text de Weber *Tractat d'Àlgebra* (*Lehrbuch der Algebra*), al final del tercer i darrer volum.

Les idees de Dedekind sobre la divisibilitat en els anells d'enters dels cossos de nombres foren ràpidament acceptades i transmeses per Weber, a Königsberg. Entre els seus

estudiants hi havia Hilbert. Posteriorment, la noció d'ideal deguda a Dedekind, seria estesa per Hilbert i per Emmy Noether a un anell qualsevol.

És remarcable la influència que exercí Dedekind en Peano. Pel seu treball sobre la inducció matemàtica, que el portà a definir els conceptes de conjunt finit i de conjunt infinit, es pot considerar Dedekind un dels iniciadors de la teoria de conjunts. De fet, l'any 1874 coneixeria Cantor i, més endavant, mostraria el seu acord amb l'obra d'aquest.

L'any 1888, Dedekind publicà el seu volum *Què són i què han d'ésser els nombres* (*Was sind und was sollen die Zahlen*), text que, a més de desenvolupar una primera teoria de conjunts, conté una axiomàtica per a l'estudi dels nombres naturals. L'any següent, 1889, Peano publicà el seu text en llatí *Principis d'aritmètica, exposats per un nou mètode* (*Arithmetices principia, nova methodo exposita*), en què, citant Dedekind, definia els nombres naturals en termes de conjunts. Aquest és el text que serviria per a popularitzar l'axiomàtica de Dedekind, avui coneguda amb el nom d'axiomes de Peano o, millor, axiomes de Dedekind–Peano.

La influència de l'obra de Dedekind no solament rau en la importància del seu contingut, sinó també en la seva manera d'exposar la matemàtica; per les seves precisió, claredat i concisió, determinaria un estil a imitar per les generacions futures.

Dedekind fou l'editor de les obres de Gauss, Dirichlet i Riemann.

D'altra banda, l'obra de Dedekind fou editada en tres volums per Fricke, Emmy Noether i Ore, i publicada per Vieweg & Sohn, a Brunsvic, entre els anys 1930 i 1932.

Dedekind fou nomenat membre de l'Acadèmia de Göttingen (1862), de l'Acadèmia de Berlín (1880), de l'Acadèmia de Roma, de l'Acadèmia de Ciències de París (1900), i de l'Acadèmia Leopoldino–Carolina dels Curiosos de la Natura (*Leopoldino–Carolina Naturae Curiosorum Academia*). L'any 2008, aquesta darrera institució, fundada l'any 1652 i amb seu a Halle, passà a denominar-se Acadèmia Nacional de Ciències (*Nationale Akademie der Wissenschaften*).

3.4 Funcions zeta

Una eina fonamental per a l'estudi dels nombres primers és la funció zeta de Riemann:

$$\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s} = \prod_p \frac{1}{1 - \frac{1}{p^s}}, \quad \Re(s) > 1.$$

Com que $\mathbb{Z}$ és un domini de factorització única, en la descomposició d'aquesta funció en producte d'Euler apareixen tots els nombres primers exactament una vegada.

La teoria d'ideals en els anells de Dedekind permet associar una funció zeta a cada cos de nombres, d'acord amb el model establert per Euler i per Riemann. La funció zeta de Dedekind d'un cos de nombres K es defineix per

$$\zeta(K, s) = \sum_{\mathfrak{a}} \frac{1}{N(\mathfrak{a})^s} = \prod_{\mathfrak{p}} \frac{1}{1 - \frac{1}{N(\mathfrak{p})^s}}, \quad \Re(s) > 1.$$

En ella, el sumatori s'estén a tots els ideals $\mathfrak{a}$ no nuls de l'anell $\mathcal{O}_K$ dels enters de K , $N(\mathfrak{a}) = \#\mathcal{O}_K/\mathfrak{a}$ denota la norma de l'ideal $\mathfrak{a}$, i el producte s'estén a tots els ideals primers $\mathfrak{p}$ no nuls de $\mathcal{O}_K$. Com que la sèrie anterior és uniformement convergent en els compactes de $\Re(s) > 1$, la funció zeta és holomorfa en aquest semiplà. La descomposició dels ideals no nuls de $\mathcal{O}_K$ com a producte d'una quantitat finita d'ideals primers, i de manera única, es tradueix en l'expressió de la funció ζ com a producte d'Euler en què apareixen tots els ideals primers no nuls de $\mathcal{O}_K$ exactament una vegada. De la descomposició en forma de producte d'Euler es dedueix que $\zeta(K, s)$ no s'anul·la per a $\Re(s) > 1$.

La funció $\zeta(K, s)$ de Dedekind associada a un cos de nombres admet una prolongació analítica a una funció meromorfa del pla complex que té un únic pol, simple, en $s = 1$; i un cop completada amb factors Γ adequats, satisfà una equació funcional. En el cas de la funció zeta de Riemann ($K = \mathbb{Q}$), la demostració d'aquests fets és deguda al mateix Riemann. En el cas general, la demostració és deguda a Hecke. La demostració de Hecke es basa a expressar la funció zeta com una transformada integral de funcions theta. L'equació funcional de les funcions theta permet l'obtenció de la prolongació analítica de $\zeta(K, s)$.

El mètode de Hecke s'estén a les funcions $L(\chi, s)$ de Dirichlet i a les funcions $L(\psi, s)$ de Hecke, associades a caràcters més generals i de les quals parlarem més endavant.

Els càlculs de Dirichlet relatius a la fórmula analítica del nombre de classes dels cossos quadràtics foren generalitzats per Hecke a qualsevol cos de nombres, obtenint així la coneguda fórmula analítica del nombre de classes d'ideals.

Mitjançant un càlcul d'integrals múltiples, s'obté que

$$\lim_{s \rightarrow 1} (s-1)\zeta(K, s) = \frac{2^{r_1} (2\pi)^{r_2} h_K R_K}{w_K \sqrt{|D_K|}}.$$

En aquesta fórmula, r_1 i r_2 denoten els nombres d'immersiions reals i de parelles d'immersiions complexes conjugades no reals de K , respectivament; h_K és l'ordre del grup de les classes d'ideals de K ; R_K és el regulador del cos K , que mesura el volum d'un paralelepípede fonamental del grup de les unitats; w_K és el nombre d'arrels de la unitat incloses en K ; i $|D_K|$ és el valor absolut del discriminant de K , que mesura el volum d'un paralelepípede fonamental de l'anell dels enters.

La fórmula analítica del nombre de classes es considera un dels miracles de la teoria de nombres. En particular, en el cas $K = \mathbb{Q}$, el fet que el pol en $s = 1$ de la funció zeta de Riemann sigui de residu 1,

$$\lim_{s \rightarrow 1} (s-1)\zeta(s) = 1,$$

sintetitza els fets aritmètics següents: $\mathbb{Z}$ és un domini d'ideals principals ($h = 1$) que té dues arrels de la unitat ($w = 2$) i cap unitat d'ordre infinit ($R = 1$); cap ideal de $\mathbb{Z}$ no és ramificat ($D = 1$); $\mathbb{Q}$ té una única immersió en $\mathbb{R}$ ($r_1 = 1$) i cap immersió complexa no real ($r_2 = 0$).

3.5 Klein

Felix Christian Klein (Düsseldorf, 25 d'abril de 1849; Göttingen, 22 de juny de 1925)

Klein cursà ciències matemàtiques i naturals a la Universitat de Bonn; es doctorà en matemàtica per la Universitat de Berlín (1869) i s'habilità per la Universitat de Göttingen (1871). Fou catedràtic de la Universitat d'Erlangen (1872), de l'Escola Tècnica Superior de Munic (1875) i de les universitats de Leipzig (1880) i de Göttingen (1886).

La figura de Klein és recordada especialment pel *Programa d'Erlangen*, una concepció unitària de les geometries que, basada en l'estructura algebraica de grup, exposà en el seu discurs d'ingrés com a professor de la Universitat d'Erlangen, l'any 1872. La seva obra conté aportacions fonamentals a l'estudi de la geometria hiperbòlica, de les funcions automorfes i, a més, alguns dels seus textos han estat un referent en moviments de renovació pedagògica.

Quan Klein fou nomenat professor de la Universitat de Göttingen, l'any 1886, comptava 37 anys. Sota la seva direcció, l'Institut Matemàtic d'aquella universitat esdevingué el centre mundial de més renom del seu temps per al cultiu de la matemàtica. Un seguit de joves procedents de països diversos estudiaren en les seves aules, atrets per la qualitat d'un quadre docent que comptava amb Klein, Hilbert, Minkowski i Emmy Noether, entre altres. L'any 1895, Klein dirigí la tesi a l'estudiant anglesa Grace Young, i fou aquesta la primera matemàtica a obtenir el títol de doctora per una universitat prussiana. Les activitats de l'Institut Matemàtic de la Universitat de Göttingen prosseguiren fins a l'any 1933, en què la instauració del nacionalsocialisme en provocà la davallada. El seu model influiria en altres institucions americanes, com ara l'Institut d'Estudis Avançats de Princeton i l'Institut Courant de Nova York, centres que

acolliren una part significativa del personal científic europeu durant la Segona Guerra Mundial.

A la universitat, Klein organitzà nombrosos seminaris per a estudiants a fi d'afavorir-los l'aprenentatge autònom. Procurà que tinguessin una sala d'estudi i, conjuntament amb el matemàtic Hermann Schwarz, muntà exposicions orientades a la visualització de conceptes abstractes per mitjà de figures geomètriques. Moltes d'aquelles creacions estudiantils encara es poden contemplar en unes vitrines de l'actual Institut Matemàtic de la Universitat de Göttingen.

Klein donava molta importància a l'educació matemàtica rebuda en els primers anys d'escolarització. Per a afavorir-la, sostenia que el professorat de qualsevol nivell havia de renovar i mantenir al dia els seus coneixements. Conseqüentment, impartí nombrosos cursos adreçats a professorat de secundària. Els apunts d'aquells cursos presos pels seus ajudants eren litografiats i distribuïts per al seu ús general. Posteriorment, Klein recopilà aquell material en un tractat en tres volums titulat *Matemàtica elemental des d'un punt de vista superior*, que fou editat entre els anys 1908 i 1913. Un segle després, aquesta obra encara es tradueix, es reedita i manté el seu encant. L'any 1893, Klein promogué a la Universitat de Göttingen la creació de la primera càtedra per a la didàctica de la matemàtica. En el Congrés Internacional dels Matemàtics celebrat a Roma l'any 1908, Klein fou nomenat president de la Comissió Internacional per a la Instrucció Matemàtica (ICMI).

Quan Klein inicià la carrera acadèmica, la sortida natural dels estudis de matemàtica era la docència. Però Klein suggerí obrir-los a especialitats més aplicades. D'entrada, els seus punts de vista no foren acceptats per la resta del

professorat. Després d'un viatge a Chicago, l'any 1893, i d'haver comprovat que les universitats nord-americanes es finançaven bàsicament amb fons privats, Klein insistí a captar l'interès de la indústria vers la universitat. Començà per l'organització d'un seminari sobre la matemàtica de les assegurances —que fou un èxit— i promogué la creació de seminaris de geodèsia i d'estadística. L'any 1898 fou fundada la primera organització alemanya que establí lligams entre la indústria i la universitat: la Societat de Göttingen per a la Promoció de la Física Aplicada. Tant per a Klein com per a Hilbert i Minkowski, la física ofería un camp especialment atractiu d'aplicabilitat de la matemàtica. A instàncies de Klein, la societat fou ampliada al cap d'un any per a incloure-hi la matemàtica. Matemàtics i físics s'implicaren en la docència de cursos avançats i, la tercera dècada del segle XX, Göttingen esdevingué un centre mundial per als estudis de física i de matemàtiques.

En la seva època d'estudiant de doctorat a Berlín, Klein es féu amic del matemàtic noruec Lie, aleshores també estudiant. L'estiu de l'any 1870, els dos amics decidiren anar a París per a visitar Jordan. Aquest matemàtic acabava de publicar el *Tractat de les substitucions i de les equacions algebraïques* amb una posada a punt de la teoria de Galois. Klein i Lie quedaren fascinats per les idees d'aquest jove matemàtic. Galois havia associat a cada polinomi un grup de substitucions, format per les transformacions algebraïques de les seves arrels i, en traslladar-ne l'estudi al del grup, obtenia la caracterització de les equacions que eren resolubles per radicals. Els matemàtics italians del Renaixement havien descobert fórmules per a la resolució per radicals de les equacions generals de grau tres i de grau quatre, però ni ells ni els seus successors no havien estat

capaços de trobar-ne per a les equacions generals de grau més gran o igual a cinc, malgrat tots els intents. La teoria de Galois explicava el perquè d'aquests suposats fracassos: s'havien estat cercant durant més de 300 anys unes fórmules que no podien existir. L'estada de Klein i de Lie a París fou molt profitosa i els serví per a adonar-se que l'estructura algebraica de grup capta matemàticament el concepte de simetria.

Klein i Lie prosseguiren l'estudi dels grups durant tota la seva vida. Lie es concentrà en l'estudi dels grups continus de transformacions d'equacions diferencials. Klein ho féu en els grups discrets de moviments del pla hiperbòlic, anomenats modulars, i en les funcions automorfes que en resulten. L'estudi dels grups modulars i de les funcions associades permeté avançar en el coneixement de les arrels de les equacions. En particular, Klein demostrà que les arrels complexes de les equacions de grau cinc es poden calcular per mitjà de valors especials de funcions modulars de nivell $N = 5$. Per a tal fi, identificà el grup de Galois d'una equació de grau cinc, general i normalitzada, amb el grup de rotacions d'un icosaèdre, i presentà aquest grup com a quocient de dos grups modulars. Els càlculs necessaris, que són elaborats, foren aplegats per Klein en el llibre *Lliçons sobre l'icosaèdre i la resolució de l'equació de grau cinc*, publicat l'any 1884.

Entre els nombrosos estudiants de doctorat de Klein hi ha Bieberbach, Bolza, Fricke, Furtwängler, Hurwitz, Lindemann, Ostrowski i Grace Young.

3.6 Hilbert

David Hilbert (Königsberg, 23 de gener de 1862; Göttingen, 14 de febrer de 1943)

Els primers anys de la vida de Hilbert transcorregueren a Königsberg on, a la seva universitat, inicià els estudis de matemàtica l'any 1880, s'hi doctorà l'any 1885, sota la direcció de Lindemann, s'hi habilità l'any 1886, i hi esdevingué professor ordinari l'any 1892.

L'any 1895 es traslladà a la Universitat de Göttingen, on desenvolupà la resta de la seva carrera. L'any 1930 hi fou nomenat professor emèrit, però encara continuà impartint lliçons fins a l'any 1934, nou anys abans de la seva mort.

Sota el mestratge de Klein i de Hilbert, la Universitat de Göttingen s'havia convertit en un pol d'atracció per a estudiants de matemàtica d'arreu. Crida l'atenció la quantitat d'aquests que hi feien estades, ja fossin predoctorals o postdoctorals, becats pels seus propis governs, a més de nombrosos professors visitants. De 1890 a 1920, Klein havia dirigit 27 tesis a Göttingen i, de 1898 a 1934, Hilbert n'hi dirigí 74.

En la producció científica de Hilbert es poden distingir sis etapes, cadascuna dedicada a temes diferents:

- (a) Teoria d'invariants (1885–1893)
- (b) Teoria de cossos de nombres algebraics (1893–1898)
- (c) Fonaments de la geometria (1898–1902)
- (d) Equacions integrals (1902–1912)

(e) Física (1910–1922)

(f) Fonaments de la matemàtica en general (1922–1930)

L'any 1888, Hilbert publicà el teorema de la base finita en els *Mathematische Annalen* —revista que aleshores era dirigida per Klein. Hilbert resolí així un problema de la teoria d'invariants que havia estat plantejat per Gordan. La demostració de Hilbert, de caràcter purament existencial, fou tan innovadora que no estigué exempta de polèmica. En el llenguatge actual, Hilbert provava l'existència d'un sistema finit de generadors per a tot ideal de l'anell de polinomis; si bé la demostració de l'existència d'aquests era impecable, no en donava cap construcció. La polèmica fou només l'inici de futurs enfrontaments acalorats entre dos corrents matemàtics: el del *formalisme*, el màxim representant del qual fou Hilbert, i el del *constructivisme*, el màxim representant del qual fou el matemàtic holandès Brouwer. En general, es pot dir que els matemàtics de Göttingen es decantaren cap al formalisme, i els de Berlín, cap al constructivisme. No és difícil detectar encara avui matemàtics amb tendències orientades fortament en l'un o l'altre sentit.

Hem comentat més amunt que l'any 1890 s'havia fundat la Societat Matemàtica Alemanya. L'any 1893, aquesta societat encarregà a Hilbert i Minkowski la preparació d'un informe sobre l'estat de la teoria de nombres en aquells moments. Minkowski s'hagué d'enretirar del projecte al cap de poc temps, i Hilbert el continuà tot sol. L'any 1896, Hilbert presentà un monumental tractat sobre teoria de nombres, conegut com a *Zahlbericht*, que seria editat posteriorment i que representaria un avenç important res-

pecte de la teoria tal com l'havia expressada Dedekind a partir de les lliçons de Dirichlet. En aquest tractat hi ha el teorema conegut com a “Teorema 90 de Hilbert” sobre l'estructura de les extensions cícliques; la teoria de la ramificació; nocions de densitat relatives a ideals primers que descomponen completament; la llei de reciprocitat per als residus de potències; l'estudi de les extensions de Kummer i el símbol de residus nòrmics i certes versions de les lleis de reciprocitat, de manera que ja s'hi pot llegir l'inici d'allò que esdevindria, vint anys després, la teoria de cossos de classes. En aquest context, recordem que el cos conegut com a *cos de classes de Hilbert* d'un cos de nombres donat proporciona l'extensió abeliana no ramificada maximal d'aquest cos, de grup de Galois isomorf al grup de classes d'ideals del cos base.

El teorema 131 del llibre recull la primera demostració completa del teorema de Kronecker–Weber, d'acord amb el qual, tota extensió de Galois del cos dels nombres racionals amb grup de Galois abelià està inclosa en el cos generat per una arrel de la unitat. (Per analogia amb el teorema 90, potser el podríem anomenar el teorema 131 de Hilbert.) El llibre s'acaba amb la demostració de Kummer del Teorema de Fermat per als primers regulars.

L'obra de Hilbert és molt extensa i es desenvolupà d'acord amb les sis etapes esmentades més amunt. Publicà els llibres *La teoria dels cossos de nombres algebraics* (*Die Theorie der algebraischen Zahlkörper*) —aquest és el llibre conegut com el *Zahlbericht*, que ja hem anomenat anteriorment diverses vegades—, i *Fonaments de la geometria* (*Grundlagen der Geometrie*), l'any 1899; *Trets fonamentals d'una teoria general de les equacions integrals lineals*

(*Grundzüge einer allgemeinen Theorie der linearen Integralgleichungen*), l'any 1912; els dos volums dels *Méthodes de la física matemàtica* (*Methoden der mathematischen Physik*), de coautor R. Courant, els anys 1924 i 1937; *Trets fonamentals de la lògica teòrica* (*Grundzüge der theoretischen Logik*), de coautor W. Ackermann, l'any 1928; *Geometria visual* (*Anschaulische Geometrie*), de coautor S. Cohn Vossen, l'any 1932; i els dos volums dels *Fonaments de la matemàtica* (*Grundlagen der Mathematik*), de coautor P. Bernays, els anys 1934 i 1939. A més, J. Springer publicà en el període 1932–1935 el recull d'una part de la seva obra, que inclou el *Zahlbericht*, en els tres volums de les *Obres completes* (*Gesammelte Abhandlungen*). La correcció i la revisió de les obres de Hilbert fou feta per Olga Taussky, amb supervisió d'Emmy Noether.

L'editorial Springer publicà de nou les obres de Hilbert l'any 1968; aquesta vegada l'edició, també en tres volums, anà a càrrec de Serre.

L'obra de Hilbert exerciria una influència directa en diverses branques de la matemàtica. El seu estudi d'invariants influiria enormement en la teoria que desenvoluparien Emmy Noether i Frobenius en el camp de les representacions de grups, i en noves idees en el camp de la física teòrica (invariància de la velocitat de la llum, per exemple); el teorema de la base de Hilbert conduí al concepte d'anell noetherià; el seu estudi de les sizígies (terme que prové de l'astronomia i que denota la posició relativa d'un planeta i una lluna seva quan estan alineats amb el seu sol) desembocà en el naixement de l'àlgebra homològica; el seu teorema dels zeros, en la geometria algebraica moderna; el de les extensions abelianes del cos dels nombres racionals,

en la teoria de cossos de classes; els seus fonaments de la geometria i de la matemàtica en general portarien a la crisi de fonaments i la teoria de models; i el seu estudi de les equacions integrals es continuaria amb el dels operadors en els espais de Hilbert, bàsics per al desenvolupament de la mecànica quàntica. Efectivament, la teoria espectral de Hilbert es convertiria en l'instrument idoni amb el qual formular la teoria de la mecànica quàntica, inaugurada amb els treballs de Heisenberg i Schrödinger de l'any 1923. No oblidem que, abans de marxar a Amèrica, von Neumann fou col·laborador de Hilbert.

3.7 Els 23 problemes de Hilbert

Hilbert fou convidat a impartir una conferència en el Segon Congrés Internacional de Matemàtics, que havia de tenir lloc a París. Per una recomanació de Minkowski, i a fi d'ésser recordat, Hilbert preparà per a l'ocasió una llista de problemes. El 8 d'agost de 1900, Hilbert hi pronuncià una conferència titulada “Problemes matemàtics”. En ella, hi plantejà vint-i-tres problemes oberts que recollien la inquietud matemàtica del moment i que configurarien en gran mesura la investigació matemàtica del segle que entrava.

Hilbert creia que cada branca de la matemàtica podia ésser descrita formalment mitjançant un sistema d'axiomes i que tot problema matemàtic podia ésser resolt, sempre que s'hi esmerçés prou esforç. Conforme a això, distribuí els problemes de la seva ponència en dos blocs: els problemes relatius als fonaments de les ciències matemàtiques —els sis

primers— i els problemes específics procedents de la seva pròpia praxi —els disset restants.

Problemes relatius als fonaments de l'anàlisi. Les recerques de Dedekind sobre els nombres reals i de Cantor sobre les sèries trigonomètriques havien donat lloc a la creació per Cantor, l'any 1874, de la teoria de conjunts. Encara que, l'any 1925, Hilbert afirmés que “ja ningú ens podrà expulsar del paradís que Cantor ha creat per a nosaltres”, és cert que les dificultats no havien tardat a aparèixer, i que havien desembocat en una crisi de fonaments.

H1 El problema de Cantor del nombre cardinal del continu: es tracta de saber quants punts hi ha en una línia recta (“continu”). Per a Cantor, la resposta la donava la hipòtesi del continu: “tot conjunt infinit de nombres reals o bé és numerable o bé és de la potència del continu”. Hilbert també estava convençut de la seva validesa, però tant Cantor com ell mateix fracassaren en múltiples intents per a provar-la.

L'any 1938, Gödel demostrà la consistència relativa de la hipòtesi del continu respecte dels axiomes de Zermelo i Fraenkel (1904, 1919). Vint-i-cinc anys després, P. J. Cohen (1963) demostrà que si s'admet la consistència del sistema formal de Zermelo–Fraenkel, la hipòtesi del continu és independent del sistema. Amb això, en el marc usual de la teoria de conjunts no es podien demostrar ni la hipòtesi del continu ni la seva negació.

H2 La compatibilitat dels axiomes aritmètics: els axiomes de Peano (1889), o de l'aritmètica, regeixen les regles de càlcul habituals.

L'any 1930, Gödel demostrà els seus cèlebres teoremes d'incompletesa. En el primer, posà de manifest que, si l'aritmètica és consistent, llavors en qualsevol sistema que contingui una part prou àmplia de l'aritmètica hi ha proposicions tals que ni elles ni les seves negacions no poden ésser demostrades dins del sistema. En el segon, demostrà la impossibilitat de provar la pròpia consistència de qualsevol sistema formal que contingui una part suficientment àmplia de l'aritmètica.

Els teoremes de Gödel feren trontollar el programa formalista de Hilbert. El seu impacte repercutí no solament en la matemàtica sinó també en la lògica i la filosofia de la ciència.

Fonaments de la geometria i de les ciències físiques.

En el seu Programa d'Erlangen, Klein (1872) remetia l'estudi de cada geometria particular al dels invariants d'un grup de transformacions. El text de Hilbert sobre fonaments de la geometria (1899) acabava de sortir a la llum. En els problemes següents, Hilbert proposa examinar la utilitat de certs axiomes.

H3 La igualtat dels volums de dos tetràedres de bases iguals i altures iguals: l'axioma d'Arquimedes era usat en el mètode d'exhaustió, que era l'equivalent grec del càlcul integral. Hilbert és del parer que aquest axioma és imprescindible en una teoria dels volums dels políedres.

Mitjançant una construcció d'invariants algebraics, el seu alumne Dehn (1900) provà l'existència de dos po-

líedres del mateix volum que no podien ésser descompostos en una quantitat finita de tetràedres congruos dos a dos, fet que donava la raó a Hilbert.

H4 El problema de la línia recta com a distància més curta entre dos punts: el problema es remunta a Beltrami (1866), professor de geodèsia a Pisa. Hilbert planteja la construcció i el tractament sistemàtic de totes les geometries de l'espai projectiu per a les quals les geodèsiques (corbes de longitud mínima) són rectes.

El seu alumne Hamel (1903) inicià la seva recerca, que derivà posteriorment en la identificació de geometries no arquimedianes i de geometries desarguianes.

H5 El concepte de Lie de grup continu de transformacions sense la suposició de la diferenciabilitat: en el seu estudi de les equacions diferencials, Lie havia desenvolupat el concepte de grup continu de transformacions. Hilbert proposa distingir la condició de continuïtat de la condició de diferenciabilitat en les funcions que defineixen el grup. El problema es concretà en la pregunta: Tot grup localment euclidià, és un grup de Lie?

Els treballs de Gleason (1952) i de Montgomery i Zipin (1952) proporcionaren una resposta afirmativa.

H6 Tractament matemàtic dels axiomes de la física: Hilbert parla d'un possible tractament axiomàtic de la mecànica i del càlcul de probabilitats, i encoratja l'ús dels grups de Lie en l'estudi matemàtic de problemes de física.

L'axiomatització del càlcul de probabilitats estigué a càrrec de Kolmogorov (1933). Els grups de Lie es fan servir avui, per exemple, en mecànica quàntica, sistemes dinàmics, teoria ergòdica i mecànica estadística. El curs 1926–1927, Hilbert impartí unes lliçons de mecànica en què participà von Neumann, que era, en aquells anys, ajudant de Hilbert. La influència de Hilbert es reflectiria en el text pioner de von Neumann sobre els fonaments matemàtics de la mecànica quàntica (1932). Però, en la seva formulació general, H6 resta obert.

Problemes específics d'aritmètica. Les *Disquisicions aritmètiques* de Gauss (1801) havien posat els fonaments per al desenvolupament de la teoria algebraica de nombres, que tingué lloc al llarg del segle XIX. Recordem que els nombres algebraics són les arrels dels polinomis en una indeterminada i de coeficients racionals; per al seu estudi, s'agrupen en cossos. Els nombres transcendents es defineixen per contraposició als algebraics. La transcendència del nombre π , provada per Lindemann (1882), havia tancat el problema de la impossibilitat de la quadratura del cercle amb regle i compàs.

H7 Irracionalitat i transcendència de certs nombres: Hilbert demana provar la transcendència de a^b , per a tota base algebraica $a \neq 0, 1$ i tot exponent algebraic irracional b .

El teorema fou demostrat per Gelfond (1934) i Schneider (1934). Baker (1966) n'obtingué una generalització notable.

H8 Problemes sobre nombres primers: en la memòria de Riemann (1859) sobre les lleis que regeixen la distribució dels nombres primers, hi ha l’afirmació que “a l’interior d’aquestes fronteres es troben aproximadament unes tantes arrels reals, i és molt probable que totes les arrels siguin reals” (cf. més avall, pàgines 214, 231). Amb el canvi de variable adequat, l’afirmació és que “tots els zeros no trivials de la funció zeta estan sobre la recta $\Re(x) = 1/2$ ”, afirmació que s’anomena la hipòtesi de Riemann. Hilbert en demana una demostració. En [H8], Hilbert també menciona la conjectura de Goldbach i la dels nombres primers bessons.

Tots tres problemes encara són oberts.

H9 Demostració de la llei de reciprocitat més general en qualsevol cos de nombres: descoberta per Legendre (1798) i provada per Gauss (1801), la llei de reciprocitat quadràtica dóna compte del comportament recíproc de parelles de nombres primers senars com a residus quadràtics.

D’aquesta llei se n’obtingueren generalitzacions diverses, englobades en la llei de reciprocitat d’Artin (1927). La llei equival a la igualtat entre dues funcions de variable complexa associades a cossos de nombres abelians: les funcions L d’Artin i les funcions L de Hecke.

H10 Determinació del caràcter resoluble d’una equació diofantina donada: Hilbert pregunta si existeix un “procés general” que permeti decidir en un nombre finit de passos si una equació diofantina donada té o no solucions enteres.

L'any 1953, Davis conjecturà que els conjunts que podien ésser generats per una màquina de Turing, també anomenats recursivament enumerables, són di-ofantins. Com que se sabia que hi ha conjunts recursivament enumerables la funció característica dels quals no és computable, la conjectura de Davis implica que l'algoritme que demana Hilbert no pot existir. Contribucions de Julia Robinson, Putnam i el mateix Davis conduïren a la demostració, per part de Matijasevich (1971), de la conjectura de Davis; així, el problema quedà tancat negativament.

H11 Formes quadràtiques de coeficients nombres enters algebraics: es demana avançar en l'estudi de les formes quadràtiques de coeficients algebraics. Les formes quadràtiques binàries sobre els nombres enters racionals havien estat estudiades per Gauss (1801); molts autors generalitzaren els seus resultats: per exemple, Hermite, Eisenstein i Minkowski.

En el context que proposa Hilbert, són destacables les aportacions de Hasse (1923, 1924) i de Siegel (1935).

H12 Extensió del teorema de Kronecker sobre cossos abelians a altres dominis de racionalitat: Hilbert es fa ressò del bonic Somni de Joventut de Kronecker (cf. la secció 2.7): generalitzar, a qualsevol cos de nombres, el paper que juguen la funció exponencial i les funcions el·líptiques en l'estudi del cos dels nombres racionals i dels cossos quadràtics imaginaris.

Els problemes [H9], [H11] i [H12] impulsaren la creació i l'avenç de la teoria de cossos de classes, englobada avui en el programa de Langlands. El nivell

assolit en aquesta direcció féu possible la demostració de Wiles i Taylor (1995) del Teorema de Fermat.

Problemes específics d'àlgebra i de geometria. A la segona meitat del segle XIX les estructures algebraïques de grup, d'anell i de cos s'havien consolidat. El concepte de grup es forjà en els escrits de Galois (1830) sobre la impossibilitat de resoldre per radicals l'equació general de grau més gran o igual que 5.

H13 Impossibilitat de la resolució de l'equació general de grau 7 per mitjà de funcions de només dues variables. El mètode nomogràfic d'Ocagne (1899) permetia aproximar les arrels d'equacions de grau 5 o de grau 6 per mitjà de dibuixos de famílies de corbes dependents d'un paràmetre.

El problema que Hilbert planteja derivà en un problema d'anàlisi matemàtica sobre reducció de funcions contínues de més d'una variable a funcions contínues d'una quantitat menor de variables. Fou resolt per Kolmogorov i Arnold (1957), mitjançant l'aplicació de conceptes procedents de la teoria de la comunicació de Shannon (1948).

H14 Prova de la finitud de certs sistemes complets de funcions: el concepte d'anell noetherià sorgí de les recerques de Hilbert i d'Emmy Noether en teoria d'invariants. En aquest problema, Hilbert formula una pregunta que equival a la noetherianitat de certs anells. Zariski la traduí geomètricament i Nagata (1959) en proporcionar un contraexemple. El problema conduí a

l'estudi dels grups reductius per part de Weyl, alumne de Hilbert.

H15 Fonamentació rigorosa del càlcul enumeratiu de Schubert: per aplicació del seu principi de conservació del nombre, el professor d'institut H. Schubert (1870) havia obtingut resultats sorprenents. Per exemple, que en l'espai projectiu hi ha exactament 666.841.048 superfícies quàdriques que són tangents a 9 superfícies quàdriques donades. Hilbert demana una justificació rigorosa del càlcul enumeratiu de Schubert.

Les primeres contribucions foren obtingudes per Severi (1912), van der Waerden (1929) i Weil (1946). El problema influí en la gestació de tècniques de geometria algebraica.

H16 Un problema de la topologia algebraica de corbes i superfícies: Hilbert demana una descripció qualitativa de les configuracions possibles dels òvals d'una corba real plana de grau donat. El nombre màxim d'aquests es coneixia per Harnack (1876).

Per a corbes planes, la solució de **[H16]** només es coneix fins a grau 7; per a superfícies de l'espai, només fins a grau 4. Virginia Ragsdale (1906), estudiant de Hilbert, formulà una conjectura sobre el tema que continua oberta. Hilbert menciona la connexió del problema amb recerques de Poincaré relatives al nombre màxim i a la posició de cicles límit de corbes definides per equacions diferencials. El problema continua obert.

H17 Expressió mitjançant quadrats de formes definides: A instàncies de Minkowski, Hilbert pregunta si tota

funció polinòmica no negativa és suma de quadrats de funcions racionals.

Artin (1927) tancà el problema afirmativament. Resultats quantitativs foren obtinguts, més endavant, per Pfister (1967).

H18 Configuració de l'espai mitjançant políedres congrus: Hilbert proposa la recerca dels possibles políedres congrus que poden omplir un espai euclidià, que comporta alhora la dels grups cristal·logràfics.

En una tesi dirigida per Hilbert, Bieberbach (1911) demostrà que, en qualsevol dimensió, la quantitat de grups cristal·logràfics és finita; això confirmà, en particular, que n'hi ha 17 en dimensió 2 (els grups de l'Alhambra). Avui es coneix el seu nombre fins a dimensió quatre. Hilbert també recorda el problema de Kepler: “demostrar que la manera més eficient d'apilar taronges és l'habitual en els mercats”. El problema de Kepler, anomenat també d'apilament d'esferes, ha estat resolt per Hales (1998) però la solució, donada la seva longitud, només és consultable en línia.

Les tècniques involucrades en aquests problemes són d'aplicació a altres ciències (cristal·lografia, química, medicina) i són a la base matemàtica de les noves tecnologies.

Problemes específics d'anàlisi matemàtica. Els estudis de Green i de Gauss (1830) sobre electricitat i magnetisme havien afavorit el desenvolupament de la teoria del potencial, en la qual s'emmarca el problema de Dirichlet, íntimamente lligat al càlcul de variacions. La teoria de Cantor permetia la interpretació de les funcions com a punts d'un espai, aplanant el camí de l'anàlisi funcional.

H19 Les solucions d'un problema regular en el càlcul de variacions, són necessàriament analítiques? El problema bàsic del càlcul de variacions és trobar una corba, una superfície, etcètera, en la qual una certa integral pren un valor estacionari.

Les primeres respostes a **[H19]** es donaren en la tesi de Berstein (1904). A mitjan anys cinquanta, se sabé que totes les solucions suficientment llises d'un problema regular de variacions són analítiques. La precisió d'aquests conceptes propicià l'ús d'espais de Sobolev. Entre molts d'altres, s'hi compten els resultats de De Giorgi (1957) i Nash (1958).

H20 El problema general dels valors frontera: el controvertit principi de Dirichlet havia estat usat per Riemann (1857) en la seva memòria sobre les funcions abelianes. Hilbert en demana una justificació. Es tracta més aviat d'un programa per a l'estudi de l'existència de solucions en problemes regulars del càlcul de variacions.

Les primeres aportacions es deuen a Berstein (1910). El problema repercutí en l'important desenvolupament de l'anàlisi funcional.

H21 Demostració de l'existència d'equacions diferencials lineals amb grup de monodromia prescrit: aquest problema invers s'origina en estudis de Riemann sobre l'equació hipergeomètrica de Gauss. En ell, Hilbert demana l'existència d'una equació diferencial lineal de tipus fuchsian amb singularitats i grup de monodromia donats prèviament.

El problema ha estat resolt sota criteris diferents, analítics i geomètrics, alguns dels quals han estat refutats per Anosov i Bolibrukh (1989).

H22 Uniformització de relacions analítiques per mitjà de funcions automorfes: Uniformitzar una corba algebraica o analítica significa representar-la paramètricament mitjançant funcions d'una variable.

Al voltant d'aquest problema, maduraren els conceptes de recobriment universal, de representació conforme, de grup fuchsian, de funcions theta, etcètera. Destaquen aportacions de Schottky (1875), Klein, Poincaré (1899), Koebe (1907), Ahlfors (1938) i Griffiths (1971).

H23 Extensió dels mètodes del càlcul de variacions: Hilbert menciona les recerques de Poincaré sobre el problema de tres cossos com un exemple d'aplicació del càlcul de variacions, i recomana un pla d'actuació futura.

En els nostres dies, el càlcul de variacions intervé en la resolució de problemes específics de la teoria del control òptim, originats en física nuclear, electrònica, vols espacials o llançament de míssils, entre d'altres.

3.8 Àlgebres no commutatives

En el comentari següent de Gauss s'hi ha llegit un primer intent d'anar més enllà dels nombres complexos:

Per què les relacions entre coses que representen una multiplicitat de més de dues dimensions no poden proporcionar altres tipus de quantitats permissibles en aritmètica general?

C. F. Gauss, *Werke* 2, p. 169–178

Les multiplicitats de més de dues dimensions en les quals les operacions aritmètiques hi són permeses s'anomenaren, primerament, nombres hipercomplexos i, més endavant, àlgebres (de dimensió finita, primer, i no necessàriament finita, posteriorment). Comportaren, però, haver de treballar amb estructures no commutatives. Els inicis de l'àlgebra no commutativa foren lents, precisament per la dificultat d'identificar estructures no commutatives (a més de les obtingudes mitjançant les àlgebres de matrius).

Històricament, el primer exemple d'estructura no commutativa se situa en la invenció per part de Hamilton, l'any 1843, dels quaternions:

$$\mathbb{H} = \langle 1, i, j, k : i^2 = j^2 = k^2 = ijk = -1 \rangle_{\mathbb{R}}.$$

Es tracta d'una àlgebra sobre el cos dels nombres reals, $\mathbb{R}$, de dimensió 4, que, a més, és un cos.

Els cossos no necessàriament commutatius es coneixen en la literatura amb noms diferents: *Schiefkörper*, en alemany; *skew field* o bé *division ring*, en anglès, i *corps gauche*, en francès. Nosaltres els anomenarem anells de divisió, els representarem sovint per D , i reservarem les lletres K , L , etcètera, per a designar, com és habitual, els cossos commutatius.

El terme K -àlgebra serà emprat per a designar les àlgebres A sobre un cos K , de dimensió finita, $[A : K] < \infty$,

associatives i amb element unitat. Una K -àlgebra A se-rà anomenada central quan el seu centre $Z(A)$ coincideixi amb el cos K .

Recordem tanmateix que una K -àlgebra A és anomenada simple si no té ideals bilaterals no trivials. Una K -àlgebra A és semisimple si és isomorfa a una suma directa d'àlgebres simples.

Els primers exemples d'àlgebres simples són proporcionats per les àlgebres de matrius. Així, les K -àlgebres de matrius $M(n, K)$ són centrals i simples. Tota K -àlgebra de divisió D és una K -àlgebra simple i les àlgebres de matrius $M(n, D)$ són simples.

L'any 1870, Benjamin Peirce presentà una memòria a l'Acadèmia Nacional de Ciències (*National Academy of Sciences*) de Washington titulada *Àlgebres associatives lineals* (*Linear Associative Algebras*) [296], que fou publicada amb caràcter pòstum l'any 1881. En aquest treball es troben les nocions d'element nilpotent i d'element idempotent d'una àlgebra, així com també les descomposicions associades a un element idempotent central:

$$A = Ae \oplus A(1 - e), \quad e^2 = e.$$

El conjunt $I = Ae$ constitueix un ideal per l'esquerra de A , que satisfà la identitat $Ie = I$; el conjunt $J = A(1 - e)$ és un altre ideal per l'esquerra, per al qual $Je = 0$. A la mateixa memòria, Peirce investigà els possibles tipus d'àlgebres de dimensió ≤ 6 . Posteriorment, el seu fill, Charles Peirce demostrà que tota $\mathbb{R}$ -àlgebra de divisió D de dimensió ≤ 7 és isomorfa a $\mathbb{R}$, $\mathbb{C}$ o bé a $\mathbb{H}$. L'any 1884, Weierstrass obtenia que tota $\mathbb{R}$ -àlgebra commutativa de dimensió $n > 2$ té divisors de zero.

L'any 1878, Frobenius demostrà el rellevant resultat segons el qual tota $\mathbb{R}$ -àlgebra de divisió i central D és isomorfa a $\mathbb{R}$ o bé a $\mathbb{H}$. Per tant, no és estrany que Hamilton hagués tingut tantes dificultats per construir un cos no commutatiu sobre $\mathbb{R}$, car el teorema de Frobenius posava de manifest que, d'aquests, només n'hi havia un.

Molien, nascut a Riga, Letònia, entrà en contacte amb Klein quan aquest era encara professor a la Universitat de Leipzig. (Posteriorment, Molien esdevingué professor a la Universitat de Tomsk, a Sibèria.) En la seva tesi, de l'any 1893, hi ha el concepte d'àlgebra simple (de fet, ell en diu primitiva: *ursprünglich*). Molien obté que tota $\mathbb{C}$ -àlgebra simple és isomorfa a una àlgebra de matrius $M(n, \mathbb{C})$ [276]. Són remarcables les eines que s'utilitzen en aquest treball: formes bilineals, polaritzacions, formes traça i un equivalent a la representació regular. La seva tesi fou valorada com un antecedent dels treballs de Killing en àlgebres de Lie. Part dels resultats de Molien foren redescoberts per Cartan, l'any 1898 (cf. [386]).

Els teoremes d'estructura per a les K -àlgebres de dimensió finita arribarien, l'any 1908, de la mà de Wedderburn. En el treball [392], Wedderburn demostra que tota K -àlgebra A s'escriu com $A \simeq \text{Rad}(A) \oplus A_{ss}$, on A_{ss} és una K -àlgebra semisimple i $\text{Rad}(A)$ denota el radical de A . Wedderburn obté que, per a tota K -àlgebra A , simple, existeix una K -àlgebra de divisió D tal que $A \simeq M(n, D)$. Per tant, aquest teorema fa palès que la recerca dels anells de divisió sobre un cos commutatiu és equivalent a la de les àlgebres simples sobre aquest cos. Dels resultats de Wedderburn se'n dedueix, així mateix, que tot cos finit és commutatiu. Posteriorment, Witt, a instàncies d'Emmy

Noether, donà una demostració directa de la commutativitat dels anells de divisió finits, independent dels resultats de Wedderburn, basada únicament en propietats dels polinomis ciclotòmics (cf. [11]) (tal com deia Witt: “els fets senzills han de tenir demostracions senzilles”).

Les recerques anteriors culminaren en l'anomenat teorema de Wedderburn-Artin, de l'any 1927, de classificació dels anells semisimples. Donats un anell semisimple per l'esquerra R i un sistema complet de R -mòduls per l'esquerra simples $\{V_i\}$, si es té que $R \simeq n_1 V_1 \oplus \cdots \oplus n_r V_r$, aleshores,

$$R \simeq \prod_{i=1}^r M(n_i, D_i^o), \quad D_i \simeq \text{End}_R(V_i),$$

on, en general, D^o denota l'anell de divisió oposat d'un anell de divisió D . Si R és simple, aleshores $r = 1$ i $R \simeq \text{End}_D(V)$.

Hem de fer esment que, prèviament a aquest resultat, es produïren els treballs de Dickson.

L'any 1908, Dickson obtingué que si D és una K -àlgebra de divisió central i si L és un subcòs commutatiu maximal, $K \subseteq L \subseteq D$, tal que $[L : K] = n$, aleshores $[D : K] = n^2$. En relació amb la construcció de possibles estructures algebraïques noves, Dickson compta amb dos treballs importants, de 1914 i 1926. En el treball [100] construeix les àlgebres cícliques, que generalitzen els quaternions. En el treball [101] introdueix els sistemes de factors.

Donada una extensió cíclica de cossos $L = K(z)$, de grau $[L : K] = n$ i de grup de Galois $G = \langle g \rangle$, i donat un element $a \in K^*$, l'àlgebra cíclica $A = (L|K, g, a)$ es

defineix segons

$$(L|K, g, a) := \langle L, u : u^n = a, zu = uz^g, z \in L \rangle_K.$$

Per a $z \in L$ i $g \in G$, hem denotat per z^g l'acció de g en z . De la definició es dedueix que l'àlgebra $(L|K, g, a)$ està generada pels elements de L i per un element auxiliar u , subjecte a determinades relacions. Se satisfà que $K \subseteq L \subseteq A$ i L esdevé un subcòs commutatiu maximal de A . A més, $(L|K, g, a)$ és un anell de divisió si, i només si, $a^i, 0 < i < n$, no és norma en $L|K$. Alhora, $(L|K, g, a)$ és isomorfa a l'àlgebra de matrius $M(n, K)$ si, i només si, $a \in N_{L|K}(L^*)$, és a dir, l'element a de partida és una norma de l'extensió cíclica. Notem que, en partir d'extensions quadràtiques d'un cos K , reobtenim com a casos particulars les àlgebres de quaternions sobre aquest cos: $\left(\frac{a, b}{K}\right)$, $i^2 = a$, $j^2 = b$, $ij = -ji$, alhora que un criteri per a decidir si aquestes són o no anells de divisió.

Al seu torn, les àlgebres cícliques es generalitzaren en les àlgebres producte creuat. Donada una extensió de Galois $L|K$, de grup de Galois $G = \text{Gal}(L|K)$ i de grau $[L : K] = n$, es defineix l'àlgebra producte creuat com $L \cdot G :=$

$$\left\langle \sum_{g \in G} z_g u_g : zu_g = u_g z^g, z \in L; u_g u_h = u_{gh} a_{g,h}, a_{g,h} \in L^* \right\rangle.$$

En aquest cas, per a garantir l'associativitat del producte, cal que se satisfacin les identitats

$$a_{g,hk} a_{h,k} = a_{gh,k} a_{g,h}^k, \text{ per a tot } g, h, k \in G.$$

Els elements corresponents, $\{a_{g,h}\}$, s'anomenen un sistema de factors definidor de l'àlgebra. La K -àlgebra que en resulta és simple i central, i de grau $[L \cdot G : K] = n^2$.

Brauer tingué la idea brillant de classificar i organitzar les K -àlgebres simples i centrals en forma de grup. Donades dues K -àlgebres simples i centrals, es defineix, d'acord amb Brauer,

$$A \sim B \iff A \simeq M_n(D), \quad B \simeq M_m(D).$$

Donada una K -àlgebra simple i central A , denotarem per $[A]$ la seva classe d'equivalència així definida i per $\text{Br}(K)$ el conjunt de totes aquestes classes. El producte tensorial dota aquest conjunt d'una estructura de grup abelià, atès que se satisfan les propietats:

$$[A] \otimes [B] := [A \otimes_K B] \text{ és un producte ben definit en } \text{Br}(K),$$

$$[A] \otimes [B] = [B] \otimes [A],$$

$$[A] \otimes [K] = [A],$$

$$[A] \otimes [A^o] = [K].$$

En aquest context, donada una K -àlgebra simple i central A , una extensió finita L de K és un cos neutralitzador de A si $A \otimes_K L$ és isomorfa a una àlgebra de matrius sobre L . Se satisfà que tot subcòs commutatiu maximal $L \subseteq A$ és un subcòs neutralitzador de A . A més, tot cos neutralitzador L de A és subcòs maximal d'una K -àlgebra simple i central B tal que $[B] = [A]$.

La manca d'estructures no commutatives constatada inicialment es pot resumir en l'estructura dels grups de Brauer dels cossos considerats fins aleshores. Dels teoremes de Molien, Wedderburn i Frobenius es desprèn que

$\text{Br}(C) = (0)$, per a tot cos algebraicament tancat C ,

$\text{Br}(\mathbb{F}) = (0)$, per a tot cos finit $\mathbb{F}$,

$\text{Br}(\mathbb{R}) = \mathbb{Z}/2\mathbb{Z}$, atès que $\mathbb{H} \otimes_{\mathbb{R}} \mathbb{H} \simeq M(4, \mathbb{R})$.

Es pot dir que la recerca de cossos susceptibles de tenir un grup de Brauer més gran s'inicià amb els treballs de Brauer, Hasse i Emmy Noether. Tal com veurem, d'aquests treballs en resultaren la determinació del grup de Brauer dels cossos $\mathfrak{p}$ -àdics $\text{Br}(K_{\mathfrak{p}})$, i del grup de Brauer $\text{Br}(K)$ d'un cos de nombres K qualsevol. En ambdós casos, els grups de Brauer són infinits. Els resultats corresponents, d'obtenció gens fàcil, es provaren al mateix temps que alguns teoremes de la teoria de cossos de classes.

3.9 Teoria de cossos de classes

La teoria de cossos de classes descriu les extensions abelianes dels cossos de nombres. Les seves fites principals són:

- (a) Relacionar les extensions abelianes de qualsevol cos de nombres amb els grups de classes d'ideals d'aquest cos.
- (b) Obtenir teoremes de densitat per als ideals primers dels anells d'enters dels cossos de nombres.
- (c) Establir lleis generals de reciprocitat, vàlides per a qualsevol extensió abeliana de cossos de nombres.

El desenvolupament de la teoria és degut, entre d'altres, a Gauss, Dirichlet, Kummer, Kronecker, Heinrich Weber, Hilbert, Furtwängler, Fueter, Takagi, Txebotarev, Artin, Hasse, Chevalley, Tate i Serre.

A partir de resultats de Gauss i de Dirichlet, es demostra que tota extensió quadràtica de $\mathbb{Q}$ és ciclotòmica; és a dir, està continguda en un cos $\mathbb{Q}(\zeta_m)$ generat per una arrel m -èsima de la unitat.

Kronecker i Weber generalitzaren el resultat anterior en adonar-se que tota extensió abeliana de $\mathbb{Q}$ és ciclotòmica. El resultat, conegut amb el nom de teorema de Kronecker-Weber, fou enunciat per Kronecker l'any 1853, donant-ne una demostració incompleta. L'any 1886, Weber en proporcionà una altra demostració, tampoc no exempta de crítiques. Tal com ja hem dit, la primera demostració acceptada del teorema de Kronecker-Weber és deguda a Hilbert, l'any 1896. Hilbert demostrà el teorema per mitjà de la seva teoria de la ramificació superior.

L'any 1829 es publicaren els treballs d'Abel relatius a la construcció d'extensions abelianes de $\mathbb{Q}(i)$.

Donat un cos de nombres K , denotarem per $\mathcal{O}_K$ el seu anell d'enters; per $I(K)$, el grup dels seus ideals fraccionaris; per $P(K)$, el subgrup format pels ideals fraccionaris principals; i per $\text{Cl}(K) := I(K)/P(K)$, el grup de classes d'ideals.

L'any 1880, Kronecker observà que, donat un cos quadràtic imaginari qualsevol K , el grup de Galois de l'extensió $K(j(\tau))|K$ és isomorf al grup de classes d'ideals $\text{Cl}(K)$. L'extensió $K(j(\tau))|K$ és no ramificada i cada ideal de K esdevé principal en $K(j(\tau))$.

Weber considerà uns grups de classes d'ideals més generals, $I_{\mathfrak{m}}/H$, on $P_{\mathfrak{m}}^+ \subseteq H \subseteq I_{\mathfrak{m}}$, $\mathfrak{m}$ denota un mòdul de K format pel producte d'ideals primers i de places d'aquest cos, $P_{\mathfrak{m}}^+$ és un cert grup d'ideals principals, i $I_{\mathfrak{m}}$ és el grup dels ideals fraccionaris de K que són coprimers amb el mòdul $\mathfrak{m}$. Weber demostrà que, donats un mòdul $\mathfrak{m}$ i un grup H d'ideals de K de mòdul $\mathfrak{m}$, si per a una extensió de Galois $L|K$ se satisfà que $\text{Spl}(L|K) \subseteq H$, aleshores $[I_{\mathfrak{m}} : H] \leq [L : K]$. Si $\text{Spl}(L|K) = H$, aleshores $[I_{\mathfrak{m}} : H] = [L : K]$ i cada classe lateral de $I_{\mathfrak{m}}/H$ conté infinits ideals primers. Aquí hem denotat per $\text{Spl}(L|K)$ el conjunt d'ideals de K que descomponen completament en L .

Els resultats de Weber conduïren Hilbert a conjecturar, l'any 1898, que, per a cada cos de nombres K , hauria d'existir una extensió finita $K'|K$, única, tal que

- (1) $K'|K$ és de Galois i $\text{Gal}(K'|K) \simeq \text{Cl}(K)$.
- (2) $K'|K$ és no ramificada.
- (3) Per a cada ideal primer $\mathfrak{p}$ de $\mathcal{O}_K$, el seu grau residual $f_{\mathfrak{p}}$ coincideix amb l'ordre de $\mathfrak{p}$ en $\text{Cl}(K)$.
- (4) Tot ideal de $\mathcal{O}_K$ esdevé principal en $\mathcal{O}_{K'}$.

El cos K' , l'existència del qual es conjecturava, fou denominat el cos de classes de Hilbert de K . En la demostració de la seva existència hi treballaren Fueter i Takagi.

Takagi havia visitat Göttingen durant els anys 1898 a 1901. Associat a un mòdul $\mathfrak{m}$ d'un cos de nombres K ,

Takagi defineix un grup d'ideals

$$H_{\mathfrak{m}}(L|K) := P_{\mathfrak{m}}N_{\mathfrak{m}}(L|K).$$

Segons Takagi, una extensió abeliana de cossos de nombres $L|K$ és un cos de classes mòdul $\mathfrak{m}$ quan

$$[I_{\mathfrak{m}} : H_{\mathfrak{m}}(L|K)] = [L : K].$$

En aquest cas, es diu que el mòdul $\mathfrak{m}$ és admissible per a l'extensió $L|K$. Donada una extensió abeliana $L|K$, el mòdul admissible més petit segons la relació de divisibilitat, $\mathfrak{f}_{L|K}$, s'anomena el conductor de l'extensió.

L'any 1920, Takagi demostrà els resultats següents, per a tot cos de nombres K :

- (1) (Existència) Per a cada grup d'ideals $H \subseteq I(K)$, existeix un cos de classes L sobre K . Si el mòdul de H és $\mathfrak{m}$, se satisfà que $\text{Gal}(L|K) \simeq I_{\mathfrak{m}}/H$.
- (2) (Completesa) Tota extensió abeliana de K és un cos de classes.
- (3) (Conductor) Les places de K que divideixen el conductor $\mathfrak{f}_{L|K}$ d'una extensió abeliana són les ramificades en $L|K$.
- (4) (Llei de descomposició) Si $\mathfrak{p} \nmid \mathfrak{m}$, el grau residual $f_{\mathfrak{p}}(L|K)$ coincideix amb l'ordre de $\mathfrak{p}$ en $I_{\mathfrak{m}}/H$.

Takagi obtingué els resultats anteriors amb posterioritat al seu pas per Göttingen, treballant aïlladament en el seu país, en el decurs dels anys de la Primera Guerra Mundial.

Els resultats esmentats conformaren de mica en mica l'edifici de la teoria de cossos de classes. Un punt culminant d'aquesta teoria fou l'obtenció per part d'Artin, l'any 1927, de la llei de reciprocitat.

La llei de reciprocitat d'Artin fa explícit l'isomorfisme

$$\mathrm{Gal}(L|K) \simeq I_{\mathfrak{m}}/H$$

obtingut per Takagi en el seu teorema d'existència. Concretament, donats una extensió abeliana $L|K$ de cossos de nombres i un mòdul $\mathfrak{m}$ de K , divisible per les places de K que ramifiquen en L , se satisfà que

$$\varphi : I_{\mathfrak{m}}/H_{\mathfrak{m}} \simeq \mathrm{Gal}(L|K), \quad \text{on } \varphi(\mathfrak{p}) := \mathrm{Frob}(\mathfrak{p}, L|K).$$

L'anomenat element de Frobenius, $\mathrm{Frob}(\mathfrak{p}, L|K)$, només està definit en les places de K que no ramifiquen en L i és un generador específic del grup de descomposició $D_{\mathfrak{p}}(L|K)$ de $\mathfrak{P}|\mathfrak{p}$. (Precisament en les places no ramificades tots els grups de descomposició són cíclics.)

Les aportacions d'Emmy Noether i de Hasse a la teoria de cossos de classes se centraren en l'obtenció de diversos principis locals globals. Hasse demostrà la coneguda com a *Führerdiskriminantenproduktformel*:

$$\mathcal{D}(L|K) = \prod_{\chi} f_{\chi, \mathrm{fin}},$$

segons la qual el discriminant d'una extensió relativa de cossos de nombres s'expressa com a producte dels conductors finits associats als caràcters del grup de Galois de l'extensió.

Hasse edificà la teoria local de cossos de classes, però molts resultats de la teoria local es demostraren primerament a partir de resultats de la teoria global, provats amb anterioritat. Fou sota la influència d'Emmy Noether que s'obtingueren les demostracions locals, primerament, i, a partir d'aquestes, els teoremes de la teoria global. En parlaré tot seguit perquè aquest procés es desenvolupà en paral·lel al del càlcul dels grups de Brauer dels cossos $\mathfrak{p}$ -àdics i dels cossos de nombres. El 8 de novembre de l'any 1931, Emmy Noether escrivia a Hasse:

Ara faig un seminari de teoria de nombres: teoria de cossos de classes en petit [local], conductor d'Artin, teorema de l'ideal principal (per cert, la senyoreta Taussky és aquí), etcètera; les demostracions que segueixen són les que han d'ésser exposades, però el meu objectiu personal és entendre aquestes coses hipercomplexament.

Emmy Noether

L'any 1954, Chevalley deduí la teoria global de cossos de classes a partir de la teoria local, d'una manera unificada. Per a tal fi, introduí el grup d'ideles d'un cos de nombres. Aquest grup és el grup multiplicatiu de l'anell dels adeles del cos de nombres. El tractament adèlic de la teoria de cossos de classes permet formular els resultats també per a les extensions abelianes no finites dels cossos de nombres.

Les tècniques anteriors foren unificades els anys 1950–1960 amb el tractament cohomològic, tant de la teoria local com de la teoria global. Els resultats foren presentats sota la noció de formació de classes, essent les seves primeres

presentacions les dels textos d'Artin–Tate [13] i de Serre [341].

3.10 Emmy Noether

Emmy Amalie Noether (Erlangen, 23 de març de 1882; Bryn Mawr, Estats Units, 14 d'abril de 1935)

Emmy Noether era filla de Max Noether. Es doctorà als 25 anys a la Universitat d'Erlangen sota la direcció de Gordan, un dels especialistes de l'època en teoria d'invariants. De 1907 a 1915 treballà a l'Institut de Matemàtiques d'Erlangen, institució de la qual el seu pare també era professor i a qui ella suplia en alguna de les classes. L'any 1915 s'incorporà a la Universitat de Göttingen, a instàncies de Klein i de Hilbert. L'any 1919, quan comptava 37 anys, esdevingué la primera dona matemàtica habilitada per la Universitat de Göttingen; en aquella ocasió el tribunal estigué format per Klein, Hilbert, Courant, Landau i Debye. Un cop habilitada, li fou concedida la *venia legendi* amb el títol d'encarregat de curs. L'any 1922 fou nomenada *nichtbeamter ausserordentlicher Professor*; és a dir, professor extraordinari no funcionari.

Les seves classes solien tractar temes de la seva pròpia recerca en els quals estava treballant. Aquest fet dotava les seves lliçons d'un caràcter poc metòdic, però viu i participatiu per part dels estudiants, que sovint n'editaven apunts.

En comparar els cursos impartits per Emmy Noether a Göttingen amb les dates i els continguts de les seves publi-

cacions, es posa de manifest l'estret lligam que ella sabia establir entre docència i recerca. Així, veiem que l'hivern de 1924–1925 impartí un curs sobre teoria de grups i nombres hipercomplexos; l'hivern de 1927–1928, un altre sobre sistemes hipercomplexos i teoria de la representació i, tot seguit, l'any 1929, publicà el treball

Noether, E.: Hyperkomplexe Grössen und Darstellungstheorie. *Math. Z.* **30** (1929), p. 641–692.

Al mateix temps, l'estiu de 1928 impartí un curs sobre àlgebra no commutativa, com a avançament de la publicació

Noether, E.: Nichtkommutative Algebren. *Math. Z.* **37** (1933), p. 514–541.

L'estiu de 1929 impartí un curs sobre aritmètica no commutativa, en el qual desenvolupà la seva teoria de productes creuats (*verschränkte Producte*). En aquest cas, els seus resultats no foren publicats per ella, sinó que foren exposats (citant-ne la procedència) per Hasse a

Hasse, H.: Theory of cyclic algebras over an algebraic number field. *Trans. AMS* **34** (1932), p. 180–200;

i per Deuring en el text pioner

Deuring, M.: *Algebren*. Ergebnisse der Mathematik IV. Springer, 1935.

Durant el semestre d'hivern de l'any 1928, fou convidada a impartir un curs d'àlgebra a la Universitat de Moscou. L'any 1932, fou la primera dona matemàtica a presentar una conferència plenària en un Congrés Internacional de Matemàtics (*International Congress of Mathema-*

ticians, ICM), celebrat aquell any a Zuric. És remarcable que Emmy Noether fou la primera matemàtica convidada a impartir una conferència plenària en un dels Congressos Internacionals de Matemàtics. De ben segur, hi devia ajudar el fet que van der Waerden, aleshores professor a Zuric, en fos un dels organitzadors. Fins avui, no es pot dir que la presència femenina en aquests tipus d'actes hagi estat gaire lluïda, atesa la migradesa de conferenciantes plenàries en els congressos internacionals de matemàtics.

L'any 1933, i després de l'arribada dels nazis al poder, Emmy Noether hagué d'emigrar als Estats Units per la seva condició de jueva. A Amèrica, la trobem com a professora del *Bryn Mawr College* de Pensilvània. El *Bryn Mawr College* era una institució dedicada a l'educació de les noies que comptava amb estudis de matemàtica. Aquests havien estat iniciats per Charlotte Scott, la primera doctora anglesa en matemàtica. Charlotte Scott compta amb una extensa producció matemàtica.

Entre els matemàtics que col·laboraren amb Emmy Noether arran del seu pas per Göttingen, esmentarem Weyl, Artin, Hasse, Krull, Brauer, van der Waerden, Köthe, Weil, Olga Taussky, Deuring, Herbrand i Witt.

Artin féu estades a Göttingen els anys 1921 i 1922; després mantingué amb Emmy Noether un contacte permanent.

Hasse hi féu una estada predoctoral l'any 1920 i en fou professor durant els anys 1934 a 1939, com a successor de Weyl. Mantingué durant molts anys correspondència matemàtica amb Emmy Noether.

Van der Waerden hi féu una estada postdoctoral l'any 1924, becat per la fundació Rockefeller, i una altra l'any 1928, com a professor visitant. A més, com és ben conegut, a partir dels cursos d'Emmy Noether i dels d'Artin, van der Waerden escriuria el seu famós text *Moderne Algebra*, editat en dos volums els anys 1930 i 1931, i que encara es continua reeditant.

Köthe fou alumne d'Emmy Noether a Göttingen l'any 1928. Posteriorment no es dedicà a l'àlgebra, sinó que ho féu a l'anàlisi funcional.

Krull estudià a Göttingen en el decurs dels anys 1920–1921, en el seminari de Klein. Emmy Noether exercí una gran influència en l'obra de Krull sobre la teoria d'ideals i mantingué amb ell una amistat durant tota la vida.

Olga Taussky, quan ja era doctora, fou contractada a Göttingen en els anys 1931–1932, amb l'encàrrec específic de revisar i preparar l'edició de les obres de Hilbert.

Weil visità Göttingen l'any 1927, com a alumne predoc-toral, i hi tornà l'any 1931, ja com a doctor. Herbrand i Deuring hi foren l'any 1931 i Witt, l'any 1934.

Deuring i Witt formen part dels 13 estudiants a qui Emmy Noether dirigí la tesi; entre aquests, també hi trobem Fitting, Tsen, Schilling i Werner Weber.

Fitting és conegut per les seves recerques en grups finits. Schilling fou un dels difusors de la teoria de valoracions. De Tsen es recorda especialment el teorema fonamental de la seva tesi (llegida l'any 1936) sobre el caràcter quasi algebraicament tancat dels cossos de funcions d'una variable sobre un cos algebraicament tancat. Aquest mateix resul-

tat es retroba anys després en la tesi de Lang, llegida l'any 1951 i publicada l'any 1952, que fou dirigida per Artin.

Weyl, que prèviament havia fet la tesi a Göttingen sota la direcció de Hilbert, en fou el successor. Fou professor de la Universitat de Göttingen durant els anys 1930 a 1933. Després tornaria a coincidir amb Emmy Noether als Estats Units, quan Weyl era professor a l'Institut d'Estudis Avançats de Princeton i Emmy Noether era professora del *Bryn Mawr College*. Com que Princeton estava relativament a prop de Bryn Mawr, i comunicat amb tren, Weyl convidà Emmy Noether a impartir cursos d'àlgebra a l'Institut, la qual cosa ella feia setmanalment. A Bryn Mawr, Emmy Noether també coincidí amb Olga Taussky.

Hasse havia tingut dos directors de tesi: Hensel i Hecke. Del primer, que era el creador dels nombres p -àdics, li agradava rememorar que havia après a valorar la bellesa de la matemàtica. En canvi, solia dir que les nombroses fórmules emprades pel segon l'espantaven. En la seva tesi, Hasse demostrà la validesa del principi local-global per a la classificació i la representació de nombres per formes quadràtiques definides sobre cossos de nombres. Les seves recerques generalitzaven resultats previs sobre formes quadràtiques definides sobre el cos dels nombres racionals, deguts a Minkowski i que aquest havia obtingut per mitjà de congruències, sense fer ús dels nombres p -àdics.

Hasse i Noether mantingueren correspondència durant molts anys. Les cartes de Hasse a Noether s'han perdut, però no així les de Noether a Hasse. Les cartes del període 1925–1935 han estat editades recentment per Roquette (a qui Hasse dirigí la tesi) i per Lemmermeyer (a qui Roquette dirigí la tesi). En aquestes cartes, d'un alt contingut

matemàtic i que posen de manifest la infatigable energia d'Emmy Noether, s'hi troben al·lusions a estudiants que feien estades a Göttingen, com ara Herbrand o Weil.

Per les seves cartes a Hasse, coneixem que, al *Bryn Mawr College*, Emmy Noether donava classe a tres noies (els explicà el primer volum del text d'àlgebra de van der Waerden i els primers capítols del text de teoria algebraica de nombres de Hecke) i es mostrava molt satisfeta per l'interès de les seves alumnes per resoldre problemes. Alhora, dirigia la tesi a una estudiant, Ruth Stauffer.

El 7 d'abril de l'any 1935, Noether escrivia a Hasse:

Benvolgut Sr. Hasse,

Moltes gràcies per enviar-me els seus extrets —com sempre, m'admira la quantitat de feina que fa— i per la còpia de la carta a Albert [...]

Sobre aquest punt, Brauer es permet remarcar que la relació entre formes quadràtiques i àlgebres (p. 18) inclosa en la demostració de la descomposició en producte $H = \prod_{i \leq k} (a_i, a_k)$ (Artin) és ben coneguda pels físics: Dirac l'ha utilitzada i serà emprada en la teoria de spinors en una nota de Weyl i seva (com a ajudant). En el cas especial de les sumes de quadrats, ja es deu trobar en l'article de Cartan sobre sistemes hipercomplexos de l'Enciclopèdia francesa. Ho sap Witt que és conegut que, en el cas multiplicatiu, la descomposició dels sistemes de factors és condició necessària i suficient per a l'existència d'extensions? Aquest és el resultat

de Brauer que vostè esmenta en el seu informe anual 44.

[Segueixen uns resultats sobre bases normals explícites de la seva alumna de doctorat.]

Va anar vostè a Hèlsinki? i, què farà a l'estiu? Jo no sé si aquest any tornaré; en tot cas, a finals de juny. Penso que hauré d'estar present en la festa de graduació de l'esmentada doctoranda, en què la Presidenta li imposa una mena de caputxa.

Cordialment, Emmy Noether

Emmy Noether

Al cap d'una setmana d'aquesta carta, concretament el 14 d'abril de l'any 1935, Hasse s'assabentava que Emmy Noether havia mort per causa d'una intervenció quirúrgica a l'hospital de Bryn Mawr.

A la Universitat de Göttingen i des del curs 2001–2002 funciona una càtedra de matemàtiques per a professores visitants, que porta el nom d'Emmy Noether i que la universitat descriu d'aquesta manera:

En honor de la gran matemàtica Emmy Noether, la Facultat de Matemàtiques de la Universitat de Göttingen ha creat una càtedra de professora visitant d'acord amb la científica que va estudiar, ensenyar i fer recerca a Göttingen des de 1915 fins a 1933. Un cop l'any, la Facultat concedeix la càtedra Emmy Noether a una matemàtica de relleu, la qual visitarà Göttingen entre 3 i 4 setmanes per a presentar un camp actual de recerca en conferències i seminaris.

En la producció d'Emmy Noether es distingeixen tres etapes, no només cronològiques sinó de continguts. En la primera etapa, de 1908 a 1919, el seu interès se centrà en la teoria d'invariants, el problema invers de la teoria de Galois i el càlcul de variacions. En la segona etapa, de 1920 a 1926, es dedicà a l'estudi dels anells commutatius i a la teoria d'ideals. En aquest període preparà també l'edició de l'obra de Dedekind. En la tercera etapa, de 1927 a 1935, Emmy Noether treballà en sistemes hipercomplexos i en el desenvolupament de la teoria de les representacions dels grups, com un cas particular de la teoria de mòduls.

Podem consignar els treballs següents a la primera etapa:

Noether, E.: Über die Bildung des Formensystems der ternären biquadratischen Formen. *J. reine u. angew. Math.* **134** (1908), p. 23–90.

Aquesta extensa publicació conté la seva tesi. Gordan, el seu director, havia obtingut un sistema complet format per 54 invariants per a la forma quàrtica particular $X_1^3 X_2 + X_2^3 X_3 + X_3^3 X_1$. (Del seu director de tesi, Emmy Noether en diria que era un algoritmista.) Ella proporciona un sistema complet d'invariants per a qualsevol forma quàrtica en tres variables. En la seva tesi, Emmy Noether calcula sistemes complets d'invariants que contenen més de 300 fórmules. Indirectament, és possible que el seu interès posterior per la recerca d'estructures algebraiques i per principis generals fos motivat per l'esforç de càlcul tan extraordinari que l'elaboració de la tesi li portà.

Noether, E.: Gleichungen mit vorgeschriebener Gruppe. *Math. Ann.* **78** (1918), p. 221–229.

Aquest treball donà lloc a l'anomenat problema de Noether, en el context del problema invers de la teoria de Galois. Donat un grup finit G que opera en una extensió transcendent pura $k(X_1, \dots, X_n)|k$, es tracta de trobar condicions sobre G que permetin afirmar que l'extensió proporcionada pel cos d'invariants $k(X_1, \dots, X_n)^G|k$ és, també, transcendent pura. Emmy Noether demostrà que això és així per a $n \leq 4$. L'any 1969, Swan en trobà un contraexemple per a $n = 47$ i G un grup cíclic d'aquest ordre. El problema de Noether és encara avui motiu d'una intensa recerca.

Noether, E.: Invariante Variationsprobleme. *Nachr. v. d. Gesellsch. d. Wiss. zu Göttingen*. (1918), p. 235–257. Vorgelegt von F. Klein.

Aquest treball fou presentat, per ella, a la Societat de Matemàtiques de Göttingen i, per Klein, a la Societat de Ciències de Göttingen, que no l'acceptà mai entre els seus membres, per la seva condició de dona. Constitueix la contribució d'Emmy Noether a la física. En el treball hi ha el famós teorema de Noether segons el qual tot sistema dinàmic invariant per l'acció d'un grup de Lie de n paràmetres admet n invariants, o quantitats conservades, en el decurs de la seva evolució. D'aquest teorema se n'han fet posteriorment múltiples versions i generalitzacions. En teoria de camps, el teorema descriu quina és la quantitat que es conserva quan es coneix el grup de simetries de l'equació en derivades parcials definidora del camp (cf. més avall).

Els principals treballs de la segona etapa són:

Noether, E.: Idealtheorie in Ringbereichen. *Math. Ann.* **83** (1921), p. 24–66.

Noether, E.: Abstrakter Aufbau der Idealtheorie im algebraischen Zahl und Funktionenkörpern. *Math. Ann.* **96** (1927), p. 26–61.

En la tercera etapa, s'hi inscriuen els articles següents:

Noether, E.; Brauer, R.: Über minimale Zerfällungskörper irreduzibler Darstellungen. *Sitz. Ber. d. Preuss. Akad. d. Wiss.* (1927), p. 221–228. Vorgelegt von I. Schur.

El treball de Brauer i Noether fa referència als graus dels cossos neutralitzadors minimalis d'una àlgebra simple. Hi demostren que tots els cossos K_n cíclics sobre $\mathbb{Q}$, de grau 2^n , i en els quals -1 és una suma de dos quadrats, són cossos neutralitzadors minimalis sobre $\mathbb{Q}$ del cos dels quaternions

$$\left(\frac{-1, -1}{\mathbb{Q}} \right).$$

Demostren que si $2^n \mid (p-1)$, p primer, i el cos $K_n \subseteq \mathbb{Q}(e^{2\pi i/p})$ és tal que $[K_n : \mathbb{Q}] = 2^n$, aleshores K_n és un cos neutralitzador minimal del cos dels quaternions, cíclic de grau 2^n . Per tant, d'aquests n'hi ha infinits i el seu grau tendeix a infinit.

Noether, E.: Hyperkomplexe Größen und Darstellungstheorie. *Math. Z.* **30** (1929), p. 641–692.

Aquesta publicació conté l'aportació més significativa de Noether a l'estudi de les àlgebres i de les seves representacions. En ella, Noether retroba el teorema de Skolem (de l'any 1927) segons el qual els automorfismes de les àlgebres simples són tots interns, i dóna compte, per primera vegada, de fenòmens lligats a la inseparabilitat d'extensions del cos base. S'hi demostra la semisimplicitat de l'anell de grup $K[G]$, quan $\text{car}(K) \nmid \#G$ (teorema de Maschke

(1899)) i que el nombre de representacions absolutament irreductibles d'un grup finit G és igual al nombre de classes de conjugació de G .

A la història de les matemàtiques de Bourbaki [44], aquest treball és valorat en els termes següents:

Krull (1926) havia fet el lligam entre el concepte de grup abelià amb operadors i representacions lineals de grups; punt de vista generalitzat a àlgebres i desenvolupat amb detall per E. Noether en un treball fonamental de l'any 1929 que, per la importància de les idees introduïdes i per la claredat de l'exposició, mereix figurar, al costat de la memòria de Steinitz sobre els cossos commutatius, com un dels pilars de l'àlgebra lineal moderna.

N. Bourbaki: Éléments d'histoire des mathématiques

A fi de fer-nos càrrec de manera més precisa d'aquesta aportació de Noether, en detallem el contingut:

Capítol I. Fonaments de teoria de grups

1. Grups amb operadors. 2. Els teoremes d'isomorfia. 3. Sèries de composició. 4. Producte directe i interseccions. 5. Grups completament reductibles. 6. Mòduls respecte de cossos. Sistemes hipercomplexos. 7. Matrius.

Capítol II. Teoria no commutativa d'ideals

8. Teorema d'homomorfia per a anells. 9. Elements idempotents. Descomposició en suma directa d'ideals per la dreta. 10. Descomposició en ideals bilaterals. 11. El centre. 12. Ideals nilpotents. 13. Anells completament reductibles. 14. Anells simples pels dos costats, completament reductibles i amb element unitat.

Capítol III. Teoria de mòduls i de representacions

15. Representacions i mòdul de representació. 16. Representacions reductibles. 17. Descomposició en suma directa de mòduls de representació sobre anells amb element unitat. 18. Teoria de mòduls i de representacions sobre anells completament reductibles. 19. Els factors de composició simples per a mòduls i mòduls de representacions.

Capítol IV. Representacions de grups i de sistemes hipercomplexos

20. Ordenació de sistemes hipercomplexos. 21. Extensió del cos base. Les representacions del centre. 22. Aplicació als grups abelians. 23. Determinant d'un sistema hipercomplex. 24. Traçes i caràcters. 25. Discriminants. 26. Ordenació de l'anell de grup.

Hasse havia provat que tota àlgebra de divisió central sobre un cos de nombres $\mathfrak{p}$ -àdics és cíclica i Artin havia fet notar que aquest era un resultat que podia molt bé ésser

vàlid en el cas dels cossos de nombres. Noether i Hasse decidiren estudiar aquest problema a fi de, en cas de resoldre'l, enviar-lo al número especial de la *Revista de Crelle* que es preparava amb motiu del 70è aniversari de Hensel. Roquette ha recopilat en un llibre [328] les dificultats que ambdós matemàtics tingueren per a provar aquest resultat. Veient que se'ls acabava el termini per a presentar el treball, demanaren ajut a Brauer, qui aportà la idea del final de la prova. D'aquesta manera es gestà la publicació

Brauer, R.; Hasse, H.; Noether, E.: Beweis eines Hauptsatzes in der Theorie der Algebren. *J. reine u. angew. Math.* **167** (1932), p. 399–404.

Els seus autors inicien el treball amb les paraules següents:

Finalment, els nostres afanys conjunts han pogut demostrar que se satisfà el teorema següent, el qual és important per a la teoria relativa a l'estructura de les àlgebres sobre els cossos de nombres algebraics, així com també per a qüestions de fonament.

Teorema principal. *Tota àlgebra de divisió normal sobre un cos de nombres algebraics és cíclica (o, com també es diu, de tipus Dickson).*

Observem que, en aquella època, s'anomenaven normals les àlgebres que avui es designen amb el nom de centrals. La demostració original del teorema de Brauer-Hasse-Noether compta amb tres reduccions:

La reducció primera és deguda a Hasse. Consisteix a veure que, per a demostrar que tota àlgebra de divisió cen-

tral sobre un cos de nombres és cíclica, n'hi ha prou amb provar el teorema següent.

Teorema 1. *Tota àlgebra A central simple sobre un cos de nombres Ω que descompongui localment arreu, descompon sobre Ω . És a dir, si, per a tot $\mathfrak{p}$, $[A \otimes_{\Omega} \Omega_{\mathfrak{p}}] = [\Omega_{\mathfrak{p}}]$ en $\text{Br}(\Omega_{\mathfrak{p}})$, aleshores $[A] = [\Omega] \in \text{Br}(\Omega)$.*

La reducció segona és deguda a Brauer. Consisteix a veure que, per a demostrar el teorema 1, n'hi ha prou amb provar el resultat següent.

Teorema 2. *Tota àlgebra A central simple sobre un cos de nombres Ω que descompongui localment arreu, i amb un cos neutralitzador resoluble sobre Ω , descompon sobre Ω .*

La reducció tercera és deguda a Emmy Noether i també, independentment, a Brauer. Consisteix a veure que, per a demostrar el teorema 2, n'hi ha prou amb provar la simplificació següent.

Teorema 3. *Tota àlgebra A central simple sobre un cos de nombres Ω que descompongui localment arreu, i amb un cos neutralitzador de grau primer sobre Ω , descompon sobre Ω .*

D'aquest teorema, Noether en proporciona dues demostracions diferents. Una es basa en resultats de Hasse i l'altra en resultats de Hilbert i de Furtwängler.

El treball fou redactat per Hasse i, en ell, hi trobem el paràgraf següent:

En connexió amb el teorema de la norma nosaltres remarquem, a més, que s'ha d'interpretar el teorema 1 com la formulació correcta d'aquell teorema en casos més generals (també no

abelians), ja que, com mostrà Hasse, la seva generalització literal no és correcta en general.

Aquest paràgraf recull una idea original d'Emmy Noether (cf. *nosaltres remarquem*). En el cas de les extensions cícliques, se sabia la validesa del principi local-global per a les normes; però aquest principi deixava de satisfer-se per a les normes d'extensions més generals, tal com Hasse havia posat de manifest amb exemples de normes locals en totes les places d'un cos de nombres per a una extensió donada, que no eren normes globals per a aquella extensió. En canvi, Noether insistí en el fet que la generalització del principi local-global nòrmic calia formular-la amb àlgebres, tal com resultà ésser cert, segons el teorema 1 anterior.

En el mateix treball, s'hi troben moltes altres consideracions i resultats. Entre aquests, la resposta a una pregunta de Schur formulada l'any 1906:

Teorema. *Totes les representacions absolutament irreducibles d'un grup finit G d'ordre n són realitzables en el cos de les arrels n^h -èsimes de la unitat, sempre que h sigui prou gran.*

El teorema fou reproduït per Deuring en el seu llibre *Algebren* [81].

Un altre dels treballs cabdals de Noether en àlgebra no commutativa és

Noether, E.: Nichtkommutative Algebren. *Math. Z.* **37** (1933), p. 514–541.

Noether hi considera per primera vegada representacions lineals (per l'esquerra i per la dreta) d'àlgebres simples A

en anells de matrius sobre cossos no commutatius D , D^0 . Hi demostra teoremes d'estructura d'àlgebres simples i semisimples. Hi desenvolupa una teoria de Galois per a àlgebres simples i hi simplifica una demostració d'un resultat de Köthe segons el qual tota àlgebra simple admet un cos de descomposició minimal que és separable. A més, tots els resultats es discuteixen en qualsevol característica.

Noether, E.: Hyperkomplexe Systeme in ihren Bezeichnungen zur kommutativen Algebra und Zahlentheorie. *Verhandl. Intern. Math. Kongress Zürich* **1** (1932), p. 189–194.

El treball resumeix la seva intervenció en el Congrés Internacional de Zuric, com a conferenciant plenària. En aquest treball trobem allò que Emmy Noether anomena “Principi de l'aplicació de la no-commutativitat en la commutativitat”:

Mitjançant la teoria d'àlgebres, s'intenta aconseguir expressions senzilles i invariants de fets coneguts sobre formes quadràtiques o sobre cossos cíclics; és a dir, fets tals que només depenen de propietats purament estructurals d'àlgebres. Aleshores, un cop aquestes expressions invariants s'han demostrat, una transferència d'aquests fets a cossos galoisians qualssevol cau pel seu propi pes.

En aquesta exposició, Noether presenta un resum de les seves aportacions principals i d'aportacions de Brauer, Hasse, Chevalley i Speiser en el context de la teoria d'àlgebres.

Noether, E.: Der Hauptgeschlechtssatz für relativ galoische Zahlkörper. *Math. Ann.* **108** (1933), p. 411–419.

Els resultats obtinguts en aquest treball foren reproduïts en el text de Deuring *Algebren* [81]. Es tracta de teoremes d'Emmy Noether sobre sistemes de factors. Donada una extensió de Galois $L|K$ de cossos de nombres, Noether defineix el producte creuat del grup de classes d'ideals de L pel grup de Galois $G = \text{Gal}(L|K)$

$$\text{Cl}(L) \cdot G.$$

Expressa els productes creuats anteriors en termes de sistemes de factors, els classifica, i analitza els que proporcionen la classe trivial. Amb l'ús de sistemes de factors, obté una demostració alternativa del principi local-global de Hasse relatiu al grup de Brauer d'un cos de nombres.

Els resultats de Noether, Hasse i Brauer relatius al grup de Brauer d'un cos local i d'un cos global se solen expressar avui de la manera següent (per comoditat, ens limitarem únicament al cas dels cossos de nombres i dels seus completats).

Siguin K un cos de nombres i $\mathcal{O}_K$ el seu anell d'enters. Donat un ideal primer $\mathfrak{p}$ de $\mathcal{O}_K$, existeix un isomorfisme

$$\text{inv}_{\mathfrak{p}} : \text{Br}(K_{\mathfrak{p}}) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}.$$

Si $\mathfrak{p}$ és un primer real de K , existeix un isomorfisme

$$\text{inv}_{\mathfrak{p}} : \text{Br}(K_{\mathfrak{p}}) \xrightarrow{\sim} \{0, \frac{1}{2}\} \subseteq \mathbb{Q}/\mathbb{Z}.$$

Si $[A] \in \text{Br}(K_{\mathfrak{p}})$, l'element $\text{inv}_{\mathfrak{p}}[A]$ s'anomena el seu invariant de Hasse.

El grup de Brauer $\text{Br}(K)$ es caracteritza per l'existència d'una successió exacta

$$0 \rightarrow \text{Br}(K) \rightarrow \bigoplus_{\mathfrak{p}} \text{Br}(K_{\mathfrak{p}}) \rightarrow \mathbb{Q}/\mathbb{Z} \rightarrow 0,$$

on $\text{inv} := \sum \text{inv}_{\mathfrak{p}}$.

Des dels anys 1930, l'avenç més important que s'ha produït en l'estudi del grup de Brauer d'un cos és el teorema de Merkurjev-Suslin, de l'any 1982. El teorema descriu la n -torsió del grup de Brauer d'un cos qualsevol quan aquest conté les arrels n -èsimes de la unitat.

Teorema. (Merkurjev-Suslin, 1982) *Sigui F un cos arbitrari que contingui una arrel primitiva n -èsima de la unitat ζ . Existeix un isomorfisme, dit de residus nòrmics,*

$$R_{F,n} : K_2(F)/nK_2(F) \rightarrow H^2(F, \mu_n^2) \simeq \text{Br}(F)[n]$$

$$\{a, b\} \mapsto [A_{\zeta}(a, b)]$$

on $A_{\zeta}(a, b)$ és la F -àlgebra (central, simple i cíclica) definida per

$$A_{\zeta}(a, b) = \langle i, j : i^n = a, j^n = b, ij = \zeta ji \rangle.$$

El teorema anterior té moltes conseqüències. Per a més informació sobre aquestes i la seva demostració, es pot consultar el llibre *Groups de Brauer de cossos (Brauergruppen von Körpern)* [225], d'Ina Kersten. (Kersten es doctorà amb Witt; és, per tant, una néta científica d'Emmy Noether. Des de 2003, Kersten és la degana de la Facultat de Matemàtiques i Ciències de la Computació de la Universitat de Göttingen.)

Durant els anys 1950, Artin i alguns membres de la seva escola començaren la traducció de la teoria de cossos de classes en termes de cohomologia galoisiana. Recordem que Artin havia emigrat també a Amèrica i que dos dels seus deixebles foren Lang i Tate. Per a parlar d'aquestes traduccions, començarem per esmentar uns resultats generals de cohomologia de grups. (Per $\widehat{H}^i$ denotem els grups de cohomologia modificats o de Tate.)

Teorema. (Tate, 1952) *Siguin G un grup finit i C un G -mòdul. Suposem que per a tots els subgrups H de G se satisfan les condicions següents:*

$$(a) \quad H^1(H, C) = 0.$$

$$(b) \quad H^2(H, C) \text{ és un grup cíclic d'ordre } \#H.$$

Aleshores, per a tot $r \in \mathbb{Z}$, existeix un isomorfisme

$$\widehat{H}^r(G, \mathbb{Z}) \rightarrow \widehat{H}^{r+2}(G, C),$$

obtingut per cup producte amb la classe fonamental.

En una carta datada el 2 de juny de 1931, Emmy Noether comentava a Hasse l'arribada imminent de Herbrand, un jove doctor que en aquells moments estava treballant amb Artin. Prèviament, Herbrand havia presentat una tesi en lògica matemàtica.

Després de la seva estada a Göttingen, Herbrand féu una excursió als Alps, en el decurs de la qual trobà la mort en un accident. El 24 d'agost de 1931, Noether comentava a Hasse que no es podia treure del cap la mort de Herbrand.

En teoria de nombres, Herbrand és conegut pel teorema de Herbrand-Ribet, relatiu a l'estructura galoisiana del grup de classes d'ideals del cos ciclotòmic $\mathbb{Q}(\zeta_p)$, per a p un nombre primer. I, també, per l'anomenat quocient de Herbrand en cohomologia de grups:

Proposició. (Herbrand) *Siguin G un grup cíclic finit i M un G -mòdul amb cohomologia finita. Siguin*

$$h(M) := \frac{\#\widehat{H}^0(G, M)}{\#\widehat{H}^1(G, M)}.$$

Aleshores,

- (a) $h(M)$ és multiplicatiu respecte de successions exactes.
- (b) $h(M) = 1$ per a tot G -mòdul M finit.

Quan els resultats de cohomologia de grups s'apliquen a grups de Galois, s'obtenen teoremes relatius a cohomologia galoisiana. El teorema següent proporciona una interpretació del teorema de la base normal en termes de grups de cohomologia de Tate, atès que aquest teorema ens diu que el grup additiu L d'una extensió de Galois $L|K$, de grup de Galois G , és un G -mòdul induït:

Teorema. (Speiser, 1916) *Per a tota extensió de Galois $L|K$ se satisfà que*

$$\widehat{H}^n(\mathrm{Gal}(L|K), L) = 0, \quad \text{per a tot } n \in \mathbb{Z}.$$

D'altra banda, donada una extensió de Galois $L|K$, el grup de Brauer relatiu

$$\mathrm{Br}(L|K) := \ker(\mathrm{Br}(K) \rightarrow \mathrm{Br}(L)), \quad [A] \mapsto [A \otimes_K L],$$

admet la interpretació cohomològica següent:

$$\mathrm{Br}(L|K) \simeq H^2(\mathrm{Gal}(L|K), L^*).$$

A més, si $L|K$ és cíclica,

$$\mathrm{Br}(L|K) \simeq K^*/N_{L|K}(L^*),$$

la qual cosa permet recuperar, en el cas cíclic, el principi nòrmic local-global.

Donat un cos de nombres L , denotem per $\mathbb{A}_L$ el seu anell d'adeles, per $\mathbb{I}_L := \mathbb{A}_L^*$ el grup d'ideles corresponent, i per $\mathbb{C}_L := \mathbb{I}_L/L^*$ el grup de classes d'ideles. Aleshores, el teorema 90 de Hilbert i la generalització d'aquest deguda a Emmy Noether es reinterpreten com

Teorema. (Emmy Noether) *Per a tota extensió de Galois $L|K$ se satisfà que*

- (a) $H^1(\mathrm{Gal}(L|K), L^*) = 0$.
- (b) $H^1(G, \mathbb{C}_L) = 0$, si L i K són cossos de nombres.

Finalment, el teorema de Tate abans esmentat i la determinació de la cohomologia de les classes d'ideles dels cossos de nombres permeten deduir la llei de reciprocitat d'Artin:

Teorema. (Artin-Tate, 1961) *Siguin $L|K$ una extensió de Galois de cossos de nombres i $G = \mathrm{Gal}(L|K)$. Aleshores,*

- (a) $H^1(G, \mathbb{C}_L) = 0$.
- (b) $H^2(G, \mathbb{C}_L)$ és un grup cíclic d'ordre $\#G$.

(c) *Si L/K és abeliana, existeix un isomorfisme*

$$\phi : \mathbb{C}_K/N_{L|K}(\mathbb{C}_L) \xrightarrow{\sim} \text{Gal}(L|K)$$

els components locals del qual són donats pels símbols d'Artin.

La producció d'Emmy Noether fou editada íntegrament per l'editorial Springer, l'any 1983, sota la revisió de Jacobson [284]. L'obra aplega 43 treballs i, que coneguem, es tracta de l'única recopilació que Springer ha fet de l'obra d'una matemàtica:

Noether, E.: *Gesammelte Abhandlungen. Collected Papers*. N. Jacobson, ed. Springer Verlag, 1983; p. viii + 777.

3.11 Deuring

Max Friedrich Deuring (Göttingen, 9 de desembre de 1907; Göttingen, 20 de desembre de 1984)

Deuring es crià en un ambient liberal de la ciutat de Göttingen. L'any 1926 entrà a la Universitat de la seva ciutat natal, on féu tots els estudis de matemàtica i de física, llevat d'un semestre, que cursà a Roma.

Emmy Noether fou la directora de la seva tesi, que presentà l'any 1930 i defensà l'any 1931 amb el títol *Teoria aritmètica de les funcions algebraïques* (*Arithmetische Theorie der algebraischen Funktionen*).

En el seu treball *Teoria de la ramificació de cossos valorats* (*Verzweigungstheorie bewerteter Körper*), també de

l'any 1931, presentà una generalització a cossos valorats abstractes de la teoria de la ramificació de Hilbert, que aquest havia establert per als divisors primers d'extensions de Galois de cossos de nombres.

Aquell mateix any, Deuring se n'anà a la Universitat de Leipzig com a ajudant de van der Waerden, amb qui prèviament havia coincidit a Göttingen en el cercle de joves matemàtics que col·laboraven amb Emmy Noether.

L'any 1935, Deuring publicà el seu llibre *Älgebres* (*Algebren*), que fou el volum 41 de la col·lecció *Ergebnisse der Mathematik und ihrer Grenzgebiete* de Springer. Aquest tractat, juntament amb el del matemàtic americà A. A. Albert, *Estructura de les àlgebres* (*Structure of algebras*), publicat per la Societat Matemàtica Americana quatre anys més tard, popularitzà les bases per a l'estudi de l'àlgebra no commutativa.

Amb aquestes publicacions, Deuring pretengué, l'any 1935, presentar la seva habilitació a Leipzig. En aquells moments, Hasse era el director de l'Institut Matemàtic de la Universitat de Göttingen i l'encoratjà a presentar-la a Göttingen. Però en tots dos casos l'intent fou bloquejat pel Ministeri a causa de pressions de professors i estudiants simpatitzants del règim. Deuring restà a Leipzig, sense el dret d'impartir docència.

Després de diverses estades com a professor a les universitats de Jena, Posen, Göttingen, Marburg i Hamburg, iniciades l'any 1937, Deuring aconseguí, l'any 1950, una càtedra a la Universitat de Göttingen, que havia quedat vacant l'any 1946 quan obligaren Herglotz a renunciar-hi, per causa de malaltia greu. Deuring ocupà la càtedra fins

que esdevingué emèrit, l'any 1976; i encara continuà les seves activitats fins a la seva mort, l'any 1984.

L'any 1932, Hasse introduí la funció zeta per als cossos de funcions el·líptiques amb cos de constants finit; i l'any 1936, establí l'anàleg de la hipòtesi de Riemann relatiu a la situació dels seus zeros. El desig de Deuring d'estendre els resultats de Hasse a cossos de gènere més alt el conduí a la creació de la seva teoria de correspondències d'una corba; és a dir, a l'estudi de l'anell d'endomorfismes de la seva jacobiana. En particular, més endavant sobresortiria el treball del qual presentem la traducció: *Els tipus d'anells de multiplicadors dels cossos de funcions el·líptiques* (*Die Typen der Multiplikatorenringe elliptischer Functionenkörper*), de l'any 1941.

Aquests treballs sobre les funcions zeta de corbes serviren de base a Weil per a la formulació, l'any 1940, de les seves conjectures sobre el nombre de punts i les funcions zeta de les varietats definides sobre cossos finits. En el cas de les corbes, les conjectures foren provades pel mateix Weil en el seu llibre *Sobre les corbes algebraiques i les varietats que se'n dedueixen* (*Sur les courbes algébriques et les variétés qui s'en déduisent*), publicat l'any 1948. La demostració general de les conjectures de Weil no s'aconseguiria completar fins l'any 1974, per Deligne, després de la creació de la teoria d'esquemes i de la cohomologia ℓ -àdica per part de Grothendieck i els seus col·laboradors.

Deuring, igual que Hasse, també s'hagué d'ocupar en diverses ocasions de fenòmens de bona reducció de cossos de funcions algebraiques. En el seu treball *Reducció de cossos de funcions algebraiques segons divisors primers del cos de constants* (*Reduktion algebraischer Funktionenkörper nach*

Primdivisoren des Konstantenkörpers) hi desenvolupà aspectes de la teoria general que ja havia emprat en el treball de 1941. En els anys seixanta, aquesta teoria s'ampliaria en treballs de Shimura i Taniyama, i de Serre i Tate.

En el decurs del seu període com a professor de Göttingen, Deuring féu dues estades llargues a l'estranger: una a l'Institut d'Estudis Avançats de Princeton, als Estats Units, i l'altra a l'Institut Tata de Recerca Fonamental de Bombai, a l'Índia, on impartí diversos cursos. D'altra banda, Deuring havia participat en el cèlebre Simposi Internacional de Teoria Algebraica de Nombres de Tokyo Nikko, l'any 1955, on presentà una comunicació sobre les funcions zeta dels cossos de funcions el·líptiques amb multiplicació complexa. En aquest congrés, Taniyama formulà el problema que donaria peu més endavant a la conjectura de modularitat per a les corbes el·líptiques definides sobre $\mathbb{Q}$, dita també conjectura de Shimura, Taniyama i Weil i, avui, teorema de Wiles.

Si bé la producció matemàtica de Deuring és prou extensa i significativa, atès que hi podem comptar més de 50 títols, la seva obra completa no ha estat encara editada. La varietat de temes que s'hi tracten inclou aritmètica de cossos de funcions, especialment cossos de funcions el·líptiques —ramificació, mòduls, correspondències, normes, formes normals—; zeros i propietats de funcions zeta; teoria de la multiplicació complexa; consideracions sobre el teorema de densitat de Txebotarev; teoria de Galois i de representacions de grups; teoria d'àlgebres; nombre de tipus d'ordres maximals en àlgebres de quaternions —definides i de discriminant primer—; i també propietats de divisibilitat de mòduls singulars de cossos de funcions el·líptiques.

En aquesta llista de temes es pot intuir la gran influència que l'obra de Deuring exercí en els anys posteriors, i que arriba als nostres dies.

D'altra banda, i com a conseqüència de les lliçons impartides en la seva estada a l'Índia l'any 1958, quinze anys més tard Deuring publicà a Springer les *Lliçons sobre la teoria de funcions algebraiques d'una variable* (*Lectures on the theory of algebraic functions of one variable*).

Consta que, entre els anys 1948 i 1979, Deuring dirigí 42 estudiants de tesi, ja en qualitat de primer o de segon director. També fou membre de l'Acadèmia de Ciències i Literatura de Mainz, de l'Acadèmia de Ciències de Göttingen i de l'Acadèmia Germànica Leopoldina de Ciències Naturals.

3.12 Funcions L de corbes el·líptiques

L'any 1814, en l'entrada 146 i darrera del seu diari, Gauss havia escrit que si $a + bi$ és un nombre primer per al qual $a - 1 + bi$ és divisible per $2 + 2i$, aleshores el nombre de solucions de la congruència

$$1 \equiv x^2 + y^2 + x^2y^2 \pmod{a + bi},$$

incloent-hi les donades per $x = \infty$, $y = \pm i$ i $y = \infty$, és igual a $(a - 1)^2 + b^2$.

Sota punts de vista diferents i complementaris, l'afirmació anterior seria treballada per Eisenstein, Artin, F. K. Schmidt, Hasse, Deuring i Weil, entre d'altres, i constitueix

un dels punts de partida de l'estudi de les funcions zeta de les varietats algebraïques definides sobre cossos finits.

En denotar per N_p el nombre de solucions de la congruència

$$1 \equiv x^2 + y^2 + x^2y^2 \pmod{p},$$

i tenir present el resultat de Gauss, s'obté que

$$|p + 1 - N_p| = |a^b + b^2 + 1 - (a - 1)^2 - b^2| = |2a|,$$

la qual cosa, juntament amb la desigualtat evident,

$$2|a| < 2\sqrt{a^2 + b^2} = 2\sqrt{p},$$

proporciona la desigualtat $|p + 1 - N_p| < 2\sqrt{p}$. Com veurem tot seguit, aquest és un cas particular d'un teorema provat per Hasse l'any 1934.

Artin, en la seva tesi de 1920, i Deuring, en la seva de 1931, es dedicaren a l'estudi aritmètic de cossos de funcions algebraïques d'una variable. Deuring intentà estendre la teoria de Hilbert de la ramificació a aquests cossos. Artin conjecturà un anàleg de la hipòtesi de Riemann per a cossos de funcions el·líptiques de cossos de constants finits. Mentre que la hipòtesi de Riemann fa referència a les lleis que regeixen la distribució dels nombres primers, la conjectura d'Artin és equivalent a l'obtenció de fites uniformes per al nombre de divisors primers de grau 1 en el cas de les corbes el·líptiques sobre cossos finits.

La denominada hipòtesi de Riemann per a cossos de funcions el·líptiques definides sobre cossos de constants finits fou provada per Hasse l'any 1934 per a corbes que s'obtenen per reducció de corbes el·líptiques amb multiplicació complexa i, l'any 1936, per a corbes el·líptiques generals.

Hasse considerà un cos $K_0 = k_0(x, y)$ de funcions algebraiques d'una variable, de característica un nombre primer p , de gènere 1, definit sobre un cos de constants finit k_0 de $q = p^f$ elements. La funció zeta associada,

$$L(s) := 1 - \frac{(q + 1 - N_1)}{q^s} + \frac{q}{q^{2s}},$$

té en compte el nombre N_1 de divisors primers de primer grau de K_0 . Per mitjà del canvi de variable $z = q^s$, s'obté que

$$z^2 L(s) = P(z) = z^2 - (q + 1 - N_1)z + q.$$

El teorema de Riemann-Roch permet afirmar que

$$h = L(0) = P(1) = N_1,$$

on h és el nombre de classes de divisors de grau zero de K_0 .

Hasse considerà l'endomorfisme de K_0 definit per

$$\pi : (x, y) \mapsto (x^q, y^q);$$

i demostrà que satisfà una equació quadràtica de la forma

$$Q(\pi) = \pi^2 - \ell\pi + q, \quad \ell^2 \leq 4q.$$

El resultat final s'obté a partir de la igualtat dels polinomis $P(z) = Q(z)$, la qual proporciona la desigualtat

$$(q + 1 - N_1)^2 \leq 4q.$$

D'acord amb el model proporcionat per la funció zeta de Riemann en l'estudi dels nombres primers, Hasse associà a cada corba el·líptica $E|\mathbb{Q}$ una sèrie

$$L(E|\mathbb{Q}, s) := \prod_p \frac{1}{1 - a_p(E)p^{-s} + \psi(p)p^{1-2s}}, \quad \Re(s) > 3/2,$$

on

$$a_p := p + 1 - \#\tilde{E}(\mathbb{F}_p),$$

i ψ és el caràcter trivial mòdul un cert enter N_E . La sèrie L conté informació aritmètica de E , ja que en la seva definició hi intervenen els nombres de punts de les reduccions $\tilde{E}$ en els diferents primers. Atès que, pel teorema de Hasse, se satisfà que $|a_p| < 2p^{1/2}$, el producte infinit convergeix absolutament i uniformement sobre els compactes del semiplà definit per $\Re(s) > 3/2$. Per tant, $L(E, s)$ defineix una funció holomorfa i sense zeros en aquest semiplà.

Com en el cas de la funció zeta de Riemann, la funció L ha d'ésser completada amb factors proporcionats per la funció Γ d'Euler:

$$\Lambda(E|\mathbb{Q}, s) := N_E^{s/2} (2\pi)^{-s} \Gamma(s) L(E|\mathbb{Q}, s), \quad \Re(s) > 3/2.$$

La constant N_E es determina per mitjà dels símbols de Kodaira de les fibres de reducció dolenta de la corba, i es denomina el conductor aritmètic de E .

Per analogia amb la funció zeta de Riemann, Hasse i Weil conjecturaren, en els anys 1940–1950, que la funció completada $\Lambda(E|\mathbb{Q}, s)$ admetia una prolongació analítica a una funció entera i satisfieia una equació funcional de la forma

$$\Lambda(E|\mathbb{Q}, 2-s) = w(E) \Lambda(E|\mathbb{Q}, s), \quad s \in \mathbb{C}, \quad w(E) = \pm 1.$$

Per causa d'aquesta simetria, la regió $0 \leq \Re(s) \leq 2$ s'anomena la banda crítica, i $\Re(s) = 1$, la recta crítica de la funció L .

En els anys 1950–1960, la conjectura de Hasse-Weil fou demostrada per Deuring en el cas particular de les corbes

el·líptiques dotades de multiplicació complexa. El camí emprat per Deuring consistí a expressar la funció L d'aquestes corbes com a producte de la funció zeta de Riemann i de funcions L definides per caràcters de Hecke; per tant, ambdues prolongables analíticament. Els seus resultats foren presentats a Tokyo Nikko, l'any 1955.

Poc després es veuria que la conjectura de Hasse-Weil és certa per a totes les corbes el·líptiques $E|\mathbb{Q}$ parametritzables analíticament per funcions modulars. Atès que, tal com ara detallarem, en les darreres dècades s'ha pogut demostrar el teorema de modularitat segons el qual totes les corbes el·líptiques $E|\mathbb{Q}$ són parametritzables per funcions modulars, la conjectura de Hasse-Weil és certa.

L'any 1955, Taniyama intuï que la prolongació analítica —conjectural— de les sèries L de les corbes el·líptiques, que predeïa la conjectura de Hasse-Weil, podria molt ben ésser una conseqüència de propietats d'automorfia —també conjecturals— d'aquestes funcions. Taniyama, que aleshores comptava 27 anys, exposà la seva sospita en un problema d'una llista de problemes oberts que es distribuï als assistents al Simposi Internacional de Teoria Algebraica de Nombres celebrat a Tokyo Nikko que s'ha esmentat més amunt.

Una dècada més tard, el problema de Taniyama donà peu a la formulació de la conjectura de Shimura-Taniyama-Weil, segons la qual, donada una corba el·líptica $E|\mathbb{Q}$, de conductor aritmètic N , existeix un morfisme no constant, definit sobre $\mathbb{Q}$, de la corba modular $X_0(N)$ en la corba el·líptica E ,

$$X_0(N) \longrightarrow E.$$

Si això és així, la conjectura de Hasse-Weil és certa per a la corba $E|\mathbb{Q}$ atès que, aleshores, la funció $L(E|\mathbb{Q}, s)$ és la transformada de Mellin d'una forma modular de nivell N i pes 2. Per tant, $\Lambda(E|\mathbb{Q}, s)$ s'estén a una funció entera i satisfà una equació funcional en què el conductor analític coincideix amb el conductor aritmètic de E .

Potser seria ara el moment de posar de manifest un fet paradoxal. Des de Jacobi i Weierstrass, les corbes el·líptiques complexes havien estat parametritzades per funcions doblement periòdiques, segons una xarxa de períodes que provenia del pla euclidià. Des de Dedekind, Kronecker, Weber i Klein, les corbes modulars es parametritzaven per funcions periòdiques segons una xarxa de períodes que provenia del pla hiperbòlic. Shimura-Taniyama-Weil deia aproximadament que, independentment de l'anàlisi, hi havia unes funcions polinòmiques de coeficients racionals que lligaven els dos mons (sorprenent!). En els anys 1960–1970, una sèrie de càlculs que es portaren a terme amb l'ajut dels primers ordinadors serviren per a convèncer, fins i tot els més escèptics, que la conjectura de Shimura-Taniyama-Weil podia molt ben ésser certa.

L'enrenou s'organitzà l'any 1986 gràcies a un treball de Frey [129], publicat en el número 1 d'una modesta revista de la Universitat de Saarbrücken. En aquest treball, Frey —un deixeble de Roquette, que alhora ho havia estat de Hasse— s'adonava que si el Teorema de Fermat era fals, la conjectura de Shimura-Taniyama-Weil probablement també ho seria. Això anava de la manera següent: una solució no trivial de l'equació de Fermat, $a^p + b^p = c^p$, on $p > 2$ és un nombre primer, donaria lloc a una corba el·líptica

$$E_{a,b,c} : Y^2 = X(X - a^p)(X + b^p),$$

definida sobre $\mathbb{Q}$, per a la qual Frey sospitava que la funció $\Lambda(E_{a,b,c}, s)$ no es podria estendre a una funció entera, atesa la natura del conductor aritmètic de $E_{a,b,c}$ que ell havia calculat. Per tant, si Fermat era fals i Frey tenia raó, també serien falses la conjectura de Hasse-Weil i, de retruc, la conjectura de Shimura-Taniyama-Weil.

Treballs molt profunds de Serre [346] i de Ribet [314] donaren com a resultat que, efectivament, la sospita de Frey era correcta i que, per tant, de la validesa de la conjectura de Hasse-Weil se'n seguia la del Teorema de Fermat. La prova del Teorema de Fermat es remetia així a la de la prolongació analítica de les sèries L introduïdes per Hasse.

L'any 1995, Wiles [414] i Taylor–Wiles [380] provaren la conjectura de Shimura-Taniyama-Weil per a una classe de corbes el·líptiques $E|\mathbb{Q}$ que era prou àmplia per a contenir, en cas que existís, la corba $E_{a,b,c}$. Com que $E_{a,b,c}$ hauria estat alhora modular —segons Wiles i Taylor— i no modular —segons Frey, Serre i Ribet—, es concloïa clarament que Fermat tenia raó: la solució (a, b, c) no podia existir.

La demostració de Shimura-Taniyama-Weil per a totes les corbes el·líptiques $E|\mathbb{Q}$ es coneix avui com a teorema de modularitat i fou aconseguida finalment gràcies als treballs, a més dels esmentats de Wiles i de Taylor–Wiles, de Diamond [98], de Conrad–Diamond–Taylor [63], i de Breuil i altres [46]. Aquests autors estengueren suficientment el mètode de Wiles a fi de poder incloure en la demostració totes les corbes el·líptiques $E|\mathbb{Q}$. La demostració del teorema de modularitat de les corbes el·líptiques definides sobre el cos dels racionals és un dels resultats més espectaculars demostrats en teoria de nombres en els darrers anys.

3.13 Richert

Hans-Egon Richert (Hamburg, 1924; Blaustein, 25 de novembre de 1993)

Després que, en el període del Tercer Reich fos expulsat de l'escola pública per “inclinacions anglòfiles”, Richert hagué d'acabar els estudis secundaris en institucions privades. L'any 1946, després del servei militar i als 22 anys, pogué començar a estudiar matemàtiques a Hamburg, on es doctorà l'any 1950, dirigit per Deuring.

El mateix any 1950, Richert se n'anà a Göttingen com a ajudant de Deuring, quan aquest hi fou nomenat catedràtic. Allà, Richert hi obtingué l'habilitació l'any 1954, i fou encarregat de la biblioteca, una de les millors del país.

Després d'ocupar interinament una càtedra a Göttingen, li fou oferta una càtedra a la Universitat de Marburg, on contribuí de manera essencial a conformar l'Institut Matemàtic d'aquella universitat i dedicà una atenció especial a la seva biblioteca.

L'any 1972, Richert se n'anà a la (aleshores jove) Universitat d'Ulm, on fou el segon catedràtic del Departament de Matemàtiques. Allí hi estigué fins a la seva jubilació, com a emèrit, fet que es produí l'any 1991.

El camp d'interès de recerca per a Richert fou la teoria analítica de nombres. Contribuí de manera notable a la teoria additiva de nombres i, després, en mètodes de garbell. Així, per exemple, treballà en sèries de Dirichlet, sumabilitat de Riesz, l'anàleg multiplicatiu del teorema d'Erdős i Fuchs de l'any 1956, estimacions del nombre de grups abe-

lians no isomorfs, i fites per a sumes exponencials útils per a l'estimació del terme d'error en el teorema del nombre primer.

La seva col·laboració amb Halberstam, motivada pel seu interès comú en garbells i que s'inicià després de 1965, fou intensa i productiva i durà la resta de la seva vida. D'ella nasqué el llibre sobre mètodes de garbell [178] que ha esdevingut bàsic per a l'estudi d'aquesta part de la teoria analítica de nombres.

Richert fou durant molts anys un dels organitzadors de les reunions sobre teoria analítica de nombres que tenien lloc a Oberwolfach. Entre els anys 1961 i 1983 dirigí 8 tesis doctorals.

Capítol 4

Impacte del nacionalsocialisme

L'adveniment del nacionalsocialisme causà un final sobtat a l'atmosfera científica que les universitats i les institucions acadèmiques alemanyes havien forjat en el decurs de més de tres-cents anys.

4.1 Irrupció del règim nazi a la vida cultural i científica

Des de final del segle XIX, la població jueva d'Alemanya es veié incrementada amb prop de 80.000 persones que emigraren de Rússia per causa dels pogroms del règim dels tsars —dos milions més ho feren als Estats Units per la mateixa raó. En la seva major part s'incorporaren a la

classe proletària i molts participaren en la Primera Guerra Mundial com a membres de l'exèrcit alemany.

En finalitzar la guerra, molts jueus acceptaren i donaren suport a la República de Weimar. En aquest període, l'aportació jueva a la cultura és especialment rellevant. Entre els seus exponents podem citar, per exemple, Albert Einstein, Sigmund Freud, Fritz Lang, Else Lasker-Schüler, Arnold Schönberg o Kurt Weill. Entre els matemàtics, hi trobem Bernays, Bernstein, Courant, Dehn, Epstein, Hausdorff, Hensel, Landau, von Mises, Emmy Noether, Schur o Toeplitz.

Les lleis de Nuremberg de l'any 1935 establiren criteris estrictes per a classificar la població en funció de la seva ascendència jueva o no. D'acord amb aquestes lleis, les persones determinades com a jueves foren apartades de la vida cívica i els seus drets, restringits. Com a conseqüència, es produí una gran emigració de població alemanya —no només jueva— preferentment cap als Estats Units i Gran Bretanya, però també cap a Dinamarca o Suïssa.

Amb l'adveniment del règim nazi, la matemàtica estigué marcada per una politització radical creixent dirigida cap a la creació d'una *Matemàtica Alemanya* (*Deutsche Mathematik*). Un exponent en fou la creació d'una revista amb aquest mateix nom. Entre els que s'involucraren en el moviment trobem Bieberbach, Teichmüller i Vahlen, a Berlín; i Werner Weber, Hellmuth Kneser i Hasse, a Göttingen.

L'any 1930 la revista *Zentralblatt für Mathematik* ja havia començat a rebutjar censors jueus. Com a protesta, una quantitat important de censors d'Anglaterra i dels Es-

tats Units se'n donaren de baixa. Com ja s'ha dit, aquest fet propicià la creació de la revista *Mathematical Reviews*, amb objectius similars de revisió, per part de la Societat Matemàtica Americana.

A partir de l'any 1933, l'Acadèmia Leopoldina veié com els seus membres jueus n'eren expulsats; fins a l'any 1938, ho foren més de 70.

Durant el règim nazi, l'interès per la ciència bàsica experimentà un desprestigi considerable a favor d'una promoció decidida de la tècnica i dels aspectes més aplicats d'aquella. En aquest sentit, les Olimpíades de Berlín de l'any 1936 oferiren, a més de les transmissions radiofòniques, les primeres transmissions televisades directes, i es convertiren en un instrument impagable de propaganda per al règim. Els radars es feren presents en aplicacions diverses; la física teòrica, conduïda per Heisenberg, propicià l'avenç cap a l'experimentació nuclear; programes relatius a tecnologia aeroespacial foren liderats per von Braun; Alwin Walther fou dels primers a desenvolupar tècniques que avui es classificarien com d'arquitectura de computadors; i, entre els anys 1936 i 1938, Konrad Zuse ideà el Z1, el primer computador programable. També és ben conegut que estaven en possessió de la màquina Enigma, emprada en els conflictes bèl·lics per al xifratge de missatges. El fet que tots acabessin amb la salutació habitual del règim nazi propicià el desxifratge dels missatges per part d'Alan Turing i el seu equip de matemàtics de Bletchley Park.

4.2 Impacte a l'escola matemàtica de Berlín

A la conferència de Casablanca de 1943, Churchill i Roosevelt donaren el vistiplau, entre d'altres qüestions, als atacs aeris massius sobre Alemanya. En particular, Berlín, que havia estat la capital del Regne de Prússia (1701–1918), de l'Imperi Alemany (1871–1918), de la República de Weimar (1919–1933) i del Tercer Reich (1933–1945), fou, gairebé literalment, reduïda a cendres.

Després de la separació de la ciutat en quatre parts a la fi de la guerra, la part oriental de Berlín esdevingué la capital de la República Democràtica Alemanya, mentre que la capital de la República Federal Alemanya es traslladà a Bonn. La *Friedrich Wilhelms Universität* quedà situada a la part oriental, sota l'administració del règim soviètic, i s'anomenà simplement *Universität de Berlín* (*Universität Berlin*).

Les persones que manifestaven desacord amb les idees d'aquell règim marxista leninista foren separades de les seves funcions i condemnades a treballs forçats per part de tribunals militars; algunes, desaparegueren. En contraposició al fet que la vinculació familiar a la classe jueva havia estat motiu de rebuig per part del règim nazi, la vinculació familiar a la classe obrera era ara motiu suficient d'acceptació a la universitat, malgrat no estar en possessió d'una habilitació, per al professorat, o no tenir el diploma de l'ensenyament secundari, per a l'alumnat.

Com a reacció a aquesta política universitària, un grup de dotze persones, entre les quals hi havia tres estudiants,

un d'ells de doctorat, decidiren, el mes de gener de l'any 1948, iniciar les gestions per a l'establiment d'una nova universitat, lliure, a la part occidental de la ciutat. La *Universität Lliure de Berlín* (*Freie Universität Berlin*) fou fundada el 2 de setembre de 1948; a l'octubre, havia assolit la xifra de 5.000 estudiants matriculats; i al desembre, la seva biblioteca havia assolit la xifra de 350.000 llibres. S'iniciava, així, la recuperació científica de la ciutat.

4.3 Impacte a l'escola matemàtica de Göttingen

Abans de la Segona Guerra Mundial, la població jueva de Göttingen comptabilitzava unes 400 persones, molt poques de les quals pogueren sobreviure al genocidi. A la Universitat, la majoria del professorat jueu fou acomiadada i enviada a l'exili.

Ben aviat, Emmy Noether, Weyl i Courant emigraren cap a Amèrica. Noether i Courant ho feren per la seva condició de jueus; Weyl, per la de la seva esposa. Tots tres intentarien traslladar a institucions americanes l'esperit de Göttingen. Noether, al Col·legi de Bryn Mawr —per un temps relativament curt—; Weyl, a l'Institut d'Estudis Avançats de Princeton; i Courant, a l'Institut que ell mateix fundà, a Nova York, l'any 1935.

Entre els anys 1932 i 1937, el nombre d'estudiants de matemàtica o de física de Göttingen disminuï en un 90%. La biblioteca —que tant havia impressionat Gauss— també patí greuges greus, en tant que una part important del seu

contingut, considerada “de poca utilitat”, fou cremada pels nazis el 10 de maig de 1933.

Hilbert, que s’havia retirat de les tasques acadèmiques l’any 1930, romangué a Göttingen fins a la seva mort, ocorreguda l’any 1943. En patí totes les conseqüències d’aïllament i hagué d’assistir, impotent, a la davallada de la institució que ell tant havia contribuït a engrandir. Sembla que, l’any 1940, les úniques classes de matemàtica fonamental que s’impartien a Göttingen eren les de Herglotz i Kaluza.

Hasse romangué a Alemanya durant tot el conflicte bèl·lic; prengué les regnes de l’Institut Matemàtic de la Universitat de Göttingen en temps relativament difícils i col·laborà en la seva restauració un cop acabada la guerra.

Hausdorff, que era jueu i romangué a Göttingen, se suïcidà l’any 1942 a fi d’evitar la deportació a camps de concentració. El mateix havia fet Epstein, l’any 1939 a la ciutat de Dornbusch, per a evitar la tortura de la Gestapo.

Neugebauer, que tot i no ser jueu s’oposà al nacionalsocialisme des dels seus inicis, fou expulsat de la seva plaça acadèmica i emigrà als Estats Units. En certa ocasió deixà escrit: *Si no has sentit mai el so de les botes nazis darrere teu, al carrer, no pots comprendre la història del període.*

Una de les revistes més prestigioses del moment, *Mathematische Annalen* —fundada l’any 1868 i que havia tingut com a editors Klein i Hilbert—, així com també el *Jahresbericht* —editat per la Societat Matemàtica Alemanya— es convertiren en instruments de lluita pel poder. En ocasions s’arribà a proposar-ne l’exclusió d’autors estrangers.

La recentment creada revista *Deutsche Mathematik* aplegà els matemàtics més radicals.

En contraposició amb el que succeí a Berlín, la ciutat de Göttingen fou respectada pels bombardejos de la Segona Guerra Mundial —com ho serien, també, Oxford i Cambridge al Regne Unit—. De fet, poc després de la rendició alemanya, el mes de maig de 1945, la Universitat de Göttingen pogué reprendre de seguida les seves activitats; concretament, el mes de setembre de 1945, i fou la primera institució universitària alemanya a fer-ho.

L'any 1948 es fundà, a la ciutat de Göttingen, la Societat Max Planck, el primer president de la qual fou el físic Otto Hahn. Planck pogué viure a Göttingen els darrers anys de la seva vida i Heisenberg hi retornà com a professor des de 1947 a 1958. Després d'haver estat uns quants anys a l'Institut d'Estudis Avançats de Princeton, Siegel retornà també com a professor de Göttingen l'any 1951, càrrec que mantingué fins que es retirà, l'any 1959.

Sortosament, però, la feina feta per aquelles generacions de matemàtics, que crearen ininterrompudament durant gairebé dos segles, no fou en va. Les seves descobertes havien estat ja sembrades en les ments d'una munió de deixebles que, amb més o menys dificultats, portarien els ensenyaments dels seus mestres i col·legues cap a un continent nou. La matemàtica, i molt especialment l'aritmètica, trobà més enllà de l'Atlàntic un terreny favorable per a la seva fructificació. Allí, de la mà de matemàtics alemanys, austríacs, francesos, japonesos, anglesos, americans, belgues, hongaresos, canadencs, holandesos —o d'on fos— han sorgit teoremes i edificis matemàtics que, en paraules de Jacobi, són avui *un honor per a l'esperit humà*.

Part II

Antologia

Capítol 5

Riemann

L'obra *Sobre la quantitat de nombres primers per sota d'una quantitat donada* (*Über die Anzahl der Primzahlen unter einer gegebenen Grösse*) de Riemann, el manuscrit de la qual no arriba a sis pàgines, representà un canvi de paradigma en l'estudi dels nombres primers. En aquest treball, Riemann posà de manifest que les lleis que regeixen la distribució dels nombres primers depenen en gran part del comportament de la sèrie harmònica, quan aquesta s'estén a una funció de variable complexa.

5.1 1859: La memòria sobre els nombres primers

Donat un nombre complex $z \in \mathbb{C}$, denotarem per $\Re(z)$, $\Im(z)$ les seves part real i part imaginària, respectivament.

La funció zeta de Riemann es defineix a partir de la sèrie harmònica, però interpretada com una funció de variable complexa:

$$\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s} = \frac{1}{\Gamma(s)} \int_0^{\infty} \frac{x^{s-1}}{e^x - 1} dx, \quad s \in \mathbb{C}, \quad \Re(s) > 1.$$

La funció així definida és analítica per a $\Re(s) > 1$. La representació integral anterior permet la prolongació de la funció zeta a una funció meromorfa de $\mathbb{C}$. La funció estesa, $\zeta(s)$, té un únic pol en $s = 1$, que és simple i de residu igual a 1. En completar la funció zeta amb factors convenientes (en $p = \infty$), s'obté la funció

$$\widehat{\zeta}(s) := \frac{1}{2} s(s-1) \pi^{-\frac{s}{2}} \Gamma\left(\frac{s}{2}\right) \zeta(s).$$

En deformar convenientment el camí d'integració, Riemann obté l'equació funcional:

$$\widehat{\zeta}(s) = \widehat{\zeta}(1-s), \quad \text{per a tot } s \in \mathbb{C}.$$

Aquesta equació funcional posa de manifest que el comportament de $\zeta(s)$ per a $\Re(s) < 0$ està determinat pel comportament de $\zeta(s)$ per a $\Re(s) > 1$ i, per tant, pel producte d'Euler corresponent. Els valors de $\zeta(s)$ que aporten més informació són els situats a la banda crítica, definida per

$$0 \leq \Re(s) \leq 1.$$

L'eix de simetria de la banda crítica, o sigui la recta

$$\Re(s) = \frac{1}{2},$$

rep el nom de recta crítica.

L'equació funcional permet avaluar la funció zeta en els enters negatius, en els quals pren valors racionals. Concretament,

$$\zeta(-2m+1) = -\frac{B_{2m}}{2m}, \quad \zeta(-2m) = 0, \quad \text{per a tot } m \geq 1.$$

Les fórmules anteriors són equivalents a les fórmules donades per Euler. Fixem-nos que la funció zeta s'anul·la en els enters negatius parells; aquests zeros són els anomenats zeros trivials.

Riemann proporciona un esbós de la fórmula del producte

$$\widehat{\zeta}(s) = \widehat{\zeta}(0) \prod_{\rho} \left(1 - \frac{s}{\rho}\right),$$

en la qual ρ recorre els zeros de $\zeta(s)$ a la banda crítica.

La fórmula del producte per a la funció zeta sense completar s'escriu

$$\zeta(s) = \frac{e^{[\log(2\pi) - 1 - \gamma/2]s}}{2(s-1)\Gamma\left(1 + \frac{s}{2}\right)} \prod_{\rho} \left(1 - \frac{s}{\rho}\right) e^{\frac{s}{\rho}},$$

on γ és la constant d'Euler-Mascheroni:

$$\gamma = \lim_{n \rightarrow \infty} \left(1 + \frac{1}{2} + \cdots + \frac{1}{n} - \log n\right) = 0.577216 \dots$$

Se sospita que aquesta constant és un nombre irracional, però la seva irracionalitat no ha estat provada.

Els primers zeros no trivials de la funció zeta foren calculats a mà pel mateix Riemann, però no els inclogué en la memòria esmentada:

$$\rho_1 = \frac{1}{2} \pm i 14.13 \dots, \quad \rho_2 = \frac{1}{2} \pm i 21.02 \dots, \quad \rho_3 = \frac{1}{2} \pm i 25.01 \dots$$

Riemann establí que la funció zeta té una infinitat de zeros a la banda crítica, i donà una estimació del nombre de zeros d'altura fitada per T a la banda crítica:

$$N(T) := \#\{\rho : \zeta(\rho) = 0, 0 < \Im(\rho) \leq T\} \sim \frac{T}{2\pi} \log\left(\frac{T}{2\pi e}\right).$$

Així, a l'altura T , l'espaiat mitjà entre els zeros de ζ hauria de ser asimptòticament equivalent a $2\pi/\log T$.

Escrivim, d'acord amb Riemann:

$$\xi(t) := \pi^{-\frac{s}{2}} \Gamma\left(\frac{s}{2}\right) \zeta(s), \quad s = \frac{1}{2} + it.$$

Riemann fa el comentari següent sobre els zeros de $\xi(t)$ (cf. més avall, a la pàgina 231).

[...] i és molt probable que totes les arrels siguin reals. Certament, seria desitjable tenir una demostració més rigorosa d'aquest fet; tot i així, per ara he deixat de banda la cerca d'aquesta després d'alguns intents vans i escàpols, atès que sembla supèrflua per a l'objectiu immediat de la meua recerca.

Riemann

Es coneix com a *hipòtesi de Riemann* l'afirmació segons la qual tots els zeros no trivials de la funció zeta de Riemann es troben sobre la recta crítica:

$$(HR) \quad \zeta(\rho) = 0, \quad 0 \leq \Re(\rho) \leq 1 \quad \Rightarrow \quad \Re(\rho) = \frac{1}{2}.$$

El resultat central obtingut per Riemann en la seva memòria és una fórmula explícita per al càlcul de $\pi(x)$. A

partir del desenvolupament

$$\begin{aligned}\log \zeta(s) &= - \sum \log(1 - p^{-s}) = \\ &= \sum p^{-s} + \frac{1}{2} \sum p^{-2s} + \frac{1}{3} \sum p^{-3s} + \cdots ,\end{aligned}$$

vàlid per a $\Re(s) > 1$, Riemann escriu

$$\log \zeta(s) = s \int_0^\infty \Pi(x) x^{-s-1} dx, \quad \Re(s) > 1,$$

on

$$\Pi(x) := \pi(x) + \frac{1}{2}\pi(\sqrt[2]{x}) + \frac{1}{3}\pi(\sqrt[3]{x}) + \cdots .$$

Fixem-nos que la suma

$$\pi(x) = \sum_{n \geq 1} \frac{\mu(n)}{n} \Pi(x^{1/n}),$$

on μ denota la funció de Möbius, conté únicament un nombre finit de termes no nuls. Per a obtenir la fórmula explícita, Riemann utilitza inversió de Fourier, càlcul de residus i la fórmula d'inversió de Möbius. La fórmula en qüestió és

$$\begin{aligned}\Pi(x) &= \text{Li}(x) - \sum_{\Im(\rho) > 0} (\text{Li}(x^\rho) + \text{Li}(x^{1-\rho})) + \\ &+ \int_x^\infty \frac{dt}{t(t^2 - 1)\log t} + \log \widehat{\zeta}(0),\end{aligned}$$

vàlida per a tot $x > 1$.

Aquesta fórmula de Riemann permet connectar la quantitat de primers inferiors a una quantitat donada amb els

zeros de la funció zeta. El mateix Riemann observa que, en la fórmula

$$\pi(x) - \sum_{n \geq 1} \frac{\mu(n)}{n} \text{Li}(x^{1/n}) = \sum_{n=1}^N \sum_{\rho} \text{Li}(x^{\rho/n}) + O(1),$$

s'hi detecten tres tipus de termes:

- (a) Termes que no creixen quan x creix: inclosos en $O(1)$.
- (b) Termes que creixen quan x creix: $\text{Li}(x^{1/n})$.
- (c) Termes que creixen en valor absolut quan x creix, però que oscil·len en signe: $\text{Li}(x^{\rho/n})$.

Riemann designa amb el nom de periòdics els termes oscil·latoris. I interpreta que són els causants de les fluctuacions observades experimentalment en el nombre de primers dels diferents intervals.

La memòria de Riemann exercí i continua exercint una influència molt remarcable. Hadamard afirmà que havia necessitat tres dècades per a comprendre'n el contingut i que havia pogut demostrar totes les afirmacions de Riemann, llevat d'una: la hipòtesi de Riemann.

L'any 1892, Hadamard obtingué la descomposició de $\zeta(s)$ en forma de producte infinit, tal com havia predit Riemann:

$$\widehat{\zeta}(s) = \widehat{\zeta}(0) \prod_{\rho} \left(1 - \frac{s}{\rho}\right),$$

on ρ descriu els zeros de $\zeta(s)$ a la banda crítica i el producte es realitza en l'ordre creixent de $|\Im(\rho)|$.

L'any 1894, von Mangoldt demostrà el resultat, ja enunciat també per Riemann, sobre el nombre de zeros complexos d'altura fitada de la funció zeta:

$$N(T) = \frac{T}{2\pi} \log \left(\frac{T}{2\pi e} \right) + O(\log T).$$

La fórmula explícita de Riemann fou reescrita i provada per von Mangoldt en la forma

$$\psi(x) = x - \sum_{\rho} \frac{x^{\rho}}{\rho} - \frac{1}{2} \log \left(1 - \frac{1}{x^2} \right) - \log(2\pi), \quad x > 1.$$

L'any 1914, Hardy demostrà que $\xi(t)$ té una infinitat de zeros reals.

L'any 1942, Hardy i Littlewood demostraren que

$$N(T) \geq K T \log(T), \quad T \gg 0,$$

on $K > 0$ és una constant.

L'any 1896, Hadamard i de la Vallée Poussin demostraren de manera independent el teorema dels nombres primers:

$$\pi(x) \sim \frac{x}{\log x}, \quad x \rightarrow \infty.$$

Essencialment, el seu mètode consistí en l'estimació dels termes oscil·latoris de la fórmula explícita de Riemann. Un punt essencial en les demostracions d'ambdós autors estableix que la funció zeta no s'anul·la en els extrems de la banda crítica:

$$\zeta(1+it) \neq 0, \quad \text{per a tot } t \in \mathbb{R}.$$

La demostració de de la Vallée Poussin proporciona, a més, una fita del terme d'error:

$$|\pi(x) - \text{Li}(x)| = O(xe^{-\sqrt{c \log(x)}}).$$

Més generalment, es pot demostrar que l'absència de zeros a l'esquerra de la recta $\Re(s) = 1$ controla el terme d'error en el teorema dels nombres primers. Sigui $1/2 < \alpha < 1$. Si $\zeta(s) \neq 0$ per a $\alpha < \Re(s) < 1$, aleshores $\vartheta(x) - x = O(x^\alpha (\log x)^2)$. Recíprocament, si $\vartheta(x) - x = O(x^\alpha (\log x)^\beta)$, aleshores $\zeta(s) \neq 0$ per a $\alpha < \Re(s) < 1$. Per tant, la hipòtesi de Riemann és certa si, i només si,

$$|\pi(x) - \text{Li}(x)| = O(x^{1/2} \log x).$$

Una simplificació apreciable en la demostració del teorema dels nombres primers es produí l'any 1980, gràcies a un teorema de Newman.

L'anomenada conjectura de Hilbert–Pólya forma part d'una creença popular. Proposa una interpretació espectral dels zeros no trivials de la funció zeta de Riemann. Més concretament, hauria d'existir un operador lineal Δ els valors propis del qual es relacionessin amb els zeros no trivials de la funció zeta tal com s'indica:

$$\text{zero de } \zeta \quad \longleftrightarrow \quad \text{valor propi de } \Delta$$

$$\rho = \frac{1}{2} + i\gamma \quad \longleftrightarrow \quad \lambda = \rho(1 - \rho) = \frac{1}{4} + \gamma^2.$$

L'operador Δ seria positiu i s'escriuria com $\Delta = D(1 - D)$, essent $i(D - \frac{1}{2})$ un operador lineal autoadjunt.

Atès que el nombre de zeros de la funció zeta de Riemann és infinit, si fos certa l'atribució que es fa a Hilbert de

la interpretació espectral dels zeros de la funció zeta, Hilbert hauria estat pensant en un espai vectorial complex, de dimensió no finita, dotat d'un producte hermític, complet (en un espai de Hilbert!) i en certs operadors d'espectre discret positiu.

Es diu que Hilbert anomenà *espectre* el conjunt dels valors propis d'un operador hermític per analogia amb les línies, anomenades espectre, produïdes per les freqüències de radiació dels àtoms. Més endavant, la mecànica quàntica confirmaria aquesta interpretació: les línies espectrals es corresponen amb els valors propis d'operadors hermítics que proporcionen el hamiltonià de sistemes mecànic-quàntics. (Born, Heisenberg i von Neumann estudiaren amb Hilbert a Göttingen.)

La interpretació espectral dels zeros de la funció zeta ha resultat certa en un context molt diferent: per a certes funcions zeta sorgides de l'estudi de varietats algebraïques definides sobre cossos finits. A tota varietat X , algebraica, projectiva, llisa, definida sobre el cos finit $\mathbb{F}_q$ de $q = p^f$ elements, on p és un primer, se li pot associar una funció zeta de variable complexa,

$$Z(X, q^{-s}),$$

que té cura del nombre de punts de la varietat en el cos $\mathbb{F}_q$ i en totes les seves extensions algebraïques. Aquests punts poden ésser interpretats com a punts fixos de l'anomenat automorfisme de Frobenius:

$$X(\mathbb{F}_{q^n}) = X(\overline{\mathbb{F}}_{q^n})^{\text{Frob}_{q^n}}.$$

La funció $Z(X, q^{-s})$ és una funció racional en q^{-s} ; satisfà una equació funcional; i satisfà l'anàleg de la hipòtesi

de Riemann. Aquests resultats foren obtinguts per Artin, Hasse, Weil, Grothendieck i Deligne, entre d'altres.

La hipòtesi de Riemann, provada en el context de les varietats algebraiques sobre cossos finits per Deligne, està en la base dels principals resultats obtinguts els darrers anys en l'estudi d'equacions diofantines. Els espais vectorials predits per Hilbert provenen aquí de la cohomologia ℓ -àdica de la varietat, que proporciona espais vectorials en característica zero i de dimensió finita. L'operador és l'automorfisme de Frobenius en operar a la cohomologia. Deligne aconsegueix la demostració de la hipòtesi de Riemann en característica p a partir d'una fórmula de traces (de Lefschetz) anàloga a la fórmula explícita de Riemann. L'acció d'un grup de monodromia associat a certes famílies de varietats és, també, un ingredient essencial de la prova.

Les dificultats vençudes en característica p per a provar la hipòtesi de Riemann no són, però, directament traslladables al cas de la característica zero, on els espais vectorials implicats són de dimensió no finita.

Una altra funció zeta, introduïda per Selberg l'any 1957 per a superfícies de Riemann convenientment uniformitzades, satisfà, també, la hipòtesi de Riemann. Per a provar aquest resultat, Selberg demostrà prèviament una fórmula de traces per al grup especial lineal $SL(2, \mathbb{R})$. Els resultats de Selberg han estat objecte de generalitzacions diverses. En aquest cas, l'operador és l'operador de Laplace–Beltrami i els espais vectorials en què opera són de dimensió no finita.

A les taules 5 i 6 donem compte d'algunes funcions zeta, de l'àmbit al qual pertanyen, i d'algunes de les seves

propietats més notables. Hi incloem els noms d’alguns dels seus investigadors.

	Funcions zeta i funcions L aritmètiques	
Riemann	$\zeta(s)$	nombres enters; nombres primers; equació funcional; fórmula explícita
Dirichlet	$L(\chi, s)$	cossos ciclotòmics; progressions aritmètiques; equació funcional; fórmula explícita
Dedekind	$\zeta(K, s)$	cossos de nombres; ideals primers; equació funcional; fórmula explícita
Artin	$L(\rho, s)$	representacions de Galois; distribució d’ideals primers; fórmula explícita
p -àdiques		Leopoldt; Iwasawa; cossos de nombres abelians i no abelians
	Funcions zeta i funcions L aritmètico-geomètriques	
Hasse–Weil	$Z(X, q^{-s})$	varietats sobre cossos finits; fórmula de Lefschetz; equació funcional; HR
Serre	$\zeta(X, s), L(X, s)$	Hasse–Weil; teoria de Hodge; esquemes aritmètics
Grothendieck	$L(M, s)$	motius
p -àdiques		varietats algebraïques sobre cossos de nombres; motius
	Funcions L automorfes	
Hecke	$L(\psi, s)$	grups de classes d’ideles; equació funcional
Jacquet	$L(\pi, s)$	Hecke; Shimura; grups de Lie; equació funcional (cas estàndard); traces
p -àdiques		Mazur, Tate i Teitelbaum; representacions automorfes de grups de Lie p -àdics

Taula 5: Una selecció de funcions zeta i funcions L

	Funcions zeta i funcions L espectrals
Selberg	superfícies de Riemann; grups kleinians; geodèsiques tancades; fórmula de traces; HR
Connes	grups de Lie adèlics; C^* -sistemes dinàmics
Stark	Terras; grafs finits; circuits tancats; HR per a grafs de Ramanujan
	Funcions zeta i funcions L algebraiques
Epstein	formes quadràtiques; no satisfan HR
Godement	Hey; Tamagawa; àlgebres simples
Lusztig	automorfismes de grups lliures
	Funcions zeta i funcions L dinàmiques
Nielsen	espais topològics; sistemes dinàmics; òrbites periòdiques
Ruelle	Smale; difeomorfismes de varietats compactes; fluxos; òrbites periòdiques
Deninger	foliacions; fórmula de Lefschetz
Carlitz	autòmats
Gutzwiller	Hawking; sistemes quàntics; cosmologia quàntica; teoria quàntica de camps

Taula 6: Una selecció de funcions zeta i funcions L (cont.)

Si denotem per

$$M(x) := \sum_{n \leq x} \mu(n),$$

Mertens havia conjecturat que

$$|M(x)| < x^{1/2}, \quad \text{per a tot } x > 1.$$

Un treball numèric portat a terme per Odlyzko en l'estudi dels zeros de la funció zeta permeté concloure que la conjectura de Mertens és falsa, atès que

$$\limsup_{x \rightarrow \infty} M(x)x^{-1/2} > 1.06.$$

Però, d'altra banda, és sabut que la hipòtesi de Riemann és equivalent a

$$|M(x)| = O(x^{1/2+\varepsilon}), \quad \text{per a tot } \varepsilon > 0.$$

L'any 1932, Siegel portà a terme un acurat estudi dels manuscrits de Riemann. Siegel opinà que la llegenda segons la qual Riemann hauria obtingut els seus resultats mitjançant idees d'una gran generalitat i sense utilitzar les eines formals de l'anàlisi no era sostenible. Segons Siegel, la força de la tècnica analítica de Riemann es posava de manifest especialment en la seva derivació i transformació de la sèrie semiconvergent per a $\zeta(s)$.

Els darrers anys han conegut un avenç impressionant en els algorismes de verificació de la hipòtesi de Riemann. Les eines més importants que s'han anat succeint, i els seus temps d'execució són:

La fórmula de sumació d'Euler–Maclaurin: $O(n^{2+\varepsilon})$,

La fórmula integral de Riemann–Siegel: $O(n^{3/2+\varepsilon})$,

El mètode d'Odlyzko–Schönhage: $O(n^{1+\varepsilon})$.

En els càlculs, és essencial la fórmula

$$N(T) - 1 = -\frac{1}{2\pi i} \int_{\partial \mathcal{R}} \frac{\zeta'}{\zeta}(s) ds,$$

que permet obtenir el nombre de zeros en un interval mitjançant una integració. Els avenços en el disseny d'algorismes han permès no solament la verificació de la hipòtesi de Riemann en intervals molt amplis sinó, a més, obtenir els seus zeros amb una gran precisió.

n	ρ_n
1	$\frac{1}{2} + i 14.13472514173469379045 \dots$
2	$\frac{1}{2} + i 21.02203963877155499262 \dots$
3	$\frac{1}{2} + i 25.01085758014568876321 \dots$
4	$\frac{1}{2} + i 30.42487612585951321031 \dots$
5	$\frac{1}{2} + i 32.93506158773918969066 \dots$
$\vdots$	$\vdots$

Taula 7. Primers zeros de la funció zeta de Riemann

n	ρ_n
$\vdots$	$\vdots$
10^{20}	$\frac{1}{2} + i 15\,202\,440\,115\,920\,747\,268.62902990 \dots$
$10^{22} - 1$	$\frac{1}{2} + i 1\,370\,919\,909\,931\,995\,308\,226.490240 \dots$
10^{22}	$\frac{1}{2} + i 1\,370\,919\,909\,931\,995\,308\,226.627511 \dots$
$10^{22} + 1$	$\frac{1}{2} + i 1\,370\,919\,909\,931\,995\,308\,226.680160 \dots$
$\vdots$	$\vdots$

Taula 8. Altres zeros de la funció zeta de Riemann

Investigador	any	nombre de zeros
Gram	1903	15
Bäcklund	1914	79
Hutchinson	1925	138
Titchmarsh et al.	1935	1 041
Turing	1952	1 054
Lehmer	1956	25 000
Meller	1958	35 337
Lehman	1966	250 000
Rosser et al.	1968	3 500 000
Brent	1979	81 000 000
de Riele et al.	1986	1 500 000 000
van de Lune	2001	10 000 000 000
Wedeniowski	2004	900 000 000 000
Gourdon et al.	2004	10 000 000 000 000

Taula 9. Nombre de zeros de la funció zeta de Riemann

La xarxa ZetaGrid, dedicada a la verificació de la hipòtesi de Riemann, aplegà en el seu moment més d'11.000 estacions de treball i 4.000 usuaris. Es calcularen més de 10^9 zeros de la funció zeta per dia. La hipòtesi de Riemann ha estat comprovada per als 10 primers bilions de zeros.

En el context del caos quàntic aritmètic, s'han proposat alguns models físics per a l'estudi de $\zeta(s)$. Des del punt de vista de la física, fórmules explícites de Riemann, Weil, Selberg, Gutzwiller han estat interpretades com lligams entre propietats clàssiques i propietats quàntiques de sistemes mecànic-quàntics. Aquestes interpretacions tenen cura de: funcions de partició en mecànica estadística,

oscil·ladors bosònics amb energies $\log p$, plasmes de quarks–gluons, condensats de Bose–Einstein, etc.

En la interpretació espectral de la funció zeta, hi ha qui creu que l'operador de Riemann podria ser la quantització d'un hamiltonià clàssic. Les òrbites periòdiques clàssiques tindrien longitud $\log p$. La dinàmica de Riemann seria caòtica i amb *mass gap*. No seria invariant per inversió de la fletxa del temps. Tindria instantons de períodes múltiples de $i\pi$. En resum, i en paraules de Marcus du Sautoy (2003),

És evident que els zeros de Riemann són vibracions, però no sabem què és el que vibra.

SOBRE LA QUANTITAT DE NOMBRES PRIMERS PER SOTA D'UNA QUANTITAT DONADA

B. RIEMANN

Agraeixo la distinció que m'ha fet l'Acadèmia d'acollir-me com a membre corresponent. Em sembla que la millor manera de mostrar-hi el meu reconeixement és fer-ne ús al més aviat possible mitjançant la comunicació d'una investigació sobre la freqüència dels nombres primers; un tema que, per l'interès que els mateixos GAUSS i DIRICHLET hi han dedicat al llarg de molt de temps, fa que una tal comunicació potser no sembli de poc valor.

Per a aquesta investigació em serví com a punt de partida l'observació feta per EULER que el producte

$$\prod \frac{1}{1 - \frac{1}{p^s}} = \sum \frac{1}{n^s},$$

quan p és substituït per tots els nombres primers, n , per tots els nombres enters. Designo per $\zeta(s)$ la funció de la variable complexa s representada per aquestes dues expressions, sempre que convergeixin. Les dues només convergeixen quan la part real de s és més gran que 1; això no obstant, es pot trobar fàcilment una expressió de la funció que sempre roman vàlida. Mitjançant l'aplicació de la igualtat

$$\int_0^\infty e^{-nx} x^{s-1} dx = \frac{\Pi(s-1)}{n^s}$$

s'obté, primerament, que

$$\Pi(s-1)\zeta(s) = \int_0^\infty \frac{x^{s-1}dx}{e^x - 1}.$$

Si ara es considera la integral

$$\int \frac{(-x)^{s-1}dx}{e^x - 1},$$

estesa des de $+\infty$ fins a $-\infty$ positivament al voltant d'un domini de quantitats que conté en el seu interior el valor 0, però no cap altra discontinuïtat de la funció sota el signe integral, aleshores s'obté fàcilment aquesta igual a

$$(e^{-\pi si} - e^{\pi si}) \int_0^\infty \frac{x^{s-1}dx}{e^x - 1},$$

suposat que en la funció multivaluada

$$(-x)^{s-1} = e^{(s-1)\log(-x)}$$

el logaritme de $-x$ és determinat de manera que per a un x negatiu esdevé real. Es té, però, que

$$2 \sin \pi s \Pi(s-1)\zeta(s) = i \int_{-\infty}^\infty \frac{(-x)^{s-1}dx}{e^x - 1},$$

entesa la integral en el sentit tot just indicat.

Ara, aquesta igualtat proporciona el valor de la funció $\zeta(s)$ per a cada complex qualsevol s , i mostra que és univaluada i per a tots els valors finits de s , excepte 1, finita, com també que s'anul·la quan s és igual a un nombre parell negatiu.

Quan la part real de s és negativa, la integral també pot ésser estesa negativament al voltant del domini de quantitats que conté la totalitat de les quantitats complexes restants, en comptes de positivament al voltant del domini de quantitats indicat, atès que la integral és llavors infinitament petita per a valors de mòdul infinitament gran. A l'interior d'aquests dominis de quantitats, però, la funció sota el signe d'integral només esdevé discontinua quan x esdevé igual a un múltiple enter de $\pm 2\pi i$, per tant, la integral és igual a la suma de la integral negativa presa al voltant d'aquests valors. Però la integral al voltant del valor $n2\pi i$ és $= (-n2\pi i)^{s-1}(-2\pi i)$, per tant, s'obté que

$$2 \sin \pi s \Pi(s-1)\zeta(s) = (2\pi)^s \sum n^{s-1}((-i)^{s-1} + i^{s-1}),$$

és a dir, una relació entre $\zeta(s)$ i $\zeta(1-s)$, la qual, mitjançant la utilització de propietats ben conegudes de la funció Π , també es deixa expressar:

$$\Pi\left(\frac{s}{2} - 1\right) \pi^{-\frac{s}{2}} \zeta(s),$$

que roman invariant quan s es transforma en $1-s$.

Aquesta propietat de la funció em permet introduir en el terme general de la sèrie $\sum \frac{1}{n^s}$ la integral $\Pi\left(\frac{s}{2} - 1\right)$ en comptes de $\Pi(s-1)$, raó per la qual s'obté una expressió molt còmoda per a la funció $\zeta(s)$. De fet, es té que

$$\frac{1}{n^s} \Pi\left(\frac{s}{2} - 1\right) \pi^{-\frac{s}{2}} = \int_0^\infty e^{-nn\pi x} x^{\frac{s}{2}-1} dx,$$

és a dir, en substituir

$$\sum_1^\infty e^{-nn\pi x} = \psi(x),$$

que

$$\Pi\left(\frac{s}{2} - 1\right) \pi^{-\frac{s}{2}} \zeta(s) = \int_0^\infty \psi(x) x^{\frac{s}{2}-1} dx,$$

o bé, atès que

$$2\psi(x) + 1 = x^{-\frac{1}{2}} \left(2\psi\left(\frac{1}{x}\right) + 1 \right) \quad (\text{JACOBI, } \textit{Fund.} \text{ p. 184}),$$

que

$$\begin{aligned} \Pi\left(\frac{s}{2} - 1\right) \pi^{-\frac{s}{2}} \zeta(s) &= \int_1^\infty \psi(x) x^{\frac{s}{2}-1} dx + \int_0^1 \psi\left(\frac{1}{x}\right) x^{\frac{s-3}{2}} dx + \\ &\quad + \frac{1}{2} \int_0^1 \left(x^{\frac{s-3}{2}} - x^{\frac{s}{2}-1} \right) dx = \\ &= \frac{1}{s(s-1)} + \int_1^\infty \psi(x) \left(x^{\frac{s}{2}-1} + x^{-\frac{1+s}{2}} \right) dx. \end{aligned}$$

Ara poso $s = \frac{1}{2} + ti$ i

$$\Pi\left(\frac{s}{2}\right) (s-1) \pi^{-\frac{s}{2}} \zeta(s) = \xi(t),$$

de manera que

$$\xi(t) = \frac{1}{2} - \left(tt + \frac{1}{4} \right) \int_1^\infty \psi(x) x^{-\frac{3}{4}} \cos\left(\frac{1}{2}t \log x\right) dx$$

o també

$$\xi(t) = 4 \int_1^\infty \frac{d(x^{\frac{3}{2}} \psi'(x))}{dx} x^{-\frac{1}{4}} \cos\left(\frac{1}{2}t \log x\right) dx.$$

Aquesta funció és finita per a tots els valors finits de t i es pot desenvolupar en potències de tt en una sèrie que

convergeix molt de pressa. Atès que per a un valor de s , el component real del qual és més gran que 1, $\log \zeta(s) = -\sum \log(1 - p^{-s})$ roman finit, i que val el mateix per als logaritmes dels factors restants de $\xi(t)$, la funció $\xi(t)$ només es pot anul·lar quan la part imaginària de t cau entre $\frac{1}{2}i$ i $-\frac{1}{2}i$. El nombre d'arrels de $\xi(t) = 0$ la part real de les quals cau entre 0 i T és aproximadament

$$= \frac{T}{2\pi} \log \frac{T}{2\pi} - \frac{T}{2\pi};$$

llavors, la integral $\int d \log \xi(t)$, estesa positivament al voltant de l'interior de la regió dels valors de t la part imaginària dels quals cau entre $\frac{1}{2}i$ i $-\frac{1}{2}i$, i la part real, entre 0 i T , és igual a $(T \log \frac{T}{2\pi} - T)i$ (llevat d'una fracció de l'ordre de la quantitat $\frac{1}{T}$); però aquesta integral és igual al nombre de les arrels de $\xi(t) = 0$ que cauen en aquest domini, multiplicat per $2\pi i$. Ara, de fet, a l'interior d'aquestes fronteres es troben aproximadament unes tantes arrels reals, i és molt probable que totes les arrels siguin reals. Certament, seria desitjable tenir una demostració més rigorosa d'aquest fet; tot i així, per ara he deixat de banda la cerca d'aquesta després d'alguns intents vans i escàpols, atès que sembla supèrflua per a l'objectiu immediat de la meua recerca.

Si es designa per α cada arrel de l'equació $\xi(\alpha) = 0$, aleshores $\log \xi(t)$ es pot expressar per

$$\sum \log(1 - \frac{t\alpha}{\alpha\alpha}) + \log \xi(0);$$

atès que la densitat de les arrels de la quantitat t creix amb t només com $\log \frac{t}{2\pi}$, aquesta expressió convergeix i esdevé infinita només com $t \log t$ per a un infinit t ; per

tant, es diferencia de $\log \xi(t)$ en una funció de tt que roman contínua i infinita per a un t finit i dividida per tt esdevé infinitament petita per a un t infinit. En conseqüència, aquesta diferència és una constant, el valor de la qual es pot determinar mitjançant la substitució de $t = 0$.

Ara, amb aquestes eines, es pot determinar la quantitat de nombres primers que són més petits que x .

Sigui $F(x)$ igual a aquest nombre quan x precisament no és un nombre primer, però $\frac{1}{2}$ més gran quan x és un nombre primer, de manera que per a un x en el qual $F(x)$ canvia per salt,

$$F(x) = \frac{F(x+0) + F(x-0)}{2}.$$

Ara, si en

$$\begin{aligned} \log \zeta(s) &= - \sum \log(1 - p^{-s}) = \\ &= \sum p^{-s} + \frac{1}{2} \sum p^{-2s} + \frac{1}{3} \sum p^{-3s} + \dots \end{aligned}$$

se substitueix

$$p^{-s} \text{ per } s \int_p^\infty x^{-s-1} dx, \quad p^{-2s} \text{ per } s \int_{p^2}^\infty x^{-s-1} dx, \quad \dots,$$

aleshores s'obté que

$$\frac{\log \zeta(s)}{s} = \int_1^\infty f(x) x^{-s-1} dx,$$

quan

$$F(x) + \frac{1}{2}F(x^{\frac{1}{2}}) + \frac{1}{3}F(x^{\frac{1}{3}}) + \dots$$

es denota per $f(x)$.

Aquesta igualtat és vàlida per a cada valor complex $a + bi$ de s , quan $a > 1$. Però si en aquest contorn val la igualtat

$$g(s) = \int_0^\infty h(x)x^{-s}d\log x,$$

aleshores, amb l'ajut del teorema de FOURIER, la funció h es pot expressar mitjançant la funció g . Si $h(x)$ és real i

$$g(a + bi) = g_1(b) + ig_2(b),$$

la igualtat descompon en les dues següents:

$$g_1(b) = \int_0^\infty h(x)x^{-a}\cos(b\log x)d\log x,$$

$$ig_2(b) = -i \int_0^\infty h(x)x^{-a}\sin(b\log x)d\log x.$$

Si les dues igualtats es multipliquen per

$$(\cos(b\log y) + i\sin(b\log y))db$$

i s'integra de $-\infty$ a $+\infty$, aleshores, d'acord amb el teorema de FOURIER, s'obté $\pi h(y)y^{-a}$ en tots dos costats drets; en conseqüència, si se sumen totes dues igualtats i es multiplica per iy^a ,

$$2\pi ih(y) = \int_{a-\infty i}^{a+\infty i} g(s)y^s ds,$$

on la integració és realitzada de tal manera que la part real de s roman constant.

Per a un valor de y per al qual tingui lloc un canvi per salt de la funció $h(y)$, la integral representa el valor mitjà

dels valors de la funció h en els dos costats del salt. Per la manera de determinar la funció $f(x)$ que aquí s'ha suposat, aquesta posseeix la mateixa propietat i, per tant, es té amb completa generalitat que

$$f(y) = \frac{1}{2\pi i} \int_{a-\infty i}^{a+\infty i} \frac{\log \zeta(s)}{s} y^s ds.$$

Ara, $\log \zeta$ es pot substituir per l'expressió

$$\frac{s}{2} \log \pi - \log(s-1) - \log \Pi\left(\frac{s}{2}\right) - \sum^{\alpha} \left(1 + \frac{(s - \frac{1}{2})^2}{\alpha\alpha}\right) + \log \xi(0)$$

trobadada abans; però aleshores, les integrals dels termes aïllats d'aquestes expressions, esteses als infinits, no convergrien, raó per la qual és oportú transformar la igualtat precedent en

$$f(x) = -\frac{1}{2\pi i} \frac{1}{\log x} \int_{a-\infty i}^{a+\infty i} \frac{d \frac{\log \zeta(s)}{s}}{ds} x^s ds$$

per mitjà d'una integració parcial.

Atès que, per a $m = \infty$,

$$-\log \Pi\left(\frac{s}{2}\right) = \lim \left(\sum_{n=1}^{n=m} \log \left(1 + \frac{s}{2n}\right) - \frac{s}{2} \log m \right),$$

és a dir,

$$-\frac{d \frac{1}{s} \log \Pi\left(\frac{s}{2}\right)}{ds} = \sum_1^{\infty} \frac{d \frac{1}{s} \log \left(1 + \frac{s}{2n}\right)}{ds},$$

aleshores tots els termes de l'expressió per a $f(x)$ amb excepció de

$$\frac{1}{2\pi i} \frac{1}{\log x} \int_{a-\infty i}^{a+\infty i} \frac{1}{s} \log \xi(0) x^s ds = \log \xi(0),$$

obtenen la forma

$$\pm \frac{1}{2\pi i} \frac{1}{\log x} \int_{a-\infty i}^{a+\infty i} \frac{d\left(\frac{1}{s} \log\left(1 - \frac{s}{\beta}\right)\right)}{ds} x^s ds.$$

Però ara és

$$\frac{d\left(\frac{1}{s} \log\left(1 - \frac{s}{\beta}\right)\right)}{d\beta} = \frac{1}{(\beta - s)\beta},$$

i, quan la part real de s és més gran que la part real de β ,

$$-\frac{1}{2\pi i} \int_{a-\infty i}^{a+\infty i} \frac{x^s ds}{(\beta - s)\beta} = \frac{x^\beta}{\beta} = \int_{\infty}^x x^{\beta-1} dx,$$

o bé

$$= \int_0^x x^{\beta-1} dx,$$

segons que la part real de β sigui negativa o positiva. Per tant, es té que

$$\begin{aligned} & \frac{1}{2\pi i} \frac{1}{\log x} \int_{a-\infty i}^{a+\infty i} \frac{d\left(\frac{1}{s} \log\left(1 - \frac{s}{\beta}\right)\right)}{ds} x^s ds = \\ & = -\frac{1}{2\pi i} \int_{a-\infty i}^{a+\infty i} \frac{1}{s} \log\left(1 - \frac{s}{\beta}\right) x^s ds = \\ & = \int_{\infty}^x \frac{x^{\beta-1}}{\log x} dx + \text{const. en el primer cas,} \end{aligned}$$

i

$$= \int_0^x \frac{x^{\beta-1}}{\log x} + \text{const. en el segon.}$$

En el primer cas, es determina la constant d'integració quan es deixa que la part real de β esdevingui infinitament negativa; en el segon cas, la integral de 0 fins a x s'obté amb valors que difereixen en $2\pi i$, segons que la integració ocorre per a valors complexos d'arcs positius o bé negatius, i esdevé infinitament petita presa sobre cadascun dels camins, si el coeficient de i en els valors de β esdevé infinitament positiu, però en el darrer, si aquest coeficient esdevé infinitament negatiu. De com és determinat $\log \left(1 - \frac{s}{\beta}\right)$ al costat esquerre, en resulta després que la constant d'integració desapareix.

Per substitució d'aquests valors en l'expressió de $f(x)$, s'obté que

$$f(x) = \text{Li}(x) - \sum^{\alpha} \left(\text{Li}(x^{\frac{1}{2}+\alpha i}) + \text{Li}(x^{\frac{1}{2}-\alpha i}) \right) + \\ + \int_x^{\infty} \frac{1}{x^2-1} \frac{dx}{x \log x} + \log \xi(0),$$

quan en $\sum^{\alpha}$, α és substituït per totes les arrels positives (o bé que contenen una part real positiva) de l'equació $\xi(\alpha) = 0$, ordenades d'acord amb la seva grandària. Amb l'ajut d'una discussió més precisa de la funció ξ es pot mostrar fàcilment que, per a aquesta ordenació, el valor de la sèrie

$$\sum \left(\text{Li}(x^{\frac{1}{2}+\alpha i}) + \text{Li}(x^{\frac{1}{2}-\alpha i}) \right) \log x$$

coincideix amb el valor frontera envers el qual

$$\frac{1}{2\pi i} \int_{a-bi}^{a+bi} \frac{d\frac{1}{s} \sum \log \left(1 + \frac{(s - \frac{1}{2})^2}{\alpha\alpha} \right)}{ds} x^s ds$$

convergeix per un creixement imparable de la quantitat b ; però, per canvi d'ordenació, podria ésser obtingut qualsevol altre valor real.

Per mitjà de la inversió de la relació

$$f(x) = \sum \frac{1}{n} F\left(x^{\frac{1}{n}}\right),$$

s'obté $F(x)$ a partir de $f(x)$, i en resulta la igualtat

$$F(x) = \sum (-1)^\mu \frac{1}{m} f\left(x^{\frac{1}{m}}\right),$$

on la sèrie s'estén als nombres m que no són divisibles per cap quadrat llevat de 1 i μ designa el nombre de factors primers de m .

Si es restringeix $\sum^\alpha$ a un nombre finit de termes, aleshores la derivada de l'expressió per a $f(x)$ o bé, llevat d'un terme que decreix molt de pressa per a x creixents,

$$\frac{1}{\log x} - 2 \sum^\alpha \frac{\cos(\alpha \log x) x^{-\frac{1}{2}}}{\log x}$$

proporciona una expressió que aproxima la densitat dels nombres primers + la meitat de la densitat dels quadrats dels nombres primers + $\frac{1}{3}$ de la densitat dels cubs dels nombres primers i així successivament, de grandària x .

Per tant, la coneguda fórmula d'aproximació $F(x) = \text{Li}(x)$ és correcta únicament llevat de quantitats d'ordre $x^{\frac{1}{2}}$

i proporciona un valor aproximat massa gran; ja que els termes no periòdics en l'expressió de $F(x)$ són, llevat de quantitats que no creixen infinitament amb x ,

$$\text{Li}(x) - \frac{1}{2}\text{Li}(x^{\frac{1}{2}}) - \frac{1}{3}\text{Li}(x^{\frac{1}{3}}) - \frac{1}{5}\text{Li}(x^{\frac{1}{5}}) + \frac{1}{6}\text{Li}(x^{\frac{1}{6}}) - \frac{1}{7}\text{Li}(x^{\frac{1}{7}}) + \dots$$

De fet, ha estat posat de manifest per la comparació, empresa per GAUSS i GOLDSCHMIDT i continuada fins a $x =$ tres milions, de $\text{Li}(x)$ amb la quantitat de nombres primers inferiors a x , que aquesta quantitat sempre és més petita que $\text{Li}(x)$ ja dels primers cent mil enllà, i que, certament, la diferència entre algunes oscil·lacions creix gradualment amb x . Però l'increment i la disminució de la densitat en cada punt dels nombres primers que depenen dels termes periòdics també ha despertat la curiositat a l'hora de comptar-los, encara que, això no obstant, no se n'hagi fet notar una llei de creixement. Seria interessant perseguir, per un eventual nou comptatge, la influència de cadascun dels termes periòdics continguts en l'expressió per a la densitat dels nombres primers. La funció $f(x)$ mostraria una anada regular cap a la funció $F(x)$, la qual, ja en els primers cent, es deixa reconèixer molt clarament com a coincident en mitjana amb $\text{Li}(x) + \log \xi(0)$.

Referències de l'article

En aquest article, Riemann només fa explícitament la cita

JACOBI, *Fund.* p. 184;

es refereix a la pàgina 184 del llibre:

Jacobi, C. G. J.: *Fundamenta nova theoria functionum ellipticarum*. Regiomonti, sumtibus fratrum Borntræger, Königsberg, 1829. Reproduït a *Gesammelte Werke*, **1**, Chelsea, reimpressió (1969) p. 49–239.

Capítol 6

Kronecker

La traducció que s'ofereix correspon a un treball presentat per Kronecker a l'Acadèmia de Berlín l'any 1863, dos anys després del seu ingrés com a acadèmic en aquella institució. Mentre que Hilbert era partidari de les idees de Cantor relatives a la teoria de conjunts i, en conseqüència, acceptava sense prejudicis les demostracions de teoremes d'existència, Kronecker era partidari de proporcionar solucions explícites a aquest tipus de resultats. En la comunicació a l'Acadèmia que comentarem, Kronecker posa de manifest aquesta tendència seva i proporciona un mètode per a obtenir la solució fonamental de l'equació de Pell per via analítica però de manera explícita. No només això, sinó que el seu mètode, tal com s'ha mostrat posteriorment, és més efectiu que els que eren coneguts fins aleshores.

6.1 1863: El treball sobre l'equació de Pell

El propòsit de Kronecker és el càlcul dels enters positius més petits x, y que satisfan l'equació

$$X^2 - mY^2 = 1,$$

on $m > 1$ és un enter lliure de quadrats. L'equació anterior és coneguda amb el nom d'equació de Pell.

Casos particulars d'aquesta equació havien estat considerats ja per la matemàtica grega i la hindú. El seu nom és degut a un error d'assignació comès per Euler, que atribuï equivocadament el seu estudi al matemàtic anglès John Pell, en confondre'l amb el també matemàtic i també anglès Lord Brouncker. Sembla que aquest hauria estat el primer matemàtic europeu a donar-ne la solució general, en resposta a un desafiament de Fermat. Aquest és el motiu pel qual l'equació es coneix també amb el nom de Pell-Fermat. Un tractament més complet de la història d'aquesta equació es troba en el llibre de Weil [401].

L'equació està estretament lligada a la teoria dels nombres algebraics, atès que la descomposició

$$X^2 - mY^2 = (X + Y\sqrt{m})(X - Y\sqrt{m})$$

posa de manifest que la seva resolució equival al càlcul de les unitats de norma 1 de l'ordre $\mathbb{Z}[\sqrt{m}]$ del cos quadràtic real $\mathbb{Q}(\sqrt{m})$. Alhora, la relació

$$x_n - y_n\sqrt{m} = (x_1 - y_1\sqrt{m})^n$$

permet calcular totes les solucions de l'equació original a partir de la solució fonamental (x_1, y_1) , que és la donada pels coeficients positius x_1, y_1 més petits.

La dificultat principal a l'hora de resoldre l'equació diofantina anterior rau en el fet que valors de m molt petits poden abocar a solucions fonamentals molt grans. En aquest sentit, podem esmentar el *problema dels bous del Sol*, formulat per Arquimedes en l'*Arenari*. En aquest problema, Arquimedes insta Eratòstenes i els matemàtics alexandrins a comptar el nombre de caps de bestiar del ramat del déu Hèlios per mitjà de la resolució d'un sistema d'equacions diofantines. En particular, la resolució del problema comporta la d'una equació de Pell per al paràmetre $m = 4729494$, la qual té per solució fonamental la donada pels nombres

$$\begin{aligned}x &= 109931986732829734979866232821433543901088049, \\y &= 50549485234315033074477819735540408986340.\end{aligned}$$

En els textos d'avui se sol tractar la resolució de l'equació de Pell per mitjà de fraccions continuades, segons un mètode desenvolupat per Euler en el seu tractat *Algebra* i precisat per Lagrange l'any 1768. Per tant, es tracta d'un procediment anterior al mètode proposat per Kronecker. Euler, així com també els matemàtics hindús, donen per fet que el mètode de les fraccions continuades sempre condueix a una solució, però, de fet, és Lagrange qui publica que una tal solució sempre existeix. Atès que el mètode de les fraccions continuades requereix el càlcul del període de la fracció continuada que correspon a $\sqrt{m}$ i que aquest pot ésser molt gran, a la pràctica resulta poc eficient.

Des del punt de vista teòric, la resolució que presenta Kronecker és molt més elaborada que la d'Euler i Lagran-

ge, però té l'avantatge que proporciona un algorisme més eficient a l'hora de la seva implementació.

Diferents algorismes per a la resolució de l'equació de Pell i la discussió del seu grau de complexitat foren exposats per Lenstra, en un treball de l'any 2002 ([267]). En aquest treball, però, Lenstra no esmenta el mètode de Kronecker. Una anàlisi del mètode de Kronecker des d'un punt de vista algorítmic ha estat portat a terme més recentment en ([164]).

Kronecker parteix de l'equació quan $m = P$ i, al mateix temps, pren un segon nombre auxiliar Q . Considera que tant P com Q són nombres enters senars, positius, lliures de quadrats i coprimers per als quals el producte $D = PQ$ satisfà que $D \equiv 1 \pmod{4}$. En denotar per $H(-Q)$, $H(P)$ els nombres de classes respectius de les formes quadràtiques $(a, 2b, c)$ pròpiament primitives de determinants $-Q$ i P , demostra que el logaritme del valor

$$(T + U\sqrt{P})^{H(-Q)H(P)}$$

pot ésser expressat aproximadament com

$$\left(2 - \left(\frac{2}{R}\right)\right) \sum \left[\frac{a}{R}\right] \left(\frac{\pi\sqrt{D}}{3a} + \log a\right),$$

on el sumatori s'estén a tots els nombres a que proporcionen els primers coeficients de les diferents formes reduïdes de determinant, segons Gauss i Kronecker, $-D = b^2 - ac$, o bé de discriminant $-4D$, en la terminologia actual. Notem que el caràcter enter de la solució cercada permet la seva determinació a partir d'una aproximació suficientment bona de la solució.

Denotem per K el cos quadràtic imaginari $\mathbb{Q}(\sqrt{-D})$ i sigui $\text{Cl}(K)$ el grup de classes d'ideals de K . Per definició, un caràcter de gènere de K és un homomorfisme $\chi : \text{Cl}(K) \longrightarrow \{\pm 1\}$. Representem per X_K el grup format pel conjunt de tots aquests caràcters de gènere, amb la multiplicació definida per

$$\chi_1 \chi_2(C) = \chi_1(C) \chi_2(C), \quad C \in \text{Cl}(K).$$

Kronecker pren $R = P$, si $P \equiv 1 \pmod{4}$, i $R = Q$, si $P \equiv 3 \pmod{4}$. Cada classe de formes admet un representant $(a, 2b, c)$ en què a pot ésser pres coprimer amb qualsevol quantitat donada. Escrivim

$$K_P := \mathbb{Q}(\sqrt{P}), \quad K_{-Q} := \mathbb{Q}(\sqrt{-Q})$$

i siguin χ_P, χ_{-Q} els respectius caràcters de Kronecker d'aquests dos cossos quadràtics. El mètode de Kronecker prové d'avaluar el límit

$$\lim_{\varrho \rightarrow 0} L(\chi_P, 1 + \varrho) L(\chi_{-Q}, 1 + \varrho)$$

de dues maneres diferents i comparar els resultats obtinguts.

D'una banda, el límit anterior s'avalua directament a partir de les fórmules analítiques del nombre de classes dels cossos quadràtics, degudes a Dirichlet, la qual cosa proporciona una expressió en què figura el logaritme de la unitat fonamental del cos quadràtic real:

$$\begin{aligned} \lim_{\varrho \rightarrow 0} \sum \left(\frac{P}{m} \right) \frac{1}{m^{1+\varrho}} \sum \left(\frac{-Q}{n} \right) \frac{1}{n^{1+\varrho}} &= \\ &= \frac{\pi}{4\sqrt{D}} H(-Q) H(P) \log(T + U\sqrt{P}). \end{aligned}$$

D'altra banda, expressarà el producte anterior en termes de funcions zeta de formes quadràtiques binàries i el límit serà avaluat mitjançant valors especials de funcions theta de Jacobi i de les seves derivades. El treball fa ús del que esdevindria, anys més tard, la primera fórmula límit de Kronecker, com explicarem tot seguit.

Donada una forma quadràtica binària, definida positiva, de coeficients reals, $f(X, Y) = aX^2 + bXY + cY^2$, on $a, c > 0$ i $b^2 - 4ac = -1$, la seva funció zeta

$$\zeta(f, s) := \sum'_{m,n} \frac{1}{f(m, n)^s}, \quad \Re(s) > 1,$$

s'estén a una funció meromorfa a l'entorn de $s = 1$ i té un desenvolupament en sèrie de Laurent de la forma

$$\zeta(f, s) = \frac{2\pi}{s-1} + \kappa + O(s-1)$$

amb terme constant donat per

$$\kappa = 4\pi\left(\gamma + \frac{1}{2} \log c - \log |\eta(w)|^2\right),$$

on γ és la constant d'Euler-Mascheroni i w denota el zero de part imaginària positiva de la forma. Observem que el residu és independent de la forma, però no així el terme independent de la sèrie.

En la fórmula, η denota la funció eta de Dedekind, la qual satisfà la igualtat

$$\eta(\tau)^3 = -\frac{1}{2\pi} \theta'_1(0, \tau),$$

on $\theta_1 = \theta_{\frac{1}{2}, \frac{1}{2}}$ és una de les funcions theta amb característiques de Jacobi. En el treball, Kronecker no empra la funció η sinó que treballa directament amb la funció de Jacobi.

La part més enginyosa del treball consisteix en l'ús que Kronecker fa dels caràcters de gènere. Aquests li permeten afectar de signes les funcions zeta per a les diferents classes de formes quadràtiques binàries que intervenen en el sumatori. Amb la qual cosa, Kronecker pot aparellar cada funció zeta d'una forma quadràtica binària, afectada de signe positiu, amb una funció zeta d'una altra forma quadràtica, afectada de signe negatiu. Amb això, se simplifiquen els termes de la sèrie $\zeta(f, s)$ que divergeixen quan s tendeix a 1 i Kronecker pot obtenir el valor límit del sumatori sense dificultats.

És remarcable que en aquesta comunicació breu a l'Acadèmia, Kronecker no proporciona la demostració de la seva fórmula límit. Aquesta no apareixeria fins anys més tard, en el seu extens treball, en tretze capítols, sobre la teoria de les funcions el·líptiques, que recull sis comunicacions presentades a l'Acadèmia de Ciències de Berlín entre els anys 1883 i 1889 ([245]).

Monatsberichte der Königlich Preussischen Akademie der Wissenschaften zu Berlin (1863), 44–50

SOBRE LA RESOLUCIÓ DE L'EQUACIÓ DE PELL MITJANÇANT FUNCIONS EL·LÍPTIQUES

del Sr. L. KRONECKER a Berlín

(Llegit a l'Acadèmia de Ciències el 22 de gener del 1863)

En aquesta ocasió seria oportú donar algunes indicacions sobre els mètodes emprats en relació amb aquestes [equacions] i, al mateix temps, posar en relleu aquells resultats que es poden representar amb notacions senzilles.

Si P i Q denoten nombres senars positius sense factors quadràtics, dels quals el primer és més gran que u , i si, a més, les lletres m i n descriuen successivament tots els valors enters positius que són relativament primers amb $2P$ i $2Q$ respectivament, aleshores el límit que assoleixen les dues sèries

$$\sum \left(\frac{P}{m} \right) \frac{1}{m^{1+\varrho}}, \quad \sum \left(\frac{-Q}{n} \right) \frac{1}{n^{1+\varrho}}$$

per a $\varrho = 0$ s'obté immediatament a partir de la memòria de DIRICHLET en els volums 19 i 21 de la Revista de Crelle. A partir d'aquí, esdevé

$$\begin{aligned} \lim_{\varrho=0} \sum \left(\frac{P}{m} \right) \frac{1}{m^{1+\varrho}} \sum \left(\frac{-Q}{n} \right) \frac{1}{n^{1+\varrho}} = \\ = \frac{\pi}{4\sqrt{D}} H(-Q) H(P) \log(T + U\sqrt{P}), \end{aligned}$$

on s'ha posat $P \cdot Q = D$, i s'han designat per $H(-Q)$, $H(P)$ els nombres de classes respectius de les formes quadràtiques pròpiament primitives de determinants $-Q$ i P , i on T i U denoten els enters més petits per als quals $T^2 - PU^2 = 1$. Aquí, però, s'ha de remarcar que cal prendre $H(-1) = \frac{1}{2}$.

En el cas en què D és sense factor quadràtic i de la forma $4\nu + 1$, el producte en cadascuna de les sèries o, el que és el mateix, la sèrie doble:

$$\sum \sum \left(\frac{P}{m} \right) \left(\frac{-Q}{n} \right) \frac{1}{(mn)^{1+\varrho}}$$

es pot transformar en

$$\frac{1}{2^{2+\varrho}} \left(2^{1+\varrho} - \left(\frac{2}{R} \right) \right) \sum \left[\frac{a}{R} \right] \sum \sum \frac{1}{(ax^2 + 2bxy + cy^2)^{1+\varrho}}.$$

Aquí es pot posar R igual a P o a Q , segons que $P \equiv 1$ o bé $3 \pmod{4}$, el primer signe de suma fa referència a totes les formes pròpiament primitives no equivalents (a, b, c) de determinant $-D$, el símbol $\left[\frac{a}{R} \right]$ denota el caràcter de la forma associada per a tots els factors primers de R de manera que

$$\left[\frac{a}{R} \right] = \left(\frac{a'}{R} \right),$$

si (a', b', c') és una forma equivalent amb (a, b, c) , de la qual el primer coeficient a' no té cap divisor primer comú amb R ; finalment, els dos darrers sumatoris s'estenen a tots els valors enters positius i negatius de x i de y , amb l'única excepció del sistema de valors $x = 0$, $y = 0$. D'acord amb això, s'obté que

$$\begin{aligned} & \frac{\pi}{\sqrt{D}} H(-Q) H(P) \log(T + U\sqrt{P}) = \\ & = \left(2 - \left(\frac{2}{R} \right) \right) \lim_{\varrho=0} \sum \sum \sum \left[\frac{a}{R} \right] \frac{1}{(ax^2 + 2bxy + cy^2)^{1+\varrho}}. \end{aligned}$$

A fi de determinar el límit del costat dret d'aquesta equació, s'investigarà

$$\lim_{\varrho=0} \sum \sum \frac{e^{2\pi i(\sigma x + \tau y)}}{(ax^2 + 2bxy + cy^2)^{1+\varrho}}$$

en el cas en què σ , τ , a , b , c denoten quantitats reals arbitràries que aquí satisfan la condició $ac - b^2 = D > 0$. Aquest valor es troba expressat de la manera següent:

$$\begin{aligned} \frac{2\sigma^2\pi^2}{a} + \frac{\pi}{3\sqrt{D}} \log \frac{1}{4\pi^2} \vartheta'(0, w_1) \vartheta'(0, w_2) - \\ - \frac{\pi}{\sqrt{D}} \log \vartheta(\tau + \sigma w_1, w_1) \vartheta(\tau + \sigma w_2, w_2), \end{aligned}$$

on $\vartheta(z, w)$ denota la sèrie

$$-i \sum_{n=-\infty}^{n=+\infty} (-1)^n e^{\left(n+\frac{1}{2}\right)^2 w \pi i + (2n+1)z \pi i},$$

ϑ' el seu quocient diferencial pres en relació amb z , i on s'ha posat, per tal d'abreujar,

$$w_1 = \frac{-b + i\sqrt{D}}{a}, \quad w_2 = \frac{+b + i\sqrt{D}}{a}.$$

Mitjançant la utilització de l'expressió tot just indicada, la qual constitueix la base de totes les meves recerques corresponents, per a la diferència

$$\sum \sum \frac{1}{(ax^2 + 2bxy + cy^2)^{1+\varrho}} - \sum \sum \frac{1}{(a'x^2 + 2b'xy + c'y^2)^{1+\varrho}}$$

en la qual (a, b, c) i (a', b', c') denoten dues formes diferents de determinant $-D$, s'obté el valor límit

$$\frac{2\pi}{3\sqrt{D}} \log \frac{a\sqrt{a}}{a'\sqrt{a'}} \frac{\vartheta'(0, w'_1) \vartheta(0, w'_2)}{\vartheta'(0, w_1) \vartheta(0, w_2)},$$

quan ϱ s'apropa a zero i quan en el lloc de w'_1, w'_2 s'hi posen les expressions construïdes a partir de a', b', c' anàlogues a les quantitats w_1, w_2 . D'acord amb això, per a $D \equiv 1 \pmod{4}$ s'obté l'equació

$$H(-Q)H(P)\log(T + U\sqrt{P}) = \frac{2}{3} \left(2 - \left(\frac{2}{R} \right) \right) \sum \left[\frac{a}{R} \right] \log \frac{a\sqrt{a}}{\vartheta'(0, w_1)\vartheta'(0, w_2)},$$

en la qual, en virtut de la determinació anterior, el costat dret esdevé igual a

$$\frac{2}{3} \sum \left[\frac{a}{P} \right] \log \frac{a\sqrt{a}}{\vartheta'(0, w_1)\vartheta'(0, w_2)},$$

quan $P \equiv 1 \pmod{8}$, però al triple d'això quan $P \equiv 5 \pmod{8}$, mentre que esdevé igual a

$$\frac{2}{3} \sum \left[\frac{a}{Q} \right] \log \frac{a\sqrt{a}}{\vartheta'(0, w_1)\vartheta'(0, w_2)},$$

tan bon punt com $Q \equiv 7 \pmod{8}$ i al triple d'això tan bon punt com $Q \equiv 3 \pmod{8}$. Les sumes s'estenen, aquí i pertot, a qualsevol sistema de formes no equivalents de determinant $-D$, i el factor

$$H(P)\log(T + U\sqrt{P})$$

del costat esquerre de la igualtat precedent pot ésser substituït, d'acord amb DIRICHLET, per una expressió formada a partir d'una arrel $4P$ -èsima de la unitat.

De manera semblant, amb l'ajut de la fórmula de més amunt també es pot representar per mitjà de funcions el·líptiques el valor de

$$H(-Q)H(P)\log(T + U\sqrt{P})$$

per a totes les altres formes numèriques de P i Q i fins i tot si aquestes tenen un factor comú.

Si es té en compte que, per a una aproximació determinada, per a una forma *reduïda* (a, b, c) només es necessita prendre el primer terme de la sèrie $\vartheta'(0, w)$, aleshores es veu fàcilment que el valor de

$$H(-Q)H(P)\log(T + U\sqrt{P})$$

pot ésser expressat, aproximadament, com

$$\left(2 - \left(\frac{2}{R}\right)\right) \sum \left[\frac{a}{R}\right] \left(\frac{\pi\sqrt{D}}{3a} + \log a\right),$$

quan el sumatori s'estén a tots els nombres a que constitueixen els primers coeficients de les diferents formes reduïdes. Sense esmerçar-hi esforç, es pot obtenir una exactitud més gran mitjançant l'afegiment d'uns pocs termes de la sèrie ϑ' ; però ja aquesta primera aproximació és especialment interessant perquè, d'una banda, permet un càlcul més o menys aproximat sobre la magnitud dels nombres T, U de la manera més senzilla i, d'altra banda, dóna una informació sobre la distribució dels nombres a en les diferents xarxes. A fi i efecte de fer palesa mitjançant uns exemples la relació del tot remarcable entre dues definicions completament diferents en què es fonamenten les expressions numèriques, trio en primer lloc els casos:

$$P = D = 5, \quad P = D = 13, \quad P = D = 37,$$

en els quals els valors numèrics respectius

$$2 + \sqrt{5}, \quad 18 + 5\sqrt{13}, \quad 882 + 145\sqrt{37}$$

poden ésser aproximats per mitjà de l'expressió comuna

$$\frac{1}{8}e^{\frac{1}{2}\pi\sqrt{D}}.$$

A més, la solució fonamental de l'equació $T^2 - PU^2 = -1$ en els casos $P = 17$ i $P = 97$, a saber,

$$4 + \sqrt{17}, \quad 5604 + 569\sqrt{97},$$

pot ésser expressada de manera aproximada, respectivament, per

$$\frac{2}{9}e^{\frac{5}{18}\pi\sqrt{17}}, \quad \frac{2}{49}e^{\frac{17}{42}\pi\sqrt{97}}$$

quan en les fórmules de més amunt es posa de nou $Q = 1$. Finalment, per a $D = 85$, i segons que es prengui $Q = 1, 5$ o 17 , les solucions fonamentals de les equacions

$$T^2 - 85U^2 = -1, \quad T^2 - 17U^2 = -1, \quad T^2 - 5U^2 = -1,$$

és a dir,

$$378 + 41\sqrt{85}, \quad 4 + \sqrt{17}, \quad 2 + \sqrt{5},$$

es troba que són aproximadament iguals, respectivament, a

$$\frac{1}{8}e^{\frac{3}{10}\pi\sqrt{85}}, \quad \frac{1}{\sqrt{5}}e^{\frac{1}{10}\pi\sqrt{85}}, \quad e^{\frac{1}{20}\pi\sqrt{85}}.$$

Les formes diferents que s'obtenen d'aquesta manera (com en l'exemple anterior per a $4 + \sqrt{17}$) per a una i la mateixa solució de l'equació de PELL donen peu a moltes observacions interessants; però, de lluny, les conseqüències teòriques que són derivables dels resultats esmentats són les més importants. En aquestes, no solament esdevé palesa una relació sorprenent entre les formes quadràtiques que

corresponen a dos determinants oposats, sinó que també resulta d'aquí aquella descomposició de les equacions per als mòduls singulars que constitueix l'objecte principal de la meua comunicació del juny de l'any passat. Precisament, aquesta descomponibilitat fins i tot permet reconèixer fàcilment la possibilitat de representar *determinades* solucions de l'equació de PELL per mitjà dels mòduls singulars de les funcions el·líptiques; però, a fi de posar de manifest les relacions interessants d'aquestes amb la solució fonamental trobada, ens cal aquella aplicació del mètode de DIRICHLET a la qual l'alta matemàtica ja li ha d'agrair tants resultats sorprenents, i la qual també aquí es manifesta com a tan fructuosa per a l'àlgebra. A saber, la natura algebraica de les expressions ϑ introduïdes abans, és generalment d'especial importància per a la teoria dels mòduls singulars de les funcions el·líptiques, encara que en casos especials aquelles expressions puguin ésser substituïdes per aquests mateixos mòduls. Des d'aquest punt de vista, només cal que sigui mencionada la fórmula vàlida per a $D = 8n + 5$,

$$\prod \frac{\sin \frac{\alpha\pi}{D}}{\sin \frac{\beta\pi}{D}} = \prod \sqrt[3]{4\kappa\kappa'^2},$$

en la qual α i β denoten, respectivament, tots els nombres que són més petits que D i per als quals $(\frac{\alpha}{D}) = +1$, $(\frac{\beta}{D}) = -1$, mentre que el signe del producte del costat dret cal que s'estengui a unes sisenes parts donades de tots aquells mòduls k per als quals té lloc la multiplicació complexa per $\sqrt{-D}$. Els lligams propis de dues teories algebraiques diferents en què són inclosos tots els resultats mencionats abans es posen de manifest d'aquesta manera especial en la mesura que aquests proporcionen una relació immediata

entre les arrels de la unitat i els mòduls singulars de les funcions el·líptiques.

Referències de l'article

Recollim totes juntes les referències citades en aquest article. Encara que l'autor no les dóna explícitament, es refereix a les següents:

Dirichlet, G.L.: Recherches sur diverses applications de l'Analyse infinitesimale à la théorie des Nombres. *J. reine u. angew. Math.*, **19** (gener de 1839), p. 324–369.

Dirichlet, G.L.: Recherches sur diverses applications de l'Analyse infinitesimale à la théorie des Nombres. *J. reine u. angew. Math.*, **21** (gener de 1840), p. 1–12.

Dirichlet, G.L.: Recherches sur diverses applications de l'Analyse infinitesimale à la théorie des Nombres. Seconde Partie. *J. reine u. angew. Math.*, **21** (gener de 1840), p. 134–155.

Capítol 7

Thomae

La matemàtica és una illa plena de tresors que concedeix a qui s'ho proposi la fortuna de poder descobrir-ne alguns. És certament inhabitual, però, trobar-ne d'abandonats. L'article que presentem és una d'aquestes troballes excepcionals: l'anomenada fórmula de Thomae veié la llum fa més d'un segle, però quedà enterrada pels nombrosos avenços teòrics experimentats per la matemàtica en el decurs del segle XX. Sortosament, alguns autors conservaren *mapes del tresor* que han permès retrobar-la en els nostres dies i descobrir-ne aplicacions insospitades.

La fórmula de Thomae estableix un lligam entre el món algebraic i geomètric i el món analític. Algunes vegades és més fàcil construir un pont que creuar-lo —i aquest no és pas un fenomen exclusivament sociològic. Però els ponts romanen pacients tot esperant que els viatgers els donin vida. Les primeres aplicacions de la fórmula de Thomae es troben, més d'un segle després de la seva publicació, en les famoses *Tata Lectures* de Mumford de l'any 1984

(cf. [279]). Un cop a l'altra vora del riu, els físics copsaren ben de pressa el seu interès (cf. [38]) i, des d'aleshores, el trànsit pel pont no ha deixat de fluir.

7.1 1870: La fórmula de Thomae

A partir dels *Fundamenta Nova* de Jacobi, les funcions theta esdevingueren ubíquies a la literatura matemàtica. Estudis exhaustivament des del punt de vista de les funcions el·líptiques, el seu tractament en dimensió superior s'inicià, cap a la segona meitat del segle XIX, en relació amb les funcions abelianes. Les dificultats foren enormes, perquè el camp de batalla era molt gran i tenia molts fronts oberts. És natural, doncs, que les funcions theta *hiperel·líptiques* cospessin l'atenció d'alguns autors. El treball de Thomae que presentem segueix aquest enfocament.

El resultat més destacat del treball és la igualtat (11), actualment anomenada fórmula de Thomae. En llenguatge modern, aquesta s'expressa com

$$\theta[e](0; Z)^4 = \left(\frac{\det \Omega_1}{2\pi i g} \right)^2 \prod_{k < l} (\alpha_{i_k} - \alpha_{i_l}) \prod_{k < l} (\alpha_{j_k} - \alpha_{j_l}).$$

Convé interpretar la fórmula com un lligam entre objectes analítics i objectes algebraics. El món analític és representat per la funció theta de l'esquerra de la igualtat. El món algebraic es troba en el terme de la dreta i conté els invariants bàsics de la corba hiperel·líptica $Y^2 = (X - \alpha_1) \cdots (X - \alpha_{2g+2})$, de gènere g . A més de les abscisses α_k dels punts de ramificació de la corba, hi trobem una matriu de períodes Ω_1 respecte d'una base simplèctica

de l'homologia de la corba. L'elecció d'aquesta base fixa la matriu Z del terme de l'esquerra. La repartició concreta de les α_k en els dos productes determina la característica e per la qual es trasllada la funció theta corresponent.

Aquí no detallarem cap dels ingredients que intervenen en la fórmula. El lector, avesat o no a funcions theta, disposa de molt bones referències ([125], [279], [116]) per a llegir la fórmula i la seva demostració en llenguatge actual. Diguem, només, que el treball de Thomae és, essencialment, autocontingut, i que les eines que hi emprà romanen presents en la matemàtica actual: formes diferencials, teoria de deformacions, i equacions de Picard-Fuchs, entre d'altres.

El treball conté una altra perla matemàtica, que sovint ha passat inadvertida. La igualtat (14) expressa una constant theta jacobiana com a producte de certes constants theta, generalitzant el treball anterior de Rosenhain en dimensió 2 [329]. Aquest és un tema de “llarg recorregut” que serà tractat posteriorment en el capítol 10.

Els capricis de la història feren que el treball de Thomae caigués en l'oblit durant gairebé un segle, fins que el ressorgiment de les funcions theta cap als anys 1960 renovà l'interès per resultats clàssics.

Fay inclogué la fórmula de Thomae i la seva demostració en el seu llibre [125].

Mumford [279] la utilitzà per a descriure espais de mòduls de corbes hiperel·líptiques complexes.

Umemura, en un apèndix [384] de [279], emprà la fórmula de Thomae en un context ben diferent. És ben sabut

que no hi ha fórmules algebraiques generals per a resoldre les equacions polinòmiques de grau més gran que 4. Umemura, basant-se en el resultat de Thomae, obtingué fórmules generals que involucren funcions theta hiperel·líptiques per a expressar les arrels dels polinomis. Les fórmules d'Umemura, que tenen un interès més teòric que pràctic, es poden interpretar com una generalització ([378]) de les fórmules donades per Rosenhain per a determinar la forma normal d'una corba de gènere 2.

Mestre [274] utilitzà la fórmula de Thomae per a provar un criteri de reductibilitat d'una superfície abeliana com a producte de corbes el·líptiques. Seguint aquesta línia, Matsumoto i Terasoma [271] han definit una mitjana aritmètico-geomètrica generalitzada i n'han donat expressions en termes de períodes de corbes hiperel·líptiques, usant novament la fórmula de Thomae i generalitzant així resultats obtinguts prèviament per Gauss.

Si bé la interpretació modular de la fórmula de Thomae és força clara i la suggereix la seva pròpia demostració, el seu significat local no és obvi. Fixada una corba hiperel·líptica, la fórmula proporciona una relació entre objectes associats a ella canònicament, però el valor de les constants theta que hi intervenen no té una explicació senzilla. En canvi, la segona fórmula del treball de Thomae, que es pot interpretar com una versió jacobiana de la primera i que admet una descripció geomètrica més entenedora, ha permès desenvolupar demostracions efectives del teorema de Torelli en el cas hiperel·líptic [177]. Aquestes construccions han estat aplicades tant a nivell teòric (per exemple, en teoria d'Arakelov [222]) com pràctic (per exemple, en

[165] i en [295] s'utilitzen per a la determinació de factors de jacobianes modulars).

La irrupció, a finals del segle passat, de la geometria algebraica en la física matemàtica tingué un impacte apreciable per a ambdues disciplines. La frontera entre les anomenades matemàtica aplicada i matemàtica fonamental ha anat difuminant-se. La funció theta, que, com ja s'ha dit, sorgí dels estudis de Fourier sobre la calor [128], ha recuperat protagonisme en el panorama matemàtic actual gràcies, en part, a la seva aplicació a la integració de determinades equacions en derivades parcials.

La integració de diversos sistemes dinàmics (Korteweg-de Vries, Kadomstev-Petviashvili, sinus-Gordon, etcètera, [279]), atragué l'interès dels físics matemàtics cap a les funcions theta i, en particular, cap a la fórmula de Thomae. Ben aviat es veié la conveniència d'anar més enllà de les funcions theta hiperel·líptiques i considerar un cas més general donat per corbes del tipus $y^n = f(x)$, amb simetria cíclica. Això portà a la generalització de la fórmula de Thomae per a les funcions theta associades [38], que acabà essent demostrada per Nakayashiki [280] per mitjà de mètodes clàssics. Smirnov [361] aplicà la fórmula de Thomae generalitzada per a resoldre l'equació de Knizhnik-Zamolodchikov en nivell 0. Més recentment, la fórmula ha estat usada en [45] per a descriure la geometria d'un 3-monopol. Les fórmules de Thomae apareixen també en el context del problema de Riemann-Hilbert i en les equacions de Schlesinger associades ([74], [226]).

Les aplicacions físiques han fet que la fórmula de Thomae i les seves generalitzacions tornessin a captar l'atenció dels matemàtics. La demostració “elemental” que es tro-

ba en [116], les fórmules per als períodes hiperel·líptics de [119], i el llibre [124] fan palès que el *tesor abandonat* era, certament, valuós.

J. reine u. angew. Math. **71** (1870), 201–222

CONTRIBUCIÓ A LA DETERMINACIÓ DE $\vartheta(0, 0, \dots, 0)$ PER MITJÀ DELS MÒDULS DE CLASSES DE FUNCIONS ALGEBRAIQUES

del Sr. J. THOMAE a Halle

En un breu article en el volum 66 d'aquesta revista, he representat $d \lg \vartheta(0, 0, \dots, 0)$ com un diferencial dels mòduls de classes. Només puc portar a terme la integració d'aquesta expressió en el cas en què les p variables de la funció

$$\vartheta(v_1, v_2, \dots, v_p) = \left(\sum_{-\infty}^{+\infty} \right)^p e^{(\sum_1^p)^2 a_{\mu\mu'} \cdot m_\mu m_{\mu'} + 2 \sum_1^p v_\mu m_\mu}$$

(on els sumatoris en els exponents són respecte de μ i μ' , i els sumatoris exteriors, de $m_1, m_2, \dots, m_p$) són funcions només *bivaluades* de p integrals algebraiques finites arreu. Vaig presentar l'execució de la integració per a aquest cas, quan $p = 2$, en una memòria impresa el març de l'any 1865 a Halle (més tard, també en el *Schlömilchschen Zeitschrift für Math. und Phys.*, vol. 17, p. 427). Això no obstant, és desitjable tenir, per al cas explicat, no solament el mètode, sinó també resultats completament acabats. Per aquest motiu, en la memòria que segueix representarem $\vartheta(0, 0, \dots, 0)$, juntament amb altres constants més, com a funció dels valors de ramificació d'una superfície de RIEMANN T , $(2p + 1)$ -múltiplement connexa, quan aquesta recobreix un pla pertot només dues vegades. RIEMANN anomena $2p - 1$ d'aquests punts de ramificació els mòduls

d'una classe de sistemes de superfícies amb la mateixa ramificació, o bé algebraïques com cadascuna de les funcions ramificades, per la qual cosa $\vartheta(0, 0, \dots, 0)$ pot ésser interpretat com una funció dels mòduls de classes. En el que segueix, citaré per (R. p.) la memòria de RIEMANN sobre les funcions *abelianes* del volum 54 i mantindré arreu la notació que s'hi empra.

La primera secció conté ara la descripció i la notació de la superfície T en què es basen les nostres recerques, la qual és $(2p+1)$ -múltiplement connexa, però que recobreix pertot un pla només dues vegades, i s'hi mostraran disposats en forma de taula els valors de p integrals independents entre si per als $2p+2$ punts de ramificació. Cadascuna d'aquestes integrals conté una constant additiva arbitrària. En la secció segona es trobarà una expressió per a aquestes constants que és especialment còmoda per a la representació de funcions *abelianes* per aquelles integrals per mitjà de funcions ϑ . En la secció tercera es mostrarà que cada integral de segona espècie podria ésser representada mitjançant quocients diferencials d'integrals de primera espècie, anomenats d'acord amb els valors de ramificació, i mitjançant funcions algebraïques. Per comparació de la representació directa amb l'obtinguda mitjançant funcions ϑ , s'obtenen relacions útils entre els quocients diferencials dels mòduls de les funcions ϑ i els mòduls de periodicitat de les integrals finites arreu (per al cas $p=1$ foren trobades d'una altra manera per JACOBI en les *Fundamenta nova* p. 74). En la secció quarta, $\vartheta(0, 0, \dots, 0)$ serà representada completament com a funció dels $2p+2$ valors de ramificació. D'això es conclou de manera senzilla en la secció següent

la determinació de

$$e^{\frac{i}{4}(\sum_1^p)^2_{(\varrho\varrho')} a_{\varrho\varrho'} h_{\varrho} h_{\varrho'}} \cdot \vartheta \left(\dots, \frac{1}{2} \sum_1^p {}_{(\varrho)} a_{\mu\varrho} h_{\varrho} + \frac{i\pi}{2} g_{\mu}, \dots \right),$$

quan h_{ϱ} , g_{ϱ} són nombres enters arbitraris. Però l'expressió

$$\begin{aligned} & \vartheta_{h_1, h_2, \dots, h_p; g_1, g_2, \dots, g_p}(\dots, v_p, \dots) = \\ & = e^{\sum_1^p {}_{(\varrho)} h_{\varrho} v_{\varrho} + \frac{1}{4}(\sum_1^p)^2_{(\varrho\varrho')} a_{\varrho\varrho'} h_{\varrho} h_{\varrho'}} \cdot \\ & \cdot \vartheta \left(\dots, v_{\mu} + \frac{1}{2} \sum_1^p {}_{(\varrho)} a_{\mu\varrho} h_{\varrho} + \frac{i\pi}{2} g_{\mu}, \dots \right) \end{aligned}$$

cal que sigui anomenada abreujadament una funció ϑ parella quan

$$\sum_1^p {}_{(\varrho)} h_{\varrho} g_{\varrho} \equiv 0 \pmod{2},$$

i senar quan

$$\sum_1^p {}_{(\varrho)} h_{\varrho} g_{\varrho} \equiv 1 \pmod{2}.$$

En la secció cinquena es determinen, en funció de valors de ramificació, totes les funcions ϑ parelles d'arguments que s'anul·len, en tant que elles no s'anul·lin, i es deduirà una relació entre funcions ϑ parelles i determinants funcionals de p funcions ϑ senars per a arguments que s'anul·len. A més, aquesta secció conté encara la representació d'una classe de funcions (*abelianes*) bivaluades en T per mitjà de quocients ϑ . Si aquesta relació (14), per a la qual la deducció de $\frac{p(p+1)}{2}$ mòduls de la funció ϑ únicament conté

$2p-1$ graus de llibertat, encara fos vàlida per a mòduls arbitraris, aleshores en cada cas $\vartheta(0, 0, \dots, 0)$ seria fàcilment determinable com a funció dels mòduls de classes; això no obstant, la demostració d'aquesta en el cas general encara no m'ha sortit. En la secció sisena es representen els quocients diferencials parcials de funcions ϑ senars en arguments nuls mitjançant els valors de ramificació, sempre que aquests quocients diferencials no s'anul·lin.

Tot seguit, remarquem encara que en aquesta memòria fem servir les abreviacions $|x_{\lambda\lambda'}|$ o bé $|x_{\lambda}^{(\lambda')}|$, i expressions semblants, per als determinants

$$\begin{vmatrix} x_{11} & x_{12} & \cdots & x_{1p} \\ x_{21} & x_{22} & \cdots & x_{2p} \\ \cdots & \cdots & \cdots & \cdots \\ x_{p1} & x_{p2} & \cdots & x_{pp} \end{vmatrix} \quad \text{resp.} \quad \begin{vmatrix} x_1^{(1)} & x_1^{(2)} & \cdots & x_1^{(p)} \\ x_2^{(1)} & x_2^{(2)} & \cdots & x_2^{(p)} \\ \cdots & \cdots & \cdots & \cdots \\ x_p^{(1)} & x_p^{(2)} & \cdots & x_p^{(p)} \end{vmatrix}$$

i semblants, i que denotem amb el símbol diferencial δ una derivació parcial o bé una derivació purament formal. A més, denotem per $\prod_1^n {}_{(\varrho)}(\varphi(\varrho))$ el producte $\varphi(1) \cdot \varphi(2) \cdots \varphi(n)$; però quan en aquest hi manca el factor $\varphi(\nu)$, o sigui, per a $\prod_1^n {}_{(\varrho)}(\varphi(\varrho)) : \varphi(\nu)$, escriurem $\prod_1^n {}_{(\varrho)}^{(\nu)}\varphi(\varrho)$.

1

Denotem per T una superfície de RIEMANN $(2p+1)$ -múltiplement connexa, la qual recobreix arreu dues vegades el pla representat pels valors de la variable complexa z , i que prolonga un dels seus fulls en l'altre al voltant de $2p+2$ punts de ramificació

$$k_1, \quad k_2, \quad \dots, \quad k_{2p+1}, \quad k_{2p+2}.$$

Aleshores, cada punt ε de T pot ésser representat per una parella de valors mútuament relacionats de la quantitat z i de la funció bivaluada

$$s = \sqrt{\prod_1^{2p+2} {}_{(\varrho)}(z - k_{\varrho})} = \sqrt{(z - k_1) \cdot (z - k_2) \cdots (z - k_{2p+2})}.$$

Ens imaginem que la prolongació d'un full de la superfície T en l'altre té lloc al llarg de línies que són traçades entre k_1 i k_2 , entre k_3 i k_4 , ..., entre $k_{2\varrho-1}$ i $k_{2\varrho}$, ..., entre k_{2p+1} i k_{2p+2} de manera que no es tallen ni a si mateixes ni les unes amb les altres (cf. la fig. més avall). Portem a terme el tall de la superfície T d'acord amb el procediment donat per RIEMANN a l'article 19 de les funcions *abelianes* (R. p. 143). Això es pot realitzar d'infinites maneres diferents, i cada pas d'un sistema de talls a un altre correspon a una transformació lineal de funcions ϑ i recíprocament; a causa de les eleccions fetes aquí, la situació particular dels punts no és significativa.

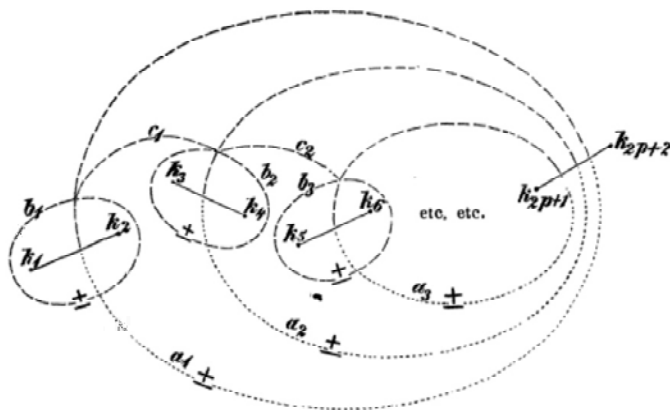


Figura 4. Talls a la superfície

Tracem al voltant de k_1, k_2 una línia b_1 d'anada i torna-da que resti sempre dins d'un full de la superfície T sense trencar-la, i aleshores portem a terme un tall a_1 de la banda positiva (interna) de b_1 a la negativa, que retorni al punt de sortida, mentre fem passar a_1 a l'altra branca de la superfície per sobre de la línia $\overline{k_1 k_2}$, i des d'allí deixem a l'esquerra els punts de ramificació $k_2, k_3, \dots, k_{2p+1}$ i tornem a la primera branca de la superfície per sobre de la línia $\overline{k_{2p+1} k_{2p+2}}$. (En la figura s'indiquen les línies en un full per mitjà d'un traç discontinu, en l'altre per mitjà de punts, i les que pertanyen a ambdós mitjançant un camí continu.) Exactament de la mateixa manera tracem una corba tancada b_2 al voltant de k_3, k_4 en el mateix full en el qual està situat b_1 , que no trobi a_1, b_1 i que no trenqui la superfície T . Des del marge positiu d'aquesta corba portem a terme un tall a_2 que passa a l'altra branca de la superfície per sobre de la línia $\overline{k_3 k_4}$, d'allí passa al primer full per sobre de la línia $\overline{k_{2p+1} k_{2p+2}}$ i retorna al punt de sortida pel marge negatiu, de manera que al llarg de tot el recorregut a_1 quedi a la dreta i els punts de ramificació $k_4, k_5, \dots, k_{2p+1}$ quedin a l'esquerra. A continuació tracem una corba tancada b_3 al voltant de k_5, k_6 que no trenqui T , que estigui situada amb b_1, b_2 en el mateix full de T , i que no trobi enlloc $a_1, a_2; b_1, b_2$. Des del marge positiu de b_3 , tracem un tall a_3 passant a l'altre full per sobre de la línia $\overline{k_5 k_6}$, deixant sempre a la dreta a_2 i a l'esquerra $k_6, k_7, \dots, k_{2p+1}$, i des d'allí passem per sobre de la línia $\overline{k_{2p+1} k_{2p+2}}$ al primer full, retornant al punt de sortida pel marge negatiu de b_3 . I així continuem, fins que hem traçat p sistemes $a_1, b_1; a_2, b_2; \dots; a_p, b_p$ i no és possible traçar-ne cap més de semblant. Si ara unim encara a_1 i b_2 mitjançant una línia c_1 que no trenqui T , de la mateixa manera a_2 i b_3 mitjançant una línia c_2 , etc., a_{p-1}

i b_p mitjançant c_{p-1} , aleshores mitjançant el sistema de línies a, b, c la superfície T queda tallada en una superfície simplement connexa T' de primera espècie tal com postula el procediment esmentat de RIEMANN.

Ara existeixen p funcions univaluades (i no més de p independents entre si), finites arreu i contínues en T' , que als dos costats dels talls a, b difereixen cadascuna en unes quantitats constants, que s'anomenen mòduls de periodicitat, però que als dos costats de les línies c prenen els mateixos valors. Aquests són les p integrals

$$w_1(s, z) = \int \frac{dz}{s}, w_2(s, z) = \int \frac{z dz}{s}, \dots, w_p(s, z) = \int \frac{z^{p-1} dz}{s}.$$

Sigui w_μ més gran a la vora positiva de a_ν que a la vora negativa segons el mòdul de periodicitat $A_\mu^{(\nu)}$, i més gran a la vora positiva de b_ν que a la vora negativa segons el mòdul de periodicitat $B_\mu^{(\nu)}$. Aleshores, $A_\mu^{(\nu)}$ és la integral $\int \frac{z^{\mu-1} dz}{s}$ presa sobre el tall b_ν , i $B_\mu^{(\nu)}$ la mateixa integral presa sobre el tall a_ν , la qual cosa indicarem escrivint b_ν , respectivament a_ν , com a límit inferior.

A partir de les quantitats $w_1, w_2, \dots, w_p$ es componen fàcilment p integrals semblants, $u_1(s, z), u_2(s, z), \dots, u_p(s, z)$, finites arreu, que en cadascun dels talls $a_1, a_2, \dots, a_p$ tenen el mòdul de periodicitat corresponent no nul $i\pi$, però en la resta el tenen nul. A saber, si es fixa

$$\alpha_\varrho^{(\mu)} = i\pi \cdot \frac{\delta \lg |A_\lambda^{(\lambda')}|}{\delta A_\varrho^{(\mu)}},$$

aleshores l'expressió $u_\mu(s, z)$ o bé

$$u_\mu = \sum_1^p {}_{(\varrho)}\alpha_\varrho^{(\mu)} w_\varrho$$

és una funció que en el tall a_μ té el mòdul de periodicitat $i\pi$, en el tall $a_{\mu'}$ ($\mu' \leq \mu$), nul. Però en el tall b_ν , u_μ té el mòdul de periodicitat

$$a_{\mu\nu} = \sum_1^p (e) \alpha_e^{(\mu)} \cdot B_e^{(\nu)} = \sum_1^p (e) \alpha_e^{(\nu)} \cdot B_e^{(\mu)} = a_{\nu\mu}.$$

Pel pas sobre les línies c aquestes integrals varien de manera contínua.

Si de moment deixem ara indeterminades les constants additives en $u_1, u_2, \dots, u_p$, i fixem

$$2u_\mu(0, k_1) = x_\mu + a_{\mu 1},$$

aleshores es troben fàcilment els valors que prenen $u_1, u_2, \dots, u_p$ en els punts de ramificació mitjançant la reflexió que la integral u_μ en el camí d'un punt de ramificació al següent creix tant en un full com de tornada en el camí congru de l'altre full, i que el creixement total és un mòdul de periodicitat. En la taula següent s'apleguen aquests valors de manera fàcilment còpsable:

	$2u_1 - x_1,$	$2u_2 - x_2,$	$\dots 2u_\mu - x_\mu,$	$\dots 2u_p - x_p$
$k_1;$	$a_{11},$	$a_{21},$	$\dots a_{\mu 1},$	$\dots a_{p1}$
$k_2;$	$a_{11} + i\pi,$	$a_{21},$	$\dots a_{\mu 1},$	$\dots a_{p1}$
$k_3;$	$a_{12} + i\pi,$	$a_{22},$	$\dots a_{\mu 2},$	$\dots a_{p2}$
$k_4;$	$a_{12} + i\pi,$	$a_{22} + i\pi,$	$\dots a_{\mu 2},$	$\dots a_{p2}$
$\dots$	$\dots$	$\dots$	$\dots \dots$	$\dots \dots$
$k_{2\mu-1};$	$a_{1\mu} + i\pi,$	$a_{2\mu} + i\pi,$	$\dots a_{\mu\mu},$	$\dots a_{p\mu}$
$k_{2\mu};$	$a_{1\mu} + i\pi,$	$a_{2\mu} + i\pi,$	$\dots a_{\mu\mu} + i\pi,$	$\dots a_{p\mu}$
$\dots$	$\dots$	$\dots$	$\dots \dots$	$\dots \dots$
$k_{2p-1};$	$a_{1p} + i\pi,$	$a_{2p} + i\pi,$	$\dots a_{\mu p} + i\pi,$	$\dots a_{pp}$
$k_{2p};$	$a_{1p} + i\pi,$	$a_{2p} + i\pi,$	$\dots a_{\mu p} + i\pi,$	$\dots a_{pp} + i\pi$
$k_{2p+1};$	$i\pi,$	$i\pi,$	$\dots i\pi,$	$\dots i\pi$
$k_{2p+2};$	$0,$	$0,$	$\dots 0,$	$\dots 0.$

Ara és important per a les nostres recerques mostrar que la funció $\vartheta(v_1, v_2, \dots, v_p)$ s'apropa al valor 1 quan substituïm els mòduls $\dots, a_{\mu\mu'}, \dots$ pels igualment denotats mòduls de periodicitat de les integrals $u_1, u_2, \dots, u_p$, si el punt de ramificació k_2 s'atansa infinitament a k_1, k_4 a $k_3, \dots, k_{2p}$ a k_{2p-1} . En aquest cas, les integrals $w_1, w_2, \dots, w_p$ esteses als talls $b_1, b_2, \dots, b_p$ romanen finites i segons el teorema de CAUCHY $A_\mu^{(\nu)}$ pren el valor

$$A_\mu^{(\nu)} = \int_{b_\nu} \frac{z^{\mu-1} \cdot dz}{\sqrt{(z - k_{2p+1}) \cdot (z - k_{2p+2})} \cdot \prod_{(e)}^p (z - k_{2e-1})} =$$

$$= \frac{2\pi i k_{2\nu-1}^{\mu-1}}{\sqrt{(k_{2\nu-1} - k_{2p+1})(k_{2\nu-1} - k_{2p+2})} \cdot \prod_{(e)}^{p(\nu)} (k_{2\nu-1} - k_{2e-1})},$$

i d'això en resulta per al determinant $|A_\lambda^{(\lambda')}|$ el valor obtingut mitjançant la igualtat següent:

$$\frac{|A_\lambda^{(\lambda')}| \cdot \sqrt{\prod_1^p (e) ((k_{2p+1} - k_{2e-1})(k_{2p+2} - k_{2e-1}))}}{(2\pi i)^p} =$$

$$= \frac{1}{\begin{vmatrix} 1 & k_1 & k_1^2 & \dots & k_1^{p-1} \\ 1 & k_3 & k_3^2 & \dots & k_3^{p-1} \\ \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots \\ 1 & k_{2p-1} & k_{2p-1}^2 & \dots & k_{2p-1}^{p-1} \end{vmatrix}}.$$

Les integrals $B_\mu^{(\nu)}$, però, creixen fins a l'infinit, quan s'emprèn l'apropament de tots aquells punts de ramificació. Però quan es pren $k_2 = k_1 + \Delta_1$, $k_4 = k_3 + \Delta_2$, $\dots$,

$k_{2p} = k_{2p-1} + \Delta_p$, el comportament de les quantitats $B_\mu^{(1)}$, $B_\mu^{(2)}$, $\dots$, $B_\mu^{(p)}$ pot ésser qualsevol mitjançant una elecció escaient del comportament de les nostres quantitats Δ_1 , Δ_2 , $\dots$, Δ_p de manera que tendixin a l'infinit, mentre que els límits de les quantitats $A_\mu^{(\nu)}$ no depenen d'aquests comportaments. Ara es té (R. p. 144) la relació

$$\sum_1^p {}_{(\varrho)}(A_\mu^{(\varrho)} B_{\mu'}^{(\varrho)} - A_{\mu'}^{(\varrho)} B_\mu^{(\varrho)}) = 0,$$

d'on en resulta, quan es té en compte l'arbitrarietat del comportament de $B_\mu^{(1)} : B_\mu^{(2)} : B_\mu^{(3)} \dots$ i la constància de les quantitats $A_\mu^{(\varrho)}$, el comportament resultant

$$B_\mu^{(\varrho)} : B_{\mu'}^{(\varrho)} = A_\mu^{(\varrho)} : A_{\mu'}^{(\varrho)} \quad \text{o bé} \quad B_\mu^{(\varrho)} = f^{(\varrho)} \cdot A_\mu^{(\varrho)}$$

per a $\Delta_1, \Delta_2, \dots, \Delta_p$ tendint a zero. D'això se'n segueix immediatament que, per a $\mu \gtrless \mu'$,

$$\begin{aligned} a_{\mu\mu'} &= i\pi \sum_1^p {}_{(\varrho)} \frac{\delta \lg |A_\lambda^{(\lambda')}|}{\delta A_\varrho^{(\mu)}} \cdot B_\varrho^{(\mu')} = \\ &= i\pi f^{(\mu')} \cdot \sum_1^p {}_{(\varrho)} \frac{\delta \lg |A_\lambda^{(\lambda')}|}{\delta A_\varrho^{(\mu)}} \cdot A_\varrho^{(\mu')} = i\pi f^{(\mu')} \cdot 0 \end{aligned}$$

són infinitament petits en comparació amb les quantitats

$$a_{\mu\mu} = i\pi f^{(\mu)} \cdot \sum_1^p {}_{(\varrho)} \frac{\delta \lg |A_\lambda^{(\lambda')}|}{\delta A_\varrho^{(\mu)}} \cdot A_\varrho^{(\mu)} = i\pi f^{(\mu)},$$

perquè les quantitats $f^{(1)}, f^{(2)}, \dots, f^{(p)}$ tenen comportament finit les unes respecte de les altres, quan els comportaments de $\Delta_1, \Delta_2, \dots, \Delta_p$ són finits. Sota el supòsit d'aquest comportament finit (el qual, per cert, no és necessari

però és còmode) se'n dedueix immediatament que la sèrie p -múltiplement infinita per a $\vartheta(v_1, v_2, \dots, v_p)$ es redueix al terme d'ordre zero, per tant al nombre 1.

2

En fixar per a les variables $v_1, v_2, \dots, v_p$ de la funció ϑ les quantitats respectives

$$u_1(s, z) - \sum_1^p (p) u_1(s_\varrho, z_\varrho),$$

$$u_2(s, z) - \sum_1^p (p) u_2(s_\varrho, z_\varrho),$$

$\dots,$

$$u_p(s, z) - \sum_1^p (p) u_p(s_\varrho, z_\varrho)$$

i per als mòduls, els mòduls de periodicitat $\dots, a_{\mu\mu'}, \dots$ de les integrals $u_1, u_2, \dots, u_p$, les constants que encara hem deixat lliures darrerament es poden determinar d'una manera i només d'una tal que $\vartheta(v_1, v_2, \dots, v_p)$ s'anul·li en els punts $(s_1, z_1), (s_2, z_2), \dots, (s_p, z_p)$ de la superfície T . Els mitjans per a aquesta determinació els ha indicat RIEMANN a l'art. 23 de les seves *Abelschen Functionen* (R. p. 148). En el nostre cas especial la recepta que s'hi dona diu que $\vartheta(v_1, v_2, \dots, v_p)$ s'ha d'anul·lar quan $\dots, v_\mu, \dots$ és substituït per les sumes $\dots, \sum_{(\varrho)}^{(p-1)} u_\mu(0, k_\varrho), \dots$, on el sumatori s'estén a cadascuna de les combinacions arbitràries de $p - 1$ valors de ramificació k_ϱ , i alhora cal que sigui

$$(2 \sum_{(\varrho)}^{(p-1)} u_1(0, k_\varrho), \quad 2 \sum_{(\varrho)}^{(p-1)} u_2(0, k_\varrho), \dots, \quad 2 \sum_{(\varrho)}^{(p-1)} u_p(0, k_\varrho)) \equiv$$

$$\equiv (0, 0, \dots, 0)$$

per als $2p$ sistemes de mòduls de la funció u . D'aquestes condicions se'n dedueix que x_μ ha de poder ésser escrit en la forma $\frac{1}{p-1} \sum_1^p (e) \delta_e a_{\mu e} + \gamma_\mu \frac{i\pi}{p-1}$, on δ_e, γ_e són nombres enters. En formar les sumes dels valors de $\dots, 2u_\mu(s, z), \dots$ per a $p-1$ punts de ramificació, amb l'ajut de la taula del primer article s'obtenen expressions de la forma

$$\dots, \sum_1^p (e) h_e a_{\mu e} + g_\mu i\pi, \dots$$

i en substituir les meitats d'aquestes sumes en les variables $\dots, v_\mu, \dots$ de la funció $\vartheta(\dots, v_\mu, \dots)$, aquesta s'anul·la d'acord amb el que hem recordat en la introducció si $\sum_1^p (e) h_e g_e \equiv 1 \pmod{2}$. Per tant, les quantitats γ_e, δ_e han d'ésser determinades de manera que se satisfaci aquesta restricció. En denotar ara la suma

$$u_\mu(0, k_\lambda) + \sum_1^{p-2} (e) u_\mu(0, k_{2e-1})$$

per $U_\mu^{(\lambda)}$ i fixar

$$1 + \delta_1 = h_1, \quad 1 + \delta_2 = h_2, \quad \dots, \quad 1 + \delta_{p-2} = h_{p-2},$$

$$\delta_{p-1} = h_{p-1}, \quad \delta_p = h_p,$$

$$p-3 + \gamma_1 = g_1, \quad p-4 + \gamma_2 = g_2, \quad \dots, \quad 1 + \gamma_{p-3} = g_{p-3},$$

$$\gamma_{p-2} = g_{p-2}, \quad \gamma_{p-1} = g_{p-1}, \quad \gamma_p = g_p,$$

trobem que

$$(A) \quad 2U_\mu^{(2\nu)} = \sum_1^p (e) h_e a_{\mu e} + g_\mu i\pi + a_{\mu\nu} + \theta_\mu i\pi,$$

on cal fixar $a_{\mu p+1} = 0$ quan la igualtat es construeix per a $\nu = p + 1$, i cal prendre $\theta_\mu = 1$ per a $\mu \leq \nu$, $\theta_\mu = 0$ per a $\mu > \nu$ i per a $\nu = p + 1$. A més,

$$(B) \quad 2U_\mu^{(2p-3)} = \sum_1^p {}_{(\varrho)}h_\varrho a_{\mu p} + a_{\mu p-1} + g_\mu i\pi + \varepsilon_\mu i\pi,$$

on cal fixar $\varepsilon_\mu = 1$ per a $\mu \leq p - 2$, $\varepsilon_\mu = 0$ per a $\mu = p - 1$, p . A continuació,

$$(C) \quad 2U_\mu^{(2p-1)} = \sum_1^p {}_{(\varrho)}h_\varrho a_{\mu p} + a_{\mu p} + g_\mu i\pi + \eta_\mu i\pi,$$

on $\eta_1 = \eta_2 = \dots = \eta_{p-1} = 1$, $\eta_p = 0$. Finalment,

$$(D) \quad 2U_\mu^{(2p+1)} = \sum_1^p {}_{(\varrho)}h_\varrho a_{\mu \varrho} + i\pi g_\mu + i\pi.$$

Ara, atès que $\vartheta(\dots, U_\mu^{(\lambda)}, \dots)$ s'ha d'anul·lar, d'acord amb (A) per a $\nu = p + 1$, se segueix en primer lloc la condició

$$\sum_1^p {}_{(\varrho)}h_\varrho g_\varrho \equiv 1 \pmod{2},$$

i quan aquesta es té en consideració, per a qualsevol altre valor de ν se segueix que

$$\sum_1^\nu h_\varrho + g_\nu \equiv 1 \pmod{2},$$

i, d'aquí, quan es resta la congruència en la qual es fixa $\nu + 1$ en lloc de ν ,

$$(a) \quad g_{\nu+1} - g_\nu \equiv h_{\nu+1} \pmod{2}.$$

De (B) se segueix que

$$\sum_1^{p-2} {}_{(\varrho)}h_{\varrho} + g_{p-1} \equiv 0 \pmod{2},$$

de (C) i (D) ,

$$\sum_1^{p-1} {}_{(\varrho)}h_{\varrho} + g_p \equiv 0 \pmod{2}, \quad \sum_1^p h_{\varrho} \equiv 0 \pmod{2},$$

i mitjançant combinacions molt fàcils a partir d'aquestes congruències es dedueixen els resultats

(b)

$$g_p \equiv g_{p-2} \equiv h_p \equiv h_{p-1} \equiv 1 \pmod{2}, \quad g_{p-1} \equiv 0 \pmod{2}.$$

En fixar ara a continuació

$$V_{\mu}^{(\lambda)} = \sum_1^{p-2} {}_{(\varrho)}u_{\mu}(0, k_{2\varrho}) + u_{\mu}(0, k_{\lambda}),$$

es té que

$$2V_{\mu}^{(2\nu-1)} = \sum_1^p {}_{(\varrho)}h_{\varrho}a_{\mu\varrho} + a_{\mu\nu} + g_{\mu}i\pi + \zeta_{\mu}i\pi,$$

d'on

$$\zeta_1 = \zeta_2 = \cdots = \zeta_{\nu-1} = 2, \quad \zeta_{\nu} = \zeta_{\nu+1} = \cdots = \zeta_{p-3} = 1,$$

$$\zeta_{p-2} = \zeta_{p-1} = \zeta_p = 0.$$

Ara, atès que $\vartheta(\dots, V_{\mu}^{(\lambda)}, \dots)$ s'anul·la, se'n segueix, quan $\nu \leq p-2$ i amb exclusió de múltiples enters de 2, que

$$g_{\nu} \equiv 1 + h_{\nu} + h_{\nu+1} + \cdots + h_{p-2} \pmod{2},$$

de la qual se'n segueix novament

$$(c) \quad g_{\nu+1} - g_{\nu} \equiv h_{\nu} \pmod{2},$$

i per a $\nu = p - 2$ es té $h_{p-2} \equiv g_{p-2} - 1$ i, d'acord amb (b), $h_{p-2} \equiv 0 \pmod{2}$, per tant,

$$h_1 \equiv h_2 \equiv \dots \equiv h_{p-2} \equiv 0, \quad h_{p-1} \equiv h_p \equiv 1$$

i, d'acord amb (c),

$$g_{p-2\nu-1} \equiv 0, \quad g_{p-2\nu} \equiv 1 \pmod{2}.$$

D'aquí es conclou que per als nombres γ_{ϱ} , δ_{ϱ} es poden escollir els valors

$$\delta_1 = \delta_2 = \dots = \delta_p = 1, \quad \gamma_p = 1, \quad \gamma_{p-1} = 2, \quad \dots, \quad \gamma_1 = p,$$

i d'aquí s'obtenen els valors següents ¹⁾ per a les integrals u en el punt k_1 :

$$\begin{aligned} 2u_1(0, k_1) &= \frac{pi\pi}{p-1} + \frac{1}{p-1} \sum_1^p {}_{(\varrho)}a_{1\varrho} + a_{11}, \\ 2u_2(0, k_1) &= \frac{(p-1)i\pi}{p-1} + \frac{1}{p-1} \sum_1^p {}_{(\varrho)}a_{2\varrho} + a_{21}, \\ \dots &\quad \dots \\ 2u_{\nu}(0, k_1) &= \frac{(p-\nu+1)i\pi}{p-1} + \frac{1}{p-1} \sum_1^p {}_{(\varrho)}a_{\nu\varrho} + a_{\nu 1}, \\ \dots &\quad \dots \\ 2u_p(0, k_1) &= \frac{i\pi}{p-1} + \frac{1}{p-1} \sum_1^p {}_{(\varrho)}a_{p\varrho} + a_{p1}. \end{aligned}$$

¹⁾Els mateixos valors inicials han estat també escollits pel Sr. NEUMANN.

3

Si ara, com abans, és $v_\mu = u_\mu(s, z) - \sum_1^p ({}_{(\varrho)}u_\mu(s_\varrho, z_\varrho))$, aleshores

$$\frac{d \lg \vartheta(v_1, v_2, \dots, v_p)}{dz},$$

com a funció de (s_ν, z_ν) en T' , és univaluada, pren el mateix valor a les dues bandes de les línies c i en els talls a , i en les bandes positives dels talls b_κ és més gran en

$$2 \frac{du_\kappa(s, z)}{dz} = 2 \sum_1^p ({}_{(\varrho)}\frac{\alpha_\varrho^{(\kappa)} z^{\varrho-1}}{s}$$

que en les negatives, i en el punt (s, z) , que serà denotat per ε , esdevé infinita com $\frac{1}{z - z_\nu}$, i altrament és finita i contínua en tot T' . Però mitjançant aquestes propietats una tal funció, que denotem per

$$t(\varepsilon; s_\nu, z_\nu),$$

és ja determinada llevat d'una constant additiva independent de z_ν , quan també els valors dels mòduls de periodicitat en els talls $b_1, b_2, \dots, b_p$ no són donats; perquè la diferència entre dues d'aquestes possibles funcions diferents en T' seria contínua arreu i en els p talls tindria els mòduls de periodicitat nuls, i en conseqüència seria constant. Ara

$$\frac{\partial u_\kappa(s_\nu, z_\nu)}{\partial k_\mu}$$

és una integral univaluada en T' , per a la qual únicament per a $z = k_\mu$ esdevé infinitament gran de primer ordre, però

altament és contínua en T' en creuar les línies c i a , i, en multiplicar-la per $\sqrt{z_\nu - k_\mu}$, per a $z_\nu = k_\mu$ pren el valor

$$\lim_{z=k_\mu} \sqrt{(z_\nu - k_\mu)} \cdot \frac{\partial u_\kappa(s_\nu, z_\nu)}{\partial z_\nu} = - \sum_1^p (\varrho') \frac{\alpha_{\varrho'}^{(\kappa)} k_\mu^{\varrho'-1}}{\prod_1^{2p+1} (\varrho) (k_\mu - k_\varrho)}.$$

Per tant, en la igualtat

$$\begin{aligned} t(\varepsilon; s_\nu, z_\nu) = \\ = \sum_{(\varrho)}^{(p)} \frac{\partial u_\kappa(s_\nu, z_\nu)}{\partial k_\varrho} c_{\kappa\varrho} + \frac{s \cdot \prod_{(\varrho)}^{(p)} (z_\nu - k_\varrho) + s_\nu \prod_{(\varrho)}^{(p)} (z - k_\varrho)}{2s \cdot (z - z_\nu) \prod_{(\varrho)}^{(p)} (z_\nu - k_\varrho)}, \end{aligned}$$

en la qual κ és arbitrari, i la suma i el producte s'estenen sobre p punts de ramificació escollits arbitràriament, es poden determinar les p quantitats $c_{\kappa 1}, c_{\kappa 2}, \dots, c_{\kappa p}$ de manera que la funció esdevingui infinitament gran únicament per a $(s_\nu, z_\nu) = (s, z)$ (tal com succeeix en $\frac{1}{z - z_\nu}$).

Això s'aconsegueix en fixar

$$c_{\kappa\varrho} = \frac{\prod_1^{2p+2} (\varrho) (k_\varrho - k_{\varrho'}) \cdot \prod_{(\varrho')}^{(p)} (z - k_{\varrho'})}{\sum_1^p (\varrho') \alpha_{\varrho'}^{(\kappa)} k_\varrho^{\varrho'-1} \cdot 2s(z - k_\varrho) \prod_{(\varrho')}^{(p)} (\varrho) (k_\varrho - k_{\varrho'})}.$$

D'això s'obté la igualtat

$$(1) \quad t(\varepsilon; s_\nu, z_\nu) =$$

$$\begin{aligned}
&= \sum_{(\varrho)}^{(p)} \left\{ \prod_{(\varrho')}^{(p)} \frac{(z - k_{\varrho'})}{(k_{\varrho} - k_{\varrho'})} \cdot \frac{\prod_1^{2p+2} (\varrho') (k_{\varrho} - k_{\varrho'}) \cdot \partial u_{\kappa}(s_{\nu}, z_{\nu})}{\sum_1^p (\varrho') \alpha_{\varrho'}^{(\kappa)} k_{\varrho}^{\varrho'-1} \cdot 2s \partial k_{\varrho}} \right\} + \\
&\quad + \frac{s \prod_{(\varrho)}^{(p)} (z_{\nu} - k_{\varrho}) + s_{\varrho} \prod_{(\varrho)}^{(p)} (z - k_{\varrho})}{2s \cdot (z - z_{\nu}) \prod_{(\varrho)}^{(p)} (z_{\nu} - k_{\varrho})}.
\end{aligned}$$

Escollim la constant additiva en $t(\varepsilon; s_{\nu}, z_{\nu})$ tal com es presenta en la igualtat (1). D'aquí se segueix la igualtat

$$(2) \quad \frac{d \lg \vartheta(v_1, v_2, \dots, v_p)}{dz} = \prod_1^p (\varrho) t(\varepsilon; s_{\varrho}, z_{\varrho}) + C,$$

on C depèn de s i z , i és completament independent de s_{ν} , z_{ν} . Es tenen mitjans per a determinar la quantitat C com a funció de z i de les quantitats $k_1, k_2, \dots, k_{2p+2}$, per exemple fent $(v_1, v_2, \dots, v_p) \equiv (0, 0, \dots, 0)$ en cada $2p$ sistemes de mòduls de les funcions u , la qual cosa pot succeir per a cada ε donat. Pot ésser suficient valorar aquesta constant en el cas en el qual ε col·lapsa en un punt de ramificació

k_ν . Per a aquest cas la igualtat (2) es transforma en

$$\begin{aligned}
 & \sum_1^p {}_{(\varrho)} \frac{\partial \lg \vartheta(v_1, v_2, \dots, v_p)}{\partial v_\varrho} \cdot \sum_1^p {}_{(\varrho')} \alpha_{\varrho'}^{(\varrho)} k_\nu^{\varrho'-1} = \\
 (3) \quad & = \sum_1^p {}_{(\varrho)} \frac{\prod_1^{2p+2} {}_{(\varrho')}^{(\nu)} (k_\nu - k_{\varrho'}) \cdot \partial u_\kappa(s_\varrho, z_\varrho)}{2 \cdot \sum_1^p {}_{(\varrho')} \alpha_{\varrho'}^{(\kappa)} k_\nu^{\varrho'-1} \cdot \partial k_\nu} + K_{\kappa\nu},
 \end{aligned}$$

on manifestament $K_{\kappa\nu}$ només depèn dels valors de ramificació. En comparar a continuació els mòduls de periodicitat dels dos costats de la igualtat (3) amb talls $b_{\kappa'}$ en relació amb la variable z_ϱ , se segueix que

$$(4^a) \quad 2 \sum_1^p {}_{(\varrho)} \alpha_{\varrho}^{\kappa'} \cdot k_\nu^{\varrho-1} = \frac{\prod_1^{2p+2} {}_{(\varrho)}^{(\nu)} (k_\nu - k_\varrho) \cdot \partial a_{\kappa\kappa'}}{2 \sum_1^p {}_{(\varrho')} \alpha_{\varrho'}^{(\kappa)} k_\nu^{\varrho'-1} \partial k_\nu},$$

d'on obtenim la important relació:

$$(4) \quad \frac{\partial a_{\mu\mu'}}{\partial k_\nu} = \frac{4 \sum_1^p {}_{(\varrho)} \alpha_{\varrho}^{(\mu)} k_\nu^{\varrho-1} \cdot \sum_1^p {}_{(\varrho')} \alpha_{\varrho'}^{(\mu')} k_\nu^{\varrho'-1}}{\prod_1^{2p+2} {}_{(\varrho)}^{(\nu)} (k_\nu - k_\varrho)}.$$

Però la constant $K_{\kappa\nu}$ és aquesta

$$(5) \quad K_{\kappa\nu} = - \frac{\prod_1^{2p+2} {}_{(\varrho)}^{(\nu)} (k_\nu - k_\varrho) \cdot \partial [u_\kappa(0, k_\nu)]}{2 \sum_1^p {}_{\varrho} \alpha_{\varrho}^{(\kappa)} k_\nu^{\varrho'-1} \cdot \partial k_\nu},$$

(on després del signe de diferenciació s'ha escrit un claudàtor per a posar de manifest que els límits de les integrals no s'han de considerar variables). A saber, en fixar per a $z_1, z_2, \dots, z_p$, uns tals dels k_ν punts de ramificació diferents per als quals és

$$(v_1, v_2, \dots, v_p) \equiv \left(\sum_1^p {}_{(\varrho)} a_{1\varrho} h_\varrho + g_1 i\pi, \dots, \sum_1^p {}_{(\varrho)} a_{p\varrho} h_\varrho + g_p i\pi \right),$$

on per h_ϱ, g_ϱ entenem nombres enters, la qual cosa sempre es pot fer, aleshores per mitjà de propietats conegudes de la funció ϑ , el costat esquerre de la igualtat (3) pren el valor

$$\begin{aligned} & -2 \sum_1^p {}_{(\varrho)} h_\varrho \cdot \sum_1^p {}_{(\varrho')} \alpha_{\varrho'}^{(\varrho)} k_\nu^{\varrho'-1} = \\ & = - \sum_1^p {}_{(\varrho)} h_\varrho \cdot \frac{\prod_1^{2p+2} {}_{(\nu)} (k_\nu - k_{\varrho'})}{2 \sum_1^p {}_{(\varrho')} \alpha_{\varrho'}^{(\kappa)} k_\nu^{\varrho'-1}} \cdot \frac{\partial a_{\kappa\varrho}}{\partial k_\nu}, \end{aligned}$$

d'on se segueix el costat dret de (4^a) i on κ és arbitrari. Però el costat dret de la igualtat (3) pren exactament el mateix valor quan en ell $K_{\kappa\nu}$ té el significat (5), perquè es pot escriure en forma de fracció

$$- \frac{\prod_1^{2p+2} {}_{(\nu)} (k_\nu - k_{\varrho'})}{2 \sum_1^p {}_{(\varrho')} \alpha_{\varrho'}^{(\kappa)} k_\nu^{\varrho'-1}} \cdot \frac{\partial \left(\sum_1^p {}_{(\varrho)} u_\kappa(s_\varrho, z_\varrho) - u_\kappa(0, k_\nu) \right)}{\partial k_\nu},$$

d'on la nostra afirmació se segueix immediatament.

En escriure en la igualtat (1) ε_μ en lloc de ε , amb la qual cosa un punt serà denotat (s_μ, z_μ) , i en cada igualtat s'escriu (s, z) en lloc dels punts (s_ν, z_ν) , per pas al límit trobem la igualtat:

$$(6) \quad \lim_{z=k_\nu} \frac{\partial t(\varepsilon_\mu; s, z)}{\partial z} = \frac{1}{2} \frac{\partial^2 u_\kappa(s_\mu, z_\mu)}{\partial z_\mu \partial k_\nu} \cdot \frac{\prod_1^{2p+2} \binom{(\nu)}{(\varrho)} (k_\nu - k_\varrho)}{\sum_1^p \binom{(\nu)}{(\varrho)} \alpha_\varrho^{(\kappa)} k_\nu^{\varrho-1}}.$$

Per a determinar com la funció $\frac{\partial \lg \vartheta(v_1, v_2, \dots, v_p)}{\partial v_p}$ depèn de (s, z) , hem d'observar que, en les línies c i a de T té els mòduls de periodicitat nuls, i també en les línies $b_1, b_2, \dots, b_p$, amb excepció de b_ϱ on té el -2 , i que per a (s, z) igual $(s_1, z_1), (s_2, z_2), \dots, (s_p, z_p)$ esdevé infinita, però altrament és contínua i finita en T' . Aquestes mateixes propietats té la funció

$$\begin{vmatrix} \frac{\partial u_1}{\partial z_1} & \frac{\partial u_1}{\partial z_2} & \dots & \frac{\partial u_1}{\partial z_p} \\ \dots & \dots & \dots & \dots \\ \frac{\partial u_{\varrho-1}}{\partial z_1} & \frac{\partial u_{\varrho-1}}{\partial z_2} & \dots & \frac{\partial u_{\varrho-1}}{\partial z_p} \\ -t(\varepsilon_1; s, z) & -t(\varepsilon_2; s, z) & \dots & -t(\varepsilon_p; s, z) \end{vmatrix} : \left| \frac{\partial u_{\lambda'}}{\partial z_\lambda} \right|, \begin{vmatrix} \frac{\partial u_{\varrho+1}}{\partial z_1} & \frac{\partial u_{\varrho+1}}{\partial z_2} & \dots & \frac{\partial u_{\varrho+1}}{\partial z_p} \\ \dots & \dots & \dots & \dots \\ \frac{\partial u_p}{\partial z_1} & \frac{\partial u_p}{\partial z_2} & \dots & \frac{\partial u_p}{\partial z_p} \end{vmatrix}$$

on $\frac{\partial u_\kappa}{\partial z_\nu}$ abreuja $\frac{\partial u_\kappa(s_\nu, z_\nu)}{\partial z_\nu}$. Aquestes dues funcions poden diferir únicament en una constant additiva independent de (s, z) . A saber, la diferència de les dues funcions és univalueada en T i en p , i només p , punts prefixats *arbitràriament* $(s_1, z_1), (s_2, z_2), \dots, (s_p, z_p)$ esdevé infinita de primer ordre. Una tal funció és necessàriament constant en relació amb (s, z) , perquè entre els p punts en els quals una funció d'una superfície $(2p + 1)$ -múltiplement connexa T esdevé infinitament gran de primer ordre, necessàriament hi ha d'haver una relació (R. p. 122). En derivar respecte de z la igualtat que d'aquí resulta, el quocient diferencial s'allibera d'aquella constant i es té que

$$(7) \left\{ \begin{array}{l} - \left| \frac{\partial u_{\lambda'}}{\partial z_{\lambda}} \right| \cdot \sum_1^p \frac{\partial \lg \vartheta(v_1, v_2, \dots, v_p)}{\partial v_{\varrho} \partial v_{\varrho'}} \frac{u_{\varrho'}(s, z)}{\partial z} = \\ \left| \begin{array}{cccc} \frac{\partial u_1}{\partial z_1} & \frac{\partial u_1}{\partial z_2} & \dots & \frac{\partial u_1}{\partial z_p} \\ \dots & \dots & \dots & \dots \\ \frac{\partial u_{\varrho-1}}{\partial z_1} & \frac{\partial u_{\varrho-1}}{\partial z_2} & \dots & \frac{\partial u_{\varrho-1}}{\partial z_p} \\ -t'(\varepsilon_1; s, z) & -t'(\varepsilon_2; s, z) & \dots & -t'(\varepsilon_p; s, z) \\ \frac{\partial u_{\varrho+1}}{\partial z_1} & \frac{\partial u_{\varrho+1}}{\partial z_2} & \dots & \frac{\partial u_{\varrho+1}}{\partial z_p} \\ \dots & \dots & \dots & \dots \\ \frac{\partial u_p}{\partial z_1} & \frac{\partial u_p}{\partial z_2} & \dots & \frac{\partial u_p}{\partial z_p} \end{array} \right| \end{array} \right.$$

quan per $t'(\varepsilon_\mu; s, z)$ s'entén el quocient diferencial

$$\frac{\partial t(\varepsilon_\mu; s, z)}{\partial z}.$$

En multiplicar ara la igualtat (7) per s i fixar $z = k_\mu$ se segueix, quan es té en compte (6),

$$\begin{aligned} & \left| -\frac{\partial u_{\lambda'}}{\partial z_\lambda} \right| \cdot \sum_1^p \varrho' \frac{\partial^2 \lg \vartheta(v_1, v_2, \dots, v_p)}{\partial v_{\varrho} \cdot \partial v_{\varrho'}} \\ & \frac{\sum_1^p \binom{p}{r} \alpha_r^{(\varrho')} k_\mu^{r-1} \cdot \sum_1^p \binom{p}{r'} \alpha_{r'}^{(\kappa)} k_\mu^{r'-1}}{\prod_1^{2p+2} \binom{(\mu)}{(\nu)} (k_\mu - k_\nu)} = \\ & = \frac{1}{2} \begin{vmatrix} \frac{\partial u_1}{\partial z_1} & \frac{\partial u_1}{\partial z_2} & \dots & \frac{\partial u_1}{\partial z_p} \\ \dots & \dots & \dots & \dots \\ \frac{\partial u_{\varrho-1}}{\partial z_1} & \frac{\partial u_{\varrho-1}}{\partial z_2} & \dots & \frac{\partial u_{\varrho-1}}{\partial z_p} \\ \frac{\partial z_1}{\partial u_\kappa} & \frac{\partial z_2}{\partial u_\kappa} & \dots & \frac{\partial z_p}{\partial u_\kappa} \\ \frac{\partial z_1 \partial k_\mu}{\partial u_{\varrho+1}} & \frac{\partial z_2 \partial k_\mu}{\partial u_{\varrho+1}} & \dots & \frac{\partial z_p \partial k_\mu}{\partial u_{\varrho+1}} \\ \frac{\partial z_1}{\partial u_p} & \frac{\partial z_2}{\partial u_p} & \dots & \frac{\partial z_p}{\partial u_p} \\ \dots & \dots & \dots & \dots \\ \frac{\partial u_p}{\partial z_1} & \frac{\partial u_p}{\partial z_2} & \dots & \frac{\partial u_p}{\partial z_p} \end{vmatrix}. \end{aligned}$$

En escollir el nombre ϱ per al nombre arbitrari κ i aplicarlo al costat esquerre de la igualtat (4) i formar la suma de les expressions obtingudes per a $\varrho = 1, \varrho = 2, \dots, \varrho = p$, se'n segueix la igualtat

$$\frac{1}{4} \left(\sum_1^p \right)_{(\varrho \varrho')}^2 \frac{\partial^2 \lg \vartheta(v_1, v_2, \dots, v_p)}{\partial v_{\varrho} \cdot \partial v_{\varrho'}} \frac{\partial a_{\varrho \varrho'}}{\partial k_\mu} = -\frac{1}{2} \frac{\partial \lg \left| \frac{\partial u_{\lambda'}}{\partial z_\lambda} \right|}{\partial k_\mu}.$$

Quan ara es fixa

$$(v_1, v_2, \dots, v_p) = (0, 0, \dots, 0),$$

se satisfan les igualtats (R. p. 151)

$$\frac{1}{2} \frac{\partial^2 \lg \vartheta}{\partial v_\varrho \partial v_{\varrho'}} = \frac{\partial \lg \vartheta}{\partial a_{\varrho \varrho'}}, \quad \frac{1}{4} \frac{\partial^2 \lg \vartheta}{\partial v_\varrho \partial v_\varrho} = \frac{\partial \lg \vartheta}{\partial a_{\varrho \varrho}},$$

de les quals se segueix, en aplicar-hi (8),

(9)

$$\frac{\partial \lg \vartheta(0, 0, \dots, 0)}{\partial k_\mu} = -\frac{1}{2} \frac{\partial \lg |\alpha_\lambda^{(\lambda')}|}{\partial k_\mu} + \frac{1}{2} \frac{\partial \lg}{\partial k_\mu} \sqrt{\prod_1^p {}_{(\varrho)}(z_\varrho^{(\mu)} - k_\mu)},$$

on $z_1^{(\mu)}, z_2^{(\mu)}, \dots, z_p^{(\mu)}$ denoten uns tals punts de ramificació (diferents de k_μ) per als quals és

$$(\dots, u_\nu(0, k_\mu) - \sum_1^p {}_{(\varrho)}u_\nu(0, z_\varrho^{(\mu)}), \dots) \equiv (0, 0, \dots, 0).$$

Per a deduir el costat dret de la igualtat (9) a partir de la igualtat (8), s'utilitza el teorema del producte dels determinants.

Podem denotar per $\text{Discr}(h_1, h_2, \dots, h_p; g_1, g_2, \dots, g_p)$ el producte de totes les diferències, on el punt amb índex més gran sempre és el minuend, de $p + 1$ dels valors de ramificació que tenen la propietat que

$$\begin{aligned} & (\dots, -\sum_{{}_{(\varrho)}}^{(p)} u_\nu(0, k_\varrho) + u_\nu(0, k_{\varrho'}), \dots) \equiv \\ & \equiv (\dots, g_\nu \frac{i\pi}{2} + \sum_1^p {}_{(\varrho)}h_\varrho \frac{a_{\nu \varrho}}{2}, \dots) \end{aligned}$$

per als $2p$ sistemes de mòduls de la funció u , i també per

$$\text{Discr}'(h_1, h_2, \dots, h_p; g_1, g_2, \dots, g_p)$$

el producte de les diferències igualment ordenades dels $p+1$ punts de ramificació restants que tenen la mateixa propietat. Aleshores, com es reconeix de seguida, per integració de la relació (9) esdevé la igualtat

$$(10) \quad \lg \vartheta(0, 0, \dots, 0) =$$

$$= \text{Const} + \lg \sqrt{\frac{|A_{\lambda}^{(\lambda')}|}{(2\pi i)^p}} + \lg \sqrt[4]{\text{Discr}(0, 0, \dots, 0) \text{Discr}'(0, 0, \dots, 0)},$$

on la constant és independent de k_{μ} i, atès que μ és arbitrària, del conjunt de valors de ramificació. $\text{Discr}(0, 0, \dots, 0)$ conté els punts de ramificació amb índexs parells, però $\text{Discr}'(0, 0, \dots, 0)$ els punts de ramificació amb índexs senars.

A fi de determinar la constant, prenem $k_2 = k_1 + \Delta_1$, $k_4 = k_3 + \Delta_2$, ..., $k_{2p} = k_{2p-1} + \Delta_p$ i permetem que Δ convergeixi cap a zero. Aleshores (d'acord amb la secció

1), $\lg \vartheta(0, 0, \dots, 0)$ pren el valor zero i $\sqrt{\frac{|A_{\lambda}^{(\lambda')}|}{(2\pi i)^p}}$ el valor

$$\frac{1}{\sqrt[4]{\text{Discr}(0, 0, \dots, 0) \text{Discr}'(0, 0, \dots, 0)}},$$

d'on s'obté que la constant additiva ha d'ésser nul·la. Aleshores en l'expressió

(11)

$$\vartheta(0, 0, \dots, 0) = \sqrt{\frac{|A_{\lambda}^{(\lambda')}|}{(2\pi i)^p}} \sqrt[4]{\text{Discr}(0, 0, \dots, 0) \text{Discr}'(0, 0, \dots, 0)}$$

només es pot presentar un dubte sobre el valor de l'arrel quarta de la unitat, que està immers en el signe radical. A fi de fixar-lo, les quantitats $k_1, k_2, \dots, k_{2p+2}$ es prenen reals, i ordenades d'acord amb les desigualtats

$$k_1 < k_2 < k_3 < \dots < k_{2p+2}.$$

Aleshores tots els $A_\mu^{(\nu)}$ són quantitats purament imaginàries i els $B_\mu^{(\nu)}$ purament reals, i, per tant, el costat dret de (11) és real, llevat del producte per una arrel quarta de la unitat. Però tots els $a_{\mu\mu'}$ són aleshores purament reals (per descomptat satisfent sempre les condicions de convergència), d'on cada terme de la sèrie ϑ , d'on $\vartheta(0, 0, \dots, 0)$, és una quantitat real positiva. Segons això, les arrels del costat dret han d'ésser preses de manera que tota l'expressió sigui real positiva.

El signe per a cadascuna de les altres posicions dels punts de ramificació s'obté per desplaçament continu d'aquests cap als reals, amb posició ordenada donada com en la posició precedent.

5

El valor de $u_\mu(0, k_\nu)$ es pot expressar en la forma

$$\sum_1^p {}_{(\varrho)}h_\varrho^{(\nu)} a_{\mu\varrho} + g_\mu^{(\nu)} i\pi,$$

on $h_\varrho^{(\nu)}, g_\mu^{(\nu)}$ són fraccions el denominador de les quals és $2(p-1)$. En el que segueix, fixem

$$v_\mu^{(\nu)} = u_\mu(0, k_\nu) - \sum_1^p {}_{(\varrho)}u_\mu(s_\varrho, z_\varrho)$$

i

$$\vartheta_\nu = e^{2 \sum_{\varrho=1}^p h_{\varrho}^{(\nu)} v_{\varrho}^{(\nu)}} \cdot \vartheta(v_1^{(\nu)}, v_2^{(\nu)}, \dots, v_p^{(\nu)}).$$

Aleshores el quocient

$$\frac{\sum_{\varrho=1}^p h_{\varrho}^{(\mu)} (u_{\varrho}(0, k_{\mu}) - u_{\varrho}(0, k_{\nu}))}{\sum_{\varrho=1}^p h_{\varrho}^{(\nu)} (u_{\varrho}(0, k_{\nu}) - u_{\varrho}(0, k_{\mu}))} \cdot \frac{\vartheta_{\nu}}{\vartheta_{\mu}}$$

és una funció bivaluada en T (R. p. 54) que en el punt k_{μ} esdevé infinita, i en el punt k_{ν} nul·la, en relació amb cadascuna de les variables $z_1, z_2, \dots, z_p$, i tal que als dos costats dels talls pren valors que es diferenciïn únicament en arrels quadrades de la unitat. Per tant, es pot expressar en la forma

$$\text{Const} \sqrt{\prod_{\varrho=1}^p \frac{z_{\varrho} - k_{\nu}}{z_{\varrho} - k_{\mu}}}.$$

Si, d'una banda, $z_1, z_2, \dots, z_p$ es fan coincidir amb p valors de ramificació diferents de k_{μ}, k_{ν} i, de l'altra, $z_1, z_2, \dots, z_p$ amb els p valors de ramificació diferents restants de k_{μ}, k_{ν} , sota aquests dos supòsits, per als ϑ -quocients de més amunt s'obtenen valors recíprocs llevat del signe, d'on per

a la constant, que denotem per $C_{\mu\nu}$, en resulta el valor ²⁾

$$\sqrt[4]{\prod_1^{2p+2} \binom{(\nu,\mu)}{(\varrho)} \frac{k_\mu - k_\varrho}{k_\nu - k_\varrho}},$$

que dóna lloc a la igualtat

$$(12) \quad \frac{\sum_{\varrho=1}^p \binom{(\nu,\mu)}{(\varrho)} h_\varrho^{(\mu)} (u_\varrho(0, k_\mu) - u_\varrho(0, k_\nu))}{\sum_{\varrho=1}^p \binom{(\nu,\mu)}{(\varrho)} h_\varrho^{(\nu)} (u_\varrho(0, k_\nu) - u_\varrho(0, k_\mu))} \cdot \frac{\vartheta_\nu}{\vartheta_\mu} =$$

$$= \frac{\sqrt[4]{\prod_1^{2p+2} \binom{(\nu,\mu)}{(\varrho)} (k_\mu - k_\varrho)}}{\sqrt[4]{\prod_1^{2p+2} \binom{(\nu,\mu)}{(\varrho)} (k_\nu - k_\varrho)}} \cdot \sqrt{\prod_1^p \binom{(\nu,\mu)}{(\varrho)} \frac{z_\varrho - k_\nu}{z_\varrho - k_\mu}}.$$

En això només és dubtosa encara l'elecció de l'arrel quarta de la unitat que està implícita en el signe radical. A partir de la igualtat (12), sota la hipòtesi

$$\sum_1^p \binom{(\nu,\mu)}{(\varrho)} h_\varrho g_\varrho \equiv 0 \pmod{2},$$

²⁾ Com a explicació de la notació serveixi la igualtat $\prod_1^n \binom{(\nu,\mu)}{(\varrho)} \varphi(\varrho) =$

$$\frac{\prod_1^n \binom{(\nu,\mu)}{(\varrho)} \varphi(\varrho)}{\varphi(\nu) \cdot \varphi(\mu)}.$$

feta sobre els nombres enters h, g , es dedueix la igualtat (cf. la Introducció en relació amb la notació)

(13)

$$\vartheta_{h_1, h_2, \dots, g_p}(0, 0, \dots, 0) = \sqrt{\frac{|A_{\lambda}^{(\lambda')}|}{(2\pi i)^p}} \sqrt[4]{\text{Discr}(h_1, h_2, \dots, g_p) \cdot \text{Discr}'(h_1, h_2, \dots, g_p)},$$

on, per a reals, les quantitats ordenades segons els índexs k prenen arrels reals positives, i les quantitats h, g reconeixen només el valor 0 o bé 1. Amb això el signe complex de la igualtat (12) és determinat quan h, g no són d'aquells nombres per als quals la igualtat (13) es converteix en $0 = 0$.

Ara denotem per $\sigma_1, \sigma_2, \dots, \sigma_p$, p punts de ramificació i per $\vartheta_{\sigma_{\varepsilon}}$ aquelles funcions theta $\vartheta_{h_1, h_2, \dots, g_p}$ en les quals els h i els g satisfan la congruència

$$(A) \quad \left(\dots, \sum_1^p {}_{(\varrho)}u_{\kappa}(\sigma_{\varrho}) - u_{\kappa}(\sigma_{\varepsilon}), \dots \right) \equiv \\ \equiv \left(\dots, \frac{1}{2} \sum_1^p {}_{(\varrho)}a_{\kappa\varrho}h_{\varrho} + g_{\kappa} \frac{i\pi}{2}, \dots \right).$$

Denotem per $\tau_1, \tau_2, \dots, \tau_{p+2}$ els restants punts de ramificació i per $\vartheta_{\tau_{\varepsilon}}$ aquelles funcions theta $\vartheta_{h_1, h_2, \dots, g_p}$ en les quals h i g satisfan la congruència

$$(B) \quad \left(\dots, u_{\kappa}(\tau_{\nu}) - \sum_1^p {}_{(\varrho)}u_{\kappa}(\tau_{\varrho}), \dots \right) \equiv \\ \equiv \left(\dots, \frac{1}{2} \sum_1^p {}_{(\varrho)}a_{\kappa\varrho}h_{\varrho} + g_{\kappa} \frac{i\pi}{2}, \dots \right),$$

en la qual en la suma del costat esquerre τ descriu els p punts de ramificació diferents de τ_ν , τ_ε . Per tant, en prendre els arguments $v_1, v_2, \dots, v_p$ de les funcions ϑ tots iguals a zero, podem provar la igualtat

$$(14) \quad \left| \frac{\partial \vartheta_{\sigma_{\lambda'}}}{\partial v_\lambda} \right| = \pm \vartheta_{\tau_1} \cdot \vartheta_{\tau_2} \cdots \vartheta_{\tau_{p+2}},$$

la qual, en el cas $p = 2$ ja va ésser indicada pel Sr. ROSENHAIN en el seu valuós treball sobre funcions quàdruplement periòdiques (Gl. 116).

Fins al final denotarem encara per $\vartheta_{\tau_\varepsilon, \sigma}$ aquelles funcions theta $\vartheta_{h_1, h_2, \dots, g_p}$ per a les quals h, g satisfan la congruència

$$(C) \quad (\dots, u_\kappa(\tau_\varepsilon) - \sum_1^p {}_{(\varrho)}u_\kappa(\sigma_\varrho), \dots) \equiv \\ \equiv (\dots, \frac{1}{2} \sum_1^p {}_{(\varrho)}a_{\kappa\varrho}h_\varrho + g_\kappa \frac{i\pi}{2}, \dots),$$

on denotem per $\Delta(\sigma)$ el producte (una vegada) de totes les diferències de les quantitats $\sigma_1, \sigma_2, \dots, \sigma_p$; per $\Delta^{(\nu)}(\sigma)$ el de les quantitats $\sigma_1, \sigma_2, \dots, \sigma_{\nu-1}, \sigma_{\nu+1}, \dots, \sigma_p$; per $\Delta(\tau)$ el producte de totes les diferències de les quantitats $\tau_1, \tau_2, \dots, \tau_{p+2}$; per $\Delta(\tau, \sigma_\nu)$ el de les quantitats $\tau_1, \tau_2, \dots, \tau_{p+2}, \sigma_\nu$; i per $\Delta^\nu(\tau)$ el de les quantitats $\tau_1, \tau_2, \dots, \tau_{\nu-1}, \tau_{\nu+1}, \dots, \tau_{p+2}$; per $\text{Discr}(\tau_\varepsilon)$, $\text{Discr}'(\tau_\varepsilon)$ les quantitats $\text{Discr}(h_1, h_2, \dots, g_p)$, $\text{Discr}'(h_1, h_2, \dots, g_p)$, quan h, g satisfan la congruència (B); per $\text{Discr}(\tau_\varepsilon, \sigma)$, $\text{Discr}'(\tau_\varepsilon, \sigma)$ les quantitats $\text{Discr}(h_1, h_2, \dots, g_p)$, $\text{Discr}'(h_1, h_2, \dots, g_p)$, quan h, g satisfan la congruència (C); per $Q_\mu^{(\nu)}$, però, el quocient del costat esquerre de la igualtat (12), quan s'hi substitueix

k_μ per τ_μ , i k_ν per σ_ν . Aleshores, a partir de (12), tenim que

$$\frac{\partial Q_\mu^{(\nu)}}{\partial z_{\nu'}} = \frac{1}{2} C_{\mu\nu} \sqrt{\prod_1^p {}_{(\varrho)} \frac{z_\varrho - \sigma_\nu}{z_\varrho - \tau_\mu}} \cdot \left(\frac{1}{z_{\nu'} - \tau_\mu} - \frac{1}{z_{\nu'} - \sigma_\nu} \right),$$

i, d'aquí, que

$$\begin{aligned} & 2^p \left| \frac{\partial Q_\mu^{(\lambda')}}{\partial z_\lambda} \right| \cdot \sqrt{\frac{\prod_1^p {}_{(\varrho)} (z_\varrho - \sigma_\nu)^p}{(\prod_1^p {}_{(\varrho\varrho')})^2 (z_\varrho - \sigma_{\varrho'})}} = \\ &= 2^p \left| \frac{\partial u_{\lambda'}}{\partial v_\lambda} \right| \cdot \left| \frac{\partial Q_\mu^{(\lambda')}}{\partial z_\lambda} \right| \cdot \sqrt{\frac{\prod_1^p {}_{(\varrho)} (z_\varrho - \sigma_\nu)^p}{(\prod_1^p {}_{(\varrho\varrho')})^2 (z_\varrho - \sigma_{\varrho'})}} = \\ &= C_{\mu 1} \cdot C_{\mu 2} \cdots C_{\mu p} \cdot \left| \frac{1}{z_\lambda - \tau_\mu} - \frac{1}{z_\lambda - \sigma_{\lambda'}} \right|, \end{aligned}$$

on $C_{\mu 1}, C_{\mu 2}, \dots, C_{\mu p}$ són les quantitats que s'obtenen a partir de les $C_{\mu 1}, \dots$ inicials en substituir-hi k_μ per τ_μ , i k_ν per σ_ν . Si ara fixem $z_1 = \sigma_1, z_2 = \sigma_2, \dots, z_p = \sigma_p$, se segueix d'aquí, quan incloem el signe en l'arrel, que

(15)

$$\begin{aligned} \left| \frac{\partial Q_\mu^{(\lambda')}}{\partial v_\lambda} \right| &= \frac{\Delta(\sigma) \cdot \prod_1^p {}_{(\varrho)} C_{\mu \varrho}}{2^p |\alpha_\lambda^{(\lambda')}|} \cdot \sqrt{\frac{\prod_1^p {}_{(\varrho)} \prod_1^{p+2} {}_{(\varrho')} (\sigma_\varrho - \tau_{\varrho'})}{\prod_1^p {}_{(\varrho)} (\sigma_\varrho - \tau_\mu)^p}} = \\ &= \frac{|A_\lambda^{(\lambda')}|}{(2\pi i)^p}. \end{aligned}$$

$$\cdot \sqrt[4]{\frac{(\Delta(\sigma))^2 \cdot \prod_1^{p+2} {}_{(\varrho)}^{(\nu)} (\tau_\mu - \tau_\rho) \prod_1^p {}_{(\varrho)} \prod_1^{p+2} {}_{(\varrho')} (\sigma_\varrho - \tau_{\varrho'})}{\prod_1^p {}_{(\varrho)} (\sigma_\varrho - \tau_\mu)^p}}.$$

Però a partir de la igualtat (13) l'expressió $\frac{\vartheta_{\tau_1} \vartheta_{\tau_2} \cdots \vartheta_{\tau_{p+2}}}{(\vartheta_{\tau_\mu, \sigma})^p}$ és igual a

$$\begin{aligned} & \frac{|A_{\lambda}^{(\lambda')}|}{(2\pi i)^p} \cdot \sqrt[4]{\frac{\text{Discr}(\tau_1) \cdots \text{Discr}(\tau_{p+2}) \text{Discr}'(\tau_1) \cdots \text{Discr}'(\tau_{p+2})}{(\text{Discr}(\tau_\mu, \sigma) \text{Discr}'(\tau_\mu, \sigma))^p}} = \\ & = \sqrt[4]{\frac{(\Delta(\tau))^p \cdot (\Delta(\tau))^{p+2} \cdot \prod_{(\varrho)}^p \prod_{(\varrho')}^{p+2} (\tau_{\varrho'} - \sigma_{\varrho})}{(\Delta(\sigma))^p \cdot \prod_{(\varrho)}^p (\tau_\mu - \sigma_{\varrho})^p \left(\frac{\Delta(\tau)}{\prod_{(\varrho)}^{p+2} (\tau_\mu - \tau_{\varrho})} \right)^p}}. \end{aligned}$$

I d'aquí se segueix, llevat d'una arrel quarta de la unitat que s'incorpora en el signe radical,

$$(16) \quad \frac{\prod_{(\varrho)}^{p+2} \vartheta_{\tau_{\varrho}}}{(\vartheta_{\tau_\mu, \sigma})^p} = \frac{|A_{\lambda}^{(\lambda')}|}{(2\pi i)^p}.$$

$$\cdot \sqrt[4]{\frac{\prod_{(\varrho)}^{p+2} (\tau_\mu - \tau_{\varrho})^p \cdot (\Delta(\sigma))^2 \cdot \prod_{(\varrho)}^p \prod_{(\varrho')}^{p+2} (\tau_{\varrho'} - \sigma_{\varrho})}{\prod_{(\varrho)}^p (\tau_\mu - \sigma_{\varrho})^p}}.$$

De la igualtat dels costats drets de les dues relacions (15) i (16) se segueix ara la validesa de la igualtat (14), quan haurem demostrat que també és vàlida en relació amb l'arrel quarta de la unitat, la qual a causa que hem deixat de banda el signe en el nostre càlcul, requereix encara una investigació especial. Però la validesa de l'arrel de la unitat donada en la igualtat (14) es reconeix quan se suposen tots

els $a_{\mu\mu'} \dots$ reals, la qual cosa sempre pot succeir. Però encara roman indeterminat el signe, que depèn de l'ordenació de les files del determinant.

6

S'han d'expressar a més els quocients diferencials parcials de les funcions ϑ senars per a arguments que s'anul·len per mitjà de valors de ramificació, sempre que aquells mateixos quocients no s'anul·lin. Si mantenim la notació de les seccions precedents, tenim les p igualtats

$$\begin{aligned}
 & \sum_1^p {}_{(\varrho)} \frac{\partial Q_\mu^{(\nu)}}{\partial v_\varrho} \cdot \frac{\partial u_\varrho}{\partial z_1} = \\
 &= \frac{1}{2} C_{\mu\nu} \sqrt{\prod_1^p {}_{(\varrho)} \frac{z_\varrho - \sigma_\nu}{z_\varrho - \tau_\mu} \cdot \left(\frac{1}{z_1 - \tau_\mu} - \frac{1}{z_1 - \sigma_\nu} \right)}, \\
 & \sum_1^p {}_{(\varrho)} \frac{\partial Q_\mu^{(\nu)}}{\partial v_\varrho} \cdot \frac{\partial u_\varrho}{\partial z_2} = \\
 &= \frac{1}{2} C_{\mu\nu} \sqrt{\prod_1^p {}_{(\varrho)} \frac{z_\varrho - \sigma_\nu}{z_\varrho - \tau_\mu} \cdot \left(\frac{1}{z_2 - \tau_\mu} - \frac{1}{z_2 - \sigma_\nu} \right)}, \\
 & \quad \dots \quad \dots \\
 & \sum_1^p {}_{(\varrho)} \frac{\partial Q_\mu^{(\nu)}}{\partial v_\varrho} \cdot \frac{\partial u_\varrho}{\partial z_p} = \\
 &= \frac{1}{2} C_{\mu\nu} \sqrt{\prod_1^p {}_{(\varrho)} \frac{z_\varrho - \sigma_\nu}{z_\varrho - \tau_\mu} \cdot \left(\frac{1}{z_p - \tau_\mu} - \frac{1}{z_p - \sigma_\nu} \right)},
 \end{aligned}$$

de les quals se segueix que

$$\begin{aligned}
 & \frac{2 \frac{\partial Q_{\mu}^{(\nu)}}{\partial v_{\nu'}} \cdot \left| \frac{\partial u_{\lambda'}}{\partial z_{\lambda}} \right|}{C_{\mu\nu} \cdot \sqrt{\prod_{(\varrho)}^p \frac{z_{\varrho} - \sigma_{\nu}}{z_{\varrho} - \tau_{\mu}}}} = \\
 & \left| \begin{array}{cccccc}
 \frac{\partial u_1}{\partial z_1} & \frac{\partial u_2}{\partial z_1} & \dots & \frac{\partial u_{\nu'-1}}{\partial z_1} & \frac{1}{z_1 - \tau_{\mu}} - \frac{1}{z_1 - \sigma_{\nu}} & \frac{\partial u_{\nu'+1}}{\partial z_1} \dots \frac{\partial u_p}{\partial z_1} \\
 \frac{\partial u_1}{\partial z_2} & \frac{\partial u_2}{\partial z_2} & \dots & \frac{\partial u_{\nu'-1}}{\partial z_2} & \frac{1}{z_2 - \tau_{\mu}} - \frac{1}{z_2 - \sigma_{\nu}} & \frac{\partial u_{\nu'+1}}{\partial z_2} \dots \frac{\partial u_p}{\partial z_2} \\
 \dots & \dots & \dots & \dots & \dots & \dots \dots \dots \\
 \dots & \dots & \dots & \dots & \dots & \dots \dots \dots \\
 \frac{\partial u_1}{\partial z_p} & \frac{\partial u_2}{\partial z_p} & \dots & \frac{\partial u_{\nu'-1}}{\partial z_p} & \frac{1}{z_p - \tau_{\mu}} - \frac{1}{z_p - \sigma_{\nu}} & \frac{\partial u_{\nu'+1}}{\partial z_p} \dots \frac{\partial u_p}{\partial z_p}
 \end{array} \right|
 \end{aligned}$$

o bé que

$$\begin{aligned}
 & \frac{2 \frac{\partial Q_{\mu}^{(\nu)}}{\partial v_{\nu'}}}{C_{\mu\nu} \cdot \sqrt{\prod_{(\varrho)}^p \frac{z_{\varrho} - \sigma_{\nu}}{z_{\varrho} - \tau_{\mu}}}} = \\
 & = \sum_{1 \leq p}^p \left(\frac{s_{\varrho}}{z_{\varrho} - \tau_{\mu}} - \frac{s_{\varrho}}{z_{\varrho} - \sigma_{\nu}} \right) \cdot \frac{\delta \lg \left| \left(\sum_{1 \leq p}^p (\varrho') z_{\lambda}^{\varrho'-1} \cdot \alpha_{\varrho'}^{(\lambda')} \right) \right|}{\delta \left(\sum_{1 \leq p}^p (\varrho') \alpha_{\varrho'}^{(\nu')} z_{\varrho}^{\varrho'-1} \right)}.
 \end{aligned}$$

Si s'aplica a això un conegut teorema (BALTZER, §6, 5) sobre determinants i es fixa $z_1 = \sigma_1, z_2 = \sigma_2, \dots, z_p = \sigma_p$, se segueix, llevat de l'elecció de l'arrel quarta de la unitat, que

$$\begin{aligned}
\frac{\partial \vartheta_{\sigma_\nu}}{\partial v_{\nu'}} &= \\
&= \frac{1}{2} \vartheta_{\tau_\mu, \sigma} \cdot C_{\mu\nu} \cdot \frac{\Pi_1^{p(\nu)}(\sigma_\nu - \sigma_\varrho) \cdot \sqrt{\Pi_1^{p+2}(\varrho)(\sigma_\nu - \tau_\varrho)}}{\sqrt{\Pi_1^p(\varrho)(\sigma_\varrho - \tau_\mu)}} \cdot \\
&\quad \cdot \sum_1^p(r) \frac{\delta \lg |\alpha_\lambda^{(\lambda')}|}{\delta \alpha_{\nu'}^{(r)}} \cdot \frac{\delta \lg |\sigma_\lambda^{\lambda'-1}|}{\delta \sigma_\nu^{r-1}} = \\
&= \frac{1}{2} \vartheta_{\tau_\mu, \sigma} \cdot C_{\mu\nu} \sqrt{\frac{\Pi_1^{p+2}(\varrho)(\sigma_\nu - \tau_\varrho)}{\Pi_1^p(\varrho)(\sigma_\varrho - \tau_\mu)}} \cdot \\
&\quad \cdot \sum_1^p(r) \frac{\delta \lg |\alpha_\lambda^{(\lambda')}|}{\delta \alpha_{\nu'}^{(r)}} \cdot S_{r-1}^{(\nu)}(\sigma),
\end{aligned}$$

on cal prendre

$$S_0^{(\nu)} = 1,$$

$$S_1^{(\nu)}(\sigma) = \sigma_1 + \sigma_2 + \dots + \sigma_{\nu-1} + \sigma_{\nu+1} + \dots + \sigma_p,$$

$$S_2^{(\nu)} = \sigma_1 \sigma_2 + \sigma_1 \sigma_3 + \dots + \sigma_1 \sigma_{\nu-1} + \sigma_1 \sigma_{\nu+1} + \dots +$$

$$+ \sigma_1 \sigma_p + \sigma_2 \sigma_3 + \dots + \sigma_{p-1} \sigma_p,$$

...

$$S_{p-1}^{(\nu)} = \sigma_1 \cdot \sigma_2 \cdots \sigma_{\nu-1} \cdot \sigma_{\nu+1} \cdots \sigma_p.$$

Si ara encara substituïm $\vartheta_{\tau_\nu, \sigma}$ per l'expressió que hem trobat a la igualtat (13) trobem, després d'algunes reduccions, que

$$(17) \quad \frac{\partial \vartheta_{\sigma_\nu}}{\partial v_{\nu'}} = \frac{\frac{1}{2} \sqrt{\Delta^{(\nu)}(\sigma) \Delta(\tau, \sigma_\nu)} \cdot \sum_1^p(\varrho) A_{\nu'}^{(\varrho)} S_{\varrho-1}^{(\nu)}(\sigma)}{2\pi i \sqrt{(2\pi i)^p} \cdot \sqrt{|A_\lambda^{(\lambda')}|}}.$$

Per a reals, les quantitats ordenades segons els índexs k , cal prendre les arrels de manera que el costat dret sigui real positiu.

Amb això s'ha aconseguit l'objectiu previst. Encara es pot demostrar fàcilment que les funcions ϑ parelles que no s'anul·len en els arguments v es poden expressar totes elles en la forma $\vartheta_{\tau\nu,\sigma}$ i per consegüent són representades per arguments que s'anul·len. El nombre de les funcions ϑ parelles representables és però $\frac{1}{2} \frac{2p+1}{1} \frac{2p+1}{2} \frac{2p}{3} \dots \frac{p+2}{p+1}$, el nombre de les funcions ϑ parelles disponibles és $2^{2p-1} + 2^{p-1}$, i, per tant, per a $p = 3$ ja hi ha una funció ϑ parella amb els arguments que s'anul·len, per a $p > 3$, diverses. De la mateixa manera, per a $p > 2$, els quocients diferencials parcials d'algunes funcions ϑ senars s'anul·len amb els arguments. En tots dos casos hi ha quocients diferencials d'ordre superior, que no s'anul·len amb els arguments, l'avaluació dels quals en arguments que s'anul·len pot ésser desenvolupada amb mitjans semblants als que hem aplicat aquí. Però s'obté el sistema de nombres h, g per als quals primerament els quocients diferencials segons o bé superiors de $\vartheta_{h_1, h_2, \dots, g_p}(v_1, v_2, \dots, v_p)$ no s'anul·len amb els arguments, mentre que els més baixos i la mateixa funció s'anul·len quan aquests nombres satisfan la congruència

$$\begin{aligned}
 (\dots, u_{\kappa}(0, k_{\mu}) - \sum_{(\varrho)}^p u_{\kappa}(0, k_{\varrho}), \dots) &\equiv \\
 &\equiv (\dots, \frac{1}{2} \sum_1^p a_{\kappa\varrho} h_{\varrho} + g_{\kappa} \frac{i\pi}{2}, \dots)
 \end{aligned}$$

i d'entre ells es permeten dos o més punts de ramificació arbitraris k_ϱ en la suma $\sum_{(\varrho)}^p u_\kappa(0, k_\varrho)$.

Halle, juny i juliol de 1869

Referències de l'article

Recollim totes juntes les referències citades en aquest article.

Baltzer, R.: *Theorie und Anwendung der Determinanten*. Primera edició, Leipzig, S. Hirzel, 1857.

Jacobi, C. G. J.: *Fundamenta nova theoria functionum ellipticarum*. Regiomonti, sumtibus fratrum Bornträger, Königsberg, 1829. Reproduït a *Gesammelte Werke*, **1**, Chelsea, reimpressió (1969), p. 49–239.

Riemann, B.: Theorie der Abel'schen Functionen. *J. reine u. angew. Math.*, **54** (gener de 1857), p. 115–155.

Rosenhain, J.: Sur les fonctions de deux variables et à quatre périodes, qui sont les inverses des intégrales ultra-elliptiques de la première classe. *Mémoires couronnées et mémoires des savants étrangers, publiées par l'Académie royale des sciences, des lettres et des beaux-arts de Belgique*, **XI** (1851), p. 362–468.

Thomae, J.: Bestimmung von $\text{dlg}\vartheta(0, 0, \dots, 0)$ durch die Classenmoduln. *J. reine u. angew. Math.*, **66** (gener de 1866), p. 92–96.

Thomae, J.: Über die elliptische Constante $\vartheta(0)$. *Zeitschrift für Math. und Phys.*, **11** (1866), p. 247–248.

Capítol 8

Dedekind

Segons es desprèn de les primeres paraules de l'autor, l'article de Dedekind del qual presentem una traducció obeeix a una invitació de Borchardt, aleshores editor de la *Revista de Crelle*, a Dedekind, a fi que aquest hi publicués les seves conclusions sobre un cert tema que l'intrigava.

La història es remunta uns quants anys enrere, en què, arran de les pròpies recerques de Dedekind sobre la determinació del nombre de classes dels cossos cúbics, aquest s'havia interessat en l'estudi i l'aprofundiment dels treballs de Kronecker sobre els mòduls singulars de les funcions el·líptiques. Recordem que els mòduls singulars intervenen en la teoria de la multiplicació complexa i que són a la base del Somni de Joventut de Kronecker (cf. la secció 2.7).

En el moment de la invitació de Borchardt a Dedekind, Fuchs havia sotmès a la *Revista de Crelle* el treball *Sobre algunes propietats de les integrals de les equacions diferencials que satisfan els mòduls de periodicitat de les integrals*

ellíptiques de les dues primeres espècies. (Extret d'una carta adreçada al Sr. Hermite) (Sur quelques propriétés des intégrales des équations différentielles, auxquelles satisfont les modules de périodicité des intégrales elliptiques des deux premières espèces. (Extrait d'une lettre adressée à M. Hermite)). Com especifica el títol, el treball és una còpia d'una carta seva adreçada a Hermite. Aquest treball de Fuchs contenia l'enunciat d'un resultat que Dedekind considerarà d'importància cabdal per a les seves pròpies recerques i sobre el qual Hermite també havia cridat l'atenció del mateix Fuchs. Tot seguit, Dedekind presentà a Borchardt un esbós d'una teoria que estava desenvolupant sobre algunes qüestions relacionades amb el resultat de Fuchs, i aquell li'n demanà una exposició més detallada.

Des del punt de vista històric, totes aquestes anades i vingudes són molt rellevants i no fan altra cosa que reflectir la perplexitat d'uns matemàtics davant la descoberta d'unes funcions noves. Aquestes funcions, amb el temps, rebrien noms diferents: funcions modulars, funcions fuchsianes, o funcions automorfes, per exemple. A poc a poc, uns quants matemàtics s'adonaren que els fenòmens de doble periodicitat descoberts per Gauss, Abel, Jacobi i Weierstrass, i que havien estat a la base de l'anàlisi matemàtica de la primera meitat del segle XIX, podien anar molt més enllà quan es consideraven, a més de les transformacions pròpies de la geometria euclidiana, les periodicitats que provenien de la geometria hiperbòlica. El fet era nou i, per tant, no són estranyes les vacil·lacions mostrades en el moment de treure l'entrellat de les possibles repercussions que la geometria hiperbòlica podia tenir en l'anàlisi.

8.1 1877: La funció *valència*

La introducció de l'article és més que una mera declaració d'intencions; de fet, després d'explicar-ne la motivació, Dedekind ja proporciona una millora del resultat de Fuchs, amb una correcció de l'enunciat i una nova demostració. (I això, només a la introducció; l'article promet!)

Segons el mateix Fuchs comenta en un peu de pàgina del seu article, la remarca que Hermite li havia fet és la següent.

No valdria la pena observar que, si posem $\kappa^2 = f(H)$, resulta de la seva anàlisi que totes les solucions de l'equació $f(H) = f(H_0)$ són donades per la fórmula $H = \frac{\nu i + \varrho H_0}{\lambda + \mu i H_0}$, insistir sobre la importància extrema d'aquest resultat per a la determinació dels mòduls singulars del SR. KRONECKER, i remarcar que els bells descobriments de l'il·lustre geòmetra sobre les aplicacions de la teoria de les funcions el·líptiques a l'aritmètica semblen reposar essencialment sobre aquesta proposició, la demostració de la qual encara no havia estat donada?

En aquesta remarca, $H = \frac{K'}{K}$ és el quocient dels períodes d'una integral el·líptica, κ n'és el mòdul, i f és una funció tal que el quadrat del mòdul s'expressa en la forma $\kappa^2 = f(H)$.

Dedekind anomena $\omega := \frac{K'}{K}i$, $k = \kappa^2$, i fa servir, en la seva pròpia notació, l'expressió funcional $k = \varphi(\omega)^8$ que ja havia usat el mateix Hermite. I, amb aquestes notacions, comenta que el resultat que ha provat Fuchs és que la funció $k(\omega)$ és invariant si ω es canvia per

$$\frac{\gamma + \delta\omega}{\alpha + \beta\omega},$$

per a $\alpha, \beta, \gamma, \delta$, nombres enters tals que $\alpha\delta - \beta\gamma = 1$ i β, γ , parells.

Val la pena observar que en l'enunciat que hi ha a l'article de Fuchs només es diu, amb el corresponent canvi de notació, que α, β, γ i δ són nombres enters tals que $\alpha\delta - \beta\gamma = 1$. Però en aquest enunciat no s'esmenta que β i γ han de ser parells, com, en canvi, s'ha fet servir en els propis càlculs de Fuchs de la demostració. I sembla que aquest fet passa per alt tant a Fuchs com a Hermite.

En llenguatge actual, el resultat provat per Fuchs és que la funció $k(\omega)$ és automorfa per al grup de congruència

$$\Gamma(2) := \ker(\mathrm{SL}(2, \mathbb{Z}) \longrightarrow \mathrm{SL}(2, \mathbb{F}_2)).$$

I, tot seguit, Dedekind proporciona una demostració del fet que aquesta funció no és Γ -automorfa per a cap subgrup Γ de $\mathrm{SL}(2, \mathbb{Z})$ que contingui estrictament $\Gamma(2)$, fet que fa palesa la necessitat de la condició obviada per Fuchs i Hermite (cf. la secció 9.1, p. 361, més avall). Per a la demostració d'aquest fet, Dedekind només fa servir les expressions de les funcions el·líptiques $\sin am$, $\cos am$ i Δam com a quocients de funcions theta i les propietats de semiperiodicitat de les funcions theta, ja ben conegudes en aquella època (cf. la

subsecció 1.11, p. 38), en la mateixa línia de la demostració de Fuchs.

Finalment, Dedekind acaba la introducció amb la declaració que la teoria que desenvoluparà a continuació ha estat feta, en part, a fi de qüestionar l’afirmació —que nosaltres considerem una mica imprudent i que ell també atribueix a Hermite— segons la qual “no hi ha cap altre camí que mení a aquestes funcions modulars llevat del proporcionat pels fundadors de la teoria de les funcions el·líptiques”. No-tem, doncs, que Dedekind ja usa el terme “modular” per a referir-se a les funcions invariants per subgrups de congruència de $SL(2, \mathbb{Z})$, probablement influït per Kronecker, i que la seva teoria, que desenvoluparà a partir d’aquest punt de l’article, té com a objectiu trobar les propietats d’automorfia de la funció $k(\omega)$ independentment de la teoria de les funcions theta. Fem-ne un resum del contingut.

A la primera secció, Dedekind considera que dos punts $\omega, \omega' \in \mathbb{C} \cup \{\infty\}$ són equivalents si estan relacionats de la manera

$$\omega' = \frac{\gamma + \delta\omega}{\alpha + \beta\omega}, \quad \alpha, \beta, \gamma, \delta \in \mathbb{Z}, \quad \alpha\delta - \beta\gamma = 1;$$

és a dir, en llenguatge actual, si pertanyen a la mateixa òrbita per l’acció estàndard de $SL(2, \mathbb{Z})$, però modificada per l’automorfisme involutiu

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \mapsto \begin{pmatrix} \delta & \gamma \\ \beta & \alpha \end{pmatrix},$$

fet que no modifica les òrbites. I, sense parlar en cap moment d’acció, fa notar que aquesta és estable en el semiplà superior, que ell denota per $\mathbf{S}$, i en $\mathbb{Q} \cup \{\infty\}$, que denota per $\mathbf{R}$, conjunt del qual diu que “s’ha de veure com la frontera completa del domini $\mathbf{S}$ ”.

Aquest fet sobre la frontera és explicat a la secció segona, després que estudia el domini fonamental usual, definit per les condicions

$$|\Re(z)| \leq \frac{1}{2}, \quad |z| \geq 1.$$

Aquest domini no era gens aliè a Dedekind, atès que Gauss i Kronecker també hi havien arribat; el primer, en relació amb la seva teoria de la reducció de les formes quadràtiques binàries enteres; el segon, en el seu estudi dels mòduls singulars. De fet, Dedekind remet la demostració que aquest conjunt és un domini fonamental a la mateixa que es fa en l'estudi de la reducció de les formes quadràtiques binàries enteres; només diu que cal estendre el concepte de forma reduïda a formes de coeficients reals.

Després de veure quines són les identifikacions del domini, i que aquest és un triangle curvilini amb l'eix imaginari com a eix de simetria, Dedekind estudia la tessellació del semiplà que s'obté amb els triangles transformats d'aquest domini fonamental pels elements de $SL(2, \mathbb{Z})$, i explica per què cal veure $\mathbb{Q} \cup \{\infty\}$ com la frontera completa del semiplà. En particular, Dedekind també estudia el comportament diferent de les tesselles que intersequen una recta vertical segons que l'abscissa d'aquesta sigui racional, o bé irracional. En el segon cas, la successió de vèrtexs sobre l'eix real és una successió de nombres racionals de denominadors creixents que té per límit l'abscissa de la recta vertical. Aquest estudi condueix Dedekind a corregir, al final de la secció sisena, un altre resultat de Fuchs de la memòria esmentada més amunt; concretament, el resultat II de la pàgina 27, en què estudia com és l'apropament a la frontera d'un radi del cercle unitat. Aquí cal fer notar

que Fuchs no utilitza el semiplà superior com a model del pla hiperbòlic, com fa Dedekind, sinó el cercle unitat.

Dedekind dedica la secció tercera a un dels punts clau de la seva teoria: la introducció de la funció que ell anomena valència i que, multiplicada pel factor 1728 esdevindrà més endavant l'invariant modular j , també anomenat de Klein. Dedekind construeix la funció, de moment només de manera existencial, a partir dels principis de Riemann de la representació conforme; i demostra que queda completament determinada en imposar que prengui els valors 0, 1, ∞ en els vèrtexs $\rho := \frac{-1 + \sqrt{-3}}{2}$, $i = \sqrt{-1}$, ∞ , respectivament, del domini fonamental.

A fi d'aconseguir una determinació analítica de la funció valència, Dedekind comença per estudiar, a la secció quarta, com és el comportament local de la funció en un entorn de cadascun dels vèrtexs del domini fonamental; en llenguatge més actual, diríem que Dedekind calcula un cert paràmetre d'uniformització local a l'entorn de cada punt el·líptic i de cada punt parabòlic.

A la secció cinquena, i un cop ha calculat aquests paràmetres uniformitzadors, Dedekind procedeix al càlcul d'una equació diferencial per a la funció valència, $v(\omega)$. Després de comentar les propietats generals de l'operador diferencial de tercer ordre que més endavant es coneixeria com la derivada schwarziana (cf. la secció 2.8, p. 77), i que actualment s'acostuma a escriure de la manera

$$[v, w] = \frac{2D(v, w)D^3(v, w) - 3D^2(v, w)^2}{D(v, w)^2},$$

Dedekind s'aplica en el càlcul de l'equació diferencial de tercer ordre $[v, w] = F(v)$ satisfeta per la funció valència.

Troba que $F(v)$ és una certa funció racional de v , que pot fer explícita en la forma

$$F(v) = \frac{36v^2 - 41v + 32}{36v^2(1-v)^2}.$$

I un cop determinada aquesta equació diferencial, n'obté la integral general, $v'(w)$, en la forma

$$v'(w) = v \left(\frac{Aw + B}{Cw + D} \right),$$

on A, B, C, D , són constants arbitràries.

Dedekind dedica la secció sisena a l'estudi de les funcions modulars el·líptiques i, en particular, introdueix la funció que, més endavant, serà anomenada la funció eta de Dedekind. De fet, és la secció que incorpora els resultats bàsics de la seva teoria de les funcions el·líptiques. A partir de la funció valència, $v(\omega)$, Dedekind posa

$$\eta(\omega) := C \cdot v(\omega)^{-\frac{1}{6}} (1 - v(\omega))^{-\frac{1}{8}} \left(\frac{dv(\omega)}{d\omega} \right)^{\frac{1}{4}},$$

on tria la constant C de manera que per a $\omega = \infty$ sigui

$$\exp(-2\pi i \omega / 24) \eta(\omega) = 1.$$

A partir d'aquesta definició i de les propietats d'automorfia de la funció valència, Dedekind determina les lleis de transformació de la funció $\eta(\omega)$, així com també les de les funcions auxiliars

$$\eta_1(\omega) := \eta(2\omega), \quad \eta_2(\omega) := \eta\left(\frac{\omega}{2}\right), \quad \eta_3(\omega) := \eta\left(\frac{1+\omega}{2}\right),$$

i les fa servir per a obtenir les relacions entre la funció $\eta(\omega)$ i les funcions el·líptiques κ , κ' , $k = \kappa^2$, $\varphi(\omega) = \sqrt[4]{\kappa}$, de les quals dedueix les relacions ja conegudes entre les funcions el·líptiques. En particular, també obté l'expressió

$$v(\omega) = \frac{4}{27} \frac{(k + \rho)^3 (k + \rho^2)^3}{k^2 (1 - k)^2}$$

o, equivalentment,

$$j(\omega) := 1728v(\omega) = 216 \frac{(k^2 - k + 1)^3}{k^2 (1 - k)^2},$$

més habitual actualment.

A continuació, i encara a la mateixa secció, obté les relacions

$$\varphi(\omega)^8 = k, \quad \varphi(\omega + 1)^8 = \frac{k}{k - 1}, \quad \varphi(-1/\omega)^8 = 1 - k,$$

a partir de les quals diu que es pot deduir l'equació diferencial

$$[k, \omega] = \frac{(k + \rho)(k + \rho^2)}{k^2 (1 - k)^2},$$

satisfeta per k i semblant a l'equació que satisfà la funció valència. Finalment, i amb l'ús de la teoria de les funcions theta, Dedekind proporciona l'expressió de la funció eta com a producte infinit

$$\eta(\omega) = \exp(2\pi i \omega / 24) \prod_{n \geq 1} (1 - \exp(2\pi i n \omega)).$$

A la setena i darrera secció de l'article, Dedekind fa l'estudi dels polinomis que actualment anomenem polinomis

modulars. Després de considerar les funcions transformades de la funció valència en la forma

$$v_n(\omega) = v\left(\frac{C + D\omega}{A + B\omega}\right),$$

per a A, B, C, D , nombres enters tals que $AD - BC = n$ i $\text{mcd}(A, B, C, D) = 1$ —o sigui, els elements primitius de norma n de l'àlgebra de matrius $M(2, \mathbb{Z})$ —, Dedekind compta el nombre, $\psi(n)$, de funcions diferents que hi ha a partir d'obtenir un conjunt explícit de representants de les classes mòdul l'acció de $SL(2, \mathbb{Z})$, tal com fem avui. A continuació, defineix el polinomi $F_n(X, v)$ que té per arrels aquestes funcions —o sigui, el polinomi modular de nivell n per a la funció v —, estableix la seva irreductibilitat i la seva simetria, i observa que els seus coeficients són racionals. Finalment, Dedekind acaba l'article amb un comentari sobre el fet que, a partir del discriminant dels polinomis modulars, o també dels polinomis $F_n(X, X)$, s'arriba a la teoria dels mòduls singulars, de la qual només diu que deixa per a una altra ocasió una explicació més detallada.

Tot el bastiment teòric que Dedekind desenvolupa en aquest article ha estat bàsic en les recerques posteriors sobre les funcions modulars. Aquestes investigacions han donat lloc a les formes modulars i les corbes modulars, i són molts els matemàtics que hi han fet aportacions. A tall d'exemple, podem citar que ja ben aviat Klein i Fricke, i després Poincaré, hi feren les primeres contribucions importants després de Dedekind. Però aportacions a la teoria han estat fetes també per Ogg, Shimura, Mazur, Serre, Ribet i Frey, entre molts altres (cf. per exemple [15], [21]).

Notem que Dedekind no es preocupa d'obtenir desenvolupaments en sèrie per a la seva funció valència. Més en-

davant s'obtindria el desenvolupament en sèrie de Fourier d'aquesta funció i, recentment, els seus desenvolupaments en els punts de multiplicació complexa (cf. [35] i [37]). Diuem que una generalització i posada al dia del mètode de Dedekind ens ha permès obtenir equacions diferencials de funcions automorfes hexagonals. La teoria ha estat aplicada a la uniformització de corbes de Shimura, i en el treball [36] (cf. també [37]) hem obtingut, per primera vegada, desenvolupaments en sèrie, a l'entorn de punts de multiplicació complexa, per a funcions automorfes no modulars. Els valors d'aquestes funcions transcendents en els punts de multiplicació complexa del domini fonamental hiperbòlic corresponent proporcionen nombres complexos algebraics els quals, en relació amb la teoria de cossos de classes, són l'extensió natural dels mòduls singulars de la teoria clàssica considerats per Kronecker o bé, si es prefeix, de les arrels de la unitat, tractades prèviament per Kummer, Kronecker i Weber.

J. reine u. angew. Math. **83** (1877), 265–292

ESCRIT AL SR. *BORCHARDT* SOBRE LA TEORIA DE LES FUNCIONS MODULARS EL·LÍPTIQUES

del Sr. R. DEDEKIND a Brunsvic

Vostè m'ha encoratjat a elaborar una exposició quelcom més detallada sobre les investigacions de les quals jo, motivat per la publicació de FUCHS ¹⁾, em vaig permetre recentment comunicar-n'hi un breu resum. En la mesura que en aquest escrit porto a terme la seva invitació, em limito essencialment a la part d'aquestes investigacions que es relaciona amb la memòria esmentada, alhora que li prego que tingui la bondat de disculpar el tractament superficial d'algunes qüestions col·laterals, atès que de moment em manca temps per a explicitar-ne tots els detalls.

Les recerques esmentades ja em tingueren ocupat fa una sèrie d'anys, quan vaig reconèixer que la determinació del nombre de classes d'ideals en cossos cúbics (és a dir, en dominis de nombres construïts a partir d'arrels d'equacions de tercer grau) està estretament relacionada amb la teoria dels mòduls singulars de les funcions el·líptiques, per als quals té lloc la multiplicació complexa.

En els meus intents d'aprofundir en aquesta per a mi imprescindible teoria i de facilitar-me l'accés als resultats

¹⁾ En el primer fascicle d'aquest volum, p. 13.

extraordinàriament bells de KRONECKER, els quals dissortadament resulten encara tan difícils d'abastar, vaig reconèixer de seguida la importància fonamental d'una qüestió sobre el treball de FUCHS (p. 29), sobre la qual HERMITE ha cridat també l'atenció recentment, i que a la pràctica ha esdevingut bàsica per a la meua teoria. Es tracta del següent. Si

$$\omega = \frac{K'i}{K}$$

denota la raó dels períodes de les funcions el·líptiques ($= Hi$, segons la notació de FUCHS), aleshores el quadrat $k = \kappa^2$ del mòdul enter κ és una funció univaluada de ω , que HERMITE designa per $\varphi(\omega)^8$, i, a partir de les transformacions de primer ordre, se segueix fàcilment que k resta invariant quan ω se substitueix per

$$\omega_1 = \frac{\gamma + \delta\omega}{\alpha + \beta\omega},$$

on $\alpha, \beta, \gamma, \delta$ denoten quatre enters racionals que satisfan la relació

$$\alpha\delta - \beta\gamma = 1,$$

i dels quals β, γ són parells. Aleshores, el teorema consisteix a demostrar que, llevat d'aquests nombres ω_1 , no n'existeix cap altre que proporcioni el mateix valor $k = \varphi(\omega)^8 = \varphi(\omega_1)^8$. Abans que passi a l'exposició de la meua teoria, vull evidenciar en primer lloc que aquest teorema també es pot derivar sense dificultat de la teoria usual de les funcions el·líptiques.

Si ω denota una quantitat complexa de part imaginària positiva, z , a més, una variable arbitrària, i ens servim de

les notacions següents

$$\begin{aligned} \mathbf{1}^z &= e^{2\pi iz}, \\ \vartheta(z, \omega) &= \sum \mathbf{1}^{s^2 \frac{\omega}{2} + s(z - \frac{1}{2})}, \\ \vartheta_1(z, \omega) &= \sum \mathbf{1}^{(s + \frac{1}{2})^2 \frac{\omega}{2} + (s + \frac{1}{2})(z - \frac{1}{2})}, \\ \vartheta_2(z, \omega) &= \sum \mathbf{1}^{(s + \frac{1}{2})^2 \frac{\omega}{2} + (s + \frac{1}{2})z}, \\ \vartheta_3(z, \omega) &= \sum \mathbf{1}^{s^2 \frac{\omega}{2} + sz}, \end{aligned}$$

on s recorre tots els nombres enters de $-\infty$ fins a $+\infty$; a més,

$$\sqrt{\kappa} = \frac{\vartheta_2(0, \omega)}{\vartheta_3(0, \omega)} = \varphi(\omega)^2, \quad \sqrt{\kappa'} = \frac{\vartheta(0, \omega)}{\vartheta_3(0, \omega)} = \psi(\omega)^2,$$

aleshores és

$$\kappa^2 + \kappa'^2 = 1,$$

i podem posar

$$\sqrt{x} = \frac{1}{\sqrt{\kappa}} \frac{\vartheta_1(z, \omega)}{\vartheta(z, \omega)} = \sin \operatorname{am}(2Kz, \kappa),$$

$$\sqrt{1-x} = \frac{\sqrt{\kappa'}}{\sqrt{\kappa}} \frac{\vartheta_2(z, \omega)}{\vartheta(z, \omega)} = \cos \operatorname{am}(2Kz, \kappa),$$

$$\sqrt{1-\kappa^2 x} = \sqrt{\kappa'} \frac{\vartheta_3(z, \omega)}{\vartheta(z, \omega)} = \Delta \operatorname{am}(2Kz, \kappa),$$

$$\frac{d\sqrt{x}}{dz} = 2K \sqrt{1-x} \sqrt{1-\kappa^2 x},$$

on

$$2K = \frac{\vartheta_3(0, \omega) \vartheta_1'(0, \omega)}{\vartheta(0, \omega) \vartheta_2(0, \omega)} = \pi \vartheta_3(0, \omega)^2.$$

Ara, si la quantitat ω_1 té igualment una part imaginària positiva i proporciona el mateix valor,

$$\frac{\vartheta_2(0, \omega_1)^4}{\vartheta_3(0, \omega_1)^4} = \kappa_1^2 = \kappa^2 = k,$$

que ω , aleshores es posa

$$2K_1 = \pi \vartheta_3(0, \omega_1)^2$$

i s'introdueix una nova variable z_1 mitjançant l'equació

$$K_1 z_1 = Kz;$$

si, a més, denotem per $\sqrt{x_1}$, $\sqrt{1-x_1}$, $\sqrt{1-kx_1}$ les quantitats que depenen de z_1 , ω_1 de la mateixa manera que $\sqrt{x}$, $\sqrt{1-x}$, $\sqrt{1-kx}$ [ho fan] de z , ω , s'obté que

$$\frac{d\sqrt{x}}{\sqrt{1-x}\sqrt{1-kx}} = \frac{d\sqrt{x_1}}{\sqrt{1-x_1}\sqrt{1-kx_1}},$$

i d'aquí, per integració,

$$\sqrt{x}\sqrt{1-x_1}\sqrt{1-kx_1} - \sqrt{x_1}\sqrt{1-x}\sqrt{1-kx} = C(1-kxx_1);$$

però la constant C ha d'ésser igual a 0, perquè per a $z = 0$ també és $z_1 = 0$, per tant, $\sqrt{x}$ i $\sqrt{x_1}$ s'anul·len simultàniament. D'aquí se segueix que $x = x_1$ idènticament (i també que $\sqrt{x} = \sqrt{x_1}$, $\sqrt{1-x} = \sqrt{1-x_1}$, $\sqrt{1-kx} = \sqrt{1-kx_1}$); en conseqüència cadascuna de les quatre funcions

$$\vartheta(z, \omega), \quad \vartheta_1(z, \omega), \quad \vartheta_2(z, \omega), \quad \vartheta_3(z, \omega)$$

s'anul·larà si, i només si, s'anul·la la corresponent de les quatre funcions,

$$\vartheta(z_1, \omega_1), \quad \vartheta_1(z_1, \omega_1), \quad \vartheta_2(z_1, \omega_1), \quad \vartheta_3(z_1, \omega_1).$$

Però la funció $\vartheta_1(z, \omega)$ s'anul·la per a tots els valors $z = r + s\omega$ i només per a aquests, on r i s denoten nombres enters arbitraris ²⁾; per tant, si prenem

$$z_1 = 1, \quad \text{llavors se satisfà que} \quad z = \frac{K_1}{K} = \alpha + \beta\omega,$$

$$z_1 = \omega_1, \quad \text{llavors se satisfà que} \quad z = \frac{K_1}{K}\omega_1 = \gamma + \delta\omega,$$

on $\alpha, \beta, \gamma, \delta$ denoten nombres racionals enters; en conseqüència, és

$$(1) \quad \omega_1 = \frac{\gamma + \delta\omega}{\alpha + \beta\omega}, \quad (\alpha + \beta\omega)z_1 = z.$$

Recíprocament, si prenem

$$z = 1, \quad \text{aleshores se satisfà que} \quad z_1 = \alpha_1 + \beta_1\omega_1,$$

$$z = \omega, \quad \text{aleshores se satisfà que} \quad z_1 = \gamma_1 + \delta_1\omega_1,$$

on $\alpha_1, \beta_1, \gamma_1, \delta_1$ denoten igualment nombres enters; s'obté, doncs, que

$$(\alpha + \beta\omega)\alpha_1 + (\gamma + \delta\omega)\beta_1 = 1,$$

$$(\alpha + \beta\omega)\gamma_1 + (\gamma + \delta\omega)\delta_1 = \omega,$$

d'on, perquè ω no és real,

$$\alpha\alpha_1 + \gamma\beta_1 = 1, \quad \beta\alpha_1 + \delta\beta_1 = 0,$$

$$\alpha\gamma_1 + \gamma\delta_1 = 0, \quad \beta\gamma_1 + \delta\delta_1 = 1,$$

²⁾ Això se segueix de la representació de $\vartheta_1(z, \omega)$ com a producte infinit, o també del teorema $\int d \log \vartheta_1(z, \omega) = 2\pi i$, on la integral s'estén a la frontera d'un paral·lelogram elemental.

per tant,

$$(\alpha\delta - \beta\gamma)(\alpha_1\delta_1 - \beta_1\gamma_1) = 1,$$

i en conseqüència se segueix que ³⁾

$$\alpha\delta - \beta\gamma = \alpha_1\delta_1 - \beta_1\gamma_1 = \pm 1.$$

Però, com a conseqüència de (1), en la fórmula anterior només s'ha de prendre el signe positiu, perquè el coeficient de la i en les dues quantitats ω i ω_1 té el mateix signe (positiu); per tant, se satisfà que

$$(2) \quad \alpha\delta - \beta\gamma = +1.$$

A més, atès que el valor de z_1 per al qual $\vartheta(z_1, \omega_1)$ s'anul·la coincideix amb els valors $r + (s + \frac{1}{2})\omega_1$, se satisfà al mateix temps que

$$z = \frac{\omega}{2}, \quad z_1 = r + (s + \frac{1}{2})\omega_1;$$

en conseqüència, se segueix de (1) que

$$(\alpha + \beta\omega)r + (\gamma + \delta\omega)(s + \frac{1}{2}) = \frac{\omega}{2},$$

$$\alpha r + \gamma(s + \frac{1}{2}) = 0,$$

per tant,

$$(3) \quad \gamma \equiv 0 \pmod{2}.$$

De la mateixa manera, de l'anul·lació simultània de les funcions $\vartheta_2(z, \omega)$, $\vartheta_2(z_1, \omega_1)$ per a $z = \frac{1}{2}$, també s'obté que

$$(4) \quad \beta \equiv 0 \pmod{2},$$

³⁾ Això és només un cas especial d'un teorema general de la teoria dels sistemes numèrics, que jo he anomenat *mòduls finits*.

amb la qual cosa el teorema que tenim entre mans s'ha demostrat completament.

Aquesta demostració es fonamenta, evidentment, en el fet que les funcions el·líptiques $\sin \operatorname{am}(u, \kappa)$, $\cos \operatorname{am}(u, \kappa)$ i $\Delta \operatorname{am}(u, \kappa)$ també són funcions univaluades de $k = \kappa^2$. Però el mateix teorema em bastà aviat per a investigar, de manera independent de la teoria de les funcions el·líptiques, el lligam entre les quantitats ω , k , K , i en aquesta aspiració em va esperonar una remarca posada en relleu per HERMITE en un punt del seu breu resum sobre la teoria de les funcions el·líptiques, segons la qual no hi ha cap altre camí que mení a aquestes funcions modulars llevat del proporcionat pels fundadors de la teoria de les funcions el·líptiques. Ara em permeto desenvolupar-li des de la base la meua teoria aleshores naixent; en una altra ocasió, potser em permetré presentar-li l'aplicació a la teoria dels mòduls singulars, a la qual s'adreça tota la recerca.

1. NOMBRES EQUIVALENTS

En el que segueix, caldrà que dos nombres ω , ω_1 es diguin *equivalents* quan existeixin quatre nombres enters (racionals) α , β , γ , δ que satisfacin les dues condicions següents:

$$\omega_1 = \frac{\gamma + \delta\omega}{\alpha + \beta\omega}, \quad \alpha\delta - \beta\gamma = 1;$$

evidentment, la condició que acabem d'expressar és recíproca en ω , ω_1 , atès que, de la mateixa manera, els quatre nombres δ , $-\beta$, $-\gamma$, α satisfan les relacions

$$\omega = \frac{(-\gamma) + \alpha\omega_1}{\delta + (-\beta)\omega_1}, \quad \delta\alpha - (-\beta)(-\gamma) = 1.$$

Si, igualment, ara es dóna que ω_2 és equivalent a ω , existeixen també quatre nombres enters $\alpha_1, \beta_1, \gamma_1, \delta_1$ que satisfan les relacions

$$\omega = \frac{\gamma_1 + \delta_1 \omega_2}{\alpha_1 + \beta_1 \omega_2}, \quad \alpha_1 \delta_1 - \beta_1 \gamma_1 = 1;$$

per la qual cosa escriurem, de la manera habitual,

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} \alpha_1 & \beta_1 \\ \gamma_1 & \delta_1 \end{pmatrix} = \begin{pmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{pmatrix},$$

és a dir:

$$\alpha' = \alpha \alpha_1 + \beta \gamma_1, \quad \beta' = \alpha \beta_1 + \beta \delta_1,$$

$$\gamma' = \gamma \alpha_1 + \delta \gamma_1, \quad \delta' = \gamma \beta_1 + \delta \delta_1;$$

atès que aquests nombres $\alpha', \beta', \gamma', \delta'$ satisfan les dues condicions equivalents

$$\omega_1 = \frac{\gamma' + \delta' \omega_2}{\alpha' + \beta' \omega_2}, \quad \alpha' \delta' - \beta' \gamma' = 1,$$

se segueix que, si dos nombres ω_1, ω_2 són equivalents a un mateix nombre ω , aleshores també són equivalents entre si. Per aquest motiu es pot dividir el domini total dels nombres en *classes*, de manera que dos nombres s'assignen a la mateixa o a dues classes diferents segons que siguin equivalents o no. Cada nombre ω pot ésser interpretat com a *representant* de la classe que consta de tots els nombres equivalents a ω .

Si anomenem els nombres reals x, y les coordenades, i, certament, x l'abscissa i y l'ordenada, del nombre complex $\omega = x + iy$ que es forma a partir d'elles, aleshores s'obté

fàcilment que les ordenades de dos nombres equivalents ω , ω_1 , tenen el mateix signe, o bé que les dues s'anul·len. En el que segueix considerarem el domini $\mathbf{S}$ d'aquells nombres ω les ordenades dels quals són *positives* i, a més, únicament els nombres reals *racionals*, els quals clarament constitueixen una única classe $\mathbf{R}$, perquè tots ells són equivalents al 0; es posarà de manifest que aquesta classe $\mathbf{R}$, que conté alhora el nombre ∞ , s'ha de veure com la *frontera* completa del domini $\mathbf{S}$.

2. SISTEMA COMPLET DE REPRESENTANTS

Es tracta ara de posar de manifest un sistema complet de representants ω_0 de totes les classes que constitueixen el domini $\mathbf{S}$, de manera que cada nombre ω d'aquest domini sigui equivalent a un, i en general només a un, representant ω_0 . Això és conseqüència del teorema següent, en el qual la notació $\mathbf{N}(x + iy)$ denota la norma $(x^2 + y^2)$ del nombre complex $x + iy$:

En cada classe del domini $\mathbf{S}$, inclosa $\mathbf{R}$, hi ha un, i també com a regla general només un representant ω_0 , que satisfà les tres condicions següents:

- (1) $\mathbf{N}(\omega_0 - 1) \geq \mathbf{N}(\omega_0)$,
- (2) $\mathbf{N}(\omega_0 + 1) \geq \mathbf{N}(\omega_0)$,
- (3) $\mathbf{N}(\omega_0) \geq 1$.

La demostració es pot portar a terme amb els mateixos mitjans que permeten demostrar que en la teoria de les formes quadràtiques binàries de discriminant negatiu, cadascuna d'aquestes formes és equivalent a una, i per regla general només a una, forma *reduïda*. Aquí m'acontento

amb enllestir la primera part del teorema mitjançant les consideracions següents. Si ω és un cert nombre del domini $\mathbf{S}$, aleshores, perquè ω no és real, se segueix que entre tots els parells de nombres α, β relativament primers n'hi ha un per al qual $\mathbf{N}(\alpha + \beta\omega)$ esdevé el més petit possible; una vegada hem escollit α i β d'aquesta manera, totes les solucions en nombres enters γ, δ de l'equació $\alpha\delta - \beta\gamma = 1$ s'obtenen a partir d'una solució única γ', δ' , en prendre $\gamma = \gamma' - m\alpha, \delta = \delta' - m\beta$, i m es deixa recórrer tots els nombres enters de $-\infty$ a $+\infty$; si m s'escull de manera que

$$\mathbf{N}\left(\frac{\gamma + \delta\omega}{\alpha + \beta\omega}\right) = \mathbf{N}\left(\frac{\gamma' + \delta'\omega}{\alpha + \beta\omega} - m\right)$$

sigui el més petit possible, aleshores el nombre

$$\omega_0 = \frac{\gamma + \delta\omega}{\alpha + \beta\omega},$$

equivalent a ω , té totes les propietats expressades en (1), (2), (3). Perquè a partir de la definició de α i β se segueix que ω_0 satisfà la condició (3) i, de la mateixa manera, a partir de la definició de m , que ω_0 satisfà les condicions (1) i (2).

De manera geomètrica, tots aquests nombres ω_0 es representen per mitjà d'un tros del semiplà $\mathbf{S}$, anomenat camp fonamental, i que ha d'ésser denotat per (ω_0) . Aquest és delimitat per tres línies que es corresponen amb els signes d'igualtat en les condicions (1), (2), (3); si posem $\omega_0 = x_0 + y_0i$, les condicions anteriors adopten la forma:

$$\begin{aligned} (1) \quad & x_0 \leq \frac{1}{2}, \\ (2) \quad & x_0 \geq -\frac{1}{2}, \\ (3) \quad & x_0^2 + y_0^2 \geq 1; \end{aligned}$$

el camp (ω_0) es troba entre les dues rectes que corren paral·leles a l'eix de les ordenades a les distàncies $\pm \frac{1}{2}i$, al mateix temps, a l'exterior del semicercle que és descrit a partir de l'origen i del radi 1. Evidentment, aquest camp és descompost per l'eix de les ordenades en dues meitats simètriques. Les dues paral·leles (2) i (1) es tallen en el punt ∞ , el representant de la classe **R** dels nombres racionals, i tallen el cercle en els punts

$$\rho = \frac{-1 + i\sqrt{3}}{2}, \quad -\rho^2 = 1 + \rho = \frac{-1}{\rho},$$

mentre que l'eix de simetria talla el cercle en el punt

$$i = \frac{-1}{i}.$$

Si ara ω_0 pertany a la línia fronterera (2), és a dir, si és $x_0 = -\frac{1}{2}$, aleshores és palès que el nombre equivalent $1 + \omega_0$ pertany a la línia fronterera (1), i aquests dos punts ω_0 , $1 + \omega_0$ es disposen simètricament a les dues bandes de l'eix d'ordenades. A més, si ω_0 pertany a la circumferència (3), aleshores el mateix es pot dir del nombre equivalent $\frac{-1}{\omega_0} = -x_0 + y_0i$, i aquests dos punts ω_0 , $\frac{-1}{\omega_0}$ igualment es disposen simètricament a les dues bandes de l'eix d'ordenades. Cada dos punts simètrics de la frontera de (ω_0) són, doncs, representants d'una classe i solament una. Ara també es pot demostrar fàcilment que, excepte en aquests casos, mai dos punts diferents, o bé dos nombres del camp (ω_0) , poden pertànyer a la mateixa classe, tant si es troben a l'interior com a la frontera de (ω_0) . Per a abreujar, suprimixo aquesta demostració que, com s'ha remarcat abans, transcorre de la mateixa manera que la demostració

del teorema segons el qual dues formes quadràtiques binàries de discriminant negatiu, reduïdes i diferents, només poden ser equivalents en determinats casos excepcionals (cf. *Zahlentheorie* de DIRICHLET, segona edició, §65); n'hi haurà prou amb remarcar que, si x , y denoten variables arbitràries, la forma quadràtica binària

$$\mathbf{N}(x + y\omega_0) = (1, x_0, x_0^2 + y_0^2),$$

de determinant $= -y_0^2$ és sempre *reduïda* quan aquest concepte és traslladat a formes de coeficients reals, racionals o bé irracionals.

Si ara α , β , γ , δ denoten quatre nombres enters determinats, que satisfan la condició $\alpha\delta - \beta\gamma = 1$, i es posa

$$\omega_0 = \frac{\gamma + \delta\omega}{\alpha + \beta\omega}, \quad \omega = \frac{-\gamma + \alpha\omega_0}{\delta - \beta\omega_0},$$

és fàcil reconèixer que al camp principal (ω_0) correspon un camp (ω) delimitat per tres arcs de circumferència de centres situats en l'eix d'abscisses, i que poden ser línies rectes; els punts angulars del camp (ω) que corresponen als punts angulars

$$\rho, -\rho^2, \infty$$

del camp principal són

$$\frac{-\gamma + \alpha\rho}{\delta - \beta\rho}, \quad \frac{-\gamma - \alpha\rho^2}{\delta + \beta\rho^2}, \quad \frac{-\alpha}{\beta},$$

l'últim dels quals pertany a la classe **R**. Evidentment, correspon als quatre nombres $-\alpha$, $-\beta$, $-\gamma$, $-\delta$ el mateix camp (ω) ; però, altrament, com mostra una recerca exacta, a dos sistemes diferents de quatre nombres α , β , γ , δ els corresponen dos camps diferents (ω) que estan situats completament l'un fora de l'altre i que poden compartir, a tot

estirar, una línia de frontera o, també, únicament un punt angular. Tot el semiplà **S** incloent-hi **R** es compon d'infinits d'aquests camps (donats pels diferents sistemes o substitucions $\pm\alpha$, $\pm\beta$, $\pm\gamma$, $\pm\delta$ corresponents als triangles amb costats circulars (ω)), que s'acumulen en nombre i petitesa infinites a l'eix d'abscisses.

Però un qualsevol d'aquests camps (ω) no conté mai un valor real *irracional*, i, en aquest sentit, dic que en la nostra recerca la classe **R** dels nombres *racionals* forma tota la frontera del domini **S**. Si r és un nombre racional determinat, aleshores existeixen infinits camps (ω) que comparteixen aquest valor r (cf. §4, III); la frontera del domini **G**(r) format per tots aquests camps és constituïda per infinits arcs de circumferència, que corresponen a la línia (3). Si x és ara una constant real, però amb valor irracional, i y va de $+\infty$ a 0, aleshores $\omega = x + iy$ travessa infinits d'aquests dominis **G**(r), i els nombres r , els denominadors dels quals sempre creixen, s'apropen infinitament al valor x . Sempre que ω pertany a un mateix domini **G**(r), el nombre equivalent ω_0 descriu arcs de circumferència del camp principal, els quals condueixen sempre cap a una determinada de les dues línies (1), (2), a partir d'aquí salten als punts simètrics i mitjançant desplaçaments es deixen col·locar junts en un únic cercle; però finalment un d'aquests últims arcs ha de conduir a la línia (3); aleshores ω entra en el domini **G**(r') següent, i ara ω_0 comença, a partir del punt simètric de la línia (3), un nou moviment en l'arc de circumferència en (ω_0), que correspon al recorregut de la variable ω a través d'un nombre finit de camps del domini **G**(r') (cf. el final de §6). L'apropament dels nombres r , r' , ... al valor x no deixa de tenir interès, i em prometo (potser erradament) mitjançant una recerca més propera, obtenir-ne encara un

resultat útil, almenys per al cas que x sigui l'arrel d'una equació quadràtica de coeficients racionals.

3. LA VALÈNCIA

Després d'aquests preparatius, procedeix al teorema fonamental de la meua investigació, que s'enuncia de la manera següent:

Existeix una funció v de la variable ω en el domini $\mathbf{S}$ i en la seva frontera $\mathbf{R}$, la qual pren un valor determinat per a tots els valors equivalents ω , i tal que, recíprocament, cada valor de la variable complexa no fitada v correspon a una determinada classe de valors equivalents ω .

La demostració resulta dels principis de RIEMANN (art. 21 de la Dissertació Inaugural). S'aplica una de les dues meitats simètriques del camp principal (ω_0) en una de les dues meitats del pla v en les quals es descompon mitjançant l'eix dels v reals; en això, tres constants reals romanen arbitràries, atès que els punts imatge corresponents a un punt de l'interior i a un punt de la frontera de l'original poden ésser escollits arbitràriament. Després es prolonga l'aplicació a través de l'eix de simetria del camp (ω_0) en l'altra meitat, de manera que dos punts ω_0 simètrics respecte de l'eix corresponguin a dos valors complexos conjugats v ; amb això, tot el camp (ω_0) s'aplica en tot el pla v , ja que cada dos valors equivalents ω_0 , és a dir, cada dos punts simètrics de la frontera de (ω_0), corresponen a un mateix valor (real) v ; cada dos valors ω_0 no equivalents corresponen a dos valors diferents v i, recíprocament, cada valor v correspon o bé a un únic valor ω_0 , o bé a dos valors equivalents ω_0 que pertanyen a la frontera de (ω_0). Per tant, es pot estendre l'aplicació de (ω_0) a tots els camps (ω) de

tot el semiplà $\mathbf{S}$ i a la seva frontera de manera que cada dos valors equivalents ω corresponen a un mateix valor v , i és palès que la funció v varia contínuament en traspasar d'un camp (ω) a un camp veí a través de la seva frontera.

Si ara A, B, C, D són constants reals arbitràries, la funció

$$\frac{C + Dv}{A + Bv}$$

té les mateixes propietats que v , i pren igualment cada valor real una sola vegada quan ω_0 recorre tota la frontera d'una de les meitats simètriques del camp (ω_0); ara, les tres constants de què disposem cal que siguin escollides de manera que es correspongui:

$$\begin{array}{ll} \text{al valor } \omega_0 = \rho, & \text{el valor } v = 0, \\ \text{al valor } \omega_0 = i, & \text{el valor } v = 1, \\ \text{al valor } \omega_0 = \infty, & \text{el valor } v = \infty. \end{array}$$

Anomenem la funció v completament determinada d'aquesta manera *valència* de ω , i la denotem per $\text{val}(\omega)$. Nombres ω equivalents són, segons això, nombres de valència igual.

4. PUNTS DE CIRCUMVOLUCIÓ

Per a aconseguir a partir d'aquesta definició de la funció v la seva determinació analítica, considerem primerament la seva funció inversa; si ω n'és una branca, aleshores cadascuna de les altres branques és de la forma

$$\omega_1 = \frac{\gamma + \delta\omega}{\alpha + \beta\omega},$$

on $\alpha, \beta, \gamma, \delta$ denoten quatre nombres enters, que satisfan la condició $\alpha\delta - \beta\gamma = 1$, i cal considerar quan dues d'aquestes

branques, en general diferents, poden coincidir en un punt de circumvolució ⁴⁾, per al qual esdevé $\omega = \omega_1 = \tau$. Per a tal fi, cal requerir que τ sigui una arrel de l'equació

$$\beta\tau^2 + (\alpha - \delta)\tau - \gamma = 0,$$

és a dir,

$$(2\beta\tau + \alpha - \delta)^2 = (\alpha + \delta)^2 - 4,$$

i, atès que τ o bé és racional o bé té una ordenada positiva, resulta que només són possibles els tres casos que segueixen.

$$(I) \quad \alpha + \delta = 0$$

Atès que $\alpha^2 + 1 = (\alpha + i)(\alpha - i) = -\beta\gamma$, i β es pot prendre positiu, aleshores s'obté amb facilitat, a partir de la teoria dels nombres complexos enters de GAUSS, que es pot posar

$$\begin{aligned} -\alpha + i &= (\alpha' - \beta'i)(\gamma' + \delta'i), & \gamma &= -(\gamma' + \delta'i)(\gamma' - \delta'i), \\ \beta &= (\alpha' + \beta'i)(\alpha' - \beta'i), & \alpha + i &= -(\alpha' + \beta'i)(\gamma' - \delta'i), \end{aligned}$$

on α' , β' , γ' , δ' denoten quatre nombres racionals enters, que evidentment han de satisfer la condició $\alpha'\delta' - \beta'\gamma' = 1$; els nombres complexos enters $\alpha' + \beta'i$, $\gamma' + \delta'i$ són relativament primers, i s'obté que

$$\tau = \frac{-\alpha + i}{\beta} = \frac{\gamma}{\alpha + i} = \frac{\gamma' + \delta'i}{\alpha' + \beta'i},$$

és a dir, τ és equivalent amb i , i, en conseqüència, és $v = 1$. Si ara, per exemple, prenem $\tau = i$, aleshores es té que

$$\alpha = 0, \quad \beta = 1, \quad \gamma = -1, \quad \delta = 0,$$

⁴⁾punt el·líptic (n. dels t.)

i les dues branques esmentades són

$$\omega_0 \quad \text{i} \quad \frac{-1}{\omega_0}.$$

Però aquestes, veritablement, coincideixen en el lloc $v = 1$, $\omega = i$; perquè quan v descriu una volta positiva a l'entorn de $v = 1$ partint de valors d'ordenada positiva, és a dir, creua l'eix dels v reals, primer entre 0 i 1, i, després, entre 1 i ∞ , aleshores ω_0 traspassa de la meitat del camp principal (ω_0) en la qual les abscisses són negatives, a través de l'arc de circumferència (3) entre ρ i i , primerament a la meitat del camp $\left(\frac{-1}{\omega_0}\right)$ en la qual les abscisses són negatives, i després, a través de l'eix d'ordenades, a l'altra meitat del mateix camp $\left(\frac{-1}{\omega_0}\right)$ en la qual les abscisses són positives. D'aquí resulta que $(1-v)$ esdevé tan infinitament petit com $(\omega - i)^2$, i se segueix que en aquest punt de circumvolució el producte

$$(1-v)^{-\frac{1}{2}} \frac{dv}{d\omega}$$

roman finit i diferent de 0. El mateix val per a cadascuna de les dues branques

$$\omega = \frac{\gamma' + \delta'\omega_0}{\alpha' + \beta'\omega_0} \quad \text{i} \quad \omega_1 = \frac{-\delta' + \gamma'\omega_0}{-\beta' + \alpha'\omega_0},$$

les quals per a $v = 1$ coincideixen amb un dels valors

$$\tau = \frac{\gamma' + \delta'i}{\alpha' + \beta'i}$$

equivalents a i , i entre les quals se satisfà la relació

$$\omega_1 = \frac{\gamma - \alpha\omega}{\alpha + \beta\omega} = \frac{-(\gamma'^2 + \delta'^2) + (\alpha'\gamma' + \beta'\delta')\omega}{(-\alpha'\gamma' + \beta'\delta') + (\alpha'^2 + \beta'^2)\omega}.$$

$$(II) \quad \alpha + \delta = \pm 1$$

Si es posa, per a abreujar,

$$\varepsilon = \frac{1 - \alpha + \delta}{2},$$

aleshores, segons que sigui vàlid el signe superior o l'inferior, es té que

$$\varepsilon = 1 - \alpha = \delta, \quad \text{o bé} \quad \varepsilon = -\alpha = 1 + \delta;$$

en ambdós casos se segueix que

$$(\varepsilon + \alpha - 1)(\varepsilon + \alpha) = 0,$$

per tant,

$$\alpha\delta = \alpha(2\varepsilon + \alpha - 1) = \varepsilon - \varepsilon^2;$$

en conseqüència és

$$-\beta\gamma = \varepsilon^2 - \varepsilon + 1 = (\varepsilon + \rho)(\varepsilon + \rho^2),$$

i, atès que β es pot prendre positiu, se segueix, com a conseqüència de la teoria dels nombres complexos enters construïts a partir de ρ , que es pot posar

$$\varepsilon + \rho = (\alpha' + \beta'\rho^2)(\gamma' + \delta'\rho);$$

$$\gamma = -(\gamma' + \delta'\rho)(\gamma' + \delta'\rho^2),$$

$$\beta = (\alpha' + \beta'\rho)(\alpha' + \beta'\rho^2);$$

$$\varepsilon + \rho^2 = (\alpha' + \beta'\rho)(\gamma' + \delta'\rho^2),$$

on α' , β' , γ' , δ' denoten quatre nombres racionals enters, que manifestament han de satisfer la condició $\alpha'\delta' - \beta'\gamma' =$

1; els nombres complexos enters $\alpha' + \beta'\rho$, $\gamma' + \delta'\rho$ són relativament primers, i s'obté que

$$\tau = \frac{\varepsilon + \rho}{\beta} = \frac{-\gamma}{\varepsilon + \rho^2} = \frac{\gamma' + \delta'\rho}{\alpha' + \beta'\rho},$$

és a dir, τ és equivalent a ρ , i se segueix que $v = 0$. Si ara es pren, per exemple, $\tau = \rho$, aleshores és $\varepsilon = 0$, $\beta = 1$, per tant, o bé

$$\alpha = 1, \quad \beta = 1, \quad \gamma = -1, \quad \delta = 0,$$

o bé

$$\alpha = 0, \quad \beta = 1, \quad \gamma = -1, \quad \delta = -1,$$

i, de fet, quan v fa una volta positiva a l'entorn de $v = 0$ partint d'un valor d'ordenada positiva, de les tres branques

$$\omega_0, \quad \frac{-1 - \omega_0}{\omega_0}, \quad \frac{-1}{1 + \omega_0}$$

la primera s'aplica en la segona, aquesta en la tercera, i aquesta de nou en la primera. (Si v fa el mateix recorregut partint d'un valor d'ordenada negativa, aleshores les tres branques

$$\frac{-1}{\omega_0}, \quad -1 + \omega_0, \quad \frac{-\omega_0}{-1 + \omega_0},$$

que igualment tenen en comú el vèrtex ρ , s'apliquen cíclicament l'una en l'altra). D'aquí se segueix que en aquest punt de circumvolució el producte

$$v^{-\frac{2}{3}} \frac{dv}{d\omega}$$

roman finit i diferent de 0. Anàlogament es comporta per a tots els altres valors τ equivalents a ρ .

$$(III) \quad (\alpha + \delta)^2 = 4$$

En aquest cas, i només en aquest cas, τ és racional, per tant, un representant de la frontera $\mathbf{R}$, i, per consegüent, és $v = \infty$. Si es posa (la qual cosa és permesa) $\alpha + \delta = +2$, i

$$\tau = \frac{1 - \alpha}{\beta} = \frac{-\gamma}{1 - \alpha} = \frac{m}{n},$$

on m, n són relativament primers, aleshores s'obté que

$$\alpha = 1 + gmn, \quad \beta = -gn^2, \quad \gamma = +gm^2, \quad \delta = 1 - gmn,$$

on g denota un nombre enter *arbitrari*. Si es pren, per exemple, $m = 1, n = 0$, per tant, $\tau = \infty$, aleshores es reconeix fàcilment que cadascuna de les infinites branques $(g + \omega_0)$ s'aplica en la branca següent $(g + 1 + \omega_0)$ per mitjà d'un recorregut positiu de v a l'entorn de $v = \infty$. Per tant, per a valors infinitament grans de ω , la quantitat infinitament petita

$$q^2 = \mathbf{1}^\omega$$

és una funció un a un de v , i atès que, recíprocament, v és una funció univaluada de $\mathbf{1}^\omega$ arreu, aleshores per a $\omega = \infty$ el producte

$$v\mathbf{1}^\omega$$

roman finit i diferent de zero, i alhora esdevé

$$v^{-1} \frac{dv}{d\omega} = \frac{d \log v}{d\omega} = -2\pi i.$$

D'aquí es pot derivar fàcilment el comportament de v per a tots els altres valors racionals $\omega = \frac{m}{n}$.

5. EQUACIONS DIFERENCIALS

Si u, v denoten dues variables qualssevol dependents l'una de l'altra, aleshores, per a abreujar, posarem l'expressió diferencial de tercer ordre

$$(1) \quad \frac{-4}{\sqrt{\frac{dv}{du}}} \frac{d}{dv} \frac{d}{dv} \sqrt{\frac{dv}{du}} = [v, u];$$

es troba fàcilment que aquesta posseeix les dues propietats

$$(2) \quad [u, v] = -[v, u] \left(\frac{dv}{du} \right)^2,$$

$$(3) \quad [v, u]dv^2 + [w, v]dw^2 + [u, w]du^2 = 0,$$

on, igualment, w denota una funció qualsevol de u , i, per tant, també de v . Si, a més, u, w són dues variables *col·lineals*, amb la qual cosa cal que s'expressi

$$(4) \quad w = \frac{C + Du}{A + Bu},$$

on A, B, C, D denoten constants, aleshores es té que

$$(5) \quad [u, w] = [w, u] = 0,$$

i se segueix, en termes de v , que

$$(6) \quad [v, u] = [v, w];$$

i, recíprocament, si és $[u, w] = 0$, aleshores u, w són col·lineals, és a dir, l'equació (4) és la integral general de l'equació diferencial (5).

Apliquem aquests teoremes generals a l'exemple que segueix. Si, de nou, és $v = \text{val}(\omega)$, aleshores, evidentment,

$$[v, \omega] = f(\omega)$$

és una funció univaluada de ω , atès que és construïda de manera racional a partir de les derivades de primer, segon i tercer ordre de v respecte de ω ; demostrem ara que també és una funció univaluada de v . De fet, si es posa $v_1 = \text{val}(\omega_1)$, on ω_1 denota una nova variable, aleshores és $f(\omega_1) = [v_1, \omega_1]$; i si ω_1 es relaciona amb ω mitjançant la igualtat

$$\omega_1 = \frac{\gamma + \delta\omega}{\alpha + \beta\omega},$$

on $\alpha, \beta, \gamma, \delta$ denoten nombres enters que satisfan la condició $\alpha\delta - \beta\gamma = 1$, aleshores és $v_1 = v$, per tant, $f(\omega_1) = [v, \omega_1]$; atès que, a més, ω, ω_1 són col·lineals, se segueix de (6) que $[v, \omega] = [v, \omega_1]$, per tant, és $f(\omega) = f(\omega_1)$; amb això, cada valor de v correspon únicament a un sol valor de $f(\omega)$. Doncs, podem posar

$$(7) \quad [v, \omega] = F(v),$$

on $F(v)$ denota una funció univaluada de v . A partir de la seva construcció, resulta que aquesta roman finita per a tots els valors de v , amb excepció de 1, 0, ∞ , i atès que en aquests valors de v , als quals es pot fer correspondre els valors i, ρ, ∞ de ω , els productes respectivament

$$(1-v)^{-\frac{1}{2}} \frac{dv}{d\omega}, \quad v^{-\frac{2}{3}} \frac{dv}{d\omega}, \quad v^{-1} \frac{dv}{d\omega}$$

romanen finits i diferents de zero, resulta aleshores que corresponen a

$$(1-v)^2 F(v) = \frac{3}{4}, \quad v^2 F(v) = \frac{8}{9}, \quad v^2 F(v) = 1;$$

atès que, com a conseqüència d'això, la funció univaluada $v^2(1-v)^2F(v)$ roman finita per a tots els valors de v i per a $v = \infty$ es fa infinita de segon ordre, aleshores és una funció de segon ordre entera, els coeficients de la qual s'obtenen immediatament a partir de les tres identitats anteriors; d'aquesta manera es troba que

$$(8) \quad \left\{ \begin{aligned} F(v) &= \frac{36v^2 - 41v + 32}{36v^2(1-v)^2} = \\ &= \frac{8}{9v^2} + \frac{23}{36v} + \frac{3}{4(1-v)^2} + \frac{23}{36(1-v)}. \end{aligned} \right.$$

La funció $v = \text{val}(\omega)$ és, per tant, una solució v' de l'equació diferencial de tercer ordre

$$(9) \quad [v', \omega] = F(v');$$

a fi de trobar-ne la integral general v' , es posa $v' = \text{val}(\omega')$, on ω' denota una nova variable; aleshores és $[v', \omega'] = F(v')$, per tant, $[v', \omega'] = [v', \omega]$, d'on se segueix, tenint en compte (2) i (3), que $[\omega, \omega'] = 0$, per tant,

$$(10) \quad \omega' = \frac{C + D\omega}{A + B\omega}, \quad v' = \text{val} \left(\frac{C + D\omega}{A + B\omega} \right),$$

on A, B, C, D denoten constants arbitràries. De la mateixa manera s'obté a partir de (3) que el sistema format per les dues equacions

$$(11) \quad v = \text{val}(\omega), \quad v' = \text{val} \left(\frac{C + D\omega}{A + B\omega} \right)$$

constitueix la integral general de l'equació diferencial de tercer ordre (cf. *Fundamenta nova* §§32, 33)

$$(12) \quad [v, v']dv^2 = F(v)dv^2 - F(v')dv'^2.$$

6. LES FUNCIONS MODULARS ELLÍPTIQUES

A partir de la construcció de l'expressió $[v, \omega]$ resulta que $\sqrt{\frac{dv}{d\omega}}$ satisfà una equació diferencial lineal de segon ordre respecte de v ; evidentment, val la pena introduir la quantitat

$$(1) \quad w = \text{const.} \cdot v^{-\frac{1}{3}}(1-v)^{-\frac{1}{4}} \left(\frac{dv}{d\omega} \right)^{\frac{1}{2}},$$

la qual roman finita i diferent de zero per a tots els valors de ω a l'interior de **S**, mentre que a la frontera **R** esdevé infinitament petita; amb això el $\log w$, i cada potència de w , tan bon punt sigui donat el seu valor en un punt del domini connex **S**, és una funció completament determinada i univaluada de ω . A partir de l'equació diferencial de tercer ordre anterior (7) de §5, se segueix ara que w satisfà l'equació diferencial hipergeomètrica

$$(2) \quad v(1-v) \frac{d^2 w}{dv^2} + \left(\frac{2}{3} - \frac{7}{6}v \right) \frac{dw}{dv} - \frac{1}{144}w = 0,$$

la integral general de la qual $(\text{const.} + \text{const.} \cdot \omega)w$ és continguda en l'expressió

$$\text{const.} \cdot F\left(\frac{1}{12}, \frac{1}{12}, \frac{2}{3}, v\right) + \text{const.} \cdot F\left(\frac{1}{12}, \frac{1}{12}, \frac{1}{2}, 1-v\right),$$

on F denota la sèrie de GAUSS. El mateix també s'hauria obtingut mitjançant una investigació directa de la quantitat w com una funció P de RIEMANN i, encara més fàcilment, s'arribaria al mateix objectiu amb les consideracions que constitueixen la base del capítol XXV de les Obres de RIEMANN, tal com el meu amic HEINRICH WEBER de Königsberg em comunicà fa un any. Finalment, faig notar

que el problema de l'aplicació considerat en §3, es pot enllestir també mitjançant les recerques de WEIERSTRASS i SCHWARZ.

D'interès especial és ara l'arrel quadrada de la quantitat w , la qual denotem per

$$(3) \quad \eta(\omega) = \text{const. } v^{-\frac{1}{6}}(1-v)^{-\frac{1}{8}} \left(\frac{dv}{d\omega} \right)^{\frac{1}{4}};$$

és una funció univaluada de ω , com ja s'ha remarcat, la qual roman finita i diferent de zero per a tots els valors de ω a l'interior de $\mathbf{S}$; per a $\omega = \infty$ esdevé tan infinitament petita com $v^{-\frac{1}{24}}$, així com també $\mathbf{1}^{\frac{\omega}{24}}$; trio la constant per tal que per a $\omega = \infty$ es tingui el producte

$$(4) \quad \mathbf{1}^{-\frac{\omega}{24}} \eta(\omega) = 1,$$

i, amb això, $\eta(\omega)$ queda determinada completament en tot el domini $\mathbf{S}$. Si $\alpha, \beta, \gamma, \delta$ denoten de nou nombres enters que satisfan la condició $\alpha\delta - \beta\gamma = 1$, aleshores de

$$\text{val} \left(\frac{\gamma + \delta\omega}{\alpha + \beta\omega} \right) = \text{val}(\omega)$$

se segueix la propietat

$$(5) \quad \eta \left(\frac{\gamma + \delta\omega}{\alpha + \beta\omega} \right) = c(\alpha + \beta\omega)^{\frac{1}{2}} \eta(\omega),$$

on $c^{24} = 1$; en particular, s'obté fàcilment que

$$(6) \quad \eta(1 + \omega) = \mathbf{1}^{\frac{1}{24}} \eta(\omega); \quad \eta\left(\frac{-1}{\omega}\right) = \mathbf{1}^{-\frac{1}{8}} \omega^{\frac{1}{2}} \eta(\omega),$$

on s'esdevé que $\omega^{\frac{1}{2}} = \mathbf{1}^{\frac{1}{8}}$, quan $\omega = \mathbf{1}^{\frac{1}{4}} = i$. La funció és completament determinada per les propietats esmentades;

car si $f(\omega)$ es comporta de la mateixa manera, aleshores el quocient $f(\omega) : \eta(\omega)$, com a conseqüència de (6), és una funció univaluada de $v = \text{val}(\omega)$, la qual roman finita per a tots els valors finits de v , i, com a conseqüència de (4), pren el valor 1 per a $v = \infty$, per la qual cosa se segueix que és constant = 1.

Per a establir ara la dependència entre aquesta funció $\eta(\omega)$ i el mòdul de la integral el·líptica, o el seu quadrat k , considero les funcions

$$(7) \quad \eta_1(\omega) = \eta(2\omega); \quad \eta_2(\omega) = \eta\left(\frac{\omega}{2}\right); \quad \eta_3(\omega) = \eta\left(\frac{1+\omega}{2}\right),$$

que s'obtenen mitjançant les corresponents transformacions de segon ordre i que posseeixen les propietats que segueixen. De (6), se segueix que

$$\eta_1(1+\omega) = \mathbf{1}^{\frac{1}{12}} \eta_1(\omega), \quad \eta_1\left(\frac{-1}{\omega}\right) = \mathbf{1}^{-\frac{1}{8}} \left(\frac{\omega}{2}\right)^{\frac{1}{2}} \eta_2(\omega),$$

$$\eta_2(1+\omega) = \eta_3(\omega), \quad \eta_2\left(\frac{-1}{\omega}\right) = \mathbf{1}^{-\frac{1}{8}} (2\omega)^{\frac{1}{2}} \eta_1(\omega),$$

$$\eta_3(1+\omega) = \mathbf{1}^{\frac{1}{24}} \eta_2(\omega), \quad \eta_3\left(\frac{-1}{\omega}\right) = \mathbf{1}^{-\frac{1}{8}} \omega^{\frac{1}{2}} \eta_3(\omega),$$

i, per a $\omega = \infty$, se segueix de (4) que

$$\mathbf{1}^{-\frac{\omega}{12}} \eta_1(\omega) = 1, \quad \mathbf{1}^{-\frac{\omega}{48}} \eta_2(\omega) = 1, \quad \mathbf{1}^{-\frac{\omega}{48}} \eta_3(\omega) = \mathbf{1}^{\frac{1}{48}}.$$

A partir d'aquí s'obté que la funció

$$f(\omega) = \frac{\eta_1(\omega) \eta_2(\omega) \eta_3(\omega)}{\eta(\omega)^3}$$

posseeix les propietats

$$f(1+\omega) = f(\omega), \quad f\left(-\frac{1}{\omega}\right) = f(\omega),$$

i se segueix que és una funció univaluada de $v = \text{val}(\omega)$, perquè totes les substitucions $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ es poden construir a partir de les dues substitucions $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ i $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$; per la seva pròpia definició, roman finita per a tots els valors finits de v i esdevé $= \mathbf{1}^{\frac{1}{48}}$ per a $\omega = \infty$, $v = \infty$, d'on se segueix que és una constant. Per tant, és

$$(8) \quad \eta_1(\omega) \eta_2(\omega) \eta_3(\omega) = \mathbf{1}^{\frac{1}{48}} \eta(\omega)^3,$$

i un teorema similar és vàlid per a transformacions d'ordre arbitrari. De la mateixa manera s'obté que la funció

$$f_1(\omega) = \frac{2^4 \eta_1(\omega)^8 + \eta_2(\omega)^8 + \mathbf{1}^{\frac{1}{3}} \eta_3(\omega)^8}{\eta(\omega)^8}$$

posseeix les propietats

$$f_1(1 + \omega) = \mathbf{1}^{\frac{1}{3}} f_1(\omega), \quad f_1\left(\frac{-1}{\omega}\right) = f_1(\omega),$$

d'on se segueix que $f_1(\omega)^3$ és una funció univaluada de $v = \text{val}(\omega)$, que és finita per a cada valor finit de v ; per a $\omega = \infty$, $v = \infty$, a més, esdevé $f_1(\omega) \mathbf{1}^{\frac{1}{6}} = 0$; per tant, també $f_1(\omega)^3 v^{-\frac{1}{2}} = 0$; per tant, $f_1(\omega)^3$ no pot esdevenir infinitament gran ni tan sols d'ordre $v^{\frac{1}{2}}$, i se segueix que $f_1(\omega)^3$, per tant, també $f_1(\omega)$, és una constant, i, certament, igual a 0, com s'obté de $f_1(1 + \omega) = \mathbf{1}^{\frac{1}{3}} f_1(\omega)$. Doncs, és

$$(9) \quad 2^4 \eta_1(\omega)^8 + \eta_2(\omega)^8 + \mathbf{1}^{\frac{1}{3}} \eta_3(\omega)^8 = 0.$$

Si s'introdueixen ara les notacions següents (que coincideixen amb les d'HERMITE)

$$(10) \quad \left\{ \begin{array}{l} \varphi(\omega) = \mathbf{1}^{\frac{1}{48}} \sqrt{2} \frac{\eta_1(\omega)}{\eta_3(\omega)} = \sqrt[4]{\kappa} = \sqrt[8]{k}, \\ \psi(\omega) = \mathbf{1}^{\frac{1}{48}} \frac{\eta_2(\omega)}{\eta_3(\omega)} = \sqrt[4]{\kappa'} = \varphi\left(\frac{-1}{\omega}\right), \\ \chi(\omega) = \mathbf{1}^{\frac{1}{48}} \sqrt[6]{2} \frac{\eta(\omega)}{\eta_3(\omega)}, \end{array} \right.$$

aleshores se segueix de (9) que

$$(11) \quad \varphi(\omega)^8 + \psi(\omega)^8 = 1, \quad \kappa^2 + \kappa'^2 = 1$$

i, de (8),

$$(12) \quad \varphi(\omega) \psi(\omega) = \chi(\omega)^3;$$

a més, les quantitats K , K' es poden definir mitjançant les igualtats

$$(13) \quad \sqrt{\frac{2K}{\pi}} = \mathbf{1}^{-\frac{1}{24}} \frac{\eta_3(\omega)^2}{\eta(\omega)}, \quad K'i = K\omega.$$

Ara, segons el que s'ha esmentat, per a la funció $k = \kappa^2 = \varphi(\omega)^8$ s'obtenen les propietats

$$(14) \quad \varphi(1 + \omega)^8 = -2^4 \frac{\eta_1(\omega)^8}{\eta_2(\omega)^8} = \frac{k}{k-1},$$

$$(15) \quad \varphi\left(\frac{-1}{\omega}\right)^8 = \mathbf{1}^{\frac{1}{6}} \frac{\eta_2(\omega)^8}{\eta_3(\omega)^8} = \kappa'^2 = 1 - k,$$

i, a més, és

$$(16) \quad k\mathbf{1}^{-\frac{\omega}{2}} = 2^4 \quad \text{per a } \omega = \infty.$$

D'aquí se segueix que la funció

$$f_2(\omega) = \frac{(k + \rho)^3(k + \rho^2)^3}{k^2(1 - k)^2}$$

posseeix les propietats

$$f_2(1 + \omega) = f_2(\omega), \quad f_2\left(\frac{-1}{\omega}\right) = f_2(\omega),$$

en conseqüència, és una funció univaluada de $v = \text{val}(\omega)$; per tant, pot esdevenir infinita si, i només si, $k = 0, 1, \infty$; però, atès que k i $(1 - k)$ són quocients de funcions η , això pot passar si, i només si, $v = \infty$, per exemple, per a $\omega = \infty$; però en aquest cas k esdevé, com a conseqüència de (16), infinitament petita com $\mathbf{1}^{\frac{\omega}{2}}$, per tant, com $v^{-\frac{1}{2}}$, i se segueix que $f_2(\omega)$ és infinitament gran com v ; en conseqüència, $f_2(\omega)$ és una funció entera de primer grau de v , per tant,

$$\frac{(k + \rho)^3(k + \rho^2)^3}{k^2(1 - k)^2} = av + b.$$

A fi i efecte de determinar la constant b , es posa $\omega = \rho$, per tant, $v = 0$; ara, atès que

$$\eta_3(\rho) = \eta\left(\frac{1 + \rho}{2}\right) = \eta\left(\frac{-1}{2\rho}\right),$$

d'on se segueix que

$$\eta_3(\rho)^8 = \eta\left(\frac{-1}{2\rho}\right)^8 = (2\rho)^4 \eta(2\rho)^8 = (2\rho)^4 \eta_1(\rho)^8,$$

s'obté així per a k el valor

$$(17) \quad \varphi(\rho)^8 = \mathbf{1}^{\frac{1}{6}} 2^4 \frac{\eta_1(\rho)^8}{\eta_3(\rho)^8} = -\rho,$$

i se segueix que $b = 0$. A fi i efecte de determinar a es posa $\omega = i$, per tant, $v = 1$; aleshores s'obté per a k el valor

$$(18) \quad \varphi(i)^8 = \varphi\left(\frac{-1}{i}\right)^8 = 1 - \varphi(i)^8 = \frac{1}{2},$$

d'on se segueix que $a = \frac{27}{4}$. D'aquesta manera obtenim el resultat

$$(19) \quad v = \text{val}(\omega) = \frac{4}{27} \frac{(k + \rho)^3 (k + \rho^2)^3}{k^2 (1 - k)^2}.$$

La funció v apareix d'aquesta forma en diferents llocs del famós treball d'HERMITE sobre la teoria d'equacions modulars; remarco al mateix temps que també GAUSS (cf. *Werke* III, p. 386) havia tingut el propòsit d'introduir una funció semblant.

De manera semblant a tal com s'ha procedit més amunt per a $\eta(\omega)$, es pot demostrar que la funció $k = \varphi(\omega)^8$ és completament determinada per les propietats indicades; els principis en els quals es recolza la demostració de l'existència de la funció v també condueixen de la mateixa manera fàcil a la determinació *immediata* de la funció k ; tal com resulta de la combinació de (14) i (15), aquesta requereix, per a la seva descripció completa en el domini $\mathbf{S}$, sis camps sencers o bé dotze mitjos camps (ω), que finalment poden ésser escollits disposats simètricament a les dues bandes de l'eix purament imaginari. S'obté d'aquesta manera l'equació diferencial de tercer ordre

$$(20) \quad [k, \omega] = \frac{(k + \rho)(k + \rho^2)}{k^2 (1 - k)^2}$$

i de la mateixa manera com abans hem arribat a una equació diferencial lineal de segon ordre per a $w = \text{const. } \eta(\omega)^2$, aquí en resulta, quan es posa

$$(21) \quad \frac{dk}{d\omega} = \frac{-4}{\pi i} k(1-k)K^2,$$

la coneguda equació diferencial lineal

$$(22) \quad \frac{d}{dk} \left(k(1-k) \frac{dK}{dk} \right) = \frac{1}{4} K,$$

que constitueix el punt de partida de la memòria de FUCHS. Naturalment, també s'obtindrien els mateixos resultats a partir del lligam entre k i v que hem expressat en (19).

Atès que k és unívocament determinada com a funció de ω per les propietats anteriors, i atès que la funció

$$\frac{\vartheta_2(0, \omega)^4}{\vartheta_3(0, \omega)^4},$$

que es troba en la teoria de les funcions el·líptiques o de les funcions ϑ , posseeix les mateixes propietats, resulta fàcilment de la identitat d'aquestes dues funcions que

$$(23) \quad \begin{cases} \vartheta(0, \omega) = \frac{\eta_2(\omega)^2}{\eta(\omega)}, & \vartheta'_1(0, \omega) = 2\pi\eta(\omega)^3, \\ \vartheta_2(0, \omega) = 2\frac{\eta_1(\omega)^2}{\eta(\omega)}, & \vartheta_3(0, \omega) = \mathbf{1}^{-\frac{1}{24}} \frac{\eta_3(\omega)^2}{\eta(\omega)}, \end{cases}$$

i se segueix que

$$(24) \quad \eta(\omega) = \mathbf{1}^{\frac{\omega}{24}} \prod (1 - \omega^\nu) = q^{\frac{1}{12}} \prod (1 - q^{2\nu}),$$

on ν recorre tots els nombres enters positius i s'ha posat

$$(25) \quad q = 1^{\frac{\omega}{2}}.$$

Val a dir que fins ara no he aconseguit derivar aquesta *representació* de $\eta(\omega)$ com a funció explícita de ω a partir només de la definició donada més amunt, és a dir, sense l'ajut de la teoria de les funcions ϑ .

L'ocupació específica amb aquesta funció $\eta(\omega)$, que se'm presentà per primera vegada en la recerca sobre el nombre de classes d'ideals en els cossos cúbics, m'ha estat posteriorment de gran utilitat per a l'arranjament del segon fragment XXVII de les Obres Pòstumes de RIEMANN. Els nombres (m, n) als quals m'ha portat el seu estudi posseeixen, de fet, propietats molt interessants; per exemple, si n és un enter senar positiu i m un enter relativament primer amb n , aleshores és

$$\left(\frac{m}{n}\right) \equiv \frac{n+1}{2} - (m, n) \pmod{4},$$

on $\left(\frac{m}{n}\right)$ denota el símbol de LEGENDRE i de JACOBI de la teoria dels residus quadràtics; si m és, també, positiu i senar, aleshores mitjançant la utilització del teorema

$$2m(m, n) + 2n(n, m) = 1 + m^2 + n^2 - 3mn,$$

en resulta de seguida la llei de reciprocitat generalitzada en la forma

$$\left(\frac{m}{n}\right) + \left(\frac{n}{m}\right) \equiv 2 \left(1 + \frac{m-1}{2} \frac{n-1}{2}\right) \pmod{4}.$$

Em permeto aquí cridar l'atenció sobre un punt de la memòria de FUCHS en què em sembla que ha incorregut en

un error. Si m , n són nombres relativament primers i $\omega = x + yi$ s'apropa al valor racional $\frac{m}{n}$ de manera que x roman constant $= \frac{m}{n}$, i y esdevé positiva i infinitament petita, aleshores k s'apropa al valor

$$k = \infty, \quad \text{si } m \equiv 1, \quad n \equiv 1 \pmod{2},$$

$$k = 1, \quad \text{si } m \equiv 0, \quad n \equiv 1 \pmod{2},$$

$$k = 0, \quad \text{si } m \equiv 1, \quad n \equiv 0 \pmod{2},$$

com se segueix del fragment de RIEMANN o també de la teoria d'abans; si, en canvi, $\omega = x + iy$ s'apropa de la mateixa manera a un valor real *irracional* de x , aleshores resulta de la teoria d'abans (cf. el final de §2) que k no s'apropa a *cap* valor determinat, sinó que oscil·la sense parar. Això està en contradicció amb el teorema II de la pàgina 27 de la memòria esmentada, en el qual s'afirma que la quantitat u ($= k^{-1}$ en la meua notació) sempre s'hauria d'apropar a un dels dos valors zero o u , i a mi em sembla que es deu als pensaments que es dirigeixen a la demostració d'aquesta afirmació, a saber, en el fragment que segueix a les paraules “*ou n'y parvînt pas*” (p. 26). Malgrat tot, aquesta discrepància no té cap importància significativa per al contingut essencial de la interessantíssima memòria.

7. TRANSFORMACIÓ

Tot seguit, i per a acabar, encara fonamentarem la teoria de les equacions algebriques entre valències, les quals corresponen a les equacions modulars en la teoria de les

transformacions de les funcions el·líptiques o bé de les funcions ϑ . Sigui, novament, $v = \text{val}(\omega)$, i

$$v_n = \text{val} \left(\frac{C + D\omega}{A + B\omega} \right),$$

on A, B, C, D denoten nombres *enters* arbitraris sense divisor comú i de determinant positiu

$$AD - BC = n.$$

El nombre de totes les funcions possibles v_n que corresponen a un nombre enter positiu n donat és finit i fàcil de determinar. A saber, si A, B, C, D són donats, ∂ és el màxim comú divisor positiu dels dos nombres

$$B = \partial\beta, \quad D = \partial\delta,$$

aleshores és

$$n = a\partial, \quad \text{on } a = A\delta - C\beta;$$

atès que β, δ són nombres relativament primers, ara es poden determinar d'una sola forma dos nombres enters α, γ tals que sigui $\alpha\delta - \beta\gamma = 1$ i, alhora, que el nombre

$$c = C\alpha - A\gamma$$

satisfaci la condició

$$0 \leq c < a;$$

aleshores és

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} a & 0 \\ c & \partial \end{pmatrix},$$

per tant,

$$v_n = \text{val} \left(\frac{C + D\omega}{A + B\omega} \right) = \text{val} \left(\frac{c + \partial\omega}{a} \right),$$

i, atès que A, B, C, D no tenen cap divisor comú, el mateix val també per als tres nombres a, c, ∂ . A fi d'obtenir per a un nombre donat n totes les funcions v_n possibles, només cal permetre que a recorri tots els divisors positius de n ; per a cadascun d'aquests divisors a , es determina ∂ per l'equació $a\partial = n$; si ara e és el màxim comú divisor de a, ∂ , i $\varphi(e)$ denota el nombre dels enters $0, 1, 2, \dots, (e-1)$ que són relativament primers amb e , aleshores el nombre c ha de recórrer tots els $\frac{a}{e}\varphi(e)$ nombres que són relativament primers amb e i que alhora satisfan la condició $0 \leq c < a$. A més, es pot provar fàcilment que cada dos sistemes diferents de tres d'aquests nombres a, c, ∂ corresponen també a dues funcions no idèntiques

$$v_n = \text{val} \left(\frac{c + \partial\omega}{a} \right),$$

i, en conseqüència, el nombre de les funcions v_n veritablement diferents és igual a

$$\sum \frac{a}{e} \varphi(e) = \psi(n),$$

on a recorre tots els divisors de n i e cada vegada té el significat que li hem donat abans. D'aquesta expressió se segueix de seguida, quan n, n' són nombres relativament primers, el teorema

$$\psi(nn') = \psi(n)\psi(n');$$

el cas d'una potència de primer és fàcil d'enllestir, i d'aquí s'obté en general que

$$\psi(n) = n \prod \left(1 + \frac{1}{p}\right),$$

on p recorre tots els divisors primers diferents de n .

Si per a abreujar es posa $\psi(n) = \nu$ i es denota per

$$f_1(\omega), \quad f_2(\omega), \quad \dots, \quad f_\nu(\omega),$$

totes les funcions v_n diferents contingudes en l'expressió

$$\text{val}\left(\frac{C + D\omega}{A + B\omega}\right),$$

aleshores, si $\alpha, \beta, \gamma, \delta$ denoten quatre nombres enters determinats que satisfan la condició $\alpha\delta - \beta\gamma = 1$, també les ν funcions

$$f_1\left(\frac{\gamma + \delta\omega}{\alpha + \beta\omega}\right), \quad f_2\left(\frac{\gamma + \delta\omega}{\alpha + \beta\omega}\right), \quad \dots, \quad f_\nu\left(\frac{\gamma + \delta\omega}{\alpha + \beta\omega}\right)$$

són diferents les unes de les altres; atès que, a més, cada sistema de quatre nombres enters A, B, C, D sense divisor comú i que satisfan la condició $AD - BC = n$ proporciona de nou, mitjançant la composició

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} A' & B' \\ C' & D' \end{pmatrix},$$

un sistema de quatre nombres enters A', B', C', D' que no tenen cap divisor comú i que satisfan la condició $A'D' - B'C' = n$, aleshores cadascuna d'aquestes funcions és idèntica a una de les ν funcions v_n , i se segueix que el seu

complex és idèntic al de les funcions v_n . A més, si σ denota una quantitat arbitrària independent de ω , aleshores el producte

$$\prod (\sigma - v_n),$$

construït a partir de totes les ν funcions v_n , és una funció univaluada de ω que roman invariant quan se substitueix ω per una quantitat equivalent arbitrària

$$\frac{\gamma + \delta\omega}{\alpha + \beta\omega},$$

i en conseqüència es pot posar

$$\prod (\sigma - v_n) = F_n(\sigma, v),$$

on $F_n(\sigma, v)$ denota una funció entera de grau ν -èsim de σ , els coeficients de la qual són funcions univaluades de $v = \text{val}(\omega)$. Si v és finit, aleshores ω pertany a l'interior del domini **S**, d'on se segueix que cadascun dels ν valors v_n , per tant, també $F_n(\sigma, v)$, és finit. Però si és $v = \infty$, aleshores es pot suposar que també és $\omega = \infty$; atès que en aquest cas

$$\mathbf{1}^{\omega} \text{val}(\omega) = m,$$

també serà

$$\mathbf{1}^{\frac{\partial}{\partial} \omega} \text{val} \left(\frac{c + \partial\omega}{a} \right) = m \mathbf{1}^{-\frac{c}{a}},$$

on m és finit i diferent de zero (a saber $= 2^{-6}3^{-3}$, com en resulta a partir de (16) i (19) de §6); se segueix que $F_n(\sigma, v)$ esdevé infinitament gran a la vegada que v , i, certament, de l'ordre

$$\sum \frac{\partial}{\partial} \frac{a}{e} \varphi(e) = \sum \frac{\partial}{\partial} \varphi(e) = \sum \frac{a}{e} \varphi(e) = \nu;$$

en conseqüència,

$$F_n(\sigma, v) = \sigma^\nu + V_1\sigma^{\nu-1} + V_2\sigma^{\nu-2} + \cdots + V_\nu$$

també és una funció entera de grau ν -èsim de v i, per exemple,

$$-V_1 = \sum v_n = \frac{1}{m^{n-1}}v^n + \cdots$$

és una funció entera de grau n -èsim de v . Per tant, les ν funcions v_n són funcions algebraïques de v , a saber, les arrels de l'equació

$$F_n(v_n, v) = 0.$$

Aquesta equació de valència és irreductible. A saber, si la funció $v'_n = \text{val}(n\omega)$ satisfà una equació de la forma

$$G(v'_n, v) = 0,$$

on $G(\sigma, v)$ denota una funció racional entera de les dues quantitats σ, v , aleshores és idènticament

$$G(\text{val}(n\omega), \text{val}(\omega)) = 0,$$

si els quatre nombres enters $\alpha, \beta, \gamma, \delta$ satisfan la condició $\alpha\delta - \beta\gamma = 1$, en conseqüència, també

$$G\left(\text{val}\left(\frac{n\gamma + n\delta\omega}{\alpha + \beta\omega}\right), \text{val}(\omega)\right) = 0;$$

resta demostrar ara, com es farà tot seguit, que la funció

$$\text{val}\left(\frac{n\gamma + n\delta\omega}{\alpha + \beta\omega}\right),$$

mitjançant l'elecció escaient dels quatre nombres α , β , γ , δ , es pot fer coincidir amb cadascuna de les ν funcions

$$v_n = \text{val} \left(\frac{c + \partial\omega}{a} \right),$$

de manera que cada funció v_n satisfaci l'equació $G(v_n, v) = 0$, en conseqüència $G(\sigma, v)$ és divisible per $F_n(\sigma, v)$, d'on se segueix la irreductibilitat d'aquesta darrera funció. Per tant, només resta per demostrar que donats tres nombres a , c , ∂ sense divisor comú que satisfacin la condició $a\partial = n$, sempre es poden escollir vuit nombres enters α , β , γ , δ , α' , β' , γ' , δ' , tals que se satisfaci $\alpha\delta - \beta\gamma = \alpha'\delta' - \beta'\gamma' = 1$ i

$$\begin{pmatrix} 1, & 0 \\ 0, & n \end{pmatrix} \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix} = \begin{pmatrix} \alpha', & \beta' \\ \gamma', & \delta' \end{pmatrix} \begin{pmatrix} a, & 0 \\ c, & \partial \end{pmatrix}.$$

La manera més general de trobar nombres com aquests és la següent (cf. la reducció duta a terme a l'inici d'aquest paràgraf). Si s'escull per a δ un nombre qualsevol que sigui relativament primer amb ∂ i es posa

$$\delta' = a\delta,$$

aleshores es pot escollir γ de manera que el nombre

$$\gamma' = \partial\gamma - c\delta$$

esdevingui relativament primer amb δ' ; car s'esculli com es vulgui γ , aleshores γ' en qualsevol cas no és divisible per aquells nombres primers que apareixen a la vegada en a i en δ , per tant, en e , perquè a , c , ∂ no tenen cap divisor comú i perquè δ és relativament primer amb ∂ ; si a més es designa per p el producte de tots els altres nombres primers que apareixen en a (o bé la unitat en el cas que no se'n tingui

a l'abast), aleshores ∂ és un nombre relativament primer amb p , per tant, també amb $p\delta$, se segueix que γ' recorre al mateix temps que γ un sistema complet de residus (mod $p\delta$); en conseqüència, existeix una infinitat de valors de γ per als quals γ' esdevé relativament primer amb $p\delta$, i se segueix que també amb $\delta' = a\delta$. Havent escollit δ , γ de manera que δ' , γ' siguin nombres relativament primers, si s'escull una solució qualsevol α' , β' de l'equació

$$\alpha'\delta' - \beta'\gamma' = 1,$$

i es posa

$$\alpha = a\alpha' + c\beta', \quad \beta = \partial\beta',$$

aleshores, és

$$\alpha\delta - \beta\gamma = (a\alpha' + c\beta')\delta - \partial\beta'\gamma = \alpha'\delta' - \beta'\gamma' = 1,$$

i els vuit nombres trobats satisfan les exigències anteriors, perquè

$$n\gamma = a\gamma' + c\delta', \quad n\delta = \partial\delta'.$$

La funció $F_n(\sigma, v)$ és simètrica respecte de σ i v , quan $n > 1$. Ja que de la identitat

$$F_n(\text{val}(n\omega), \text{val}(\omega)) = 0$$

se segueix l'equació

$$F_n\left(v, \text{val}\left(\frac{\omega}{n}\right)\right) = 0,$$

quan ω se substitueix per $\frac{\omega}{n}$; i, atès que $\text{val}(\frac{\omega}{n})$ és una de les ν funcions v_n , aleshores s'obté, a partir de la irreductibilitat tot just demostrada, que $F_n(v, \sigma)$ és divisible per $F_n(\sigma, v)$, i

en conseqüència cal que sigui $= \pm F_n(\sigma, v)$; atès, però, que en el cas del signe inferior la funció irreductible $F_n(\sigma, v)$ contindria el factor $(\sigma - v)$, quan $n > 1$, ha de valer el signe superior.

Atès que totes les funcions v_n constitueixen només casos especials de la funció designada per v' en l'equació (11) del §5, l'equació diferencial (12) d'allí mateix posseeix infinites solucions particulars $v' = v_n$, les quals són funcions algebraïques de v . També es pot demostrar que aquesta equació diferencial no pot posseir cap altra solució algebraica i, tal com crec, a partir d'aquí es pot deduir el teorema que tots els coeficients de la funció $F_n(\sigma, v)$ són nombres *racionals*. Remarco finalment que mitjançant la investigació de la funció entera $F_n(v, v)$, o també del discriminant de la funció $F_n(\sigma, v)$, s'arriba a la teoria dels mòduls singulars, per als quals té lloc la multiplicació complexa de les funcions el·líptiques; però m'he de reservar per a una altra oportunitat una explicació més acurada d'aquesta investigació, en la qual la composició de formes quadràtiques hi juga un paper essencial.

Brunsvic, 12 de juny de 1877

Referències de l'article

Recollim totes juntes les referències citades en aquest article.

Dirichlet, L.: *Vorlesungen über Zahlentheorie* Herausgegeben und mit Zusätzen versehen von R. Dedekind. Zweite Auflage, Brunsvic, 1871.

Fuchs, L.: Sur quelques propriétés des intégrales des équations différentielles, auxquelles satisfont les modules de périodicité des intégrales elliptiques des deux premières espèces. Extrait d'une lettre adressée à M. Hermite. *J. reine u. angew. Math.*, **83** (1877), p. 13–37.

Gauss, C. F.: Nachlass: Fortsetzung der Untersuchungen über das arithmetisch-geometrische Mittel. Art. 12–26. *Werke. Dritter Band.* Herausgegeben von der Königlichen Gesellschaft der Wissenschaften zu Göttingen, 1866, p. 375–403.

Hermite, C.: *Sur la théorie des équations modulaires et la résolution de l'équation du cinquième degré.* Mallet-Bachelier, Paris, 1859.

Jacobi, C. G. J.: *Fundamenta nova theoria functionum ellipticarum.* Regiomonti, sumtibus fratrum Bornträger, Königsberg, 1829. Reproduit a *Gesammelte Werke*, **1**, Chelsea, reimpressió (1969), p. 49–239.

Riemann, B.: Über die Anzahl der Primzahlen unter einer gegebenen Grösse. *Monatsberichte der Berliner Akademie* (November, 1859), p. 145–153.

Riemann, B.: Verbreitung der Wärme im Ellipsoid. Nachlass, Cap. XXV de *Gesammelte mathematische Werke und wissenschaftlicher Nachlass.* Herausgegeben unter Mitwirkung von Richard Dedekind von Heinrich Weber. Teubner, Leipzig, 1876, p. 437–439.

Riemann, B.: Beispiele von Flächen kleinsten Inhalts bei gegebener Begrenzung. Nachlass, Cap. XXVII de *Gesammelte mathematische Werke und wissenschaftlicher Nachlass*. Herausgegeben unter Mitwirkung von Richard Dedekind von Heinrich Weber. Teubner, Leipzig, 1876, p. 445–454.

Capítol 9

Fuchs

Per inversió d'integrals de funcions algebraiques, Jacobi i Abel havien arribat a la descoberta de les funcions abelianes. En el treball de Fuchs que hem seleccionat, l'autor es proposà estendre la inversió d'integrals de funcions més generals que les algebraiques amb la finalitat d'obtenir funcions més generals que les abelianes.

9.1 1880: El problema de la inversió d'integrals

Si $\{f_1(z), \dots, f_n(z)\}$ denota un sistema fonamental de solucions d'una equació diferencial d'ordre n , Fuchs considera d'entrada les funcions $z_i(u_j)$ que resulten per inversió de

les integrals

$$\sum_{i=1}^n \int_{\zeta_i}^{z_i} f_j(z) dz = u_j, \quad 1 \leq j \leq n.$$

Però, a l'article, Fuchs es limita a la consideració del cas en què l'equació diferencial és de segon ordre ($n = 2$),

$$\frac{d^2 y}{dz^2} + P \frac{dy}{dz} + Qy = 0,$$

de coeficients P , Q , funcions racionals, i està subjecta a les restriccions que segueixen:

- 1) Les singularitats de l'equació diferencial han d'ésser punts singulars regulars; és a dir, considera una equació diferencial del tipus que més endavant seria anomenat *fuchsian*.
- 2) Les arrels de les equacions determinadores en els punts singulars de l'equació diferencial són nombres racionals.
- 3) Les solucions de l'equació diferencial a l'entorn de cada punt singular no depenen de logaritmes.
- 4) Les singularitats de les funcions $z_1 = F_1(u_1, u_2)$ i $z_2 = F_2(u_1, u_2)$ que resulten de la inversió de les integrals es troben en valors finits dels arguments u_i .

Fuchs està especialment interessat a garantir que les funcions F_i siguin meromorfs. Sota les condicions anteriors, demostra que la quantitat de punts singulars finits de l'equació diferencial de partida pot ésser, com a màxim,

igual a 6. Atès que, en general, les equacions diferencials que satisfan les condicions anteriors no posseeixen integrals algebraïques, Fuchs està en condicions d'afirmar que les funcions a les quals arriba per inversió de les integrals corresponents no són abelianes. En notes posteriors, Fuchs donaria una taula amb els tipus d'integrals que satisfan aquestes condicions.

Per a portar a terme el seu estudi, Fuchs exigeix certes condicions auxiliars per a una funció $z(\zeta)$ que resulta d'invertir el quocient de dues solucions fonamentals de l'equació diferencial de partida,

$$\zeta(z) = \frac{f_1(z)}{f_2(z)}.$$

Observem que si γ és un camí tancat al voltant d'un punt singular i de base en un punt z_0 , aleshores en continuar analíticament les solucions al llarg de γ i tornar al punt inicial, hauran d'existir constants a_i , b_i tals que

$$\frac{f_1(z_0)}{f_2(z_0)} = \frac{a_1 f_1(z_0) + a_2 f_2(z_0)}{b_1 f_1(z_0) + b_2 f_2(z_0)}.$$

En conseqüència, per a la funció inversa $z(\zeta)$ se satisfarà la igualtat

$$z_0(f_1/f_2) = z_0 \left(\frac{a_1 f_1/f_2 + a_2}{b_1 f_1/f_2 + b_2} \right).$$

La importància històrica d'aquest treball de Fuchs rau precisament en la consideració de la funció $z(\zeta)$. Una anàlisi de les seves propietats portà a un jove Poincaré a qüestionar algunes de les afirmacions que es fan en el treball

de Fuchs. El mes de maig de 1880, el mateix any de la publicació del treball, Poincaré escriví una carta a Fuchs en què, molt educadament, li feia veure que algunes de les conclusions del seu treball no podien ésser certes, atès que conduïen a afirmacions contradictòries sobre propietats de racionalitat de la funció $z(\zeta)$.

Poincaré escrivia a Fuchs en francès i aquest li responia en alemany, també amb una educació exquisida. Segons la primera carta de resposta de Fuchs, les crítiques de Poincaré havien d'ésser aclarides si llegia una nota seva en què es precisaven més els resultats i que havia estat publicada el febrer d'aquell mateix any a *Notícies de la Societat de Ciències de Göttingen* (*Nachrichten der Gesellschaft der Wissenschaften zu Göttingen*). Sembla, però, que ni aquesta ni cap de les consideracions posteriors de Fuchs deixaren Poincaré completament satisfet.

Un estudi més aprofundit dels treballs de Fuchs conduí Poincaré a la seva descoberta particular de les funcions meromorfes del pla que són invariants respecte de subgrups discrets del grup especial lineal $SL(2, \mathbb{R})$ —un exemple de les quals era la funció $z(\zeta)$. En honor de Fuchs, que les havia considerat primer, Poincaré designà les funcions, que ell cregué noves, amb el nom de *funcions fuchsianes*.

El nom disgustà enormement Klein, per la senzilla raó que tant ell, com abans Riemann, Schwarz i Dedekind, ja havien considerat funcions de variable complexa amb propietats d'invariància respecte de subgrups discrets de moviments del pla hiperbòlic. La controvèrsia fou llarga, i d'ella se'n conserva un bon testimoni en la correspondència entre Klein i Poincaré. Aquesta fou iniciada per Klein el dia 12 de juny de 1881, després que Poincaré hagués publicat les

seves tres primeres notes sobre el tema a *Comptes rendus*, amb el títol *Sobre les funcions fuchsianes* (*Sur les fonctions fuchsiennes*).

En la segona de les seves cartes, datada el dia 19 de juny de 1881, Klein explicà a Poincaré que un treball previ de Fuchs de 1877 —i que el mateix Fuchs havia explicat en una carta a Hermite— contenia un error fonamental sobre les funcions modulars el·líptiques, i que aquest error havia estat esmenat per Dedekind en el treball [69] de 1877. Notem que Hermite havia estat el mestre de Poincaré i que d'aquest treball de Dedekind n'hem presentat una traducció en el capítol anterior.

En la carta a Klein de 27 de juny de 1881, Poincaré arribà a reconèixer que, si hagués conegut prèviament els treballs de Schwarz, probablement hauria emprat una denominació diferent per a les funcions que havia anomenat *fuchsianes*, però que ja era massa tard per a rectificar. Molt més endavant, quan rondava la cinquantena, Poincaré utilitzà l'episodi de les funcions fuchsianes per a fer palès el paper del subconscient en la gènesi dels processos creatius (cf. [303], [15]).

En honor també de Fuchs, Poincaré anomenà fuchsians els grups discrets d'isometries del pla hiperbòlic, nom que s'ha mantingut fins als nostres dies. En canvi, per recomanació de Klein, que proposà llevar del nom qualsevol referència personal, les funcions fuchsianes es coneixen avui amb la denominació de funcions automorfes.

Tant les cartes entre Fuchs i Poincaré com les cartes entre Klein i Poincaré es troben reproduïdes en el volum XI de les obres de Poincaré (cf. [305]).

J. reine u. angew. Math. **89** (1880), 151–169

SOBRE UNA CLASSE DE FUNCIONS DE MÉS D'UNA VARIABLE QUE S'ORIGINEN PER LA INVERSIÓ D'INTEGRALS DE SOLUCIONS D'EQUACIONS DIFERENCIALS LINEALS DE COEFICIENTS RACIONALS

del Sr. L. FUCHS a Heidelberg

Així com les funcions de més d'una variable que s'anomenen funcions *abelianes* deuen el seu origen a les integrals de funcions algebraïques, en les quals, d'acord amb el procediment de JACOBI, el límit superior de p integrals d'una funció algebraica escaient s'interpreta com a funció de la suma d'aquestes integrals i de $p - 1$ altres sumes construïdes de manera similar, de la mateixa manera s'origina, com mostro en el treball següent, una nova classe de funcions de més d'una variable quan es parteix de la base de les integrals de les solucions d'equacions diferencials lineals de coeficients racionals.

En primer lloc, m'he plantejat la tasca d'investigar la natura de les solucions d'una equació diferencial lineal homogènia d'ordre m quan, per mitjà de les m igualtats

$$\sum_{i=1}^m \int_{\zeta_i}^{z_i} f_a(z) dz = u_a, \quad a = 1, 2, \dots, m,$$

on $\zeta_1, \zeta_2, \dots, \zeta_m$ són constants i $f_1(z), f_2(z), \dots, f_m(z)$ denota un sistema fonamental de solucions de l'equació di-

ferencial, les $z_1, z_2, \dots, z_m$ poden ésser definides com a funcions analítiques de $u_1, u_2, \dots, u_m$.

He portat a terme aquesta tasca per a equacions diferencials de segon ordre i, en el que segueix, em permeto comunicar els resultats als quals he arribat.

Per al tractament posterior de les funcions definides aquí, en particular, per a la seva representació analítica, ens remetrem a les relacions que he desenvolupat per a les integrals de les solucions de les equacions diferencials lineals, esteses entre cada dos punts singulars, i que es troben en el meu treball contingut en aquesta revista, volum 76, p. 177.

He presentat els resultats del treball que segueix el quatre del mes actual a la Reial Societat de les Ciències de Göttingen.

1

Se suposa que les integrals de l'equació diferencial

$$(A) \quad \frac{d^2y}{dz^2} + P \frac{dy}{dz} + Qy = 0,$$

en la qual els coeficients P, Q són funcions racionals de z , tenen la propietat que, per a cada punt singular a , multiplicades per una potència de $z - a$ no esdevenen ni nul·les ni infinites per a $z = a$ (vegeu el meu treball en el volum 66 d'aquesta revista, p. 146).

Si

$$y_1 = f(z), \quad y_2 = \varphi(z)$$

és un sistema fonamental d'integrals de l'equació (A), aleshores

$$w_1 = \int_{z_0}^z f(z)dz, \quad w_2 = \int_{z_0}^z \varphi(z)dz,$$

on z_0 denota un valor arbitrari, i una constant, que fixem ara com a c , són un sistema fonamental d'integrals de l'equació diferencial

$$(A') \quad \frac{d^3 w}{dz^3} + P \frac{d^2 w}{dz^2} + Q \frac{dw}{dz} = 0.$$

Si un canvi del camí d'integració transforma w_1, w_2 en w'_1, w'_2 , respectivament, aleshores és

$$(1) \quad \begin{cases} w'_1 = \alpha_{11}w_1 + \alpha_{12}w_2 + \beta_1 c, \\ w'_2 = \alpha_{21}w_1 + \alpha_{22}w_2 + \beta_2 c, \end{cases}$$

on $\alpha_{11}, \dots, \alpha_{22}, \beta_1, \beta_2$ denoten constants.

El mateix canvi del camí porta y_1, y_2 a y'_1, y'_2 , respectivament, on

$$(2) \quad \begin{cases} y'_1 = \alpha_{11}y_1 + \alpha_{12}y_2, \\ y'_2 = \alpha_{21}y_1 + \alpha_{22}y_2. \end{cases}$$

Definim des d'ara z_1, z_2 com a funcions de u_1, u_2 mitjançant les igualtats

$$(B) \quad \begin{cases} \int_{\zeta_1}^{z_1} f(z)dz + \int_{\zeta_2}^{z_2} f(z)dz = u_1, \\ \int_{\zeta_1}^{z_1} \varphi(z)dz + \int_{\zeta_2}^{z_2} \varphi(z)dz = u_2, \end{cases}$$

on ζ_1, ζ_2 són valors arbitraris però fixats diferents dels punts singulars de l'equació (A) i, al mateix temps, $f(\zeta_1), f(\zeta_2), \varphi(\zeta_1), \varphi(\zeta_2)$ tenen valors donats, i investiguem quines propietats han de tenir $f(z), \varphi(z)$ a fi que z_1, z_2 esdevinguin funcions analítiques determinades de les variables esmentades.

Ens imaginem coincidents arreu els camins d'integració que lliguen els mateixos valors de z en les dues igualtats.

Des de cadascun dels punts singulars $a_1, \dots, a_\rho$ de l'equació (A), sigui traçat un tall arbitrari que arribi fins a l'infinit. Sigi designat per q_i el tall que pertany a a_i . Els talls no s'han d'intersecar ni a si mateixos ni els uns amb els altres. Sigi designat per T' el pla de la variable complexa z així tallat. Si totes les integrals de (B) creuen el mateix tall q_i la mateixa quantitat de vegades i en la mateixa direcció, aleshores un canvi del camí d'integració transforma u_1 en $\alpha_{11}u_1 + \alpha_{12}u_2 + \beta_1c$, u_2 en $\alpha_{21}u_1 + \alpha_{22}u_2 + \beta_2c$, quan aquest canvi del camí correspon a aplicar a y_1, y_2 la substitució

$$S = \begin{pmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{pmatrix}.$$

Les quantitats β_1, β_2 tenen un valor determinat quan el canvi del camí d'integració és un de determinat. Siguin, des d'ara,

$$(C) \quad z_1 = F_1(u_1, u_2), \quad z_2 = F_2(u_1, u_2),$$

aleshores les funcions F_1, F_2 tenen la propietat que

$$(D) \quad \begin{cases} F_1(\alpha_{11}u_1 + \alpha_{12}u_2 + \beta_1c, \alpha_{21}u_1 + \alpha_{22}u_2 + \beta_2c) = F_1(u_1, u_2), \\ F_2(\alpha_{11}u_1 + \alpha_{12}u_2 + \beta_1c, \alpha_{21}u_1 + \alpha_{22}u_2 + \beta_2c) = F_2(u_1, u_2). \end{cases}$$

A més, en general, les funcions F_1 , F_2 prenen el mateix valor per a una infinitat de valors de u_1 , u_2 , tal com resulta del fet que es pot deixar invariant el camí d'integració de ζ_2 a z_2 o bé el de ζ_1 a z_1 mentre es varia l'altre camí d'integració.

2

Suposem des d'ara que l'equació (A) posseeix únicament punts singulars essencials, és a dir, que els coeficients d'aquesta únicament esdevenen infinits per a aquells punts en els quals la integral general o bé resulta discontinua o bé experimenta una ramificació. Siguin les arrels de l'equació fonamental determinadora associada a cadascun d'aquests punts singulars nombres reals i racionals i, a més, d'acord amb el meu article del volum 76 d'aquesta revista, p. 184, dos a dos diferents, negatius i de valor absolut més petit que 1.

En canvi, siguin les arrels de l'equació fonamental determinadora associada a $z = \infty$ nombres reals i racionals, dos a dos diferents, que sobrepassin la unitat positiva.

Llavors, en l'equació (B), les quantitats z_1 , z_2 , per a valors finits u_1 , u_2 , poden coincidir amb punts singulars de l'equació (A) o bé amb punts infinitament llunyans.

Les funcions z_1 , z_2 de les variables independents u_1 , u_2 , que són definides mitjançant les igualtats (B) satisfan les equacions diferencials

$$(E) \quad \begin{cases} \Delta \cdot dz_1 = \varphi(z_2)du_1 - f(z_2)du_2, \\ \Delta \cdot dz_2 = -\varphi(z_1)du_1 + f(z_1)du_2, \end{cases}$$

on

$$\Delta = \begin{vmatrix} f(z_1) & f(z_2) \\ \varphi(z_1) & \varphi(z_2) \end{vmatrix}.$$

Si en partir dels valors 0, 0, els u_1 , u_2 segueixen camins arbitraris independents l'un de l'altre, aleshores, segons els principis desenvolupats pels Srs. BRIOT i BOUQUET (cf. *Bulletin des Sciences mathématiques*, t. III, p. 265, i BRIOT, *Théorie des fonctions Abéliennes*, p. 79), en partir dels valors ζ_1 , ζ_2 , els z_1 , z_2 es prolonguen de manera contínua en les franges corresponents, i a l'entorn dels valors de u_1 , u_2 que van prenent són holomorfs fins que z_1 , z_2 o bé esdevenen infinit o bé assoleixen els valors per als quals $\frac{f(z_1)}{\Delta}$, $\frac{f(z_2)}{\Delta}$, $\frac{\varphi(z_1)}{\Delta}$, $\frac{\varphi(z_2)}{\Delta}$ no prenen a la vegada valors finits i determinats.

La darrera circumstància es podria presentar únicament si o bé z_1 , o bé z_2 , o bé les dues quantitats, s'apropen o bé a un punt singular de l'equació (A) o bé als punts de l'infinit, o també si les mateixes quantitats prenen valors que satisfan l'equació $\Delta = 0$.

3

A continuació, suposem que per a $u_1 = v_1$, $u_2 = v_2$, z_1 coincideix amb un punt singular a de l'equació (A), però z_2 amb un punt no singular b que es troba a la part finita, encara que, en canvi, $z_1 = a$, $z_2 = b$ no satisfacin l'equació

$$(F) \quad \frac{f(z_1)}{\varphi(z_1)} = \frac{f(z_2)}{\varphi(z_2)}.$$

Si posem

$$z_1 - a = w_1, \quad z_2 - b = w_2,$$

llavors, d'acord amb el meu article del volum 66 d'aquesta revista, p. 139, a l'entorn de a és

$$(1) \quad \begin{cases} f(z_1) = c_{11}w_1^{r_1} \cdot g_1(w_1) + c_{12}w_1^{r_2} \cdot g_2(w_1), \\ \varphi(z_1) = c_{21}w_1^{r_1} \cdot g_1(w_1) + c_{22}w_1^{r_2} \cdot g_2(w_1), \end{cases}$$

on r_1, r_2 són les arrels de l'equació fonamental determinada associada a a , $c_{11}, \dots, c_{22}$ són constants, $g_1(w_1)$, $g_2(w_1)$ són holomorfs a l'entorn de a , i $g_1(0)$, $g_2(0)$ són diferents de zero.

En canvi, a l'entorn de $z_2 = b$ es té que

$$(2) \quad \begin{cases} f(z_2) = \gamma_0 + \gamma_1 w_2 + \gamma_2 w_2^2 + \dots, \\ \varphi(z_2) = \gamma'_0 + \gamma'_1 w_2 + \gamma'_2 w_2^2 + \dots, \end{cases}$$

on γ_i, γ'_i són constants determinades.

Per tant, esdevé

$$(3) \quad \Delta = w_1^{r_1} \cdot G_1(w_1, w_2) + w_1^{r_2} \cdot G_2(w_1, w_2),$$

on G_1, G_2 denoten funcions holomorfs de w_1, w_2 a l'entorn de $0, 0$, respectivament.

Sigui $r_2 > r_1$.

Atès que $z_1 = a$, $z_2 = b$ no satisfan l'equació (F) , aleshores

$$G_1(0, 0) = g_1(0)[c_{11}\gamma'_0 - c_{21}\gamma_0]$$

ha d'ésser diferent de zero.

Segons això, $\Delta \cdot w_1^{-r_1}$ és finit i diferent de zero per a $w_1 = 0$, $w_2 = 0$.

Si ara, d'acord amb la secció precedent, és

$$r_1 = -\frac{k_1}{n}, \quad r_2 = -\frac{k_2}{n},$$

on k_1 , k_2 , n denoten nombres enters positius, els dos primers dels quals són menors que n , i es posa

$$w_1 = t^n,$$

aleshores, les equacions (E) es transformen en

$$(4) \quad \begin{cases} n \cdot t^{n-1} \cdot \Delta dt = \varphi(w_2 + b) du_1 - f(w_2 + b) du_2, \\ \Delta dw_2 = -[c_{21} t^{-k_1} \cdot g_1(t^n) + c_{22} t^{-k_2} \cdot g_2(t^n)] du_1 + \\ \quad + [c_{11} t^{-k_1} \cdot g_1(t^n) + c_{12} t^{-k_2} \cdot g_2(t^n)] du_2. \end{cases}$$

Si suposem, doncs, que

$$k_1 \geq n - 1,$$

és a dir, com que $k_1 < n$,

$$(5) \quad k_1 = n - 1,$$

aleshores, els valors de $\frac{\partial t}{\partial u_1}$, $\frac{\partial t}{\partial u_2}$, $\frac{\partial w_2}{\partial u_1}$, $\frac{\partial w_2}{\partial u_2}$, obtinguts mitjançant l'equació (4), són funcions holomorfes de t , w_2 a l'entorn de $t = 0$, $w_2 = 0$.

Doncs, z_1 i z_2 són funcions holomorfes de u_1 , u_2 a l'entorn dels valors $u_1 = v_1$, $u_2 = v_2$.

A partir d'ara podria succeir $z_1 = a_1$, $z_2 = a_2$ per a $u_1 = v_1$, $u_2 = v_2$, on a_1 i a_2 són punts singulars diferents de l'equació (A), encara que, no obstant això, $z_1 = a_1$, $z_2 = a_2$ no satisfacen l'equació (F).

Si r_{11} , r_{12} són les arrels de l'equació fonamental determinadora associada a a_1 , r_{21} , r_{22} les de l'associada a a_2 , aleshores posem, d'acord amb les dues seccions precedents,

$$(1) \quad \left\{ \begin{array}{l} r_{11} = -1 + \frac{1}{n_1}, \quad r_{12} = -1 + \frac{l_1}{n_1} \\ r_{21} = -1 + \frac{1}{n_2}, \quad r_{22} = -1 + \frac{l_2}{n_2} \\ l_1 > 1, \quad l_2 > 1. \end{array} \right\} \quad \begin{array}{l} l_1, l_2, n_1, n_2 \\ \text{nombres} \\ \text{enters positius,} \end{array}$$

Si es posa, de nou,

$$z_1 - a_1 = w_1, \quad z_2 - a_2 = w_2,$$

es té, com en l'equació (1) de la secció 3, que

$$(2) \quad \left\{ \begin{array}{l} f(z_1) = c_{11}w_1^{r_{11}}g_1(w_1) + c_{12}w_1^{r_{12}}g_2(w_1), \\ \varphi(z_1) = c_{21}w_1^{r_{11}}g_1(w_1) + c_{22}w_1^{r_{12}}g_2(w_1), \\ f(z_2) = e_{11}w_2^{r_{21}}h_1(w_2) + e_{12}w_2^{r_{22}}h_2(w_2), \\ \varphi(z_2) = e_{21}w_2^{r_{21}}h_1(w_2) + e_{22}w_2^{r_{22}}h_2(w_2), \end{array} \right.$$

on $c_{11}, \dots, c_{22}, e_{11}, \dots, e_{22}$ són constants, $g_1(w_1), g_2(w_1), h_1(w_2), h_2(w_2)$ són funcions holomorfes a l'entorn de $w_1 = 0$

i $w_2 = 0$, respectivament, que esdevenen diferents de zero, respectivament, per a $w_1 = 0$ i $w_2 = 0$. Ara, Δ adopta la forma

$$(3) \quad \left\{ \begin{aligned} \Delta = & w_1^{r_{11}} w_2^{r_{21}} G_{11}(w_1, w_2) + w_1^{r_{11}} w_2^{r_{22}} G_{12}(w_1, w_2) + \\ & + w_1^{r_{12}} w_2^{r_{21}} G_{21}(w_1, w_2) + w_1^{r_{12}} w_2^{r_{22}} G_{22}(w_1, w_2), \end{aligned} \right.$$

on les funcions $G_{ik}(w_1, w_2)$ són funcions holomorfes de w_1, w_2 a l'entorn de $w_1 = 0, w_2 = 0$.

Ara,

$$G_{11}(0, 0) = [c_{11}e_{21} - e_{11}c_{21}]g_1(0)h_1(0)$$

és diferent de zero, perquè, altrament, l'equació (F) hauria d'ésser satisfeta per $z_1 = a_1, z_2 = a_2$, la qual cosa contradiu la nostra suposició.

Segons això,

$$\Delta \cdot w_1^{-r_{11}} w_2^{-r_{21}}, \quad \text{per a } w_1 = 0, w_2 = 0,$$

és finit i diferent de zero.

Si se substitueix en les equacions (E)

$$z_1 - a_1 = t_1^{n_1}, \quad z_2 - a_2 = t_2^{n_2},$$

s'obté, segons això, que $\frac{\partial t_1}{\partial u_1}, \frac{\partial t_1}{\partial u_2}, \frac{\partial t_2}{\partial u_1}, \frac{\partial t_2}{\partial u_2}$, són funcions holomorfes de t_1, t_2 a l'entorn de $t_1 = 0, t_2 = 0$. Aleshores, t_1, t_2 , i, en conseqüència, també z_1, z_2 , són funcions holomorfes de u_1, u_2 , a l'entorn de $u_1 = v_1, u_2 = v_2$.

Suposem que l'equació fonamental determinadora per a l'equació (A) associada a $z = \infty$ té arrels ρ_1, ρ_2 . Siguin

$$\rho_1 = \frac{s_1}{n}, \quad \rho_2 = \frac{s_2}{n},$$

on n, s_1, s_2 són nombres enters positius i, tanmateix, $s_2 > s_1 > n$ (vegeu el n. 2).

Suposem, d'ara endavant, que

$$(4) \quad s_1 = n + 1.$$

Sota aquest supòsit, es demostra com en els casos d'aquesta secció i de la precedent que z_1, z_2 resten univaluades també a l'entorn d'aquells valors de u_1, u_2 per als quals $z_1 = \infty$ i z_2 coincideix amb un punt singular a de l'equació (A), o bé en un punt no singular a , només quan l'equació (F) no és satisfeta pel parell de valors $z_1 = \infty, z_2 = a$.

En resumir ara els resultats d'aquesta secció i de la precedent, s'obté el teorema:

Si per a cada punt singular de l'equació (A) les arrels r_1, r_2 de l'equació fonamental determinadora associada són de la forma

$$(G) \quad \begin{cases} r_1 = -1 + \frac{1}{n}, & (n \text{ i } l \text{ nombres} \\ r_2 = -1 + \frac{l}{n}, & \text{enters positius}), \\ l > 1, \end{cases}$$

mentre que les arrels ρ_1, ρ_2 de l'equació fonamental determinadora associada a $z = \infty$ són de la forma

$$(G') \quad \begin{cases} \rho_1 = 1 + \frac{1}{n}, \rho_2 = 1 + \frac{l}{n} & (n, l \text{ nombres enters positius}), \\ l > 1, \end{cases}$$

aleshores z_1, z_2 són funcions univaluades de les variables u_1, u_2 a l'entorn de tots aquells valors d'aquestes per als quals z_1, z_2 no coincideixen en aquells punts per als quals se satisfà l'equació (F).

5

Si $f(z), \varphi(z)$ són dues integrals qualssevol de l'equació (A), aleshores, a l'entorn d'un punt singular a , és

$$(1) \quad \begin{cases} f(z) = c_{11} \cdot (z - a)^{r_1} \cdot g_1(z) + c_{12} (z - a)^{r_2} \cdot g_2(z), \\ \varphi(z) = c_{21} \cdot (z - a)^{r_1} \cdot g_1(z) + c_{22} (z - a)^{r_2} \cdot g_2(z), \end{cases}$$

on r_1, r_2 són les arrels de l'equació fonamental determinadora associada a a , $r_2 > r_1$, $c_{11}, \dots, c_{22}$ són constants diferents de zero, $g_1(z), g_2(z)$, són funcions holomorfes en un entorn de $z = a$ i $g_1(a), g_2(a)$ són diferents de zero.

Se suposarà, al llarg del present treball, *que el desenvolupament d'una integral de l'equació (A) a l'entorn d'un punt singular o bé del punt de l'infinit no conté cap logaritme.*

Si posem

$$(H) \quad \zeta = \frac{f(z)}{\varphi(z)},$$

aleshores, per a $z = a$, és $\zeta = \frac{c_{11}}{c_{21}}$; per tant, finit i diferent de zero. De la mateixa manera, resulta que per a $z = \infty$, ζ és finit i diferent de zero.

A la igualtat (H) , z ha d'ésser definida com a funció de ζ .

Suposem que a un valor arbitrari ζ_0 de ζ li correspon un valor $z = z_0$. Si, en partir d'aquest parell de valors, la funció z es vol prolongar en el pla ζ , això es pot realitzar amb l'ajut de l'equació, satisfeta per z (vegeu la meua memòria del volum 66, p. 128),

$$(J) \quad \frac{dz}{d\zeta} = \frac{\varphi(z)^2}{F(z)},$$

on

$$F(z) = C \cdot e^{-\int P dz}.$$

La quantitat C té un valor determinat i constant quan $f(z)$, $\varphi(z)$ denoten solucions determinades de l'equació (A) .

Els valors de ζ per als quals z podria deixar d'ésser holomorfa són, a més de $\zeta = \infty$, aquells valors d'aquestes variables per als quals z esdevé un punt singular de l'equació (A) , o bé $z = \infty$.

A continuació, per a $\zeta = \zeta_1$, siguin $z = a$ un punt singular de l'equació (A) i r_1, r_2 , les arrels de l'equació fonamental determinadora associada a a que satisfacin l'equació (G) .

Ara, a l'entorn de a (vegeu la meua memòria del volum 66, p. 143), és

$$F(z) = (z - a)^{r_1 + r_2 - 1} \cdot \eta(z),$$

on $\eta(z)$ és holomorfa a l'entorn de a i diferent de zero per a $z = a$.

Si considerem primerament

$$(2) \quad r_2 = r_1 + 1,$$

aleshores se segueix immediatament a partir de l'equació (J), que z és holomorfa a l'entorn de $\zeta = \zeta_1$. Si, en canvi, l'equació (2) no se satisfà, aleshores se substitueix a l'equació (J)

$$z - a = t^n.$$

S'obté, aleshores, que

$$(3) \quad n \cdot \frac{dt}{d\zeta} = t^{2-l} \cdot \frac{\psi(t)}{\eta(t)},$$

on $\psi(t)$, $\eta(t)$ són holomorfes a l'entorn de $t = 0$ i el seu quocient no és ni nul ni infinit per a $t = 0$.

En aquest cas, sigui

$$(4) \quad l = 2.$$

Llavors, se segueix de l'equació (3) que t , i, en conseqüència, també z , és holomorfa a l'entorn de $\zeta = \zeta_1$.

A més, per a $\zeta = \zeta_1$, siguin $z = \infty$ i ρ_1, ρ_2 les arrels de l'equació fonamental determinant associada a $z = \infty$ que satisfan l'equació (G').

A l'entorn de $z = \infty$ és

$$(5) \quad \begin{cases} f(z) = \gamma_{11} \left(\frac{1}{z}\right)^{\rho_1} \cdot h_1\left(\frac{1}{z}\right) + \gamma_{12} \left(\frac{1}{z}\right)^{\rho_2} \cdot h_2\left(\frac{1}{z}\right), \\ \varphi(z) = \gamma_{21} \left(\frac{1}{z}\right)^{\rho_1} \cdot h_1\left(\frac{1}{z}\right) + \gamma_{22} \left(\frac{1}{z}\right)^{\rho_2} \cdot h_2\left(\frac{1}{z}\right), \\ F(z) = \left(\frac{1}{z}\right)^{\rho_1 + \rho_2 + 1} \cdot \eta_1\left(\frac{1}{z}\right), \end{cases}$$

on $h_1\left(\frac{1}{z}\right)$, $h_2\left(\frac{1}{z}\right)$, $\eta_1\left(\frac{1}{z}\right)$ són holomorfes a l'entorn de $z = \infty$ i per a $z = \infty$ són diferents de zero. Les constants γ_{11} , $\dots$, γ_{22} són també diferents de zero, perquè $f(z)$, $\varphi(z)$ són solucions arbitràries de l'equació (A).

Si, per la seva banda, és

$$(6) \quad \rho_2 = \rho_1 + 1,$$

aleshores se segueix immediatament de l'equació (J) que z és univaluada a l'entorn de $\zeta = \zeta_2$. En canvi, si l'equació (6) no és satisfeta, aleshores se substitueix en (J)

$$z = t^{-n}$$

i s'obté que

$$(7) \quad -n \cdot \frac{df}{d\zeta} = t^{2-l} \cdot \frac{\psi_1(t)}{\eta_1(t)},$$

on $\psi_1(t)$, $\eta_1(t)$ són holomorfes a l'entorn de $t = 0$, i diferents de zero per a $t = 0$.

En aquest cas, sigui, de nou,

$$(8) \quad l = 2.$$

Llavors t és univaluada i, en conseqüència, també z , a l'entorn de $\zeta = \zeta_2$.

Finalment, si, per a $\zeta = \infty$ és $z = b$, aleshores, d'acord amb l'observació feta al començament d'aquesta secció, b no és ni un dels punts singulars de l'equació (A) ni infinit. Però, per a $z = b$ és $\varphi(z) = 0$.

Si, a l'entorn de $z = b$, és

$$(9) \quad \begin{cases} f(z) = a_0 + a_1(z - b) + \cdots, \\ \varphi(z) = a'_1(z - b) + \cdots, \end{cases}$$

aleshores s'obté que

$$(10) \quad (z - b) \frac{[a'_1 + a'_2(z - b) + \cdots]}{a_0 + a_1(z - b) + \cdots} = \frac{1}{\zeta}.$$

Atès que ara $f(z)$ i $\varphi(z)$ no s'anul·len simultàniament, perquè b no és un punt singular de l'equació (A), se segueix que a_0 és diferent de zero. Però a'_1 tampoc no es pot anul·lar perquè, altrament, se seguiria de l'equació (A) que $\varphi(z)$ es idènticament nul·la. Segons això, la igualtat (10) adquireix la forma

$$(10^a) \quad \alpha_1(z - b) + \alpha_2(z - b)^2 + \cdots = \frac{1}{\zeta},$$

on $\alpha_1 = \frac{a'_1}{a_0}$ és finit i diferent de zero.

A partir d'aquesta igualtat, ara se segueix, de manera ben coneguda, que z és una funció holomorfa de $\frac{1}{\zeta}$ a l'entorn de $\zeta = \infty$.

Per tant, del que precedeix se segueix el teorema:

I. Si, per a cada punt singular, les quantitats r_1 , r_2 satisfan les condicions

$$(K) \quad \begin{cases} r_1 = -1 + \frac{1}{n} & \text{i o bé } r_2 = r_1 + 1 & \text{o bé } r_2 = -1 + \frac{2}{n} \\ \text{i per al punt infinitament llunyà} \\ \rho_1 = 1 + \frac{1}{n} & \text{i o bé } \rho_2 = \rho_1 + 1 & \text{o bé } \rho_2 = 1 + \frac{2}{n}, \end{cases}$$

aleshores la funció z de ζ definida mitjançant la igualtat (H) és meromorfa per a tots els valors de ζ .

Una conseqüència immediata d'aquest teorema és el corollari:

La funció $\frac{f(z)}{\varphi(z)}$ no pren el mateix valor per a valors diferents de z .

Suposem, d'ara endavant que, en el cas que se satisfaci la igualtat (2) o bé la igualtat (6), el denominador de r_1 , respectivament el denominador de ρ_1 , és igual a 2.

Llavors, la funció $F(z)$ també és una funció univaluada de ζ .

A saber, si $\zeta = \zeta'$ és un valor per al qual z no coincideix amb cap dels punts singulars de l'equació (A) o bé esdevé infinita, aleshores, per descomptat, $F(z)$ és univaluada a l'entorn de $\zeta = \zeta'$.

Si ara $\zeta = \zeta_1$ és un valor per al qual z coincideix amb un punt singular a , aleshores, d'acord amb el que s'ha dit, és

$$F(z) = (z - a)^{r_1 + r_2 - 1} \eta(z),$$

on $\eta(z)$ és holomorfa a l'entorn de $z = a$ i, per a $z = a$, diferent de zero.

Si ara se satisfà la igualtat (2), aleshores, d'acord amb la hipòtesi acabada de fer, és

$$r_1 + r_2 - 1 = 2r_1 = \text{un nombre enter};$$

per tant, $F(z)$, de la mateixa manera que z , és univaluada a l'entorn de $\zeta = \zeta_1$.

Si, en canvi, té lloc la igualtat (4), aleshores és

$$r_2 + r_1 - 1 = -3 + \frac{3}{n}.$$

Segons això, és

$$F(z) = t^{3-3n} \cdot \eta(a + t^n).$$

Segons el que hem dit més amunt, t , i, en conseqüència, també $F(z)$, és univaluada a l'entorn de $\zeta = \zeta_1$.

De la mateixa manera s'obté que $F(z)$ és univaluada a l'entorn d'un d'aquells valors de ζ per als quals z esdevé infinit.

Atès que hem demostrat més amunt que z és una funció univaluada de ζ , se segueix el mateix per a la derivada $\frac{dz}{d\zeta}$.

Atès que, de la mateixa manera, no sols $\frac{dz}{d\zeta}$, sinó també $F(z)$, és una funció univaluada de ζ , aleshores l'equació (J) proporciona que $\varphi(z)^2$ i, en conseqüència, també $f(z)^2$, són funcions univaluades de ζ .

S'obté doncs el teorema següent:

II. Si les condicions (K) satisfan la restricció que, en el cas que sigui $r_2 = r_1 + 1$ o bé $\rho_2 = \rho_1 + 1$, el denominador de r_1 , o bé de ρ_1 és el nombre dos, aleshores, les funcions $\varphi(z)^2$ i $f(z)^2$ també són funcions univaluades de ζ .

6

De la secció precedent s'obté que, quan en l'equació (B) les variables independents u_1, u_2 prenen respectivament aquells valors v_1, v_2 per als quals z_1, z_2 satisfan l'equació (F) , *necessàriament ha d'ésser* $z_1 = z_2$, tan bon punt se satisfacin les equacions (K) .

En conseqüència, per a $u_1 = v_1, u_2 = v_2$, es té que $z_1 = z_2 = b$.

Si aquí tenim en compte la hipòtesi del teorema II de la secció precedent, aleshores, a partir d'aquest teorema, s'obté que les igualtats

$$(1) \quad f(z_2) = \pm f(z_1), \quad \varphi(z_2) = \pm \varphi(z_1),$$

on els signes es corresponen, se satisfan simultàniament.

Ara, distingim tres casos:

1. Si b és un punt *no singular* de l'equació (A) i, a l'entorn de $z_1 = b$, és

$$(2) \quad \begin{cases} f(z_1) = a_0 + a_1(z_1 - b) + a_2(z_1 - b)^2 + \cdots, \\ \varphi(z_1) = c_0 + c_1(z_1 - b) + c_2(z_1 - b)^2 + \cdots, \end{cases}$$

aleshores, d'acord amb les igualtats (1), és

$$(2^a) \quad \begin{cases} \pm f(z_2) = a_0 + a_1(z_2 - b) + a_2(z_2 - b)^2 + \cdots = f'(z_2), \\ \pm \varphi(z_2) = c_0 + c_1(z_2 - b) + c_2(z_2 - b)^2 + \cdots = \varphi'(z_2), \end{cases}$$

on els signes es corresponen.

Per tant, les equacions (E) esdevenen

$$(E^a) \quad \begin{cases} \Delta' \cdot dz_1 = \varphi'(z_2) \cdot du_1 - f'(z_2) \cdot du_2, \\ \pm \Delta' \cdot dz_2 = -\varphi(z_1) \cdot du_1 + f(z_1) \cdot du_2, \end{cases}$$

$$\Delta' = \begin{vmatrix} f(z_1) & f'(z_2) \\ \varphi(z_1) & \varphi'(z_2) \end{vmatrix}.$$

Si posem

$$(3) \quad \begin{cases} (z_1 - b) \pm (z_2 - b) = w_1, \\ (z_1 - b)^2 \pm (z_2 - b)^2 = w_2, \end{cases}$$

on els signes es corresponen, aleshores, de les equacions

(E^a) se segueix que

$$(4) \quad \begin{cases} \Delta' \cdot dw_1 = [\varphi'(z_2) - \varphi(z_1)]du_1 - [f'(z_2) - f(z_1)]du_2, \\ \Delta' \cdot dw_2 = 2[(z_1 - b)\varphi'(z_2) - (z_2 - b)\varphi(z_1)]du_1 - \\ \quad - 2[(z_1 - b)f'(z_2) - (z_2 - b)f(z_1)]du_2. \end{cases}$$

Si substituïm els valors de les igualtats (2) i (2^a) en Δ' , aleshores s'obté que Δ' és divisible per $(z_2 - b) - (z_1 - b)$. Els

termes del quocient són funcions simètriques, homogènies i enteres de $z_1 - b$, $z_2 - b$, i el valor d'aquests quocients per a $z_1 = b$, $z_2 = b$ és $a_0 c_1 - a_1 c_0$, que no s'anul·la, atès que $f(z)$, $\varphi(z)$ constitueixen un sistema fonamental de solucions de l'equació (A).

Els coeficients de du_1 , du_2 en les equacions (4) són divisibles, igualment, per $(z_2 - b) - (z_1 - b)$ i els quocients són funcions simètriques, homogènies i enteres de $z_1 - b$, $z_2 - b$.

Segons això, a partir de les equacions (4) s'obtenen expressions per a $\frac{\partial w_1}{\partial u_1}$, $\frac{\partial w_1}{\partial u_2}$, $\frac{\partial w_2}{\partial u_1}$, $\frac{\partial w_2}{\partial u_2}$ que depenen racionalment de w_1 , w_2 i que per a $u_1 = v_1$, $u_2 = v_2$ no esdevenen infinites. Doncs, en l'entorn de $u_1 = v_1$, $u_2 = v_2$, les w_1 , w_2 són funcions univaluades de u_1 , u_2 .

Si, des d'ara, en les equacions (3) valen els signes inferiors, aleshores resulta també que $z_1 - b$ i $z_2 - b$ i, per tant, z_1 i z_2 , són funcions univaluades de u_1 , u_2 a l'entorn de $u_1 = v_1$, $u_2 = v_2$.

Però si en l'equació (3) valen els signes superiors, se segueix que $z_1 + z_2$ i $z_1 \cdot z_2$ representen funcions univaluades en el mateix entorn.

2. Sigui b un punt singular de l'equació (A), r_1 , r_2 les arrels de l'equació fonamental determinadora associada a aquesta, és a dir, en concordança amb els teoremes I, II de la secció precedent, sigui

$$(5) \quad \begin{cases} r_1 = -1 + \frac{1}{n}, & r_2 = -1 + \frac{2}{n} \text{ o bé } r_2 = r_1 + 1 \text{ amb} \\ \text{la condició que sigui } n = 2 \text{ per al darrer cas.} \end{cases}$$

Posem, a les equacions (E) ,

$$z_1 - b = t_1^n, \quad z_2 - b = t_2^n.$$

Llavors és

$$(6) \quad \begin{cases} f(z_1) &= t_1^{1-n} [c_{11}g_1(t_1^n) + c_{12}t_1^{\varepsilon n+1-\varepsilon}g_2(t_1^n)], \\ \varphi(z_1) &= t_1^{1-n} [c_{21}g_1(t_1^n) + c_{22}t_1^{\varepsilon n+1-\varepsilon}g_2(t_1^n)], \\ \pm f(z_2) &= t_2^{1-n} [c_{11}g_1(t_2^n) + c_{12}t_2^{\varepsilon n+1-\varepsilon}g_2(t_2^n)] = f'(z_2), \\ \pm \varphi(z_2) &= t_2^{1-n} [c_{21}g_1(t_2^n) + c_{22}t_2^{\varepsilon n+1-\varepsilon}g_2(t_2^n)] = \varphi'(z_2), \end{cases}$$

on $c_{11}, \dots, c_{22}$ són constants arbitràries, $g_1(t^n), g_2(t^n)$ funcions holomorfes de t^n a l'entorn de $t = 0$ i, per a $t = 0$, diferents de zero, i $\varepsilon = 0$ o bé 1, segons que sigui $r_2 = -1 + \frac{2}{n}$ o bé $r_2 = r_1 + 1$, és a dir, $r_1 = -\frac{1}{2}$, $r_2 = +\frac{1}{2}$. Si posem, de nou,

$$\Delta' = \begin{vmatrix} f(z_1) & f'(z_2) \\ \varphi(z_1) & \varphi'(z_2) \end{vmatrix},$$

de les igualtats (6) se segueix que

$$(6^a) \quad \begin{aligned} \Delta' &= (c_{11}c_{22} - c_{12}c_{21})t_1^{1-n}t_2^{1-n} \cdot \\ &\cdot [t_2^{\varepsilon n+1-\varepsilon}g_1(t_1^n)g_2(t_2^n) - t_1^{\varepsilon n+1-\varepsilon}g_2(t_1^n)g_1(t_2^n)]. \end{aligned}$$

L'expressió $\Delta \cdot t_1^{n-1} \cdot t_2^{n-1}$ és divisible per $t_2^2 - t_1^2$ o bé per $t_2 - t_1$, segons que [sigui] $\varepsilon = 1$ o bé $\varepsilon = 0$. El valor del quocient per a $t_1 = 0$, $t_2 = 0$ és

$$(c_{11}c_{22} - c_{12}c_{21})g_1(0) \cdot g_2(0),$$

que és diferent de zero, perquè $f(z)$ $\varphi(z)$ són un sistema fonamental de solucions de l'equació (A), i perquè $g_1(0)$, $g_2(0)$ no s'anul·len.

Si posem

$$\begin{aligned} f(z_1)t_1^{n-1} &= f_1(t_1), & \varphi(z_1)t_1^{n-1} &= \varphi_1(t_1), \\ f'(z_2)t_2^{n-1} &= f_1(t_2), & \varphi'(z_2)t_2^{n-1} &= \varphi_1(t_2), \end{aligned}$$

aleshores les equacions (E) esdevenen

$$(E^b) \quad \begin{cases} n \cdot \Delta' \cdot t_1^{n-1} \cdot t_2^{n-1} \cdot dt_1 = \varphi_1(t_2)du_1 - f_1(t_2)du_2, \\ \pm n \cdot \Delta' \cdot t_1^{n-1} \cdot t_2^{n-1} \cdot dt_2 = -\varphi_1(t_1)du_1 + f_1(t_1)du_2. \end{cases}$$

Si és a) $\varepsilon = 0$, aleshores, de la mà de l'equació (E^b), de manera anàloga que en el cas 1 per a $z_1 - b$, $z_2 - b$ de la mà de l'equació (E^a), resulta que les mateixes t_1 i t_2 o bé $t_1 + t_2$, $t_1 \cdot t_2$ i, d'acord amb això, també $z_1 + z_2$ i $z_1 \cdot z_2$ són funcions univaluades de u_1 , u_2 a l'entorn de $u_1 = v_1$, $u_2 = v_2$.

Sigui b) $\varepsilon = 1$.

Si posem, segons que en les equacions (E^b) valgui el signe superior o l'inferior,

$$t_1 \pm t_2 = w_1, \quad t_1^3 \pm t_2^3 = w_2,$$

aleshores se segueix de les equacions (E^b) que

$$(7) \quad \begin{cases} n \cdot \Delta' \cdot t_1^{n-1} \cdot t_2^{n-1} dw_1 = [\varphi_1(t_2) - \varphi_1(t_1)] du_1 - \\ \quad - [f_1(t_2) - f_1(t_1)] du_2, \\ n \cdot \Delta' \cdot t_1^{n-1} \cdot t_2^{n-1} dw_2 = 3[t_1^2 \varphi_1(t_2) - t_2^2 \varphi_1(t_1)] du_1 - \\ \quad - 3[t_1^2 f_1(t_2) - t_2^2 f_1(t_1)] du_2. \end{cases}$$

En aquestes equacions, els coeficients de du_1 , du_2 són divisibles per $t_2^2 - t_1^2$, i cadascun dels termes dels quocients són funcions de t_1^2 , t_2^2 simètriques, homogènies i racionals. A més, és

$$3t_1 t_2 = \pm \left(w_1^2 - \frac{w_2}{w_1} \right).$$

Per tant, $\frac{\partial w_1}{\partial u_1}$, $\frac{\partial w_1}{\partial u_2}$, $\frac{\partial w_2}{\partial u_1}$, $\frac{\partial w_2}{\partial u_2}$ són racionals en les expressions construïdes a partir de w_1 , w_2 , que no esdevenen infinites per a $u_1 = v_1$, $u_2 = v_2$, d'on resulta que w_1 , w_2 , i consegüentment també $z_1 + z_2$ i $z_1 \cdot z_2$ són funcions univaluades de u_1 , u_2 a l'entorn de $u_1 = v_1$, $u_2 = v_2$.

3. $b = \infty$. Siguin ρ_1 , ρ_2 les arrels de l'equació fonamental determinadora associada a $z = \infty$ i, d'acord amb els teoremes I, II de la secció precedent,

$$(5^a) \quad \rho_1 = 1 + \frac{1}{n}, \quad \rho_2 = 1 + \frac{2}{n}, \quad \text{o bé } \rho_1 = \frac{3}{2}, \quad \rho_2 = \frac{5}{2}.$$

Si, en l'equació (A), posem

$$\frac{1}{z} = \xi, \quad y = \xi^2 \cdot \eta,$$

aleshores

$$\frac{f(z)}{\xi^2} = f'(\xi),$$

$$\frac{\varphi(z)}{\xi^2} = \varphi'(\xi)$$

són un sistema fonamental d'integrals de l'equació diferencial entre η i ξ . Per a aquesta equació, $\xi = 0$ és un punt singular, i

(5^b)

$$\sigma_1 = -1 + \frac{1}{n}, \quad \sigma_2 = -1 + \frac{2}{n}, \quad \text{o bé} \quad \sigma_1 = -\frac{1}{2}, \quad \sigma_2 = +\frac{1}{2}$$

són les arrels de l'equació fonamental determinadora associada a $\xi = 0$.

Però de les equacions (B) , si es posa

$$\frac{1}{z_1} = \xi_1, \quad \frac{1}{z_2} = \xi_2,$$

se segueix que

$$(E') \quad \begin{cases} f'(\xi_1) \cdot d\xi_1 + f'(\xi_2) \cdot d\xi_2 = du_1, \\ \varphi'(\xi_1) \cdot d\xi_1 + \varphi'(\xi_2) \cdot d\xi_2 = du_2. \end{cases}$$

Ara, a partir d'aquestes equacions, resulta, com en el cas 2), que $\xi_1 + \xi_2$, $\xi_1 \cdot \xi_2$ són funcions holomorfes de u_1 , u_2 a l'entorn de $u_1 = v_1$, $u_2 = v_2$.

Per consegüent, $z_1 + z_2$, $z_1 \cdot z_2$ tenen la mateixa propietat.

Si es resumeix el que precedeix, aleshores en resulta el teorema següent:

Si r_1, r_2 són les arrels de cada equació fonamental determinada associada als diferents punts singulars de l'equació (A) de tal manera que

$$r_1 = -1 + \frac{1}{n}, \quad r_2 = -1 + \frac{2}{n}$$

o bé

$$r_1 = -\frac{1}{2}, \quad r_2 = +\frac{1}{2},$$

i per a les arrels ρ_1, ρ_2 de l'equació fonamental determinada associada a $z = \infty$ és o bé

$$\rho_1 = 1 + \frac{1}{n}, \quad \rho_2 = 1 + \frac{2}{n}$$

o bé

$$\rho_1 = \frac{3}{2}, \quad \rho_2 = \frac{5}{2},$$

aleshores les funcions $F_1(u_1, u_2), F_2(u_1, u_2)$ definides mitjançant les equacions (B) són arrels d'una equació quadràtica, els coeficients de la qual són funcions univaluades de u_1, u_2 .

7

D'acord amb la meua memòria, volum 66, p. 145 d'aquesta revista, és

$$(1) \quad \sum (r_1 + r_2) + \rho_1 + \rho_2 = A - 1,$$

si es denota per A el nombre de punts singulars de l'equació (A).

Si A' és el nombre de punts singulars per als quals les equacions fonamentals determinadores tenen les arrels $-\frac{1}{2}$,

$+\frac{1}{2}$, A'' el nombre dels que resten, aleshores l'equació (1) es transforma en

$$(2) \quad 3 \sum \frac{1}{n_i} + \rho_1 + \rho_2 = A' + 3A'' - 1,$$

on la suma s'estén als denominadors de les arrels d'aquelles equacions fonamentals que s'associen a punts singulars de segon tipus. Atès que

$$\begin{aligned} \rho_1 + \rho_2 &\leq 5, \\ 3 \sum \frac{1}{n_i} &\leq \frac{3A''}{2}, \end{aligned}$$

se segueix de la igualtat (2) que

$$(3) \quad \frac{3}{2}A'' + A' \leq 6 \quad \text{o bé} \quad A + \frac{1}{2}A' \leq 6.$$

D'aquí se segueix que:

El nombre de punts singulars de l'equació (A) no és més gran que sis.

8

El que segueix és un exemple per al cas $A = 6$.

Si per a cadascun dels sis punts singulars és

$$r_1 = -\frac{1}{2}, \quad r_2 = +\frac{1}{2},$$

aleshores, d'acord amb la meva memòria del volum 81, l'equació (A) és satisfeta per l'arrel quadrada d'una funció racional. Atès que, a més, els desenvolupaments vàlids a

l'entorn de cada punt singular o bé dels punts de l'infinit no poden contenir cap logaritme, existeix encara una altra segona arrel quadrada d'una funció racional que satisfà l'equació (A) i que, juntament amb la primera, constitueix un sistema fonamental.

Si es designen per $a_1, a_2, \dots, a_6$ els punts singulars i es posa

$$(z - a_1)(z - a_2) \cdots (z - a_6) = \varphi(z),$$

aleshores el sistema fonamental té la forma

$$y_1 = \frac{g(z)}{\sqrt{\varphi(z)}}, \quad y_2 = \frac{h(z)}{\sqrt{\varphi(z)}},$$

on $g(z), h(z)$ denoten funcions racionals enteres.

Atès que en el cas present

$$\rho_1 = 2, \quad \rho_2 = 3,$$

se segueix que $g(z), h(z)$ no sobrepassen el primer grau. Per tant, en els exemples presents, les funcions $F_1(u_1, u_2), F_2(u_1, u_2)$ proporcionen les funcions hiperel·líptiques de primer ordre.

9

Però, en general, resulta de l'exemple següent que les equacions diferencials (A) que hem caracteritzat aquí no posseeixen integrals algebraïques i que, en conseqüència, *les funcions $F_1(u_1, u_2), F_2(u_1, u_2)$ són diferents de les funcions abel·lianes.*

Siguin $A = 2$; a_1, a_2 els dos punts singulars de l'equació (A);

$$r_{11} = -\frac{2}{3}, \quad r_{12} = -\frac{1}{3},$$

les arrels de l'equació fonamental determinadora associada a a_1 ;

$$r_{21} = -\frac{5}{6}, \quad r_{22} = -\frac{4}{6},$$

les arrels de l'equació fonamental determinadora associada a a_2 ;

$$\rho_1 = \frac{3}{2}, \quad \rho_2 = 2$$

les arrels de l'equació fonamental determinadora associada a $z = \infty$. Si en aquest cas se substitueix en l'equació (A)

$$y = (z - a_1)^{-1} \cdot (z - a_2)^{-\frac{5}{4}} \cdot w,$$

aleshores les arrels de l'equació fonamental determinadora de l'equació diferencial per a w associada a a_1 , a a_2 , a ∞ són, respectivament,

$$\frac{1}{3}, \frac{2}{3}; \quad \frac{5}{12}, \frac{7}{12}; \quad -\frac{3}{4}, -\frac{1}{4},$$

per tant, l'equació per a w té la forma

$$(1) \quad \frac{d^2 w}{dz^2} = P \cdot w,$$

on P és una funció racional de z .

D'acord amb la meua memòria del volum 81 d'aquesta revista, p. 135, aquesta equació diferencial no és integrable de manera algebraica, atès que les arrels de l'equació fonamental determinadora associada a a_2 són més grans que deu, llevat que cadascuna de les seves pròpies integrals, o bé una funció homogènia de segon grau de les seves integrals, sigui igual a l'arrel d'una funció racional.

Atès que els denominadors de les arrels de l'equació fonamental determinadora associada als punts singulars a_1 ,

a_2 són diferents dels nombres 1, 2, 4, aleshores, segons la mateixa memòria, pàgina 136, resta només la possibilitat que l'equació (1) sigui completament integrable per mitjà de les arrels de funcions racionals.

Però això no té lloc.

Perquè cada arrel w d'una funció racional de z que satisfés l'equació (1) hauria de tenir la forma

$$w = \psi(z) \cdot (z - a_1)^{\alpha_1} \cdot (z - a_2)^{\alpha_2},$$

on $\psi(z)$ és una funció racional entera de z que, per a $z = a_1$ i per a $z = a_2$ és diferent de zero, i on a més α_1 tindria un dels valors $\frac{1}{3}, \frac{2}{3}$; i α_2 un dels valors $\frac{5}{12}, \frac{7}{12}$. El grau μ de $\psi(z)$ hauria de satisfer la condició

$$\mu + \alpha_1 + \alpha_2 = \frac{3}{4} \text{ o bé } \frac{1}{4}.$$

Però únicament la funció

$$w = (z - a_1)^{\frac{1}{3}} \cdot (z - a_2)^{\frac{5}{12}},$$

i no cap altra arrel d'una funció racional, satisfà aquests requeriments.

D'acord amb això, l'equació (1) no és integrable completament mitjançant funcions algebraïques, per tant, *tampoc* l'equació (A).

Per a acabar, adjuntem encara la remarca següent:

Si, com en l'equació (H), posem

$$(1) \quad \frac{f(z)}{\varphi(z)} = v,$$

aleshores, segons la secció 5, teorema I, z és una funció univaluada de v . Però, també, segons el teorema II de la mateixa secció, $f(z)^2$ i $\varphi(z)^2$ són funcions univaluades de v .

Per tant, si

$$(2) \quad z = \chi(v),$$

en resulta el teorema següent:

Mitjançant les substitucions univaluades i en general no racionals

$$z_1 = \chi(v_1), \quad z_2 = \chi(v_2)$$

les equacions (B) es poden transformar en la forma

$$(L) \quad \begin{cases} \int_{\eta_1}^{v_1} \sqrt{g(v)} dv + \int_{\eta_2}^{v_2} \sqrt{g(v)} dv = u_1, \\ \int_{\eta_1}^{v_1} v \sqrt{g(v)} dv + \int_{\eta_2}^{v_2} v \sqrt{g(v)} dv = u_2, \end{cases}$$

on

$$\zeta_1 = \chi(\eta_1), \quad \zeta_2 = \chi(\eta_2)$$

i $g(v)$ és una funció de v univaluada i, en general, no racional.

Heidelberg, 14 de febrer de 1880

Referències de l'article

Recollim totes juntes les referències citades en aquest article.

Bouquet, J.: Sur l'intégration d'un système d'équations différentielles totales simultanées du premier ordre. *Bulletin des sciences mathématiques et astronomiques*, **3** (1872), p. 265–274.

Briot, M. C.: *Théorie des fonctions Abéliennes*. Paris, Gauthier Villars, 1879.

Fuchs, L.: Zur Theorie der linearen Differentialgleichungen mit veränderlichen Coefficienten. *J. reine u. angew. Math.*, **66** (1866), p. 121–160.

Fuchs, L.: Über Relationen, welche für die zwischen je zwei singulären Punkten erstreckten Integrale der Lösungen linearer Differentialgleichungen stattfinden. *J. reine u. angew. Math.*, **76** (1873), p. 177–213.

Fuchs, L.: Über die linearen Differentialgleichungen zweiter Ordnung, welche algebraische Integrale besitzen, und eine neue Anwendung der Invariantentheorie. *J. reine u. angew. Math.*, **81** (1876), p. 97–142.

Capítol 10

Frobenius

El treball del qual presentem una traducció, *Sobre els factors constants de les sèries theta* (*Über die constanten Factoren der Thetareihen*), fou publicat l'any 1885 a la *Revista de Crelle*. És el vuitè treball que l'autor publicà sobre funcions theta en el període 1880–1885.

10.1 1885: Constants theta jacobi-anes

L'origen d'aquest treball de Frobenius es remunta a la famosa fórmula del producte triple de Jacobi:

$$\theta'_{11}(0, \tau) = -\pi \theta_{00}(0, \tau) \theta_{01}(0, \tau) \theta_{10}(0, \tau)$$

que relaciona els valors de les tres funcions theta de Jacobi parelles amb la derivada de la funció theta de Jacobi senar. La generalització d'aquesta fórmula per a les funcions

theta en dimensió superior ha comportat un bon nombre de treballs que arriben als nostres dies ([213], [214]) i enllacen amb problemes actuals de la geometria algebraica. Més enllà de la seva pròpia bellesa, les identitats trobades han estat aplicades en els darrers anys en diversos camps de la geometria aritmètica. El treball de Frobenius recopila els avenços obtinguts des de l'aparició de la fórmula de Jacobi fins a l'any 1885, i hi incorpora noves extensions, així com també identitats noves entre constants theta (*Thetanullwerte*). Curiosament, després de la publicació del treball de Frobenius, les fórmules caigueren en l'oblit, fins que Weil les recuperà l'any 1976; d'aleshores ençà, han obtingut el protagonisme que mereixen.

La funció theta en dimensió 1 aparegué per primer cop l'any 1822, en el tractat de Fourier sobre la teoria de la calor [128], i es pot pensar com una generalització de la funció exponencial complexa. Jacobi n'inicià l'estudi sistemàtic en els *Fundamenta Nova* [217]. Göpel [166] i Rosenhain [329] introduïren la funció theta en dimensió 2 gairebé al mateix temps en què Weierstrass [393] i Riemann [320] ja estudiaven les funcions theta en dimensió qualsevol.

En dimensió g , la funció θ de mòdul una matriu $Z \in M(g, \mathbb{C})$ i argument un vector $u \in \mathbb{C}^g$ és definida per la sèrie

$$\theta(u, Z) := \sum_{m \in \mathbb{Z}^g} \exp(\pi i {}^t m Z m + 2\pi i {}^t m u).$$

Per tal que aquesta sèrie defineixi una funció holomorfa de $\mathbb{C}^g$, el mòdul Z no pot ésser qualsevol matriu, sinó que ha de satisfer les condicions de Riemann i Frobenius: ha d'ésser simètrica i de part imaginària definida positiva. El conjunt de les matrius complexes que satisfan aquestes con-

dicions s'anomena el semiplà superior de Siegel i es denota per $\mathcal{H}_g$.

Les propietats de quasiperiodicitat de la funció θ són ben conegudes i s'obtenen trivialment de les propietats de quasiperiodicitat del terme general que les defineix: per a qualsevol vector enter $n \in \mathbb{Z}^g$, és

$$(a) \quad \theta(u + n, Z) = \theta(u, Z),$$

$$(b) \quad \theta(u + Zn, Z) = \exp(-\pi i {}^t n Z n - 2\pi i {}^t n u) \theta(u, Z).$$

A més, la funció theta satisfà les equacions en derivades parcials

$$\frac{\partial^2 \theta(u, Z)}{\partial u_j \partial u_k} = 2^{1+\delta_{jk}} \frac{\partial \theta(u, Z)}{\partial Z_{jk}}, \quad j, k = 1, \dots, g,$$

conegudes genèricament com a *equació de la calor*.

Intrínsecament associades a la funció theta, les funcions theta amb característiques en són traslladades per vectors reals: donats $a, b \in \mathbb{R}^g$ es defineix la funció theta amb característica $\begin{bmatrix} a \\ b \end{bmatrix}$ per

$$\theta \begin{bmatrix} a \\ b \end{bmatrix} (u, Z) := \exp(\pi i {}^t a Z a + 2\pi i {}^t a (z + b)) \theta(u + Z a + b, Z).$$

Aquestes funcions tenen propietats anàlogues a les de la funció theta. Són especialment importants les funcions theta amb *thetacaracterístiques*, que són les característiques $a, b \in \{0, \frac{1}{2}\}^g$. És fàcil veure que les funcions theta corresponents són funcions parelles o senars segons la paritat del producte escalar $4a \cdot b$ format amb les característiques.

Els valors a l'origen, $\theta \begin{bmatrix} a \\ b \end{bmatrix} (0, Z)$, de les funcions theta, coneguts també com a *Thetanullwerte* o, en català, com a constants theta, se solen denotar per $\theta \begin{bmatrix} a \\ b \end{bmatrix} (Z)$ o, fins i tot, per $\theta \begin{bmatrix} a \\ b \end{bmatrix}$ quan el mòdul Z se sobreentén. Interpretats com a funcions del mòdul Z , també són funcions holomorfes en $\mathcal{H}_g$ i donen lloc a formes modulars de Siegel. Com a tals, s'utilitzen per a parametritzar les varietats abelianes complexes i intervenen en els problemes de moduli corresponents.

Les thetacaracterístiques senars donen lloc a constants theta idènticament nul·les; per a elles es consideren els gradients en el zero, que se solen tractar en bloc: donades g thetacaracterístiques senars $m_1, \dots, m_g$, es defineix la seva constant theta jacobiana (*Nullwerte jacobii*) com el determinant

$$[m_1, \dots, m_g](Z) := \pi^g \begin{vmatrix} \frac{\partial \theta[m_1]}{\partial z_1}(0; Z) & \dots & \frac{\partial \theta[m_1]}{\partial z_g}(0; Z) \\ \vdots & & \vdots \\ \frac{\partial \theta[m_g]}{\partial z_1}(0; Z) & \dots & \frac{\partial \theta[m_g]}{\partial z_g}(0; Z) \end{vmatrix}.$$

Les constants theta i les constants theta jacobianes són els ingredients que apareixen en les generalitzacions de la fórmula de Jacobi. En dimensió 1, tenim tres thetacaracterístiques parelles i una de senar, així que en la fórmula de Jacobi es relacionen totes les possibles constants theta. En dimensió superior, però, tenim moltes més possibilitats, i no totes les possibles eleccions porten a identitats. Cal restringir, doncs, la tria de les thetacaracterístiques.

En dimensió 2, la situació encara és força controlable, ja que la relació entre les thetacaracterístiques senars i les parelles és ben explícita, i encara més si tenim en compte que els mòduls Z irreductibles corresponen a matrius de períodes de corbes hiperelíptiques de gènere 2. La versió de la fórmula de Jacobi en aquest cas és donada pel resultat de Rosenhain [329] següent.

Teorema. *Donades $Z \in \mathcal{H}_2$ i dues thetacaracterístiques senars m_1, m_2 , se satisfà que*

$$[m_1, m_2](Z) = \pm \pi^2 \prod_{\substack{m \text{ senar,} \\ m \neq m_1, m_2}} \theta[m_1 + m_2 - m](Z),$$

on el signe no depèn de Z .

Aquest resultat és la fórmula (7) de la secció 2 del treball de Frobenius. En els darrers anys, s'ha aplicat en teoria d'Arakelov (cf. [43]) i en la resolució d'equacions algebraïques (cf. [177]).

Per a les funcions theta de dimensió 3 o superior, la situació és força més difícil perquè, d'entrada, no totes les matrius $Z \in \mathcal{H}_g$ provenen de períodes de corbes (si $g > 3$) i les que s'obtenen com a períodes de corbes no tenen perquè fer-ho de corbes hiperelíptiques. A més, el nombre de thetacaracterístiques creix molt i les relacions entre elles són molt més complicades.

Donades tres thetacaracterístiques m_1, m_2, m_3 , es defineix $e(m_1, m_2, m_3) := e(m_1)e(m_2)e(m_3)e(m_1 + m_2 + m_3)$, on $e(m)$ és 1 si m és parella i -1 si m és senar. La tripleta $\{m_1, m_2, m_3\}$ s'anomena *sizigètica* si $e(m_1, m_2, m_3) = 1$, i *asizigètica* en cas contrari. Una família de thetacaracterístiques $\{m_1, \dots, m_r\}$ és asizigètica si cada subtripleta ho és.

Un *sistema fonamental especial* de thetacaracterístiques és una família asizigètica de $2g + 2$ thetacaracterístiques, on les g primeres són senars i les $g + 2$ darreres, parelles. Les generalitzacions de la fórmula de Jacobi involucren aquests sistemes.

El pas següent en la generalització de la fórmula de Jacobi el donà Thomae, que, a l'article [382], del qual oferim una traducció i un comentari en el capítol 7, estengué el resultat de Rosenhain a les matrius de períodes que provenen de corbes hiperel·líptiques. El resultat de Thomae apareix com a fórmula (4) de la secció 3 del treball de Frobenius. Donada una matriu $Z \in \mathcal{H}_g$ hiperel·líptica, és a dir, Z és la matriu de períodes normalitzada d'una corba hiperel·líptica, i donat un sistema fonamental especial de thetacaracterístiques $\{m_1, \dots, m_{2g+2}\}$, se satisfà la identitat:

$$[m_1, \dots, m_g](Z) = \pm \pi^g \prod_{j=g+1}^{2g+2} \theta[m_j](Z),$$

on, novament, el signe no depèn de Z . El treball de Thomae esgota els casos *senzills*, perquè els casos no hiperel·líptics es compliquen molt, fins i tot en dimensió 3. Frobenius fou capaç de trobar una bona generalització en dimensió 3, sota una certa restricció, que amb el pas del temps es revelaria imprescindible. El resultat de Frobenius és la fórmula (2) de la secció 4 del seu treball, i resa així.

Teorema. *Donada $Z \in \mathcal{H}_3$ i fixat un sistema fonamental especial de thetacaracterístiques $\{m_1, \dots, m_8\}$ tal que la suma $m_1 + m_2 + m_3$ sigui una thetacaracterística senar, es*

té que

$$[m_1, m_2, m_3](Z) = \pm \pi^3 \prod_{j=4}^8 \theta[m_j](Z),$$

on el signe és independent de Z .

Les demostracions que donà Frobenius dels tres resultats esmentats parteixen d'una fórmula de Prym que relaciona sumes de productes de funcions theta. En donar valors a alguns dels arguments i desenvolupar per Taylor, Frobenius obtingué els desenvolupaments corresponents a les constants theta jacobianes que apareixen a les fórmules.

En la darrera secció del treball, Frobenius considerà el cas de dimensió 4 i arribà a obtenir una fórmula per a les constants theta jacobianes de sistemes fonamentals especials de funcions theta que, sorprenentment, ja involucra una suma de productes de constants theta. Només un segle després es reeixiria a aclarir la situació.

La història primerenca de les generalitzacions de la fórmula de Jacobi tingué altres actors que hi jugaren un paper més difús. M. Noether [323, p. 66] i Krazer i Wirtinger [239, p. 722] atribuïren a manuscrits de Riemann fórmules anàlogues a la donada per Frobenius per a dimensions 3, 4, 5, 6 i 7. Aquestes fórmules serien molt anteriors al treball de Frobenius, però Riemann no les va publicar mai; només es troben citades en manuscrits no publicats de Riemann, i la història ens explica que potser Riemann tenia bones raons per a no fer-ho: l'any 1979, Fay [126] demostrà que no pot existir cap fórmula en aquesta línia per a dimensió 6.

L'atenció sobre les constants theta jacobianes decaigué al llarg del segle XX, i no es recuperà fins l'any 1976, en què Weil les situà al bell mig d'un problema de caire alge-

braic. Weil estudià els *anells de constants theta*, és a dir, les àlgebres $R[\theta]$ generades per les constants theta sobre un subanell R del cos dels nombres complexos. Weil plantejà dues qüestions bàsiques: són les constants theta jacobianes polinomis de coeficients enters en les constants theta? I en cas negatiu, són almenys quocients de polinomis d'aquest tipus? Igusa donà una resposta a les dues qüestions en [213], [214]. En el primer d'aquests treballs, se centrà en el cas de dimensió 3, prenent com a punt de partida el treball de Frobenius esmentat pel propi Weil. Igusa provà que la hipòtesi addicional de la fórmula de Frobenius és imprescindible: si la suma de les tres thetacaracterístiques senars d'un sistema fonamental no és senar, la constant theta jacobiana corresponent no és un polinomi en les constants theta! De fet, donà una caracterització en qualsevol dimensió de les constants theta jacobianes que no poden ser polinomis en les constants theta. En particular, provà que l'anell $\mathbb{C}[\theta]$ no és íntegrament tancat, i desmuntà així les conjectures formulades sobre això. En sentit afirmatiu, Igusa demostrà que qualsevol constant theta jacobiana és, llevat d'una potència de π , una fracció polinòmica racional de constants theta.

Fins als treballs d'Igusa, la construcció dels sistemes fonamentals de thetacaracterístiques es feia fixant les thetacaracterístiques senars i completant-les amb les parelles. Igusa [214] es plantejà també el procés a la inversa i d'aquesta manera arribà a una expressió del tipus

$$\sum_{[m_1, \dots, m_g]} [m_1, \dots, m_g](Z) = \pi^g \sum_{[m_{g+1}, \dots, m_{2g+2}]} \pm \prod_{j=g+1}^{2g+2} \theta[m_j](Z),$$

on els subíndexs dels sumatoris recorren certs conjunts de thetacaracterístiques senars i parelles respectivament, de

manera que, en combinar-los, s'obtenen sempre sistemes fonamentals. Aquesta fórmula engloba totes les versions precedents de la fórmula de Jacobi.

J. reine u. angew. Math. **98** (1885), 244–263

SOBRE ELS FACTORS CONSTANTS DE LES SÈRIES THETA

del Sr. G. FROBENIUS a Zuric

En els *Fundamenta Nova*, JACOBI defineix les funcions theta mitjançant productes infinits, dedueix d'aquesta representació les seves propietats de periodicitat i les desenvolupa amb el seu ajut en sèries infinites. Els coeficients d'aquestes que obté per aquest camí són determinats llevat d'un factor comú. Però la determinació d'aquest factor requereix un artífici especial. (*Determinatio ipsius A artificia particularia poscit.* §63.) Consisteix en què construeix una expressió que no canvia quan q se substitueix per q^2 i dedueix d'això que és independent de q . JACOBI es troba amb una dificultat semblant en la lliçó en la qual ha derivat la teoria de les funcions el·líptiques de la teoria de les sèries theta (*Ges. Werke*, vol. I, p. 516); aquí la supera mitjançant la construcció d'una expressió que resta invariant pel canvi de q per q^4 . Si posem

$$(1) \quad \vartheta \begin{bmatrix} \nu \\ \mu \end{bmatrix} (v) = \sum_n e^{2\pi i(v + \frac{1}{2}\mu)(n + \frac{1}{2}\nu) + i\pi\tau(n + \frac{1}{2}\nu)^2},$$

i, després (d'acord amb la variant de JACOBI de la notació del senyor WEIERSTRASS),

$$(2) \quad \vartheta_0 = \vartheta \begin{bmatrix} 1 \\ -1 \end{bmatrix}, \quad \vartheta_1 = \vartheta \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad \vartheta_2 = \vartheta \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \quad \vartheta_3 = \vartheta \begin{bmatrix} 0 \\ 1 \end{bmatrix},$$

s'aconsegueix la determinació d'aquella constant a partir de la fórmula

$$(3) \quad \vartheta'_0 = \pi \vartheta_1 \vartheta_2 \vartheta_3,$$

on, per a abreujar, s'ha escrit $\vartheta_1 = \vartheta_1(0)$. Per tant, aquesta fórmula no se segueix només del fet que les funcions theta siguin holomorfes arreu i satisfacin les igualtats

$$(4) \quad \begin{aligned} \vartheta \begin{bmatrix} \nu \\ \mu \end{bmatrix} (v+1) &= (-1)^\nu \vartheta \begin{bmatrix} \nu \\ \mu \end{bmatrix} (v), \\ \vartheta \begin{bmatrix} \nu \\ \mu \end{bmatrix} (v+\tau) &= (-1)^\mu e^{-i\pi(2v+\tau)} \vartheta \begin{bmatrix} \nu \\ \mu \end{bmatrix} (v), \end{aligned}$$

sinó de la forma especial de la sèrie (1), i serveix per a la recerca dels factors independents de v que resten indeterminats per la definició esmentada.

Si es posa, per a una característica qualsevol,

$$\frac{\partial^2 \vartheta(v)}{\partial v^2} - 4\pi i \frac{\partial \vartheta(v)}{\partial \tau} = \Theta(v),$$

s'obté a partir de les igualtats (4) que aquesta funció té les mateixes propietats que $\vartheta(v)$. En conseqüència, només en pot diferir per un factor independent de q ; segons això, és

$$\frac{\partial^2 \vartheta(v)}{\partial v^2} - 4\pi i \frac{\partial \vartheta(v)}{\partial \tau} = c \vartheta(v).$$

Per a la funció particular definida per la sèrie (1), és sabut que $c = 0$. Si encara s'afegeix a les relacions (4) l'equació en derivades parcials

$$(5) \quad \frac{\partial^2 \vartheta(v)}{\partial v^2} - 4\pi i \frac{\partial \vartheta(v)}{\partial \tau} = 0,$$

aleshores la funció theta queda unívocament determinada llevat d'un factor numèric (cf. CLEBSCH i GORDAN, *Abelsche Functionen*, §90). Així, doncs, en lloc d'utilitzar la sèrie (1) per a demostrar la identitat (3), com JACOBI, també es pot emprar per a això l'equació en derivades parcials (5). En el que segueix utilitzaré aquest camí, que fou emprès per primera vegada pel senyor WEIERSTRASS en les seves lliçons sobre funcions el·líptiques. Després que en §1 hagi desenvolupat dues demostracions d'aquella fórmula, només lleugerament diferents de la deducció del senyor WEIERSTRASS, aplico el mateix mètode en els paràgrafs següents per a demostrar les fórmules anàlogues per a funcions theta de dues i tres variables i, en general, per a funcions theta hiperel·líptiques. Alhora, em serviré de les notacions que he desenvolupat en el meu treball *Über das Additionstheorem der Thetafunctionen mehrerer Variabeln* (aquesta revista, vol. 89). D'ara endavant, el citaré per **T**. Si

$$A = \begin{pmatrix} \nu_1 \cdots \nu_\varrho \\ \mu_1 \cdots \mu_\varrho \end{pmatrix}, \quad B = \begin{pmatrix} \nu'_1 \cdots \nu'_\varrho \\ \mu'_1 \cdots \mu'_\varrho \end{pmatrix}$$

són dues característiques, la funció

$$(6) \quad \vartheta[A](v) = \\ = \sum_{n_1, \dots, n_\varrho} e^{2\pi i \sum_\alpha (v^{(\alpha)} + \frac{1}{2} \mu_\alpha)(n_\alpha + \frac{1}{2} \nu_\alpha) + i\pi \sum_{\alpha, \beta} \tau_{\alpha\beta} (n_\alpha + \frac{1}{2} \nu_\alpha)(n_\beta + \frac{1}{2} \nu_\beta)}$$

és determinada exactament, llevat d'un factor independent de v , ja que és holomorfa arreu en la part finita i satisfà la igualtat

$$(7) \quad \vartheta[A](v + 2B) = (A, B) e^{-2\pi i \sum_\alpha \nu'_\alpha v^{(\alpha)} - i\pi \sum_{\alpha, \beta} \tau_{\alpha\beta} \nu'_\alpha \nu'_\beta} \vartheta[A](v),$$

per a cada característica B . En posar

$$D_\alpha \vartheta(v) = \frac{\partial \vartheta(v)}{\partial v_\alpha},$$

la sèrie (6) satisfà les equacions en derivades parcials

$$(8) \quad D_\alpha^2 \vartheta - 4\pi i \frac{\partial \vartheta}{\partial \tau_{\alpha\alpha}} = 0, \quad D_\alpha D_\beta \vartheta - 2\pi i \frac{\partial \vartheta}{\partial \tau_{\alpha\beta}} = 0,$$

mentre que de les relacions (7) únicament es pot concloure que les expressions del costat esquerre d'aquestes igualtats satisfan les mateixes relacions.

Si $\nu \equiv \varrho \pmod{4}$ i $\nu \leq 2\varrho + 2$, aleshores hi ha un sistema fonamental de $2\varrho + 2$ característiques, que en conté ν de senars i $2\varrho + 2 - \nu$ de parelles (**T**, §5). En particular, doncs, hi ha sistemes fonamentals de ϱ característiques senars i $\varrho + 2$ parelles. Si és $\varrho < 4$, aleshores les $\varrho + 2$ característiques parelles corresponents a les ϱ senars, i les ϱ senars corresponents a les $\varrho + 2$ parelles, són unívocament determinades, mentre que aquest ja no és el cas si $\varrho > 3$. Per exemple, per a $\varrho = 4$, les quatre característiques senars són determinades per les sis parelles; però les quatre característiques senars poden ser completades de dues maneres mitjançant sis parelles a un sistema fonamental. Si $A_1, \dots, A_\varrho$ són ara les ϱ característiques senars i $B_1, \dots, B_{\varrho+2}$, les $\varrho + 2$ parelles d'un sistema fonamental, se satisfà la relació

$$(9) \quad |D_\beta \vartheta[A_\alpha]| = \pm \pi^\varrho \prod_{\gamma} \vartheta[B_\gamma] \quad (\alpha, \beta = 1, \dots, \varrho; \gamma = 1, \dots, \varrho + 2),$$

per a $\varrho = 1, 2, 3$. La mateixa relació val per a un valor qualsevol de ϱ en cas que el sistema fonamental és determinat i els paràmetres $\tau_{\alpha\beta}$ satisfan les condicions inherents a les funcions hiperelíptiques.

Per a $\varrho = 2$, aquesta relació fou comunicada pel senyor ROSENHAIN sense demostració (*Mém. Sav. Étrang.*, XI) i les seves indicacions han estat demostrades mitjançant una generalització del mètode de JACOBI que hem citat abans (cf. WEBER, aquesta revista, vol. 84, p. 338.). A partir de la fórmula que ha trobat el senyor WEBER per a la raó de dos determinants de la forma (9) (*Theorie der Abelsche Functionen vom Geschlecht 3*; p. 42) es podia conjecturar que existeixi una identitat semblant per a $\varrho = 3$. Per a les funcions theta hiperelíptiques, la relació precedent ha estat deduïda pel senyor THOMAE a partir de la teoria de les integrals hiperelíptiques (aquesta revista, vol. 71, p. 218). ¹⁾

§1.

$$\varrho = 1.$$

Si $\varrho = 1$, aleshores és sabut que

$$(1) \quad \vartheta_1(v)\vartheta'_0(v) - \vartheta_0(v)\vartheta'_1(v) = c\vartheta_2(v)\vartheta_3(v),$$

on c és una constant. Si es desenvolupen els dos costats d'aquesta igualtat en potències de v , per comparació dels termes inicials, s'obté

$$\vartheta_1\vartheta'_0 = c\vartheta_2\vartheta_3$$

i, per comparació dels termes de segon ordre,

$$\vartheta_1\vartheta'''_0 + \vartheta'_1\vartheta''_0 - 2\vartheta'_0\vartheta''_1 = c(\vartheta_2\vartheta''_3 + \vartheta''_2\vartheta_3),$$

¹⁾Aquesta és la fórmula (14) de la pàgina 292 (n. dels t.).

i d'aquí, per eliminació de c ,

$$(2) \quad \frac{\vartheta_0'''}{\vartheta_0'} = \sum_{\gamma} \frac{\vartheta_{\gamma}''}{\vartheta_{\gamma}} \quad (\gamma = 1, 2, 3).$$

Com a conseqüència de l'equació en derivades parcials (5) de la introducció, resulta d'aquí que

$$\frac{d \log \vartheta_0'}{d\tau} = \sum_{\gamma} \frac{d \log \vartheta_{\gamma}}{d\tau},$$

i, en conseqüència, és

$$(3) \quad \vartheta_0' = \varepsilon \pi \prod \vartheta_{\gamma},$$

on ε és una constant numèrica. Mitjançant el desenvolupament en potències de $e^{i\pi\tau}$ i comparació dels termes inicials, s'obté que $\varepsilon = 1$. També es pot arribar a la igualtat (3) si se surt de la fórmula

$$(4) \quad \vartheta_0(2v) = c\vartheta_0(v)\vartheta_1(v)\vartheta_2(v)\vartheta_3(v)$$

i es comparen els termes de primer i tercer ordre en els desenvolupaments dels dos costats de la igualtat.

§2.

$$\varrho = 2.$$

Sigui donat un sistema de $\alpha + 1$ característiques essencialment independents, juntament amb totes les seves combinacions essencials $A, A_1, \dots, A_{a-1}$, on $a = 2^{\alpha}$. Aleshores hi ha un segon sistema de $\beta + 1$ característiques essencialment independents, juntament amb les seves combinacions

essencials $B, B_1, \dots, B_{b-1}$, on $b = 2^\beta$ i $\alpha + \beta = 2\varrho$, de manera que, entre cada dues característiques del primer sistema i cada dues del segon, se satisfà la relació

$$(1) \quad (A_\kappa A_\lambda, B_\mu B_\nu) = +1.$$

He anomenat sistemes *adjunts* (aquesta revista, vol. 96, p. 94) dos tals sistemes complets. Llavors, d'una fórmula del senyor PRYM (*Untersuchungen über die Riemannsche Thetaformel*, Leipzig 1882; p. 87), se segueix que

$$(2) \quad \begin{cases} 2^{e-\alpha} \sum (BA_\lambda) \vartheta[A_\lambda](u+v)(u-v)(u'+v')(u'-v') = \\ = (AB) \sum (AB_\lambda) \vartheta[B_\lambda](u+v')(u-v')(u'+v)(u'-v). \end{cases}$$

Particularment, si és $\alpha = \beta = \varrho$, aleshores és, en conseqüència,

$$(3) \quad \begin{cases} \sum (BA_\lambda) \vartheta[A_\lambda](u+v)(u-v)(u'+v')(u'-v') = \\ = (AB) \sum (AB_\lambda) \vartheta[B_\lambda](u+v')(u-v')(u'+v)(u'-v). \end{cases}$$

Siguin ara v_α , ($\alpha = 0, 1, \dots, 2^e - 1$), 2^e sistemes de variables. En substituir en aquella fórmula

$$u' = u, \quad v = v_\alpha, \quad v' = v_\beta$$

i servir-se de l'abreviació

$$\vartheta(u, v) = \vartheta(u+v)\vartheta(u-v),$$

s'obté que

$$\begin{aligned} \sum_\lambda (BA_\lambda) \vartheta[A_\lambda](u, v_\alpha) \vartheta[A_\lambda](u, v_\beta) = \\ = (AB) \sum_\lambda (AB_\lambda) \vartheta[B_\lambda](u, v_\alpha) \vartheta[B_\lambda](u, v_\beta). \end{aligned}$$

Però ara el determinant de grau 2^e

$$|\sum_{\lambda}(BA_{\lambda})\vartheta[A_{\lambda}](u, v_{\alpha})\vartheta[A_{\lambda}](u, v_{\beta})| \quad (\alpha, \beta = 0, 1, \dots, 2^e - 1)$$

és igual al producte dels dos determinants

$$|\vartheta[A_{\lambda}](u, v_{\alpha})| |(BA_{\lambda})\vartheta[A_{\lambda}](u, v_{\beta})|,$$

i és

$$\prod (BA_{\lambda}) \cdot |\vartheta[A_{\alpha}](u, v_{\beta})|^2 = \prod (AB_{\lambda}) \cdot |\vartheta[B_{\alpha}](u, v_{\beta})|^2.$$

A partir del teorema que he desenvolupat en aquesta revista, vol. 96, p. 87, (fórmula (2)), sobre el nombre de característiques senars d'un sistema complet, es conclou fàcilment que, en tots els casos, $\prod (BA_{\lambda}) = \prod (AB_{\lambda})$. (El mateix resultat s'obté també de la mateixa darrera fórmula en suposar-hi els paràmetres $\tau_{\alpha\beta}$ imaginaris purs i totes les variables reals, perquè aleshores els valors de les funcions theta són tots reals.) Segons això, és

$$(4) \quad |\vartheta[A_{\alpha}](u, v_{\beta})| = \pm |\vartheta[B_{\alpha}](u, v_{\beta})| \quad (\alpha, \beta = 0, 1, \dots, 2^e - 1).$$

Per a $e = 2$, siguin $A_1, A_2, A_3, B_1, B_2, B_3$ les sis característiques senars i $A = A_1 A_2 A_3 \equiv B_1 B_2 B_3 = B$. Aleshores se satisfan les condicions (1) i val la fórmula (4). Si s'hi posa $v_4 = u$, s'anul·len, en els dos determinants, els elements de l'última columna, llevat d'un que esdevé igual a $\vartheta[A](0)(2u) = \vartheta[B](0)(2u)$ i és

$$|\vartheta[A_{\alpha}](u, v_{\beta})| = \pm |\vartheta[B_{\alpha}](u, v_{\beta})| \quad (\alpha, \beta = 1, 2, 3).$$

En incrementar u amb un semiperíode arbitrari, s'obté llavors el teorema:

Si les sis característiques A, A_1, A_2, B, B_1, B_2 formen un sistema fonamental, aleshores és

$$(5) \quad |\vartheta[A_\alpha](u, v_\beta)| = \pm |\vartheta[B_\alpha](u, v_\beta)| \quad (\alpha, \beta=0,1,2).$$

Si totes sis característiques d'un sistema fonamental no són senars, aleshores quatre d'elles són parelles i dues són senars. Siguin B_1, B_2 senars, i B, A, A_1, A_2 , parelles. Si es desenvolupen els dos costats de la igualtat (5) en potències de $v - u, v_1 - u, v_2 - u$ i es comparen els coeficients de $(v'_1 - u')(v''_2 - u'')$, s'obté ²⁾

$$\prod \vartheta[A_\alpha] \cdot |D_\beta \vartheta[A_\alpha](u)| = \pm \vartheta[B] \cdot [B_1, B_2] \cdot \prod \vartheta[B_\alpha](u) \quad (\alpha, \beta = 0, 1, 2),$$

on $D_0 \vartheta(u) = \vartheta(u)$ i s'ha posat

$$[B_1, B_2] = |D_\beta \vartheta[B_\alpha]| \quad (\alpha, \beta=1,2).$$

Anomenaré el determinant de tercer grau $|D_\beta \vartheta[A_\alpha]|$ *el determinant de les tres funcions $\vartheta[A_\alpha](u)$* . Com és sabut, en dividir-lo per $(\vartheta[A](u))^3$, aquest s'aplica en el determinant funcional dels dos quocients $\frac{\vartheta[A_1](u)}{\vartheta[A](u)}$ i $\frac{\vartheta[A_2](u)}{\vartheta[A](u)}$. Si en la fórmula anterior s'incrementa u en un semiperíode qualsevol, s'obté el teorema:

El determinant de tres funcions theta d'un sistema fonamental és igual, llevat d'un factor constant, al producte de les altres tres.

²⁾La lletra u denota el sistema d'ambdues variables u', u'' .

En la fórmula (6)

$$|\vartheta[A_\alpha](u), D_1\vartheta[A_\alpha](u), D_2\vartheta[A_\alpha](u)| = c \prod \vartheta[B_\alpha](u)_{(\alpha=0,1,2)},$$

siguin ara A_1, A_2 senars i A, B, B_1, B_2 parelles. En posar-hi $u = 0$, s'obté que

$$\vartheta[A] \cdot [A_1, A_2] = c \prod \vartheta[B_\alpha].$$

Ara desenvolupo els dos costats d'aquella igualtat en potències de u (és a dir, de u' i u'') i poso, per a abreujar,

$$D\vartheta = u'D_1\vartheta + u''D_2\vartheta, D^2\vartheta = u'^2D_1^2\vartheta + 2u'u''D_1D_2\vartheta + u''^2D_2^2\vartheta.$$

En prescindir dels termes d'ordre superior al segon, s'obté que

$$\begin{vmatrix} \vartheta[A] + \frac{1}{2}D^2\vartheta[A] + \cdots & DD_1\vartheta[A] + \cdots & DD_2\vartheta[A] + \cdots \\ D\vartheta[A_1] + \cdots & D_1\vartheta[A_1] + \frac{1}{2}D^2D_1\vartheta[A_1] + \cdots & D_2\vartheta[A_1] + \frac{1}{2}D^2D_2\vartheta[A_1] + \cdots \\ D\vartheta[A_2] + \cdots & D_1\vartheta[A_2] + \frac{1}{2}D^2D_1\vartheta[A_2] + \cdots & D_2\vartheta[A_2] + \frac{1}{2}D^2D_2\vartheta[A_2] + \cdots \end{vmatrix} =$$

$$= c \prod (\vartheta[B_\alpha] + \frac{1}{2}D^2\vartheta[B_\alpha] + \cdots).$$

En el determinant de l'esquerra, resto els elements de la segona i la tercera columnes, multiplicats per u' i u'' , dels de la primera. Així, per exemple, en prescindir dels termes d'ordre superior al segon, el segon element de la primera columna esdevé

$$D\vartheta[A_1] - u'D_1\vartheta[A_1] - u''D_2\vartheta[A_1] = 0.$$

Segons això, cada determinant és igual a

$$(\vartheta[A] - \frac{1}{2}D^2\vartheta[A] + \cdots) \times$$

$$\left| \begin{array}{l} D_1 \vartheta[A_1] + \frac{1}{2} D^2 D_1 \vartheta[A_1] + \cdots D_2 \vartheta[A_1] + \frac{1}{2} D^2 D_2 \vartheta[A_1] + \cdots \\ D_1 \vartheta[A_2] + \frac{1}{2} D^2 D_1 \vartheta[A_2] + \cdots D_2 \vartheta[A_2] + \frac{1}{2} D^2 D_2 \vartheta[A_2] + \cdots \end{array} \right|.$$

En comparar els termes de segon ordre en la fórmula de més amunt, s'obté, segons això,

$$\begin{aligned} \vartheta[A] \left\{ \left| \begin{array}{cc} D^2 D_1 \vartheta[A_1] & D_2 \vartheta[A_1] \\ D^2 D_1 \vartheta[A_2] & D_2 \vartheta[A_2] \end{array} \right| + \left| \begin{array}{cc} D_1 \vartheta[A_1] & D^2 D_2 \vartheta[A_1] \\ D_1 \vartheta[A_2] & D^2 D_2 \vartheta[A_2] \end{array} \right| \right\} - \\ - D^2 \vartheta[A] \cdot [A_1, A_2] = c(\vartheta[B_1] \vartheta[B_2] D^2 \vartheta[B] + \\ + \vartheta[B_2] \vartheta[B] D^2 \vartheta[B_1] + \vartheta[B] \vartheta[B_1] D^2 \vartheta[B_2]), \end{aligned}$$

o bé, si s'insereix el valor de c i se substitueixen els símbols A, B per B_3, B_4 ,

$$\begin{aligned} \left\{ \left| \begin{array}{cc} D^2 D_1 \vartheta[A_1] & D_2 \vartheta[A_1] \\ D^2 D_1 \vartheta[A_2] & D_2 \vartheta[A_2] \end{array} \right| + \left| \begin{array}{cc} D_1 \vartheta[A_1] & D^2 D_2 \vartheta[A_1] \\ D_1 \vartheta[A_2] & D^2 D_2 \vartheta[A_2] \end{array} \right| \right\} : \left| \begin{array}{cc} D_1 \vartheta[A_1] & D_2 \vartheta[A_1] \\ D_1 \vartheta[A_2] & D_2 \vartheta[A_2] \end{array} \right| = \\ = \sum_{\gamma}^4 \frac{D^2 \vartheta[B_{\gamma}]}{\vartheta[B_{\gamma}]}. \end{aligned}$$

Tots dos costats d'aquesta igualtat són funcions quadràtiques de u' i u'' . Atès que els seus coeficients coincideixen un per un, la igualtat es manté certa quan se substitueixen $u'^2, u'u'', u''^2$ per qualssevol altres quantitats, per exemple, $d\tau_{11}, d\tau_{12}, d\tau_{22}$. Però, aleshores, com a conseqüència de l'equació diferencial (8) de la introducció, s'obté

$$d \log[A_1, A_2] = \sum_{\gamma} d \log \vartheta[B_{\gamma}],$$

on s'ha posat

$$d\vartheta = \frac{\partial \vartheta}{\partial \tau_{11}} d\tau_{11} + \frac{\partial \vartheta}{\partial \tau_{12}} d\tau_{12} + \frac{\partial \vartheta}{\partial \tau_{22}} d\tau_{22}.$$

Per integració d'aquesta igualtat, es dedueix que

$$(7) \quad [A_1, A_2] = \varepsilon \pi^2 \prod \vartheta[B_\gamma],$$

on ε és independent dels paràmetres $\tau_{\alpha\beta}$.

§3.

Funcions hiperel·líptiques

Si $A, A_1, \dots, A_{2\varrho-1}$ és un sistema fonamental de $2\varrho+2$ característiques, K la suma de totes les seves característiques senars, i C_ν la suma de ν característiques qualssevol d'aquelles, aleshores KC_ν és parella en el cas que sigui $\nu \equiv \varrho+1 \pmod{4}$, però senar en el cas que sigui $\nu \equiv \varrho-1 \pmod{2}$. Si es fixen per a ν només nombres que siguin $\equiv \varrho+1 \pmod{2}$, es poden aconseguir aquells valors dels paràmetres $\tau_{\alpha\beta}$ per als quals se satisfà que $\vartheta[KC_\nu] = 0$, en el cas que ν sigui diferent de $\varrho+1$, però que les quantitats $\vartheta[KC_\varrho]$ siguin totes diferents de zero.

Ara designem per $A, A_1, \dots, A_\varrho, B, B_1, \dots, B_\varrho$ les $2\varrho+2$ característiques del sistema fonamental donat. Si

$$(1) \quad G = KAA_1 \cdots A_\varrho \equiv KBB_1 \cdots B_\varrho,$$

aleshores $\vartheta[G]$ no és igual a zero. Si és $r = 2^e$ i $A_{\varrho+1}, \dots, A_{r-1}$ són les combinacions essencials de les característiques $A, A_1, \dots, A_\varrho$, i $B_{\varrho+1}, \dots, B_{r-1}$ les de les característiques $B_{\varrho+1}, \dots, B_{r-1}$, aleshores els dos sistemes complets GBA_λ i GBB_λ ($\lambda = 0, 1, \dots, r-1$) són adjunts i, segons la fórmula (3), §2,

$$\begin{aligned} \sum (BA_\lambda) \vartheta[GBA_\lambda] (u+v)(u-v)(u'+v')(u'-v') &= \\ = (AB) \sum (AB_\lambda) \vartheta[GBB_\lambda] (u+v')(u-v')(u'+v)(u'-v). \end{aligned}$$

Atès que és $\vartheta[G B B_\lambda] = 0$, si λ és diferent de zero, aleshores s'obté que

$$\begin{aligned} \sum (B A_\lambda) \vartheta[G B A_\lambda](u+v)(u-v)(u'+u)(u'-u) = \\ = \vartheta[G](0)(2u)(u'+v)(u'-v), \end{aligned}$$

si es posa $v' = u$. Atès que, a més, és $\vartheta[G B A_\lambda] = 0$, si és $\lambda > \varrho$, aleshores s'obté que

$$\begin{aligned} \vartheta[G](0)(2u)(u+v)(u-v) = \\ = \sum_{\alpha} (B A_\alpha) \vartheta[G B A_\alpha](0)(2u)(u+v)(u-v), \end{aligned}$$

on α es mou de 0 a ϱ , si es posa $u' = u$. En aquesta fórmula, substitueixo v per la sèrie de $\varrho + 1$ sistemes de valors diferents $v, v_1, \dots, v_\varrho$. De les $\varrho + 1$ igualtats obtingudes d'aquesta manera se segueix que

$$\begin{aligned} \frac{|\vartheta[G B A](u, v_\beta), \dots, \vartheta[G B A_{\varrho-1}](u, v_\beta), \vartheta[G B A_\varrho](u, v_\beta)|}{\vartheta[G](0)(2u)} = \\ = \pm \frac{|\vartheta[G B A](u, v_\beta), \dots, \vartheta[G B A_{\varrho-1}](u, v_\beta), \vartheta[G](u, v_\beta)|}{\vartheta[G B A_\varrho](0)(2u)} \end{aligned}$$

o bé, si s'incrementa u en GB ,

$$\begin{aligned} \frac{|\vartheta[A](u, v_\beta), \dots, \vartheta[A_{\varrho-1}](u, v_\beta), \vartheta[A_\varrho](u, v_\beta)|}{\vartheta[K A \cdots A_{\varrho-1} A_\varrho](0)(2u)} = \\ = \pm \frac{|\vartheta[A](u, v_\beta), \dots, \vartheta[A_{\varrho-1}](u, v_\beta), \vartheta[B](u, v_\beta)|}{\vartheta[K A \cdots A_{\varrho-1} B](0)(2u)}. \end{aligned}$$

Per aplicació repetida d'aquesta fórmula, es troba que el quocient

$$|\vartheta[A](u, v_\beta), \dots, \vartheta[A_\varrho](u, v_\beta)| : \vartheta[K A \cdots A_\varrho](0)(2u)$$

no canvia, llevat del signe, en prendre per a $A, A_1, \dots, A_\varrho$ qualssevol altres $\varrho + 1$ característiques del sistema fonamental. En conseqüència, és

$$\begin{aligned} & |\vartheta[A](u, v_\beta), \dots, \vartheta[A_\varrho](u, v_\beta)| : \vartheta[KA A_1 \cdots A_\varrho](0)(2u) = \\ & = \pm |\vartheta[B](u, v_\beta), \dots, \vartheta[B_\varrho](u, v_\beta)| : \vartheta[KBB_1 \cdots B_\varrho](0)(2u) \end{aligned}$$

o bé, com que $AA_1 \cdots A_\varrho \equiv BB_1 \cdots B_\varrho$,

$$(2) \quad |\vartheta[A_\alpha](u, v_\beta)| = \pm |\vartheta[B_\alpha](u, v_\beta)| \quad (\alpha, \beta = 0, 1, \dots, \varrho).$$

Aquesta igualtat es pot obtenir també de la manera següent: segons la fórmula (4), §2, és

$$|\vartheta[GA_\kappa](u, v_\lambda)| = \pm |\vartheta[GB_\kappa](u, v_\lambda)| \quad (\kappa, \lambda = 0, 1, \dots, r-1).$$

Si en aquesta igualtat es posa $v_{\varrho+1} = A_{\varrho+1}, \dots, v_{r-1} = A_{r-1}$, s'obté que

$$\begin{aligned} & (\vartheta[G](0)(2u))^{r-\varrho-1} |\vartheta[GA_\alpha](u, v_\beta)| = \\ & = \pm \left| \begin{pmatrix} BB_\lambda \\ AA_\kappa \end{pmatrix} \vartheta[GA_\kappa B_\lambda](0)(2u) \right| \cdot |\vartheta[GB_\alpha](u, v_\beta)| \\ & \quad (\alpha, \beta = 0, 1, \dots, \varrho; \kappa, \lambda = \varrho+1, \dots, r-1). \end{aligned}$$

Però si es posa $v_{\varrho+1} = B_{\varrho+1}, \dots, v_{r-1} = B_{r-1}$, s'obté que

$$\begin{aligned} & \left| \begin{pmatrix} AA_\kappa \\ BB_\lambda \end{pmatrix} \vartheta[GA_\kappa B_\lambda](0)(2u) \right| \cdot |\vartheta[GA_\alpha](u, v_\beta)| = \\ & = \pm (\vartheta[G](0)(2u))^{r-\varrho-1} |\vartheta[GB_\alpha](u, v_\beta)|. \end{aligned}$$

Ara, però, és

$$\begin{pmatrix} AA_\kappa \\ BB_\lambda \end{pmatrix} \begin{pmatrix} BB_\lambda \\ AA_\kappa \end{pmatrix} = (AA_\kappa, BB_\lambda) = 1,$$

per tant,

$$\begin{pmatrix} AA_{\kappa} \\ BB_{\lambda} \end{pmatrix} = \begin{pmatrix} BB_{\lambda} \\ AA_{\kappa} \end{pmatrix},$$

i, per consegüent,

$$|\vartheta[GA_{\alpha}](u, v_{\beta})| = \pm |\vartheta[GB_{\alpha}](u, v_{\beta})|.$$

En incrementar u en G , s'obté d'aquí la fórmula (2).

En incrementar el mateix u en $H = KB_1 \cdots B_{\varrho}$, les característiques $HB, HA, \dots, HA_{\varrho}$ esdevenen parelles; en canvi, $HB_1, \dots, HB_{\varrho}$, senars. A partir de la fórmula

$$|\vartheta[HA_{\alpha}](u, v_{\beta})| = \pm |\vartheta[HB_{\alpha}](u, v_{\beta})|$$

s'obté la relació

$$\begin{aligned} & \prod \vartheta[HA_{\alpha}] |D_{\beta} \vartheta[HA_{\alpha}](u)| = \\ & = \vartheta[HB] \cdot [HB_1, \dots, HB_{\varrho}] \prod \vartheta[HB_{\alpha}](u), \end{aligned}$$

de la mateixa manera que en §2; o bé, si s'incrementa u en H ,

$$(3) \quad |D_{\beta} \vartheta[A_{\alpha}](u)| = c \prod \vartheta[B_{\alpha}](u).$$

Ara suposo que $A_1, \dots, A_{\varrho}$ són senars, però $A, B, B_1, \dots, B_{\varrho}$ parelles. Si aquest no fos el cas per al sistema fonamental de sortida, s'aconseguiria en incrementar totes les característiques amb $KA_1 \cdots A_{\varrho}$. (Les condicions del cas hiperel·líptic resten invariants quan totes les característiques del sistema fonamental donat s'incrementen en la mateixa característica; per tant, quan aquest sistema fonamental és substituït per un qualsevol dels altres del mateix *complex*.) Si es posa en la fórmula (3) $u = 0$, s'obté que

$$\vartheta[A] \cdot [A_1, \dots, A_{\varrho}] = c \prod \vartheta[B_{\alpha}].$$

Si es desenvolupen posteriorment tots dos costats segons potències de u i es comparen els termes de segon ordre, es troba, com en §2, que

$$\begin{aligned}
 & \quad | \quad D^2 D_\alpha \vartheta[A_1], \quad D_\alpha \vartheta[A_2], \quad \dots \quad D_\alpha \vartheta[A_\varrho] | \\
 + & \quad | \quad D_\alpha \vartheta[A_1], \quad D^2 D_\alpha \vartheta[A_2], \quad \dots \quad D_\alpha \vartheta[A_\varrho] | \\
 + & \quad \dots \quad \dots \quad \dots \quad \dots \quad \dots \\
 + & \quad | \quad D_\alpha \vartheta[A_1], \quad D_\alpha \vartheta[A_2], \quad \dots \quad D^2 D_\alpha \vartheta[A_\varrho] | \\
 & = [A_1, A_2, \dots, A_\varrho] \sum_{\gamma}^{\varrho+2} \frac{D^2 \vartheta[B_\gamma]}{\vartheta[B_\gamma]},
 \end{aligned}$$

on A, B és substituïda per $B_{\varrho+1}, B_{\varrho+2}$. En aquesta igualtat se substitueix $u^{(\alpha)} u^{(\beta)}$ pel diferencial $d\tau_{\alpha\beta}$. Si les quantitats $\tau_{\alpha\beta}$ són variables independents (la variabilitat de les quals només és restringida per les condicions de convergència de la sèrie theta), aleshores es té que

$$\sum \frac{D^2 \vartheta[B_\gamma]}{\vartheta[B_\gamma]} = 4\pi i d \log \prod \vartheta[B_\gamma].$$

Aquesta igualtat es manté quan la variabilitat de les quantitats $\tau_{\alpha\beta}$ es restringeix mitjançant qualssevol d'aquelles relacions, i segons això, de les fórmules de més amunt es desprèn la relació

$$d \log [A_1, \dots, A_\varrho] = d \log \prod \vartheta[B_\gamma]$$

i d'aquí, per integració,

$$(4) \quad [A_1, \dots, A_\varrho] = \varepsilon \pi^\varrho \prod \vartheta[B_\gamma],$$

on ε és una constant numèrica.

§4.

$$\varrho = 3.$$

Si les tres característiques senars A_1, A_2, A_3 i les cinc característiques parelles $B_1, \dots, B_5$ formen un sistema fonamental, i és

$$A = \sum A_\alpha \equiv \sum B_\gamma,$$

aleshores, és

$$(1) \quad |D_\beta \vartheta[A_\alpha]| : c = \sum \frac{\vartheta[B_\gamma](2u)}{\vartheta[B_\gamma]} - \frac{\vartheta[A](2u)}{\vartheta[A]}$$

$$(\alpha, \beta = 0, \dots, 3; \gamma = 1, \dots, 5),$$

on

$$c = \frac{1}{4} \vartheta[A] \cdot [A_1, A_2, A_3]$$

és una constant.

El determinant del costat esquerre de la igualtat (1), que designem per $\varphi(u)$, és una funció theta de quart grau, que per increment dels arguments en períodes enters canvia de la mateixa manera que $\vartheta[G](2u)$, en el cas que G sigui una característica qualsevol. Les 4^{es} funcions d'igual comportament $\vartheta[G](2u)$, que s'obtenen quan G es deixa recórrer totes les característiques, són mútuament independents (**T**, p. 200). Atès que d'aquestes funcions no n'hi ha més de 4^{es}, cal que $\varphi(u)$ sigui una combinació lineal d'aquestes:

$$\varphi(u) = \sum_G c_G \vartheta[G](2u).$$

Atès que $\varphi(u)$ és parella, G necessita recórrer únicament les 36 característiques parelles

$$A, B_\gamma, A_\alpha B_\gamma B_\delta,$$

on α es mou de 1 fins a 3, i γ, δ denoten dos índexs diferents des de 1 fins a 5, diferents. Si en aquella igualtat s'incrementa u en $A_\alpha A_\beta$, on α, β són dos índexs diferents d'entre els 1, 2, 3, s'obté que

$$-\varphi(u) = \sum_G c_G(G, A_\alpha, A_\beta) \vartheta[G](2u),$$

i, per tant, cal que sigui $(G, A_\alpha, A_\beta) = -1$. Però, atès que $(A_\alpha B_\gamma B_\delta, A_\alpha, A_\beta) = +1$, aleshores G només pot ésser una de les sis característiques A, B_γ , d'on se segueix que

$$\varphi(u) = -c \frac{\vartheta[A](2u)}{\vartheta[A]} + \sum_\gamma c_\gamma \frac{\vartheta[B_\gamma](2u)}{\vartheta[B_\gamma]}.$$

Si es posa $u = B_1 B_2$, el determinant s'anul·la, perquè les tres característiques $A_\alpha B_1 B_2$ ($\alpha = 1, 2, 3$) són parelles. Atès que, a més, és $(A, B_1 B_2) = -(B_1, B_2)$ i $(B_\gamma, B_1 B_2) = -(B_1, B_2)$, en el cas que γ és diferent de 1 i 2, però igual a $+(B_1, B_2)$, en el cas que $\gamma = 1$ o bé 2, aleshores s'obté que

$$c + c_1 + c_2 = c_3 + c_4 + c_5.$$

De la mateixa manera és

$$c + c_1 + c_3 = c_2 + c_4 + c_5,$$

i per consegüent, $c_2 = c_3$, i, en general, $c_\gamma = c_\delta$ i, en conseqüència, també $c = c_\gamma$. Aleshores s'obté la fórmula (1) i, en posar-hi $u = 0$, la constant c .

Ara desenvolupo els dos costats de la igualtat (1) en potències de u i comparo els termes de segon ordre. De la mateixa manera que en §2, es troba que

$$\begin{aligned} & \{|D^2 D_\alpha \vartheta[A_1] \quad D_\alpha \vartheta[A_2] \quad D_\alpha \vartheta[A_3]| + \\ & + | \quad D_\alpha \vartheta[A_1] \quad D^2 D_\alpha \vartheta[A_2] \quad D_\alpha \vartheta[A_3]| + \\ & + | \quad D_\alpha \vartheta[A_1] \quad D_\alpha \vartheta[A_2] \quad D^2 D_\alpha \vartheta[A_3]| - \end{aligned}$$

$$\begin{aligned} & - \frac{D^2 \vartheta[A]}{\vartheta[A]} \cdot [A_1, A_2, A_3] \} : [A_1, A_2, A_3] = \\ & = - \frac{D^2 \vartheta[A]}{\vartheta[A]} + \sum \frac{D^2 \vartheta[B_\gamma]}{\vartheta[B_\gamma]} \end{aligned}$$

i, per tant,

$$d \log[A_1, A_2, A_3] = \sum d \log \vartheta[B_\gamma],$$

és a dir,

$$(2) \quad [A_1, A_2, A_3] = \varepsilon \pi^3 \prod \vartheta[B_\gamma].$$

En la fórmula (1), A_1, A_2, A_3 són tres característiques senars qualssevol, la suma de les quals, A_0 , és parella. Per a tres característiques senars, la suma de les quals sigui senar, se satisfà la proposició següent anàloga al teorema de més amunt:

Si A_0, A_1, A_2, A_3 són quatre característiques senars, la suma de les quals és nul·la, aleshores és

$$(3) \quad \begin{vmatrix} \vartheta[A_0](u) & \vartheta[A_1](u) & \vartheta[A_2](u) & \vartheta[A_3](u) \\ D_1\vartheta[A_0](u) & D_1\vartheta[A_1](u) & D_1\vartheta[A_2](u) & D_1\vartheta[A_3](u) \\ D_2\vartheta[A_0](u) & D_2\vartheta[A_1](u) & D_2\vartheta[A_2](u) & D_2\vartheta[A_3](u) \\ D_3\vartheta[A_0](u) & D_3\vartheta[A_1](u) & D_3\vartheta[A_2](u) & D_3\vartheta[A_3](u) \end{vmatrix} =$$

$$= \begin{vmatrix} \vartheta[A_0](2u) & \vartheta[A_1](2u) & \vartheta[A_2](2u) & \vartheta[A_3](2u) \\ D_1\vartheta[A_0] & D_1\vartheta[A_1] & D_1\vartheta[A_2] & D_1\vartheta[A_3] \\ D_2\vartheta[A_0] & D_2\vartheta[A_1] & D_2\vartheta[A_2] & D_2\vartheta[A_3] \\ D_3\vartheta[A_0] & D_3\vartheta[A_1] & D_3\vartheta[A_2] & D_3\vartheta[A_3] \end{vmatrix}$$

§5.

$$\varrho = 3.$$

Indiquem encara una altra demostració per a la fórmula (2), §4 suara deduïda, que és una mica més complicada però que ofereix una analogia més gran amb els desenvolupaments precedents. Si les vuit característiques A_α, B_α ($\alpha = 0, \dots, 3$) constitueixen un sistema fonamental i és

$$P = \sum B_\alpha \equiv \sum A_\alpha,$$

aleshores les característiques $A_\alpha P$ són les combinacions essencials de les A_α , i les característiques $B_\alpha P$, les de les B_α . Per tant, en la fórmula (4), §2, es pot posar $A_{4+\alpha} = A_\alpha P$,

i $B_{4+\alpha} = B_\alpha P$. Si K és la suma de les característiques senars del sistema fonamental considerat i es posa en cada fórmula $v_{4+\beta} = u + KA_\beta$, aleshores $\vartheta[B_\alpha](u, v_{4+\beta})$ ($\alpha, \beta = 0, \dots, 3$) s'anul·la i, en conseqüència, el determinant de la dreta descompon en el producte de dos determinants de quart grau. A més,

$$\vartheta[A_\alpha](u, v_{4+\beta}) \quad \text{i} \quad \vartheta[A_\alpha P](u, v_{4+\beta})$$

s'anul·len en el cas que α és diferent de β . En conseqüència, s'obté que

$$\begin{vmatrix} \vartheta[A](u, v) & \dots & \vartheta[A_3](u, v) & \vartheta[AP](u, v) & \dots & \vartheta[A_3P](u, v) \\ \vartheta[A](u, v_3) & \dots & \vartheta[A_3](u, v_3) & \vartheta[AP](u, v_3) & \dots & \vartheta[A_3P](u, v_3) \\ \vartheta[K](u, u) & \dots & 0 & \binom{P}{KA} \vartheta[KP](u, u) & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & \vartheta[K](u, u) & 0 & \dots & \binom{P}{KA_3} \vartheta[KP](u, u) \end{vmatrix} =$$

$$= \pm |\vartheta[B_\alpha](u, v_\beta)| \cdot \left| \begin{pmatrix} A_\alpha \\ B_\beta \end{pmatrix} \vartheta[KPA_\alpha B_\beta](u, u) \right|.$$

Fàcilment, es pot transformar el costat esquerre en un determinant de quart grau, i aleshores s'obté que

$$\left| \vartheta[KP](u, u) \vartheta[A_\alpha](u, v_\beta) - \binom{P}{KA_\alpha} \vartheta[K](u, u) \vartheta[A_\alpha P](u, v_\beta) \right| =$$

$$= \pm |\vartheta[B_\alpha](u, v_\beta)| \cdot \left| \begin{pmatrix} A_\alpha \\ B_\beta \end{pmatrix} \vartheta[KPA_\alpha B_\beta](u, u) \right|.$$

En posar $v_\beta = u + KPA_\beta$, s'anul·len els elements fora de la diagonal en el determinant de l'esquerra i es troba, doncs,

$$(\vartheta^2[K](u, u) - (P)\vartheta^2[KP](u, u))^4 =$$

$$= + \left| \begin{pmatrix} A_\alpha \\ B_\beta \end{pmatrix} \vartheta[KPA_\alpha B_\beta](u, u) \right|^2.$$

El signe es determina en suposar les variables reals i, el paràmetre, imaginari pur. De les dues darreres fórmules se

segueix que

$$(1) \quad \left| \vartheta[KP](u, u) \vartheta[A_\alpha](u, v_\beta) - \binom{P}{KA_\alpha} \vartheta[K](u, u) \vartheta[A_\alpha P](u, v_\beta) \right| = \\ = \varepsilon (\vartheta^2[K](u, u) - (P) \vartheta^2[KP](u, u))^2 |\vartheta[B_\alpha](u, v_\beta)|,$$

on $\varepsilon = \pm 1$. En incrementar u en P , resulta d'aquí que

$$(2) \quad \left| \vartheta[K](u, u) \vartheta[A_\alpha](u, v_\beta) - \binom{P}{KA_\alpha P} \vartheta[KP](u, u) \vartheta[A_\alpha P](u, v_\beta) \right| = \\ = \varepsilon (\vartheta^2[K](u, u) - (P) \vartheta^2[KP](u, u))^2 |\vartheta[B_\alpha](u, v_\beta)|.$$

Si R i RP són dues característiques senars diferents, $\sqrt{P}$ és una qualsevol de les dues arrels quadrades de (P) , i es posa

$$\varphi(u, v) = \varphi[R](u, v) = \vartheta[R](u, v) + \binom{P}{R} \sqrt{P} \vartheta[RP](u, v),$$

aleshores, com he demostrat en aquesta revista, vol. 96, p. 116, (fórmula (6)), és

$$|\varphi(u_\alpha, v_\beta)| = |\varphi(u_\alpha, u_\beta)|^{\frac{1}{2}} |\varphi(v_\alpha, v_\beta)|^{\frac{1}{2}} \quad (\alpha, \beta = 0, \dots, 3).$$

En posar, en aquesta igualtat, $u_\alpha = u + RA_\alpha$, on A_α ($\alpha = 0, \dots, 3$) són quatre característiques diferents qualssevol, s'obté que

$$\begin{aligned} & |\vartheta[A_\alpha](u, v_\beta) + \binom{A_\alpha P}{P} \sqrt{P} \vartheta[A_\alpha P](u, v_\beta)| = \\ & = \binom{R}{P} \Pi(A_\alpha) \cdot \\ & \cdot \left| \vartheta[RA_\alpha A_\beta](u, u) + \binom{P}{RA_\alpha A_\beta} (A_\alpha, P) \sqrt{P} \vartheta[RA_\alpha A_\beta P](u, u) \right|^{\frac{1}{2}} \cdot \\ & \cdot |\varphi(v_\alpha, v_\beta)|^{\frac{1}{2}}. \end{aligned}$$

Si ara $A, \dots, A_3$ són quatre característiques d'un sistema fonamental i P és la seva suma, aleshores

$$(A_\alpha, P) = -(P) \prod (A_\alpha)$$

té el mateix valor per a totes quatre característiques. Si se substitueix $\sqrt{P}$ per $(A, P)(P)\sqrt{P}$ en la fórmula desenvolupada, s'obté que

$$\begin{aligned} |\varphi[A_\alpha](u, v_\beta)| &= \\ &= \pm \left| (R, A_\alpha) \begin{pmatrix} A_\alpha \\ A_\alpha A_\beta \end{pmatrix} \varphi[RA_\alpha A_\beta](u, u) \right|^{\frac{1}{2}} |\psi(v_\alpha, v_\beta)|^{\frac{1}{2}}, \end{aligned}$$

on és

$$\psi(u, v) = \vartheta[R](u, v) + \begin{pmatrix} P \\ RP \end{pmatrix} (A, P)\sqrt{P}\vartheta[RP](u, v).$$

Si es posa

$$\varphi_{\alpha\beta} = -\varphi_{\beta\alpha} = (R, A_\alpha) \begin{pmatrix} A_\alpha \\ A_\alpha A_\beta \end{pmatrix} \varphi[RA_\alpha A_\beta](u, u)$$

i s'escull $R = KAA_1$, aleshores les quantitats $\varphi_{\alpha\beta}$ s'anul·len llevat de φ_{01} i φ_{23} , i en resulta, doncs,

$$|\varphi_{\alpha\beta}|^{\frac{1}{2}} = \varphi_{01}\varphi_{23} = \pm\varphi[K](u, u)\varphi[KP](u, v).$$

Sigui, a més,

$$\begin{aligned} |\psi(v_\alpha, v_\beta)|^{\frac{1}{2}} &= \psi(v, v_1)\psi(v_2, v_3) + \psi(v, v_2)\psi(v_3, v_1) + \\ &+ \psi(v, v_3)\psi(v_1, v_2) = \Phi + \Psi\sqrt{P}, \end{aligned}$$

on Φ i Ψ són independents de $\sqrt{P}$, és a dir,

$$(3) \quad \left\{ \begin{array}{l} \Phi = \vartheta[R](v + v_1)(v - v_1)(v_2 + v_3)(v_2 - v_3) + \\ \quad + \vartheta[R](v + v_2)(v - v_2)(v_3 + v_1)(v_3 - v_1) + \\ \quad + \vartheta[R](v + v_3)(v - v_3)(v_1 + v_2)(v_1 - v_2) + \\ + (P)(\vartheta[RP](v + v_1)(v - v_1)(v_2 + v_3)(v_2 - v_3) + \\ \quad + \vartheta[RP](v + v_2)(v - v_2)(v_3 + v_1)(v_3 - v_1) + \\ \quad + \vartheta[RP](v + v_3)(v - v_3)(v_1 + v_2)(v_1 - v_2)). \end{array} \right.$$

Llavors, és

$$(4) \quad \begin{aligned} |\varphi[A_\alpha](u, v_\beta)| &= \varepsilon'(\Phi + \Psi\sqrt{P}) \cdot \\ &\cdot \left(\vartheta[K](u, u) + \binom{P}{K} \sqrt{P} \vartheta[KP](u, u) \right) \cdot \\ &\cdot \left(\vartheta[KP](u, u) + \binom{P}{KP} \sqrt{P} \vartheta[K](u, u) \right), \end{aligned}$$

on $\varepsilon' = \pm 1$.

La funció entera de quart grau de la variable r

$$\begin{aligned} &\varepsilon' \left| \vartheta[A_\alpha](u, v_\beta) + \binom{P}{A_\alpha} r \vartheta[A_\alpha P](u, v_\beta) \right| - \\ &-(\Phi + \Psi r) \left(\vartheta[K](u, u) + \binom{P}{K} r \vartheta[KP](u, u) \right) \cdot \\ &\cdot \left(\vartheta[KP](u, u) + \binom{P}{KP} r \vartheta[K](u, u) \right) \end{aligned}$$

s'anulla, doncs, per a $r = \pm\sqrt{P}$ i, en conseqüència, és divisible per $1 - (P)r^2$; és a dir, igual a

$$(1 - (P)r^2)(\Lambda + Mr + Nr^2).$$

Per comparació dels termes constants i dels coeficients de r^4 , s'obté que

$$\Lambda = \varepsilon' |\vartheta[A_\alpha](u, v_\beta)| - \Phi \vartheta[K](u, u) \vartheta[KP](u, u),$$

$$N = -\varepsilon' |\vartheta[A_\alpha P](u, v_\beta)|.$$

En posar, a més,

$$r = -\left(\frac{P}{K}\right) \frac{\vartheta[K](u, u)}{\vartheta[KP](u, u)},$$

s'obté, d'acord amb la fórmula (1),

$$\begin{aligned} \varepsilon \varepsilon' (\vartheta^2[K](u, u) - (P) \vartheta^2[KP](u, u)) |\vartheta[B_\alpha](u, v_\beta)| = \\ = -(P) \left(\Lambda \vartheta^2[KP](u, u) - M \left(\frac{P}{K} \right) \vartheta[KP](u, u) \vartheta[K](u, u) + \right. \\ \left. + N \vartheta^2[K](u, u) \right). \end{aligned}$$

Però, en posar,

$$r = -\left(\frac{P}{KP}\right) \frac{\vartheta[KP](u, u)}{\vartheta[K](u, u)},$$

s'obté, d'acord amb la fórmula (2),

$$\begin{aligned} \varepsilon \varepsilon' (P) (\vartheta^2[K](u, u) - (P) \vartheta^2[KP](u, u)) |\vartheta[B_\alpha P](u, v_\beta)| = \\ = \Lambda \vartheta^2[K](u, u) - M \left(\frac{P}{KP} \right) \vartheta[K](u, u) \vartheta[KP](u, u) + \\ + N \vartheta^2[KP](u, u). \end{aligned}$$

Per addició d'aquestes dues igualtats, resulta

$$\varepsilon \varepsilon' |\vartheta[B_\alpha](u, v_\beta)| + \varepsilon \varepsilon' (P) |\vartheta[B_\alpha P](u, v_\beta)| = \Lambda - (P)N.$$

En substituir-hi les expressions obtingudes més amunt per a i N i reemplaçar-hi ε i ε' per $-\varepsilon\varepsilon'$ i ε , s'obté que

$$(5) \quad \begin{cases} \varepsilon |\vartheta[A_\alpha](u, v_\beta)| + \varepsilon(P) |\vartheta[A_\alpha P](u, v_\beta)| + \\ + \varepsilon' |\vartheta[B_\alpha](u, v_\beta)| + \varepsilon'(P) |\vartheta[B_\alpha P](u, v_\beta)| = \\ = \vartheta[K](u, u) \vartheta[KP](u, u) \cdot \Phi. \end{cases}$$

Si ϑ és una funció senar i es desenvolupa l'expressió

$$\begin{aligned} & \vartheta(v + v_1)(v - v_1)(v_2 + v_3)(v_2 - v_3) + \\ & + \vartheta(v + v_2)(v - v_2)(v_3 + v_1)(v_3 - v_1) + \\ & + \vartheta(v + v_3)(v - v_3)(v_1 + v_2)(v_1 - v_2) \end{aligned}$$

en potències de $v - u$, $v_1 - u$, $v_2 - u$, $v_3 - u$, el coeficient de $(v'_1 - u')(v''_2 - u'')(v'''_3 - u''')$ és igual a $\vartheta(2u)$ vegades

$$\begin{aligned} & D_1 \vartheta \cdot (D_2 \vartheta(2u) \cdot D_3 \vartheta - D_3 \vartheta(2u) \cdot D_2 \vartheta) + \\ & + D_2 \vartheta \cdot (D_3 \vartheta(2u) \cdot D_1 \vartheta - D_1 \vartheta(2u) \cdot D_3 \vartheta) + \\ & + D_3 \vartheta \cdot (D_1 \vartheta(2u) \cdot D_2 \vartheta - D_2 \vartheta(2u) \cdot D_1 \vartheta) = 0. \end{aligned}$$

Suposo ara que, de les vuit característiques A_α , B_α , les característiques B_1 , B_2 , B_3 són senars, en canvi, B , A , $\dots$, A_3 , parelles. Llavors, BP és parella, mentre que B_1P , B_2P , B_3P , AP , $\dots$, A_3P són senars. Aleshores, si es comparen els coeficients de $(v'_1 - u')(v''_2 - u'')(v'''_3 - u''')$ en els desenvolupaments dels dos costats de la igualtat (5), i se substitueix $2u$ per u , s'obté que

$$\begin{aligned} \varepsilon \prod \vartheta[A_\alpha] |D_\beta \vartheta[A_\alpha](u)| &= \varepsilon' \vartheta[B] \cdot [B_1, B_2, B_3] \prod \vartheta[B_\alpha](u) + \\ &+ \varepsilon'(P) \vartheta[BP][B_1P, B_2P, B_3P] \prod \vartheta[B_\alpha](u). \end{aligned}$$

Si s'incrementa u en un semiperíode qualsevol, es reconeix que quan les vuit característiques A_α, B_α constitueixen un sistema fonamental qualsevol, se satisfà una igualtat de la forma

$$(6) \quad |D_\beta \vartheta[A_\alpha](u)| = a \prod \vartheta[B_\alpha](u) + b \prod \vartheta[B_\alpha P](u)$$

en la qual a i b són constants. Les quatre característiques A_α poden ésser completades de dues maneres a un sistema fonamental, a saber, no solament amb les B_α , sinó també amb les $B_\alpha P$ (**T.**, p. 211, teorema VI). Segons això, la fórmula (6) és l'anàloga per a $\varrho = 3$ a la fórmula (6), §2, vàlida per a $\varrho = 2$.

Ara suposo que A_1, A_2, A_3 són senars, en canvi, $A, B, \dots, B_3$, parelles. Llavors, les quatre característiques $B_\alpha P$ són senars i, per tant, el desenvolupament del producte $\prod \vartheta[B_\alpha P](u)$ comença amb els termes de quart ordre. En comparar, doncs, els termes constants i els termes de segon ordre en els desenvolupaments dels dos costats de la igualtat (6), s'obté, com en §2, que

$$(7) \quad [A_1, A_2, A_3] = \varepsilon \pi^3 \prod \vartheta[B_\gamma] \quad (\gamma = 1, \dots, 5),$$

on A, B són reemplaçades per B_4, B_5 .

Per a acabar, determinem encara les constants a i b de la fórmula (6). Si, de nou, A_α, B_α és un sistema fonamental arbitrari i K és la suma de les seves característiques senars, en posar a (6) u una vegada igual a KA i l'altra vegada igual a KAP , s'obté que

$$\frac{b}{a} = \binom{P}{A} \frac{\vartheta[K][KAA_1, KAA_2, KAA_3]}{\vartheta[KP][KAA_1P, KAA_2P, KAA_3P]}.$$

Les tres característiques senars $KPAA_\kappa$ ($\kappa = 1, 2, 3$), la suma de les quals és còngrua a K , juntament amb les cinc característiques parelles KP , $KPAB_\alpha$ formen un sistema fonamental. D'acord amb la fórmula (1) §4 és, doncs,

$$\begin{aligned} & |D_\alpha \vartheta[K](u), D_\alpha \vartheta[KPAA_1](u), D_\alpha \vartheta[KPAA_2](u), D_\alpha \vartheta[KPAA_3](u)| : k = \\ &= \frac{\vartheta[KP](2u)}{\vartheta[KP]} - \frac{\vartheta[K](2u)}{\vartheta[K]} + \sum_\alpha \frac{\vartheta[KPAB_\alpha](2u)}{\vartheta[KPAB_\alpha]}. \end{aligned}$$

En incrementar en aquesta igualtat u en P , s'obté que

$$\begin{aligned} & \binom{P}{A} \binom{K}{P} |D_\alpha \vartheta[KP](u), D_\alpha \vartheta[KAA_1](u), D_\alpha \vartheta[KAA_2](u), D_\alpha \vartheta[KAA_3](u)| : k = \\ &= \frac{\vartheta[KP](2u)}{\vartheta[KP]} - \frac{\vartheta[K](2u)}{\vartheta[K]} + \sum_\alpha \frac{\vartheta[KPAB_\alpha](2u)}{\vartheta[KPAB_\alpha]}. \end{aligned}$$

Si se sumen aquestes igualtats i s'hi posa després $u = 0$, es troba que

$$\begin{aligned} & \vartheta[K][KPAA_1, KPAA_2, KPAA_3] + \\ & + \binom{P}{A} \binom{K}{P} \vartheta[KP][KAA_1, KAA_2, KAA_3] = 0. \end{aligned}$$

Amb la notació retocada, aquesta fórmula es pot expressar de la manera següent:

Si es descompon una característica P diferent de 0 en una suma de dues característiques senars de tres maneres diferents ³⁾ $A + PA, B + PB, C + PC$, *aleshores és*

$$\frac{[AP, BP, CP]}{[A, B, C]} = - \binom{P}{ABCP} \frac{\vartheta[ABC]}{\vartheta[ABCP]}.$$

Segons això, és

$$\frac{b}{a} = - \binom{K}{P} \frac{\vartheta^2[K]}{\vartheta^2[KP]}$$

³⁾ Que, llavors, ABC és parella (per a $\varrho = 3$), ja ho ha indicat RIEMANN (Ges. Werke, p. 468).

i, en conseqüència,
(8)

$$|D_\beta \vartheta[A_\alpha](u)| = \\ = \varepsilon \pi^3 \left(\vartheta^2[KP] \prod \vartheta[B_\alpha](u) - \binom{K}{P} \vartheta^2[K] \prod \vartheta[B_\alpha P](u) \right).$$

A partir de la fórmula (7), s'obté, llavors, que és $\varepsilon = \pm 1$.

§6.

$$\varrho = 4.$$

Acabo amb unes observacions sobre el cas $\varrho = 4$. Si-
gui $A_1, \dots, A_5, B_1, \dots, B_5$ un sistema fonamental de deu
característiques parelles, i siguin $A, A_6, \dots, A_{15}$ les com-
binacions essencials de A_α , i $B, B_6, \dots, B_{15}$, les de B_α , en
particular, $A = A_1, \dots, A_5$ i $B = B_1, \dots, B_5$, és a dir,
 $A \equiv B$. Llavors, A i B són parelles, en canvi, $A_6, \dots, A_{15}$,
 $B_6, \dots, B_{15}$ són senars. Segons la fórmula (3), §2, és

$$\sum (AA_\lambda) \vartheta[A_\lambda](u+v)(u-v)(u'+v')(u'-v') = \\ = \sum (AB_\lambda) \vartheta[B_\lambda](u+v')(u-v')(u'+v)(u'-v),$$

on λ es mou des de 0 fins a 15. Si es posa $u' = v' = u$,
aleshores s'obté d'això que

$$\sum (AA_\lambda) \vartheta[A_\lambda](0)(2u)(u+v)(u-v) = \\ = \sum (AB_\lambda) \vartheta[B_\lambda](0)(2u)(u+v)(u-v),$$

on λ només es mou des de 0 fins a 5. Però, atès que els
termes corresponents al valor $\lambda = 0$ coincideixen en tots

dos costats, només cal que λ es mogui des de 1 fins a 5. Si es posa en aquesta fórmula $v = u + AB_1$, s'obté que

$$\begin{aligned} \sum \binom{A_\lambda}{A} \binom{B_1}{A_\lambda} \vartheta[A_\lambda](0)(u) \vartheta[A_\lambda AB_1](0)(u) = \\ = \binom{B_1}{A} \vartheta[B_1](0)(u) \vartheta[A](0)(u). \end{aligned}$$

Amb la notació retocada, sigui ara $A_1, \dots, A_4, B_1, \dots, B_6$ un sistema fonamental de quatre característiques senars i sis parelles, i sigui

$$P = \sum B_\gamma \equiv \sum A_\alpha.$$

Llavors,

$$A_\alpha B_1 B_2, B_1, B_2, B_3 P, \dots, B_6 P$$

formen un sistema fonamental de deu característiques parelles. Podem, doncs, reemplaçar en les fórmules de més amunt

$$A_\alpha, A_5, B_1, A$$

per

$$A_\alpha B_1 B_2, B_3 P, B_2, B_3.$$

Llavors es troba que

$$\begin{aligned} \sum \binom{A_\alpha B_1}{B_3} \binom{B_2}{B_1 A_\alpha} \vartheta[A_\alpha B_1 B_2](0)(u) \vartheta[A_\alpha B_1 B_3](0)(u) - \\ - \vartheta[B_2](0)(u) \vartheta[B_3](0)(u) + \\ + \binom{B_2}{P} \binom{P}{B_3} \vartheta[B_2 P](0)(u) \vartheta[B_3 P](0)(u) = 0. \end{aligned}$$

Si s'incrementa u en B_1B_3 , aleshores s'obté d'aquí que

$$\begin{aligned} \sum \binom{B_1B_2B_3}{A_\alpha} \vartheta[A_\alpha B_1B_2] \vartheta[A_\alpha B_1B_3] \vartheta[A_\alpha B_2B_3](u) \vartheta[A_\alpha](u) - \\ - \vartheta[B_2] \vartheta[B_3] \vartheta[B_1](u) \vartheta[B_1B_2B_3](u) - \\ - (P) \vartheta[B_2P] \vartheta[B_3P] \vartheta[B_1P](u) \vartheta[B_4B_5B_6](u) = 0. \end{aligned}$$

Segons això, per comparació dels termes de primer ordre s'obté que

$$\begin{aligned} \sum_{\alpha} \binom{B_1B_2B_3}{A_\alpha} \vartheta[A_\alpha B_2B_3] \vartheta[A_\alpha B_3B_1] \vartheta[A_\alpha B_1B_2] D_\beta \vartheta[A_\alpha] - \\ - \vartheta[B_1] \vartheta[B_2] \vartheta[B_3] D_\beta \vartheta[B_1B_2B_3] - \\ - (P) \vartheta[B_1P] \vartheta[B_2P] \vartheta[B_3P] D_\beta \vartheta[B_4B_5B_6] = 0. \end{aligned}$$

De la mateixa manera és

$$\begin{aligned} \sum_{\alpha} \binom{B_4B_5B_6}{A_\alpha} \vartheta[A_\alpha B_5B_6] \vartheta[A_\alpha B_6B_4] \vartheta[A_\alpha B_4B_5] D_\beta \vartheta[A_\alpha] - \\ - (P) \vartheta[B_4P] \vartheta[B_5P] \vartheta[B_6P] D_\beta \vartheta[B_1B_2B_3] - \\ - \vartheta[B_4] \vartheta[B_5] \vartheta[B_6] D_\beta \vartheta[B_4B_5B_6] = 0. \end{aligned}$$

Aquestes igualtats proporcionen dues solucions diferents de les quatre equacions lineals

$$\sum_{\alpha} D_\beta \vartheta[A_\alpha] \cdot x_\alpha + D_\beta \vartheta[B_1B_2B_3] \cdot x_5 + D_\beta \vartheta[B_4B_5B_6] \cdot x_6 = 0$$

entre les sis incògnites $x_1, \dots, x_6$. Com és sabut, els determinants de quart grau construïts a partir dels coeficients de les equacions es comporten com els determinants de segon grau construïts a partir dels elements de les solucions (aquesta revista, vol. 82, p. 237). Per tant, de les dues igualtats de més amunt se segueix que és

$$(1) \quad [A_1, A_2, A_3, A_4] = \varepsilon \pi^4 \left(\prod \vartheta[B_\gamma] - \prod \vartheta[B_\gamma P] \right),$$

on ε és un factor de proporcionalitat que roman invariant, llevat del signe, quan $A_1, \dots, A_4$ són reemplaçades per qualssevol altres quatre de les sis característiques $A_1, \dots, A_4, B_1B_2B_3, B_4B_5B_6$, i, cada vegada, es fixen per a les B_γ sis característiques parelles que completen les quatre característiques senars escollides en un sistema fonamental. Per aplicació reiterada d'aquesta fórmula es troba que ε^2 té el mateix valor per a cada sistema fonamental de quatre característiques senars A_α i sis parelles B_γ . Per tant, és natural formular la hipòtesi que ε és independent dels paràmetres $\tau_{\alpha\beta}$. Tot i així, encara no he aconseguit trobar-ne una demostració.

Zuric, juny 1884

Referències de l'article

Recollim totes juntes les referències citades en aquest article.

Clebsch, A.; Gordan, P.: *Theorie der Abelsche Functionen*. Teubner, 1866.

Frobenius, G.: Über das Pfaffsche Problem. *J. reine u. angew. Math.* **82** (1877), p. 230–315.

Frobenius, G.: Über das Additionstheorem der Thetafunctionen mehrerer Variabeln. *J. reine u. angew. Math.* **89** (1880), p. 185–220.

Frobenius, G.: Über Gruppen von Thetacharakteristiken. *J. reine u. angew. Math.* **96** (1884), p. 81–99.

Frobenius, G.: Über Thetafunctionen mehrerer Variabeln. *J. reine u. angew. Math.* **96** (1884), p. 100–122.

Jacobi, C. G. J.: *Fundamenta nova theoria functionum ellipticarum*. Regiomonti, sumtibus fratrum Bornträger, Königsberg, 1829. Reproduit a *Gesammelte Werke*, Erster Band, Berlin, 1881, p. 49–239. Chelsea, reimpressió, 1969.

Jacobi, C. G. J.: Theorie der elliptischen Functionen, aus den Eigenschaften der Thetareihen abgeleitet. Nach einer Vorlesung Jacobis in diesen Auftrag ausgearbeitet von C. W. Borchardt. Reproduit a *Gesammelte Werke*, Erster Band, Berlin, 1881, p. 497–538. Chelsea, reimpressió, 1969.

Prym, F.: *Untersuchungen über die Riemann'sche Thetaformel und die Riemann'sche Charakteristikentheorie*. Teubner, Leipzig, 1882.

Riemann, B.: Zur Theorie der Abel'schen Functionen für den Fall $p = 3$. Nachlass, Cap. XXX de *Gesammelte mathematische Werke und wissenschaftlicher Nachlass*. Herausgegeben unter Mitwirkung von Richard Dedekind von Heinrich Weber. Leipzig, Teubner, 1876, p. 456–472.

Rosenhain, J.: Sur les fonctions de deux variables et à quatre périodes, qui sont les inverses des intégrales ultra-

élliptiques de la première classe. *Mémoires couronnées et mémoires des savants étrangers, publiées par l'Académie royale des sciences, des lettres et des beaux-arts de Belgique*, **XI** (1851), p. 362–468.

Thomae, C. J.: Beitrag zur Bestimmung von $\vartheta(0, 0, \dots, 0)$ durch die Klassenmoduln algebraischer Functionen. *J. reine u. angew. Math.* **71** (1870), p. 201–222.

Weber, H.: *Theorie der Abelsche Functionen vom Geschlecht 3*. Cornell University Library, 1876.

Weber, H.: Über die Kummersche Fläche vierter Ordnung mit sechzehn Knotenpunkten und ihre Beziehung zu den Thetafunctionen mit zwei Veränderlichen. *J. reine u. angew. Math.* **84** (1878), p. 332–354.

Capítol 11

Emmy Noether

El text de Noether que oferim a continuació és de caràcter aplicat. Si bé no forma part dels més remarcables de la seva producció, cal reconèixer que es compta entre els que tingueren un ressò més gran fora dels cercles estrictament matemàtics. Entre els físics teòrics, Noether és coneguda per la seva descoberta del lligam existent entre simetries i lleis conservatives associades a principis de variació. D'altra banda, aquesta descoberta es pot considerar estàndard per a una persona habituada a treballar en el context de la teoria de Galois i de la teoria d'invariants: n'hi ha prou amb substituir equació algebraica per equació diferencial, grup de Galois per grup de Lie i cos invariant per llei conservativa.

Els teoremes de Noether de més aplicació a la física es troben en el treball que traduïm, és a dir, *Problemes de variació invariants*, publicat l'any 1918. Atès allò que ella mateixa diu, el treball s'origina arran d'una pregunta formulada per Hilbert relativa al fet de la possible no-

conservació local de l'energia en el context de la relativitat general. Amb aquesta publicació —i onze més d'anteriors— Noether aconseguí un any més tard la seva habilitació a la Facultat de Filosofia de la Universitat de Göttingen.

11.1 1918: Simetries i lleis de conservació

L'any 1915, i pocs dies després de l'arribada de Noether a la Universitat de Göttingen, Einstein hi impartí una sèrie de sis conferències sobre relativitat general, que despertaren l'interès de Hilbert i de Klein. El mes de novembre d'aquell mateix any, Hilbert i Einstein, de manera independent l'un de l'altre, sotmeteren a publicació dos treballs amb les mateixes equacions de camp per a la relativitat general. La deducció de les equacions per part de Hilbert s'obtenia per consideració de les solucions extremals d'un problema variacional; el lagrangiana introduït per Hilbert en aquella ocasió es coneix avui com a lagrangiana de Hilbert-Einstein.

En el seu treball, Noether considera dues casuístiques diferents. La primera fa relació a un problema variacional en què el funcional que dona l'acció és preservat per l'operació d'un grup de Lie de dimensió finita. La segona parteix de la mateixa situació, però el grup que hi opera és un grup de Lie de dimensió infinita.

En el cas de dimensió finita, Noether demostra que tota simetria del sistema dona lloc a l'existència d'una quantitat invariant en el temps i, recíprocament, que tota quantitat que és preservada en el temps està associada a una simetria

del sistema. En el cas de dimensió no finita, només es pot garantir la invariància de certes quantitats en relació amb certs subgrups del grup de transformacions del sistema, la qual cosa dóna lloc a teoremes de conservació local de l'energia, anomenats per Hilbert teoremes impropis.

El primer teorema de Noether s'aplica en contextos molt diferents i s'ha generalitzat de maneres molt diverses. El trobem en mecànica clàssica, en teoria de camps i en teoria quàntica de camps. D'ell es deriven els teoremes de conservació del moment lineal i del moment angular, per exemple. Quan, a més, es tenen en compte les identitats de Bianchi, dóna lloc a teoremes de conservació de l'energia en camps electromagnètics i en camps de Yang-Mills. L'exemple més representatiu d'aplicació del segon teorema de Noether es troba en el cas ja esmentat de la relativitat general.

A continuació, ens limitarem a presentar la forma directa del primer teorema de Noether, en un context prou senzill a fi de poder comprendre la idea bàsica que sosté les consideracions que ella fa a l'article.

Suposem donat un principi variacional

$$\delta \int_{t_1}^{t_2} L(t, q(t), \dot{q}(t)) dt = 0,$$

que remet a les equacions d'Euler-Lagrange o equacions de moviment

$$\frac{d}{dt} \left(\frac{\partial L}{\partial \dot{q}^i} \right) - \frac{\partial L}{\partial q^i} = 0, \quad 1 \leq i \leq n.$$

Suposem que el lagrangiana L és regular, és a dir, que el hessià $(\partial^2 L / \partial \dot{q}^i \partial \dot{q}^j)$ és invertible, i denotem per $g^{jk}(t, q, \dot{q})$

les entrades de la matriu inversa. En escriure les equacions d'Euler-Lagrange en forma normal, tindrem que

$$\frac{d\dot{q}^i}{dt} = \Lambda^i(t, q, \dot{q}),$$

on

$$\Lambda^i(t, q, \dot{q}) = g^{ij} \left(-\frac{\partial^2 L}{\partial \dot{q}^j \partial q^k} - \frac{\partial^2 L}{\partial \dot{q}^j \partial t} + \frac{\partial L}{\partial q^j} \right).$$

Considerem la transformació infinitesimal en l'espai (t, q) donada per

$$\tilde{t} = t + \varepsilon \tau(t, q), \quad \tilde{q}^i = q^i + \varepsilon \xi^i(t, q).$$

Per mitjà d'aquesta transformació i per a valors de ε suficientment petits, cada corba $t \rightarrow q(t)$, definida en un interval $[a, b]$, es transformarà en una corba en les noves variables $\tilde{t} \rightarrow \tilde{q}(\tilde{t})$, que dependrà d'un paràmetre. Fins a primer ordre, es tindrà que

$$\frac{d\tilde{q}^i}{d\tilde{t}} = \frac{\dot{q}^i + \varepsilon \dot{\xi}^i}{1 + \varepsilon \dot{\tau}} = \dot{q}^i + \varepsilon (\dot{\xi}^i - \dot{q}^i \dot{\tau}).$$

Es diu que la transformació infinitesimal considerada deixa invariant l'acció fins a primer ordre si existeix una funció diferenciable $f(t, q)$ tal que

$$\begin{aligned} \int_{\tilde{t}_1}^{\tilde{t}_2} L \left(\tilde{t}, \frac{q(\tilde{t})}{d\tilde{t}}, \dot{\tilde{q}}(\tilde{t}) \right) d\tilde{t} &= \int_{t_1}^{t_2} L(t, q(t), \dot{q}(t)) dt + \\ &+ \varepsilon \int_{t_1}^{t_2} \frac{df}{dt}(t, q(t)) dt + O(\varepsilon^2), \end{aligned}$$

per a tota corba diferenciable $t \rightarrow q(t)$ i tot subinterval $[t_1, t_2]$ de $[a, b]$ on $q(t)$ estigui definida. Aquest serà el cas

si, i només si,

$$L\left(\tilde{t}(t), \tilde{q}(t), \frac{q(\tilde{t})}{dt}(t)\right) \frac{d(\tilde{t})}{dt}(t) = L(t, q(t), \dot{q}(t))dt + \\ + \varepsilon \frac{df}{dt}(t, q(t)) + O(\varepsilon^2).$$

Atès que la relació anterior cal que se satisfaci per a totes les corbes, s'arriba a la identitat següent, en t , q , $\dot{q}$, coneguda com a relació de Killing:

$$\frac{\partial L}{\partial t}\tau + \frac{\partial L}{\partial q^i}\xi^i + \frac{\partial L}{\partial \dot{q}^i}(\xi^i - \dot{q}^i\tau) + L\tau = \frac{df}{dt}.$$

Després d'unes quantes manipulacions, la identitat anterior es reescriu en la forma

$$(\xi^i - \dot{q}^i\tau) \left[-\frac{d}{dt} \left(\frac{\partial L}{\partial \dot{q}^i} \right) + \frac{\partial L}{\partial q^i} \right] + \\ + \frac{d}{dt} \left[L\tau + \frac{\partial L}{\partial \dot{q}^i}(\xi^i - \dot{q}^i\tau) \right] = \frac{df}{dt}.$$

Per definició, es diu que tota transformació infinitesimal per a la qual se satisfà aquesta identitat és una transformació de Noether de funció associada $f(t, q)$. Per tant, ja podem formular el teorema de Noether.

Teorema. *A tota transformació de Noether associada al principi variacional*

$$\delta \int_{t_1}^{t_2} L(t, q(t), \dot{q}(t))dt = 0$$

correspon una constant de moviment $F(t, q, \dot{q})$ donada per

$$F(t, q, \dot{q}) = f(t, q) - \left[L\tau + \frac{\partial L}{\partial \dot{q}^i}(\xi^i - \dot{q}^i\tau) \right],$$

on $f(t, q)$ és la funció associada a la transformació.

Nachr. v. d. Ges. d. Wiss. zu Göttingen 1918, 235–257

PROBLEMES DE VARIACIÓ INVARIANTS

per EMMY NOETHER

Presentat per F. Klein a la sessió del 26 de juliol de 1918 ¹⁾

Es tracta de problemes de variació que admeten un grup continu (en el sentit de LIE); les conclusions que en resulten per a les equacions diferencials corresponents troben la seva expressió més general en els teoremes formulats en §1, demostrats en els paràgrafs següents. Sobre aquestes equacions diferencials que sorgeixen de problemes de variació es poden fer afirmacions més precises que sobre equacions diferencials arbitràries que admetin un grup, les quals són l'objecte de les investigacions de LIE. El que segueix representa, per tant, una combinació dels mètodes del càlcul de variacions formal amb els de la teoria de LIE de grups. Per a grups especials i problemes de variació, aquesta combinació de mètodes no és nova; esmento HAMEL i HERGLOTZ per a grups especials finits, LORENTZ i els seus alumnes (per exemple FOKKER), WEYL i KLEIN per als especials infinits ²⁾. En particular la segona nota de KLEIN i les

¹⁾ La versió final dels manuscrits fou arranjada per primera vegada a finals de setembre.

²⁾ HAMEL: Math. Ann. Bd. 59 und Zeitschrift f. Math. u. Phys. Bd. 50. HERGLOTZ: Ann. d. Phys. (4) Bd. 36, bes. §9, p. 511. FOKKER, Verslag d. Amsterdamer Akad., 27./1. 1917. Per a d'altra

explicacions següents s'influeixen mútuament, per la qual cosa he de remetre a la remarca final de la nota de KLEIN.

§1. Remarques preliminars i formulació dels teoremes

Totes les funcions que intervenen en el que segueix cal que se suposin analítiques o, almenys, contínues i contínuament diferenciables un nombre finit de vegades, i donades de manera unívoca en el domini considerat.

Com és sabut, per un “grup de transformacions” s’entén un sistema de transformacions tal que per a cada transformació n’existeix una d’inversa en el sistema, i tal que la composició de dues transformacions qualssevol del sistema pertany de nou al sistema. El grup s’anomena un grup *continu finit* $\mathfrak{G}_\varrho$ si les seves transformacions són contingudes en una de més general que depèn analíticament de ϱ paràmetres essencials ε (és a dir, els ϱ paràmetres no han de poder ésser expressats com a ϱ funcions de menys paràmetres). En correspondència amb això, per un grup *continu infinit* $\mathfrak{G}_{\infty, \varrho}$ s’entén un grup les transformacions més generals del qual depenen analíticament de ϱ funcions arbitràries essencials $p(x)$ i de les seves derivades o, almenys, de manera contínuament diferenciable un nombre finit de vegades. Com a terme intermedi hi ha el grup que depèn d’infinits paràmetres però no de funcions arbitràries. Fi-

literatura, compari’s la segona nota de KLEIN: Göttinger Nachrichten 19. Juli 1918.

En un treball de KNESER aparegut recentment (Math. Zeitschrift Bd. 2) es tracta la formulació d’invariants per un mètode similar.

nalment, s'anomena *grup mixt* aquell que depèn tant de funcions arbitràries com de paràmetres ³⁾.

Siguin $x_1, \dots, x_n$ variables independents, $u_1(x), \dots, u_\mu(x)$ funcions que depenen d'aquestes. Si les x i les u se sotmeten a les transformacions d'un grup, aleshores per raó de la suposició de la invertibilitat de les transformacions, entre les quantitats transformades n'hi ha d'haver de nou exactament n d'independents, — $y_1, \dots, y_n$ —; siguin denotades per $v_1(y), \dots, v_\mu(y)$ les restants dependents d'aquestes. En les transformacions també poden intervenir les derivades de u respecte de x , és a dir, $\frac{\partial u}{\partial x}, \frac{\partial^2 u}{\partial x^2}, \dots$ ⁴⁾. Una funció s'anomena un *invariant* del grup quan preval una relació:

$$P\left(x, u, \frac{\partial u}{\partial x}, \frac{\partial^2 u}{\partial x^2}, \dots\right) = P\left(y, v, \frac{\partial v}{\partial y}, \frac{\partial^2 v}{\partial y^2}, \dots\right).$$

³⁾ En els “Grundlagen für die Theorie der unendlichen kontinuierlichen Transformationsgruppen” (Ber. d. K. Sächs. Ges. der Wissensch. 1891) [citat “Fonaments”] LIE defineix els grups continus infinits com els grups de transformacions les transformacions dels quals són donades per mitjà de les solucions més generals d'un sistema d'equacions en derivades parcials, sempre que aquestes solucions no depenguin solament d'un nombre finit de paràmetres. D'aquesta manera s'obté, per tant, un tipus de grups finits diferent del donat més amunt; mentre que, recíprocament, el cas límit d'infinits paràmetres no cal que satisfaci necessàriament cap sistema d'equacions diferencials.

⁴⁾ Deixo de banda els índexs —en tant que sigui possible, també en sumatoris—; és a dir, $\frac{\partial^2 u}{\partial x^2}$ per $\frac{\partial^2 u_\alpha}{\partial x_\beta \partial x_\gamma}$, etc.

Per tant, en particular, una integral I esdevindrà un invariant del grup quan prevalgui una relació:

$$\begin{aligned}
 I &= \int \cdots \int f \left(x, u, \frac{\partial u}{\partial x}, \frac{\partial^2 u}{\partial x^2}, \dots \right) dx = \\
 (1) \qquad &= \int \cdots \int f \left(y, v, \frac{\partial v}{\partial y}, \frac{\partial^2 v}{\partial y^2}, \dots \right) dy
 \end{aligned}
 \tag{5) }$$

si s'integra sobre un x -domini real *qualsevol* i el y -domini corresponent ⁶⁾.

D'altra banda, per a una integral I arbitrària, no necessàriament invariant, construeixo la primera variació δI i la transformo per mitjà d'una integració parcial segons les regles de càlcul de variacions. Tan bon punt se suposa que les δu , juntament amb totes les derivades que hi intervenen, s'anul·len a la vora, se sap que es té:

$$(2) \qquad \delta I = \int \cdots \int \delta f dx = \int \cdots \int \left(\sum \psi_i \left(x, u, \frac{\partial u}{\partial x}, \dots \right) \delta u_i \right) dx,$$

on ψ denoten les expressions lagrangianes; és a dir, el costat esquerre de les equacions de LAGRANGE del problema de variació corresponent $\delta I = 0$. A aquesta relació integral li

⁵⁾ Per a abreujar, escric dx, dy , per $dx_1 \cdots dx_n, dy_1 \cdots dy_n$.

⁶⁾ Tots els arguments $x, u, \varepsilon, p(x)$ que apareixen en les transformacions cal que siguin suposats reals, mentre que els coeficients poden ser complexos. Atès que en els resultats finals es tracta d'*identitats* en x, u , paràmetres i funcions arbitràries, aquestes també valen per a valors complexos, tan bon punt només sigui suposat que totes les funcions que hi intervenen són analítiques. De fet, una gran part dels resultats es pot argumentar sense integrals, de manera que la restricció que fem als reals tampoc no és necessària per a l'argumentació. Per contra, les consideracions al final de §2 i començament de §5 no semblen factibles sense integrals.

correspon una *identitat* en δu i les seves derivades que és lliure d'integrals, que s'obté quan s'escriuen els termes a la vora. Tal com mostra la integració parcial, aquests termes a la vora són integrals sobre *divergències*, és a dir, sobre expressions

$$\text{Div} A = \frac{\partial A_1}{\partial x_1} + \cdots + \frac{\partial A_n}{\partial x_n},$$

on A és lineal en δu i les seves derivades. Amb això s'obté:

$$(3) \quad \sum \psi_i \delta u_i = \delta f + \text{Div} A.$$

En particular, si f conté únicament derivades primeres de u , aleshores, en el cas d'integrals simples, la identitat (3) coincideix amb l'anomenada per HEUN “equació central de LAGRANGE”:

$$(4) \quad \sum \psi_i \delta u_i = \delta f - \frac{d}{dx} \left(\sum \frac{\partial f}{\partial u'_i} \delta u_i \right), \quad \left(u'_i = \frac{du_i}{dx} \right),$$

mentre que la integral n -múltiple (3) es transforma en

$$(5) \quad \begin{aligned} \sum \psi_i \delta u_i = \delta f - \frac{\partial}{\partial x_1} \left(\sum \frac{\partial f}{\partial \frac{\partial u_i}{\partial x_1}} \delta u_i \right) - \cdots - \\ - \frac{\partial}{\partial x_n} \left(\sum \frac{\partial f}{\partial \frac{\partial u_i}{\partial x_n}} \delta u_i \right). \end{aligned}$$

Per a la integral simple i κ derivades de u , (3) és donada per

$$\sum \psi_i \delta u_i = \delta f -$$

$$\begin{aligned}
& -\frac{d}{dx} \left\{ \sum \left(\binom{1}{1} \frac{\partial f}{\partial u_i^{(1)}} \delta u_i + \binom{2}{1} \frac{\partial f}{\partial u_i^{(2)}} \delta u_i^{(1)} + \cdots + \right. \right. \\
& \quad \left. \left. + \binom{\kappa}{1} \frac{\partial f}{\partial u_i^{(\kappa)}} \delta u_i^{(\kappa-1)} \right) \right\} + \\
& + \frac{d^2}{dx^2} \left\{ \sum \left(\binom{2}{2} \frac{\partial f}{\partial u_i^{(2)}} \delta u_i + \binom{3}{2} \frac{\partial f}{\partial u_i^{(3)}} \delta u_i^{(1)} + \cdots + \right. \right. \\
& \quad \left. \left. + \binom{\kappa}{2} \frac{\partial f}{\partial u_i^{(\kappa)}} \delta u_i^{(\kappa-2)} \right) \right\} + \\
& \quad + \cdots + \\
(6) \quad & + (-1)^\kappa \frac{d^\kappa}{dx^\kappa} \left\{ \sum \binom{\kappa}{\kappa} \frac{\partial f}{\partial u_i^{(\kappa)}} \delta u_i \right\}
\end{aligned}$$

i una identitat corresponent val per a integrals n -múltiples; en particular, A conté δu fins a la $(\kappa - 1)$ -èsima derivada. El fet que les expressions lagrangianes ψ_i estan definides efectivament mitjançant (4), (5) i (6) se segueix del fet que mitjançant les combinacions de les bandes dretes s'eliminen totes les derivades superiors de δu , mentre que d'altra banda se satisfà la relació (2), a la qual condueix *unívocament* la integració parcial.

Ara, en el que segueix, es tracten els dos teoremes:

I. Si la integral I és invariant respecte d'un $\mathfrak{G}_\varrho$, aleshores ϱ combinacions linealment independents d'expressions lagrangianes esdevenen divergències —recíprocament, se segueix d'això la invariància de I respecte d'un $\mathfrak{G}_\varrho$. El teorema també val en el cas límit d'infinits paràmetres.

II. Si la integral I és invariant respecte d'un $\mathfrak{G}_{\infty, \varrho}$ en el qual intervenen funcions arbitràries fins a les seves derivades σ -èsimes, aleshores subsisteixen ϱ relacions d'identitat entre les expressions de LAGRANGE i les seves derivades fins a l'ordre σ -èsim; aquí també val el recíproc ⁷⁾.

Per als grups mixtos, valen les afirmacions dels dos teoremes, és a dir, es produeixen tant dependències com relacions de divergència independents. Si es parteix d'aquestes identitats i es passa al problema corresponent de variacions, és a dir, es fa $\psi = 0$ ⁸⁾, aleshores el teorema I afirma en el cas de dimensió u —en el qual la divergència es transforma en una diferencial total— l'existència de ϱ integrals primeres, entre les quals, però, es poden donar relacions no lineals de dependència ⁹⁾; en el cas multidimensional, s'obtenen les equacions de divergència, sovint designades darrerament com a “lleis de conservació”; el teorema II ens diu que ϱ de les equacions de LAGRANGE són una conseqüència de la resta.

L'exemple més fàcil del teorema II —sense recíproc— és donat per la representació paramètrica de WEIERSTRASS; és sabut que aquí la integral és invariant, amb una homogeneïtat de primer ordre, quan la variable independent x és substituïda per una funció arbitrària de x que deixa invariant u ($y = p(x)$; $v_i(y) = u(x)$). Per tant, hi intervé una funció arbitrària, però sense derivades; i a ella li correspon la relació lineal coneguda entre les pròpies expressions

⁷⁾ Per a certs casos excepcionals trivials, compari's la remarca §2, 2.

⁸⁾ Una mica més general, es pot també prendre $\psi_i = T_i$, compari's §3, primera remarca.

⁹⁾ Compari's el final de §3.

lagrangianes: $\sum \psi_i \frac{du_i}{dx} = 0$. Un altre exemple és l'ofert per la “teoria de la relativitat general” dels físics; es tracta aquí del grup de *totes* les transformacions $y_i = p_i(x)$ dels x , mentre que els u (denotats per $g_{\mu\nu}$ i q) estan subjectes a les transformacions induïdes pels coeficients d'una forma diferencial lineal i quadràtica [transformacions] que contenen les primeres derivades d'una funció arbitrària $p(x)$. A elles els corresponen les n dependències conegudes entre les expressions lagrangianes i les seves derivades primeres ¹⁰⁾.

En particular, si s'especialitza el grup de manera que cap derivada de $u(x)$ intervingui en les transformacions i, a més, les quantitats independents transformades depenguin únicament de x i no de u , aleshores se segueix de la invariància de I (tal com es demostrarà en §5), la invariància relativa de $\sum \psi_i \delta u_i$ ¹¹⁾ i de la mateixa manera la de les divergències que intervenen en el teorema I, tan bon punt els paràmetres se sotmetin a transformacions escaients. D'això se segueix encara que les integrals primeres esmentades abans satisfan el grup. De la mateixa manera, pel teorema II, s'obté la invariància relativa de les dependències de les bandes esquerra compendiades per mitjà de funcions arbitràries; i, com a conseqüència d'això, una altra funció, la divergència de la qual s'anul·la idènticament i admet el grup —que en la teoria de la relativitat dels físics proporciona el lligam entre dependències i la llei de [conservació de] l'energia ¹²⁾. Finalment, el teorema II dóna encara, en un context de teoria de grups, la demostració d'una afirmació de HILBERT sobre la fallida de les lleis de l'energia pròpies

¹⁰⁾ Compari's tal vegada la representació de KLEIN.

¹¹⁾ És a dir, per transformació, $\sum \psi_i \delta u_i$ adquireix un factor.

¹²⁾ Compari's la segona nota de KLEIN.

de la “relativitat general.” Amb aquestes remarques addicionals, el teorema I comprèn tots els teoremes coneguts de la mecànica, etcètera, sobre integrals primeres, mentre que el teorema II pot ésser descrit com la generalització més àmplia possible de la “teoria de la relativitat general” en teoria de grups.

§2. Relacions de divergència i dependències

Sigui $\mathfrak{G}$ un grup continu —finit o infinit—; aleshores sempre es pot aconseguir que la transformació identitat correspongui al valor nul del paràmetre ε , respectivament al d’una funció $p(x)$ arbitrària ¹³⁾. Per tant, la transformació més general esdevindrà de la forma:

$$\begin{aligned} y_i &= A_i \left(x, u, \frac{\partial u}{\partial x}, \dots \right) = x_i + \Delta x_i + \dots \\ v_i(y) &= B_i \left(x, u, \frac{\partial u}{\partial x}, \dots \right) = u_i + \Delta u_i + \dots \end{aligned}$$

on Δx_i , Δu_i denoten els termes de dimensió més baixa en ε , respectivament, en $p(x)$ i en les seves derivades; que, de fet, en aquest punt, seran suposats lineals. Com es mostrarà més endavant, això no és cap restricció de la generalitat.

Ara, sigui la integral I un invariant respecte de $\mathfrak{G}$, és a dir, que satisfà la relació (1). Aleshores, en particular, I també serà invariant respecte de les transformacions infinitesimals contingudes en $\mathfrak{G}$:

$$y_i = x_i + \Delta x_i; \quad v_i(y) = u_i + \Delta u_i;$$

¹³⁾ Compari’s, tal vegada, LIE: “Fonaments” p. 331. Si es tracta de funcions arbitràries, aleshores els valors especials a^σ del paràmetre s’han de substituir per funcions fixades p^σ , $\frac{\partial p^\sigma}{\partial x}$, $\dots$; i, de la mateixa manera, els valors $a^\sigma + \varepsilon$ per $p^\sigma + p(x)$, $\frac{\partial p^\sigma}{\partial x} + \frac{\partial p}{\partial x}$ etc.

i per això la relació (1) s'aplica en:

$$(7) \quad 0 = \Delta I = \int \cdots \int f \left(y, v(y), \frac{\partial v}{\partial y}, \dots \right) dy - \\ - \int \cdots \int f \left(x, u(x), \frac{\partial u}{\partial x}, \dots \right) dx,$$

on la primera integral s'ha d'estendre sobre el domini $x + \Delta x$ que correspon al domini x . Però aquesta integració es pot canviar també en una integració sobre el domini x mitjançant la transformació que val per als Δx infinitesimals

$$(8) \quad \int \cdots \int f \left(y, v(y), \frac{\partial v}{\partial y}, \dots \right) dy = \\ = \int \cdots \int f \left(x, u(x), \frac{\partial u}{\partial x}, \dots \right) dx + \int \cdots \int \text{Div}(f \cdot \Delta x) dx.$$

Així doncs, si en lloc de la transformació infinitesimal Δu s'introdueix la variació

$$(9) \quad \bar{\delta} u_i = v_i(x) - u_i(x) = \Delta u_i - \sum \frac{\partial u_i}{\partial x_\lambda} \Delta x_\lambda,$$

aleshores (7) i (8) s'apliquen en

$$(10) \quad 0 = \int \cdots \int \{ \bar{\delta} f + \text{Div}(f \cdot \Delta x) \} dx.$$

El costat dret és la fórmula coneguda per a variacions simultànies de variables dependents i independents. Atès que la relació (10) se satisfà per integració sobre qualsevol domini arbitrari, aleshores l'integrand s'ha d'anul·lar idènticament; per tant, les equacions diferencials de LIE per a la invariància de I s'apliquen en la relació:

$$(11) \quad \bar{\delta} f + \text{Div}(f \cdot \Delta x) = 0.$$

Si aquí, segons (3), s'expressa $\bar{\delta}f$ per mitjà de les expressions de LAGRANGE, s'obté:

$$(12) \quad \sum \psi_i \bar{\delta} u_i = \text{Div} B \quad (B = A - f \cdot \Delta x),$$

i, per tant, aquesta relació representa per a cada integral invariant I una identitat en tots els arguments que hi figuren; és la forma cercada de l'equació diferencial de LIE per a I ¹⁴⁾.

Ara, suposem primerament que $\mathfrak{G}$ és un grup continu finit $\mathfrak{G}_\varrho$; atès que se suposa que Δu , Δx són lineals en els paràmetres $\varepsilon_1, \dots, \varepsilon_\varrho$, aleshores segons (9) val el mateix per a $\bar{\delta}u$ i les seves derivades; amb això A i B són lineals en ε . Per tant, si poso

$$B = B^{(1)}\varepsilon_1 + \dots + B^{(\varrho)}\varepsilon_\varrho; \quad \bar{\delta}u = \bar{\delta}u^{(1)}\varepsilon_1 + \dots + \bar{\delta}u^{(\varrho)}\varepsilon_\varrho$$

on, per tant, $\bar{\delta}u^{(1)}, \dots$ són funcions de $x, u, \frac{\partial u}{\partial x}, \dots$, aleshores, les relacions de divergència cercades,

$$(13) \quad \sum \psi_i \bar{\delta} u_i^{(1)} = \text{Div} B^{(1)}; \quad \dots \quad \sum \psi_i \bar{\delta} u_i^{(\varrho)} = \text{Div} B^{(\varrho)},$$

se segueixen de (12).

Per tant, ϱ relacions linealment independents d'expressions lagrangianes esdevenen divergències; la independència lineal se segueix del fet que, segons (9), a partir de

¹⁴⁾ En el cas trivial —que només es pot presentar si Δx , Δu també depenen de derivades de u —, (12) s'aplica en $0 = 0$ si $\text{Div}(f \cdot \Delta x) = 0$, $\bar{\delta} = 0$; per tant, aquestes transformacions infinitesimals sempre s'infereixen del grup; i només cal comptar el nombre dels paràmetres restants o bé de les funcions arbitràries, en la formulació dels teoremes. Si les transformacions infinitesimals restants encara construeixen un grup, ha d'ésser deixat en suspens.

$\bar{\delta}u = 0$, $\Delta x = 0$, se seguiria també $\Delta u = 0$, $\Delta x = 0$, és a dir, una dependència entre les transformacions infinitesimals. Però, per hipòtesi, cap d'aquestes és satisfeta per a cap valor del paràmetre, atès que, en cas contrari, el $\mathfrak{G}_\varrho$ generat per integració de transformacions infinitesimals dependria de menys de ϱ paràmetres essencials. Però l'altra possibilitat, $\bar{\delta}u = 0$, $\text{Div}(f\Delta x) = 0$, fou exclosa. Aquestes conclusions encara valen també en el cas límit d'infinit paràmetres.

Ara sigui $\mathfrak{G}$ un *grup continu infinit* $\mathfrak{G}_{\infty\varrho}$; aleshores $\bar{\delta}u$ i les seves derivades i, per tant, també B , esdevenen novament lineals en les funcions arbitràries $p(x)$ i les seves derivades ¹⁵⁾; per substitució dels valors de $\bar{\delta}u$, independentment per tant de (12), sigui

$$\sum \psi_i \bar{\delta}u_i = \sum_{\lambda, i} \psi_i \left\{ a_i^{(\lambda)}(x, u, \dots) p^{(\lambda)}(x) + b_i^{(\lambda)}(x, u, \dots) \frac{\partial p^{(\lambda)}}{\partial x} + \dots + c_i^{(\lambda)}(x, u, \dots) \frac{\partial^\sigma p^{(\lambda)}}{\partial x^\sigma} \right\}.$$

Ara, de manera anàloga a la fórmula d'integració parcial, a partir de la identitat

$$\varphi(x, u, \dots) \frac{\partial^\tau p(x)}{\partial x^\tau} = (-1)^\tau \frac{\partial^\tau \varphi}{\partial x^\tau} \cdot p(x) \quad \text{mod divergències}$$

es poden substituir les derivades de p pel propi p i per divergències, que esdevenen lineals en p i les seves derivades; d'aquesta manera es té que:

$$(14) \quad \sum \psi_i \bar{\delta}u_i = \sum_{\lambda} \left\{ (a_i^{(\lambda)} \psi_i) - \frac{\partial}{\partial x} (b_i^{(\lambda)} \psi_i) + \dots + \right.$$

¹⁵⁾ Atès que no representa cap restricció suposar p lliures de u , $\frac{\partial u}{\partial x}$, ... es mostra el recíproc.

$$+(-1)^\sigma \frac{\partial^\sigma}{\partial x^\sigma} (c_i^{(\lambda)} \psi_i) \Big\} p^{(\lambda)} + \text{Div} \Gamma$$

i en relació amb (12):

$$(15) \quad \sum_{\lambda} \left\{ (a_i^{(\lambda)} \psi_i) - \frac{\partial}{\partial x} (b_i^{(\lambda)} \psi_i) + \cdots + \right. \\ \left. + (-1)^\sigma \frac{\partial^\sigma}{\partial x^\sigma} (c_i^{(\lambda)} \psi_i) \right\} p^{(\lambda)} = \text{Div}(B - \Gamma).$$

Ara construeixo la integral n -iterada sobre (15), estesa a un domini qualsevol; i trio les $p(x)$ de manera que elles i totes les derivades que intervenen en $(B - \Gamma)$ s'anul·lin a la vora. Atès que la integral sobre una divergència es redueix a una integral de contorn, aleshores la integral sobre el costat esquerre de (15) també s'anul·la per a qualssevol $p(x)$, únicament [sota el supòsit] que elles i suficients derivades seves s'anul·lin a la vora; i segons conclusions conegudes, d'això se segueix l'anul·lació dels integrands per a cada $p(x)$, per tant les ϱ relacions:

$$(16) \quad \sum_{\lambda} \left\{ (a_i^{(\lambda)} \psi_i) - \frac{\partial}{\partial x} (b_i^{(\lambda)} \psi_i) + \cdots + \right. \\ \left. + (-1)^\sigma \frac{\partial^\sigma}{\partial x^\sigma} (c_i^{(\lambda)} \psi_i) \right\} p^{(\lambda)} = 0 \quad (\lambda = 1, 2, \dots, \varrho).$$

Aquestes són les dependències cercades entre les expressions de LAGRANGE i les seves derivades per invariància de I respecte de $\mathfrak{G}_{\infty\varrho}$; la independència lineal es demostra com més amunt, atès que el recíproc remet a (12); i com serà exposat amb més detall en §4, es pot novament passar des de les transformacions infinitesimals a les finites. Per tant, segons això, en les transformacions infinitesimals d'un $\mathfrak{G}_{\infty\varrho}$

ja hi intervenen sempre ϱ transformacions arbitràries. De (15) i (16) encara se segueix que $\text{Div}(B - \Gamma) = 0$.

Si s'introdueix oportunament un "grup mixt" i Δx i Δu es prenen lineals en els ε i en els $p(x)$, aleshores es veu, en anular primerament $p(x)$ i després ε , que se satisfan tant les relacions de divergència (13) com les de dependència (16).

§3. Recíproc en el cas de grup finit

A fi de provar el recíproc, primerament s'han de reproduir, en essència, les reflexions precedents en sentit contrari. Mitjançant la multiplicació pels ε i addició, de l'afirmació de (13) se segueix l'afirmació de (12); i, d'això, mitjançant la identitat (3), una relació $\bar{\delta} + \text{Div}(A - B) = 0$.

Per tant, si es posa $\Delta x = \frac{1}{f}(A - B)$, aleshores, per mitjà d'això s'ha guanyat (11). D'això, per integració, se segueix finalment (7): $\Delta I = 0$, és a dir, la invariància de I respecte de les transformacions infinitesimals determinades per Δx , Δu , on els Δu mitjançant (9) es determinen a partir de Δx i $\bar{\delta}u$, i Δx i Δu esdevenen lineals en els paràmetres. Però $\Delta I = 0$ manifesta de manera coneguda la invariància de I respecte de les transformacions finites, que s'obtenen per integració dels sistemes simultanis:

$$(17) \quad \frac{dx}{dt} = \Delta x_i; \quad \frac{du_i}{dt} = \Delta u_i; \quad \left(\begin{array}{c} x_1 = y \\ \text{per a } t = 0 \\ u_i = v_i \end{array} \right).$$

Aquestes transformacions finites contenen ϱ paràmetres $a_1, \dots, a_{\varrho}$, a saber, les combinacions $t\varepsilon_1, \dots, t\varepsilon_{\varrho}$. De la

suposició que hi ha d'haver ϱ i només ϱ relacions de divergència lineals independents (13), se segueix a més que les transformacions finites, en tant que no contenen les derivades $\frac{\partial u}{\partial x}$, sempre constitueixen un grup. A saber, en cas contrari, com a mínim una de les transformacions infinitesimals obtingudes per mitjà del procés dels parèntesis de LIE no seria combinació lineal de les ϱ restants; i atès que I també admet aquesta transformació, es donarien més de ϱ relacions de divergència linealment independents; o bé aquestes transformacions infinitesimals serien de la forma especial en què $\bar{\delta}u = 0$, $\text{Div}(f \cdot \Delta x) = 0$, però, aleshores, Δx o bé Δu dependrien de derivades, en contra del supòsit. Si es pot donar aquest cas quan les derivades en Δx i Δu hi intervenen, ha de romandre en suspens; aleshores, a fi de reobtenir la propietat de grup, a les relacions Δx determinades més amunt s'hi haurien d'afegir totes les funcions Δx per a les quals $\text{Div}(f \cdot \Delta x) = 0$; però, segons l'acord, els paràmetres que intervenen en això no han d'ésser tinguts en compte. *Amb això el recíproc està demostrat.*

D'aquest recíproc encara se segueix que, efectivament, Δx i Δu poden ésser suposats lineals en els paràmetres. A saber, si Δu i Δx fossin formes de grau superior en ε , aleshores, per causa de la independència lineal dels productes de potències de ε , les corresponents relacions enteres (13) només se seguirien en un nombre més gran [que ϱ] a partir del qual, pel recíproc, se segueix la invariància de I respecte d'un grup les transformacions infinitesimals del qual contindrien el paràmetre *linealment*. Si aquest grup contingués exactament ϱ paràmetres, aleshores subsistirien relacions de dependència lineal entre les relacions de divergència corresponents als termes de grau superior en ε .

Sigui, encara, remarcat que en el cas en què Δx i Δu contenen també derivades de u , les transformacions finites poden dependre d'infinites derivades de u ; atès que la integració de (17), per mitjà de la determinació de $\frac{d^2 x_i}{dt^2}$ i $\frac{d^2 u_i}{dt^2}$, condueix en aquest cas a $\Delta \left(\frac{\delta u}{\delta x_\kappa} \right) = \frac{\partial \Delta u}{\partial x_\kappa} - \sum_\lambda \frac{\partial u}{\partial x_\lambda} \frac{\partial \Delta x_\lambda}{\partial x_\kappa}$, cosa per la qual el nombre de derivades de u creix en general en cada pas. Un exemple és donat per

$$f = \frac{1}{2}u'^2; \quad \psi = -u''; \quad \psi \cdot x = \frac{d}{dx}(u - u'x); \quad \bar{\delta}u = x \cdot \varepsilon;$$

$$\Delta x = \frac{-2u}{u'^2}\varepsilon; \quad \Delta u = \left(x - \frac{2u}{u'} \right) \cdot \varepsilon.$$

Finalment, atès que l'expressió lagrangiana d'una divergència s'anul·la idènticament, el recíproc mostra encara el següent: si I admet $\mathfrak{G}_\rho$, aleshores ho fa cada integral que difereixi de I únicament en una integral de contorn, és a dir, una integral que es diferenciï en una divergència; també admet un $\mathfrak{G}_\rho$ amb els mateixos $\bar{\delta}u$ les transformacions infinitesimals del qual, en general, contindran derivades en u . Així, el corresponent a l'exemple de més amunt: $f^* = \frac{1}{2} \left\{ u'^2 - \frac{d}{dx} \left(\frac{u^2}{x} \right) \right\}$ admet la transformació infinitesimal $\Delta u = x\varepsilon$, $\Delta x = 0$; mentre que en les transformacions infinitesimals que corresponen a f hi intervenen derivades de u .

Passem al problema de variació; és a dir, si posem ¹⁶⁾
 $\psi_i = 0$, aleshores (13) es transforma en les equacions

$$\text{Div}(B^{(1)}) = 0, \quad \dots, \quad \text{Div}(B^{(\varrho)}) = 0,$$

les quals seran denominades sovint “lleis de conservació”. En el cas de dimensió 1, d’això se segueix que $B^{(1)} = \text{const}$; $\dots$, $B^{(\varrho)} = \text{const}$; i aquí les B contenen com a màxim les $(2\kappa - 1)$ primeres derivades de u (d’acord amb (6)), tan bon punt que Δu i Δx no continguin cap derivada superior a les κ -èsimes que intervinguin en f . Atès que en general en ψ intervenen derivades 2κ -èsimes, ¹⁷⁾ es té per tant l’existència de ϱ integrals primeres. La f d’abans mostra novament que entre aquestes es poden donar relacions de dependència no lineals. Les relacions linealment independents $\Delta u = \varepsilon_1$, $\Delta x = \varepsilon_2$ es corresponen amb les relacions linealment independents $u'' = \frac{d}{dx}u'$; $u'' \cdot u' = \frac{1}{2} \frac{d}{dx}(u')^2$; mentre que entre les integrals primeres $u' = \text{const.}$; $u'^2 = \text{const.}$ se satisfà una relació de dependència no lineal. Es tracta d’un cas elemental en què Δu , Δx no contenen cap derivada de u .
¹⁸⁾

¹⁶⁾ A la física, $\psi_i = 0$ o bé una mica més generalment, $\psi_i = T_i$, aquí les T_i són funcions adjuntades novament, són denominades “equacions de camp”. En el cas $\psi_i = T_i$, les identitats (13) es transformen en $\text{Div}B^{(\lambda)} = \sum T_i \delta u_i^{(\lambda)}$ que, a la física, també són denominades lleis de conservació.

¹⁷⁾ Sempre que f no sigui lineal en les κ -èsimes derivades.

¹⁸⁾ Altrament es tindria encara $u'^{\lambda} = \text{const.}$, per a cada λ , de manera corresponent:

$$u'' \cdot (u')^{\lambda-1} = \frac{1}{\lambda} \frac{d}{dx}(u')^{\lambda}.$$

§4. Recíproc en el cas de grup infinit

Demostrem, primerament, que la suposició de linealitat de Δx i Δu no representa cap restricció, cosa que aquí sense el recíproc ja proporciona que $\mathfrak{G}_{\infty, \varrho}$ depèn formalment de ϱ i de *només* $[\varrho]$ funcions arbitràries. A saber, es mostra que en el cas no lineal, per composició de transformacions en què els termes de graus d'ordre més petit se sumen, el nombre de funcions arbitràries augmenta. A tall d'exemple, sigui

$$\begin{aligned} y &= A\left(x, u, \frac{\partial u}{\partial x}, \dots; p\right) = \\ &= x + \sum a(x, u, \dots)p^\nu + b(x, u, \dots)p^{\nu-1}\frac{\partial p}{\partial x} + \\ &+ cp^{\nu-2}\left(\frac{\partial p}{\partial x}\right)^2 + \dots + d\left(\frac{\partial p}{\partial x}\right)^\nu + \dots \\ &(p^\nu = (p^{(1)})^{\nu_1} \dots (p^{(\varrho)})^{\nu_\varrho}); \end{aligned}$$

i, de manera corresponent, $v = B\left(x, u, \frac{\partial u}{\partial x}, \dots; p\right)$, aleshores, per composició amb $z = A\left(y, v, \frac{\partial v}{\partial y}, \dots; q\right)$, s'obté per als termes d'ordre més petit

$$\begin{aligned} z &= x + \sum a(p^\nu + q^\nu) + b\left\{p^{\nu-1}\frac{\partial p}{\partial x} + q^{\nu-1}\frac{\partial q}{\partial x}\right\} + \\ &+ c\left\{p^{\nu-2}\left(\frac{\partial p}{\partial x}\right)^2 + q^{\nu-2}\left(\frac{\partial q}{\partial x}\right)^2\right\} + \dots \end{aligned}$$

Si aquí un qualsevol dels coeficients diferent de a i de b és no nul, aleshores apareix realment un terme $p^{\nu-\sigma}\left(\frac{\partial p}{\partial x}\right)^\sigma +$

$q^{\nu-\sigma} \left(\frac{\partial q}{\partial x} \right)^\sigma$ per a $\sigma > 1$, per tant, aquest no es deixa escriure com a quocient diferencial d'una *única* funció o d'un producte de potències d'aquesta; per tant, el nombre de funcions arbitràries ha crescut, en contra de la suposició. Si tots els coeficients diferents de a i b s'anul·len, d'acord amb els valors dels exponents $\nu_1, \dots, \nu_\varrho$, el segon terme esdevindrà el quocient diferencial del primer (com per exemple, sempre per a un $\mathfrak{G}_{\infty 1}$), de tal manera que la linealitat també intervé efectivament, o altrament, el nombre de funcions arbitràries aquí també creix. —Les transformacions infinitesimals també satisfan, per causa de la *linealitat* de les $p(x)$, un sistema d'equacions lineals en derivades parcials; i atès que se satisfà la propietat de grup, constitueixen un “grup infinit de transformacions infinitesimals” segons la definició de LIE (Fonaments, §10).

Ara, el *recíproc* s'obté de manera semblant al cas del grup finit. Per multiplicació per $p^{(\lambda)}(x)$ i addició de les transformacions idèntiques (14), l'existència de les dependències (16) condueix a $\sum \psi_i \delta u_i = \text{Div} \Gamma$; i d'això se segueix com en §3 la determinació de Δx i Δu i la invariància de I respecte d'aquestes transformacions infinitesimals, les quals efectivament depenen linealment de ϱ funcions arbitràries i de les seves derivades fins a l'ordre σ -èsim. Com en §3 d'això se segueix que aquestes transformacions infinitesimals constitueixen de segur un grup quan no contenen cap derivada $\frac{\partial u}{\partial x}, \dots$, ja que, altrament, apareixerien per composició amb més funcions arbitràries, mentre que per suposició (16) únicament conté ϱ dependències; per tant, formen un “grup infinit de transformacions infinitesimals”. Però un tal [grup] consta de les transformacions infinitesimals més generals (Fonaments, teorema VII, p. 391) el

qual, en el sentit de LIE, estaria definit com un “grup infinit $\mathfrak{G}$ de transformacions finites”. Cada transformació finita es genera a partir de transformacions infinitesimals (Fonaments, §7) ¹⁹⁾, per tant, s’origina per integració del sistema simultani

$$\frac{dx_i}{dt} = \Delta x_i; \quad \frac{du_i}{dt} = \Delta u_i; \quad \left(\begin{array}{l} x_i = y_i \\ u_i = v \end{array} \text{ per a } t = 0 \right),$$

on, però, pot ésser necessari suposar, a més, que les $p(x)$ arbitràries depenen de t . *Per tant, $\mathfrak{G}$ depèn efectivament de ρ funcions arbitràries*; en particular, n’hi ha prou amb suposar que $p(x)$ és lliure de t , aleshores, aquesta dependència esdevé analítica en la funció arbitrària²⁰⁾ $q(x) = t \cdot p(x)$. Si hi intervenen derivades $\frac{\partial u}{\partial x}, \dots$, aleshores pot ésser necessari incloure-hi encara transformacions infinitesimals $\bar{\delta}u = 0$, $\text{Div}(f \cdot \Delta x) = 0$, abans de concloure el mateix.

Indiquem encara, en connexió amb un exemple de LIE (Fonaments §7), un cas més general, en què es pot arribar fins a fórmules explícites, les quals mostren al mateix temps que hi entren les derivades de les funcions arbitràries fins

¹⁹⁾ En particular, d’això se segueix que el grup $\mathfrak{G}$ generat a partir de les transformacions infinitesimals $\Delta x, \Delta u$ d’un $\mathfrak{G}_{\infty\varrho}$ condueix de nou a un $\mathfrak{G}_{\infty\varrho}$. Ja que $\mathfrak{G}_{\infty\varrho}$ no conté cap transformació infinitesimal de funcions dependents arbitràries que sigui diferent de $\Delta x, \Delta u$, i tampoc en pot contenir cap dependent de paràmetres que siguin independents d’aquestes, atès que, altrament, seria un grup mixt. Però, pel de més amunt, les transformacions finites estan determinades per les infinitesimals.

²⁰⁾ La pregunta de si aquest darrer cas es presenta sempre fou plantejada en una altra formulació per LIE (Fonaments, §7 i §13, final).

a l'ordre σ ; amb això, el recíproc també és complet. Succeeix que un tal grup de transformacions infinitesimals es correspon amb el grup de totes les transformacions de x i, per tant, transformacions “induïdes” de u ; és a dir, aquelles transformacions de u per a les quals Δu i, en conseqüència u , només depenen de les funcions arbitràries que intervenen en Δx ; en això, encara se suposa que les derivades $\frac{\partial u}{\partial x}, \dots$ no intervenen en Δu . Es té, per tant, que

$$\Delta x_i = p^{(i)}(x);$$

$$\Delta u_i = \sum_{\lambda=1}^n \left\{ a^{(\lambda)}(x, u) p^{(\lambda)} + b^{(\lambda)} \frac{\partial p^{(\lambda)}}{\partial x} + \dots + c^{(\lambda)} \frac{\partial^\sigma p^{(\lambda)}}{\partial x^\sigma} \right\}.$$

Atès que la transformació infinitesimal $\Delta x = p(x)$ genera cada transformació $x = y + g(y)$ amb $g(y)$ arbitrària, en particular, $p(x)$ es deixa determinar en funció de t , de manera que el grup esdevé generat per l'annexió de les

$$(18) \quad x_i = y_i + t \cdot g_i(y),$$

que, per a $t = 0$ és la identitat i, per a $t = 1$, s'aplica en la cercada $x = y + g(y)$. A saber, per mitjà de la diferenciació de (18) se segueix que

$$(19) \quad \frac{dx_i}{dt} = g_i(y) = p^{(i)}(x, t),$$

on $p(x, t)$ es determina a partir de $g(y)$ per inversió de (18); i recíprocament, (18) s'obté de (19) en virtut de la condició de contorn $x_i = y_i$ per a $t = 0$ per mitjà de la qual la integral queda unívocament determinada. En virtut de (18), les x es poden substituir en Δu per “constants d'integració” y i per t ; en això, en les $g(y)$ hi intervenen

exactament fins a la derivada σ -èsima, en el moment que en $\frac{\partial p}{\partial x} = \sum \frac{\partial g}{\partial y_\kappa} \frac{\partial y_\kappa}{\partial x}$ les $\frac{\partial y}{\partial x}$ s'expressen per mitjà de $\frac{\partial x}{\partial y}$, en general, $\frac{\partial^\sigma p}{\partial x^\sigma}$ se substitueix pel seu valor en $\frac{\partial g}{\partial y}, \dots, \frac{\partial x}{\partial y}, \dots, \frac{\partial^\sigma x}{\partial y^\sigma}$. Per tant, a fi de determinar u s'obté el sistema d'equacions

$$\frac{du_i}{dt} = F_i(g(y), \frac{\partial g}{\partial y}, \dots, \frac{\partial^\sigma g}{\partial y^\sigma}, u, t) \quad (u_i = v_i \text{ per a } t = 0),$$

en el qual únicament t i u són variables, però les $g(y)$, ... pertanyen al domini dels coeficients, de manera que la integració proporciona:

$$u_i = v_i + B_i \left(v, g(y), \frac{\partial g}{\partial y}, \dots, \frac{\partial^\sigma g}{\partial y^\sigma}, t \right)_{t=1},$$

per consegüent, transformacions que *depenen exactament de σ derivades de funcions arbitràries*. Segons (18), la identitat es dóna en això per a $g(y) = 0$; i la propietat de grup se segueix del fet que el procés indicat proporciona *cada transformació $x = y + g(y)$* , per la qual cosa la induïda de u queda unívocament determinada; per tant, el grup $\mathfrak{G}$ queda completat.

Com a producte col·lateral del recíproc encara se segueix que no representa cap restricció suposar que les funcions arbitràries només depenguin de x , no de u , $\frac{\partial u}{\partial x}, \dots$. A saber, en el darrer cas, en la transformació idèntica (14), per tant també en (15), a més de les $p^{(\lambda)}$, també hi intervenen $\frac{\partial p^{(\lambda)}}{\partial u}, \frac{\partial p^{(\lambda)}}{\partial \frac{\partial u}{\partial x}}, \dots$. Si ara se suposen les $p^{(\lambda)}$ successivament

de grau zero, primer, $\dots$, en u , $\frac{\partial u}{\partial x}$, $\dots$ amb funcions arbitràries de x com a coeficients, aleshores es reobtenen les dependències (16) només en un nombre més alt; però que segons el recíproc de més amunt es poden remetre als casos precedents per composició amb funcions arbitràries dependents només de x . De la mateixa manera es pot mostrar que l'ocurrència simultània de dependències i de relacions de divergència independents es corresponen amb els grups mixtos ²¹⁾.

²¹⁾ Com en §3, aquí també se segueix a partir del recíproc que, juntament amb I , també cada integral I^* que difereixi en una integral sobre una divergència de la mateixa manera representa un grup infinit amb el mateix $\bar{\delta}u$ encara que Δx i Δu estaran contingudes en derivades generals de u . Una integral I^* com aquesta ha estat introduïda per EINSTEIN en la teoria de la relativitat general, a fi d'obtenir una formulació més senzilla de les lleis de l'energia; per a indicar les transformacions infinitesimals que admet aquesta I^* em limito exactament a la notació de la segona nota de KLEIN. La integral

$$I = \sum \dots \sum K d\omega = \int \dots \int \mathfrak{K} dS$$

admet el grup de totes les transformacions de w i d'aquesta manera les induïdes per les $g_{\mu\nu}$; els corresponen les dependències ((30) segons KLEIN):

$$\sum \mathfrak{K}_{\mu\nu} g_{\tau}^{\mu\nu} + 2 \sum \frac{\partial g^{\mu\nu} \mathfrak{K}_{\mu\tau}}{\partial w^{\sigma}} = 0.$$

Ara esdevé: $I^* = \int \dots \int \mathfrak{K}^*$, on $\mathfrak{K}^* = \mathfrak{K} + \text{Div}$, i en conseqüència esdevé: $\mathfrak{K}_{\mu,\nu}^* = \mathfrak{K}_{\mu,\nu}$, on $\mathfrak{K}_{\mu\nu}^*$, $\mathfrak{K}_{\mu\nu}$ denoten en cada cas expressions lagrangianes. Per tant, les dependències indicades també ho són per a $\mathfrak{K}_{\mu\nu}^*$; i després de multiplicació per p^{τ} i addició s'obté

$$\sum \mathfrak{K}_{\mu\nu} p^{\mu\nu} + 2 \text{Div} \left(\sum g^{\mu\sigma} \mathfrak{K}_{\mu\tau} p^{\tau} \right) = 0;$$

$$\delta \mathfrak{K}^* + \text{Div} \left(\sum 2g^{\mu\sigma} \mathfrak{K}_{\mu\tau} p^{\tau} - \frac{\partial \mathfrak{K}^*}{\partial g_{\sigma}^{\mu\nu}} p^{\mu\nu} \right) = 0,$$

§5. Invariància de cadascun dels components de les relacions

Si s'especialitza el grup $\mathfrak{G}$ al cas considerat més senzill i habitual, en què no es permet cap derivada de u en les transformacions, i en què les variables independents transformades només depenen de x i no de u , aleshores es pot concloure la invariància de cadascun dels components en les fórmules. Segons conclusions conegudes, s'obté primerament la invariància de $\int \cdots \int (\sum \psi_i \delta u_i) dx$; per tant, la invariància relativa de $\sum \psi_i \delta u_i$ ²²⁾, en la qual δ s'entén com una variació arbitrària. A saber, d'una banda es té que

$$\begin{aligned} \delta I &= \int \cdots \int \delta f \left(x, u, \frac{\partial u}{\partial x}, \dots \right) dx = \\ &= \int \cdots \int \delta f \left(y, v, \frac{\partial v}{\partial y}, \dots \right) dy, \end{aligned}$$

en aplicar les transformacions de la diferenciació del producte en sentit invers. Per comparació amb l'equació diferencial de LIE, $\delta \mathfrak{K}^* + \text{Div}(\mathfrak{K}^* \Delta w) = 0$, d'això se segueix que

$$\Delta w^\sigma = \frac{1}{\mathfrak{K}^*} \cdot \left(\sum 2g^{\mu\sigma} \mathfrak{K}_{\mu\tau} p^\tau - \frac{\partial \mathfrak{K}^*}{\partial g_\sigma^{\mu\nu}} p^{\mu\nu} \right);$$

$$\Delta g^{\mu\nu} = p^{\mu\nu} + \sum g_\sigma^{\mu\nu} \Delta w^\sigma$$

com a transformacions infinitesimals admeses per a I^* . Per tant, aquestes transformacions infinitesimals depenen de la primera i segona derivades de $g^{\mu\nu}$, i contenen les p funcions arbitràries fins a la primera derivada.

²²⁾ És a dir, $\sum \psi_i \delta u_i$ es contreu, per transformació, a un factor, la qual cosa, en la teoria algebraica d'invariants, sempre es designa com una invariància relativa.

d'altra banda, es correspon amb

$$\int \cdots \int \delta f \left(x, u, \frac{\partial u}{\partial x}, \dots \right) dx = \int \cdots \int (\sum \psi_i(u, \dots) \delta u_i) dx;$$

$$\int \cdots \int \delta f \left(y, v, \frac{\partial v}{\partial x}, \dots \right) dy = \int \cdots \int (\sum \psi_i(v, \dots) \delta v_i) dy,$$

per a $\delta u, \delta \frac{\partial u}{\partial x}, \dots$ diferents a la vora, les quals per causa de les transformacions homogènies lineals de $\delta u, \delta \frac{\partial u}{\partial x}, \dots$ també $\delta v, \delta \frac{\partial v}{\partial y}, \dots$ [són] diferents a la vora; se segueix que

$$\begin{aligned} \int \cdots \int (\sum \psi_i(u, \dots) \delta u_i) dx &= \int \cdots \int (\sum \psi_i(v, \dots) \delta v_i) dy = \\ &= \int \cdots \int (\sum \psi_i(v, \dots) \delta v_i) \left| \frac{\partial y_i}{\partial x_\kappa} \right| dx. \end{aligned}$$

per a $\delta u, \delta \frac{\partial u}{\partial x}$ diferents a la vora. Si a la tercera integral $y, v, \delta v$ s'expressen per mitjà de $x, u, \delta u$, i s'iguala a la primera, s'obté una relació

$$\int \cdots \int (\sum \chi_i(u, \dots) \delta u_i) dx = 0$$

que s'anul·la a la vora, altrament δu [seria] arbitrari, i, com és ben sabut, d'aquí se segueix l'anul·lació de l'integrand per a δu qualsevol; *per tant, se satisfà la relació*

$$\sum \psi_i(u, \dots) \delta u_i = \left| \frac{\partial y_i}{\partial x_\kappa} \right| (\sum \psi_i(v, \dots) \delta v_i),$$

idènticament en δu , la qual posa de manifest la invariància relativa de $\sum \psi_i \delta u_i$ i en conseqüència la invariància de

$$\int \cdots \int (\sum \psi_i \delta u_i) dx \quad {}^{23}).$$

A fi d'aplicar això a les relacions de divergència i d'independència que se'n deriven, cal demostrar, primerament, que la $\bar{\delta}u$ que es deriva de Δu , Δx satisfà efectivament les lleis de transformació per a la variació δu , tan bon punt el paràmetre, respectivament les funcions arbitràries en $\bar{\delta}v$, pugui ésser determinat de manera que es correspongui amb el grup anàleg de transformacions infinitesimals en y , v . Si $\mathfrak{T}_q$ denota la transformació que porta x , u sobre y , v ; $\mathfrak{T}_p$ una infinitesimal en x , u , aleshores la semblant a això en y ,

²³⁾ Aquestes conclusions fan fallida quan y també depèn de u , atès que aleshores $\delta f \left(y, v, \frac{\partial v}{\partial y}, \dots \right)$ conté també termes $\sum \frac{\partial f}{\partial y} \delta y$, per tant, la transformació de la divergència no condueix a l'expressió lagrangiana; el mateix si es permeten derivades de u ; a saber, aleshores les δv esdevenen combinacions lineals de δu , $\delta \frac{\partial u}{\partial x}$, $\dots$, per tant, condueixen justament després d'una altra transformació de la divergència a una identitat $\int \cdots \int (\sum \chi_i(u, \dots) \delta u) dx = 0$, de manera que en conseqüència no apareixen expressions lagrangianes.

La pregunta sobre si a partir de la invariància de $\int \cdots \int (\sum \psi_i \delta u_i)$ també es pot concloure la de les que surten a partir de les relacions de divergència ja establertes és equivalent, segons el recíproc, a si d'aquesta invariància de I es pot concloure, sobre un grup, que no necessàriament condueix a les mateixes Δu , Δx , sinó a la mateixa $\bar{\delta}u$. En el cas especial d'integrals simples i únicament primeres derivades en f , a partir de la invariància de les expressions lagrangianes es pot concloure en el cas de grups finits l'existència d'integrals primeres (cf. per exemple, ENGEL, Gött. Nachr. 1916, p. 270).

v és donada per $\mathfrak{T} = \mathfrak{T}_q \mathfrak{T}_p \mathfrak{T}_q^{-1}$, on el paràmetre, respectivament les funcions arbitràries r , es determina a partir de p i q . Això s'expressa en les fórmules d'aquesta manera:

$$\mathfrak{T}_p : \xi = x + \Delta x(x, p);$$

$$u^* = u + \Delta u(x, u, p);$$

$$\mathfrak{T}_q : y = A(x, q);$$

$$v = B(x, u, q);$$

$$\mathfrak{T}_q \mathfrak{T}_p : \eta = A(x + \Delta x(x, p), q);$$

$$v^* = B(x + \Delta x(p), u + \Delta u(p), q).$$

Però d'això en resulta que $\mathfrak{T}_r = \mathfrak{T}_q \mathfrak{T}_p \mathfrak{T}_q^{-1}$, per tant,

$$\eta = y + \Delta y(r); \quad v^* = v + \Delta v(r),$$

en què per mitjà de la inversa de $\mathfrak{T}_q$ es considera x com a funció de y i únicament es tenen en compte els termes infinitesimals; per tant, es té la identitat

$$(20) \quad \eta = y + \Delta y(r) = y + \sum \frac{\partial A(x, q)}{\partial x} \Delta x(p);$$

$$\begin{aligned} v^* &= v + \Delta v(r) = \\ &= v + \sum \frac{\partial B(x, u, q)}{\partial x} \Delta x(p) + \sum \frac{\partial B(x, u, q)}{\partial u} \Delta u(p). \end{aligned}$$

Si aquí se substitueix $\xi = x + \Delta x$ per $\xi - \Delta \xi$, per la qual cosa també ξ de nou s'aplica novament en x , i també Δx s'anul·la, aleshores segons la primera fórmula (20) η també s'aplica novament en $y = \eta - \Delta \eta$; si per mitjà d'aquesta substitució $\Delta u(p)$ [s'aplica] en $\bar{\delta} u(p)$, aleshores també

$\Delta v(r)$ [s'aplica] en $\bar{\delta}v(r)$, i la segona fórmula (20) proporciona

$$v + \bar{\delta}(y, v, \dots, r) = v + \sum \frac{\partial B(x, u, q)}{\partial u} \bar{\delta}u(p),$$

$$\bar{\delta}v(y, v, \dots, r) = \sum \frac{\partial B}{\partial u_\kappa} \bar{\delta}u_\kappa(x, u, p),$$

de manera que, efectivament, també se satisfan les fórmules de transformació per a variacions tan bon punt com $\bar{\delta}v$ és pres dependent del paràmetre, respectivament de r funcions arbitràries ²⁴⁾.

Per tant, en particular, se segueix la invariància relativa de $\sum \psi_i \bar{\delta}u_i$; per tant, també, segons (12), la invariància relativa de $\text{Div} B$, atès que les relacions de divergència també són satisfetes en y, v ; i també, segons (14) i (13), la invariància relativa de $\text{Div} \Gamma$ i del costat esquerre de les dependències de les formades amb les $p^{(\lambda)}$, on sempre en les fórmules transformades les $p(x)$ arbitràries (respectivament, el paràmetre) són substituïdes per les r . D'això se segueix encara la invariància relativa de $\text{Div}(B - \Gamma)$, per tant, d'una divergència d'un sistema de funcions $B - \Gamma$, que no s'anul·la idènticament, la divergència del qual s'anul·la idènticament.

En el cas de dimensió 1 i de grup finit, a partir de la invariància relativa de $\text{Div} B$ encara es pot concloure la invariància de la primera integral. Segons (20), la transformació infinitesimal corresponent a la transformació paramètrica

²⁴⁾ De nou, això mostra que, a fi que valguin les conclusions, y ha d'ésser pres independent de u , etcètera. Com a exemple, siguin donades tal vegada les anomenades per KLEIN $\delta g^{\mu\nu}$, δq_ρ , que satisfan les transformacions per a les variacions tan bon punt les p estan subjectes a una transformació vectorial.

esdevé lineal homogènia, i per causa de la invertibilitat de totes les transformacions els ε també esdevenen lineals i homogenis en els paràmetres transformats ε^* . Aquesta invertibilitat certament es preserva quan es posa $\psi = 0$, atès que a (20) no hi entra cap derivada de u . Per tant, en igualar els coeficients de ε^* en

$$\text{Div} B(x, u, \dots, \varepsilon) = \frac{dy}{dx} \cdot \text{Div} B(y, v, \dots, \varepsilon^*)$$

també $\frac{d}{dy} B^{(\lambda)}(y, v, \dots)$ esdevenen funcions lineals i homogènies de $\frac{d}{dx} B^{(\lambda)}(x, u, \dots)$, de manera que a partir de

$$\frac{d}{dx} B^{(\lambda)}(x, u, \dots) = 0$$

o bé

$$B^{(\lambda)}(x, u, \dots) = \text{const}$$

també se segueix que

$$\frac{d}{dy} B^{(\lambda)}(y, v, \dots) = 0$$

o bé

$$B^{(\lambda)}(y, v, \dots) = \text{const.}$$

Per tant, les ϱ primeres integrals que corresponen en cada instància a $\mathfrak{G}_\varrho$ admeten el grup, de tal manera que també se simplifica la integració posterior. L'exemple més senzill d'això és que f sigui lliure de x o d'un u , la qual cosa correspon a la transformació infinitesimal $\Delta x = \varepsilon$, $\Delta u = 0$, respectivament $\Delta x = 0$, $\Delta u = \varepsilon$. Esdevé $\bar{\delta}u = -\varepsilon \frac{du}{dx}$, respectivament ε , i atès que B es deriva de f i $\bar{\delta}u$ per

diferenciació i lligams racionals, per tant també és lliure de x , respectivament u , i admet els grups corresponents ²⁵⁾.

§6. Una afirmació de Hilbert

Finalment, del que precedeix encara es conclou la demostració, i certament en una formulació generalitzada de la teoria de grups, d'una afirmació de HILBERT sobre el lligam entre la fallida de les lleis pròpies de l'energia amb la "relativitat general" (primera nota de KLEIN, Göttinger Nachr. 1917, Antwort, 1. Absatz).

Si la integral I admet un $\mathfrak{G}_{\infty\varrho}$, sigui $\mathfrak{G}_\sigma$ un grup finit qualsevol obtingut per mitjà d'especialitzacions de funcions arbitràries, per tant, un subgrup de $\mathfrak{G}_{\infty\varrho}$. Aleshores, al grup infinit $\mathfrak{G}_{\infty\varrho}$ li corresponen dependències (16), al [grup] finit $\mathfrak{G}_\sigma$, relacions de divergència (13); i recíprocament, a partir de qualsevol relació de divergència que subsisteix se segueix la invariància de I enfront d'un grup finit que és idèntic a $\mathfrak{G}_\sigma$ si, i només si, les $\bar{\delta}u$ s'expressen com a combinació lineal de les que s'obtenen de $\mathfrak{G}_\sigma$. Per tant, la invariància respecte de $\mathfrak{G}_\sigma$ no pot conduir a cap de les relacions de divergència diferents de (13). Però atès

²⁵⁾ En els casos en què ja a partir de la invariància de $\int(\sum \psi_i \delta u_i) dx$ se segueix l'existència d'integrals primeres, aquestes no admeten tot el grup $\mathfrak{G}_\varrho$; per exemple, $\int(u'' \delta u) dx$ admet la transformació infinitesimal $\Delta x = \varepsilon_2$; $\Delta u = \varepsilon_1 + x \varepsilon_3$; mentre que la integral primera $u - u'x = \text{const}$, que correspon a $\Delta x = 0$, $\Delta u = x \varepsilon_3$, no admet les altres dues transformacions infinitesimals, atès que conté explícitament tant u com x . Les transformacions infinitesimals per a f que corresponen a aquesta integral primera contenen derivades. Per tant, es veu que la invariància de $\int \cdots \int (\sum \psi_i du_i) dx$ en cada cas aporta menys que la invariància de I , la qual cosa s'ha de remarcar en relació amb la pregunta formulada en una observació precedent.

que a partir de la subsistència de (16) se segueix la invariància de I respecte de les transformacions infinitesimals Δu , Δx de $\mathfrak{G}_{\infty\varrho}$ per a $p(x)$ *arbitrari*, en particular d'això ja se segueix la invariància respecte de les transformacions infinitesimals de $\mathfrak{G}_\sigma$ obtingudes per especialització i, en conseqüència, respecte de $\mathfrak{G}_\sigma$. Per tant, les relacions de divergència $\sum \psi_i \bar{\delta} u_i^{(\lambda)} = \text{Div} B^{(\lambda)}$ han d'ésser conseqüència de les relacions de dependència (16), les darreres de les quals es poden escriure com $\sum \psi_i a_i^{(\lambda)} = \text{Div} \chi^\lambda$, on les $\chi^{(\lambda)}$ són combinacions lineals d'expressions lagrangianes i les seves derivades. Atès que ψ intervé linealment tant en (13) com en (16), llavors les relacions de divergència han d'ésser, en particular, combinacions *lineals* de les dependències (16); d'acord amb això, $\text{Div} B^{(\lambda)} = \text{Div}(\sum \alpha \chi^{(\kappa)})$; i les mateixes $B^{(\lambda)}$ es componen, per tant, linealment en les χ , és a dir, en les expressions lagrangianes i les seves derivades, i de funcions les divergències de les quals s'anul·len idènticament, com el $B - \Gamma$ trobat al final de §2 per al qual $\text{Div}(B - \Gamma) = 0$, i on al mateix temps la divergència té la mateixa propietat d'invariància. Denominaré les relacions de divergència respecte de les quals les $B^{(\lambda)}$ s'expressen per relacions lagrangianes i les seves derivades de la forma especificada com a “impròpies”, tota la resta, com a “pròpies.”

Si, recíprocament, les relacions de divergència són combinacions lineals de les dependències (16), i per tant, “impròpies,” la invariància respecte de $\mathfrak{G}_\sigma$ se segueix d'aquella respecte de $\mathfrak{G}_{\infty\varrho}$; $\mathfrak{G}_\sigma$ esdevé un subgrup de $\mathfrak{G}_{\infty\varrho}$. *Les relacions de divergència que corresponen a un grup finit $\mathfrak{G}_\sigma$ seran, llavors, impròpies si, i només si, $\mathfrak{G}_\sigma$ és un subgrup d'un grup infinit invariant respecte de I .*

Per especialització dels grups, això proporciona l’afirmació original de HILBERT. Entengui’s que “grup de desplaçaments” significa el grup finit

$$y_i = x_i + \varepsilon_i; \quad v_i(y) = u_i(x);$$

això és

$$\Delta x_i = \varepsilon_i, \quad \Delta u_i = 0, \quad \bar{\delta} u_i = - \sum_{\lambda} \frac{\partial u_i}{\partial x_{\lambda}} \varepsilon_{\lambda}.$$

La invariància respecte del grup de desplaçaments afirma, com sabem, que en

$$I = \int \cdots \int f \left(x, u, \frac{\partial u}{\partial x} \cdots \right) dx$$

les x no apareixen explícitament en f . Ens referirem a les n relacions de divergència associades

$$\sum \psi_i \frac{\partial u_i}{\partial x_{\lambda}} = \text{Div} B^{(\lambda)} \quad (\lambda = 1, 2, \dots, n)$$

com a “relacions d’energia,” ja que les “lleis de conservació” $\text{Div} B^{(\lambda)} = 0$ que corresponen al problema de variació corresponen a “lleis de conservació d’energia,” i els $B^{(\lambda)}$ als “components d’energia.” Per tant, se satisfà que: *Si I admet el grup de desplaçaments, aleshores les relacions d’energia esdevenen impròpies si, i només si, I és invariant respecte d’un grup infinit que conté com a subgrup el grup de desplaçaments* ²⁶⁾.

²⁶⁾ Les lleis de conservació d’energia de la mecànica clàssica així com les de la “teoria de la relativitat” antiga (on $\sum dx^2$ s’aplica sobre si mateix) són “pròpies,” ja que no hi apareixen grups infinits.

Un exemple de tals grups infinits es presenta per al grup de *totes* les transformacions de les x i de les transformacions induïdes de les $u(x)$ en les quals només apareixen *derivades* de les funcions arbitràries $p(x)$; el grup de desplaçaments s'obté per l'especialització $p^{(i)} = \varepsilon_i$; però restarà per decidir si aquest —i els grups generats per canvi de I per una integral de contorn— són suficients per a donar el més general d'aquests grups. Transformacions induïdes del tipus especificat sorgeixen, diguem, quan les u estan subjectes a les transformacions de coeficients d'una “forma diferencial total,” és a dir, una forma $\sum ad^\lambda x_i + \sum bd^{\lambda-1} x_i dx_\kappa + \dots$ que contingui diferencials superiors més enllà de les dx ; transformacions induïdes més especials, en les quals els $p(x)$ apareixen en només la primera derivada, són proporcionades per les transformacions de coeficients de formes diferencials ordinàries $\sum c dx_{i_1} \cdots dx_{i_\lambda}$, i només aquestes han estat considerades ordinàriament.

Un altre grup del tipus especificat —un que, a causa de l'ocurrència del terme logarítmic, no pot ésser cap transformació de coeficients— és, diguem, el següent:

$$y = x + p(x); \quad v_i = u_i + \lg(1 + p'(x)) = u_i + \lg \frac{dy}{dx};$$

$$\Delta x = p(x); \quad \Delta u_i = p'(x)^{27}); \quad \bar{\delta} u_i = p'(x) - u'_i p(x).$$

Aquí les dependències (16) esdevenen

$$\sum_i \left(\psi_i u'_i + \frac{d\psi_i}{dx} \right) = 0,$$

²⁷⁾ D'aquestes transformacions infinitesimals, les finites es calculen pel mètode de retrocés donat al final de §4.

i les relacions impròpies d'energia

$$\sum_i \left(\psi_i u'_i + \frac{d(\psi_i + \text{const.})}{dx} \right) = 0.$$

Una integral invariant senzilla del grup és

$$I = \int \frac{e^{-2u_1}}{u'_1 - u'_2} dx.$$

La I més general és determinada per integració de l'equació diferencial de LIE

$$\bar{\delta}f + \frac{d}{dx}(f \cdot \Delta x) = 0$$

que, per substitució dels valors per Δx i $\bar{\delta}u$, suposat que s'assumeixi que f depèn només de les derivades primeres de les u , s'aplica en

$$\frac{\partial f}{\partial x} p(x) + \left\{ \sum \frac{\partial f}{\partial u_i} - \frac{\partial f}{\partial u'_i} u'_i + f \right\} p'(x) + \left\{ \sum \frac{\partial f}{\partial u''_i} \right\} p''(x) = 0$$

(idènticament en $p(x)$, $p'(x)$, $p''(x)$). Aquest sistema d'equacions té solucions ja per a dues funcions $u(x)$ que realment continguin les derivades, a saber,

$$f = (u'_1 - u'_2) \Phi \left(u_1 - u_2, \frac{e^{-u_1}}{u'_1 - u'_2} \right),$$

on Φ representa una funció arbitrària dels arguments especificats.

HILBERT enuncia la seva afirmació a fi i efecte que la fallida de lleis pròpies de conservació d'energia sigui un fet característic de la “teoria general de la relativitat.” Per tant, per tal que aquesta afirmació valgui en sentit literal,

la denominació “relativitat general” s’hauria de prendre en un sentit més ampli que l’usual, i estès també als grups dependents de n funcions arbitràries ²⁸⁾ que sorgirien.

Referències de l'article

Recollim totes juntes les referències citades en aquest article.

Engel, F.: Über die zehn allgemeinen Integrale der klassischen Mechanik. *Nachr. Ges. d. Wiss. Göttingen, Math.-Phys. Kl.* **17** (1916), p. 270–291.

Fokker, A. D.: De virtueele verplaatsingen van het elektromagnetische en van het zwaartekrachtsveld bij de toepassing van het variatiebeginsel van Hamilton. *Koninklijke Akademie van Wetenschappen te Amsterdam, Verslagen van de Gewone Vergaderingen der Wis- en Natuurkundige Afdeling*, **25** (1916–1917), p. 1067–1084. Traducció anglesa: The virtual displacements of the electromagnetic and of the gravitational field in applications of Hamilton’s variation principle. Comunicat en la sessió de l’Acadèmia de Ciències holandesa el 27 de gener de 1917. *Verslag d. Amsterdamer Akad.*, **19**, n. 8, (1917) p. 968–984.

Hamel, G.: Über die virtuellen Verschiebungen in der Mechanik. *Math. Ann.* **59** (1904), p. 416–434.

²⁸⁾ Això confirma, de nou, la correcció d’un comentari de KLEIN: que el terme “relativitat”, usual en física, s’ha de canviar per “invariància relativa a un grup.” (“Über die geometrischen Grundlagen der Lorentzgruppe,” *Jahrb. d. d. Math. Vereinig.* **19** (1910), p. 287, reimprès a *Phys. Zeitschrift*.)

Hamel, G.: Die Lagrange-Eulerschen Gleichungen der Mechanik. *Zeitschrift f. Math. u. Phys.* **50** (1904), p. 1–57.

Herglotz, G.: Über die Mechanik des deformierbaren Körpers vom Standpunkte der Relativitätstheorie. *Ann. d. Phys.* **341**, n. 13 (1911), p. 493–533.

Klein, F.: Über die geometrischen Grundlagen der Lorentzgruppe. *Jahrber. d. d. Math. Vereinig.* **19** (1910), p. 287.

Klein, F.: Zu Hilberts erster Note über die Grundlagen der Physik. *Nachr. Ges. d. Wiss. Göttingen, Math.-Phys. Kl.* **18** (1917), p. 469–482.

Klein, F.: Über die Differentialgesetze für die Erhaltung von Impuls und Energie in der Einsteinschen Gravitationstheorie. *Nachr. Ges. d. Wiss. Göttingen, Math.-Phys. Kl.* **19** (1918), p. 171–189.

Klein, F.: Über die Integralform der Erhaltungssätze und die Theorie der räumlich-geschlossenen Welt. *Nachr. Ges. d. Wiss. Göttingen, Math.-Phys. Kl.* **19** (1918), p. 394–423.

Kneser, A.: Kleinste Wirkung und Galileische Relativität. *Math. Zeitschrift* **2** (1918), p. 326–349.

Lie, S.: Grundlagen für die Theorie der unendlichen kontinuierlichen Transformationsgruppen. *Ber. d. K. Sächs. Ges. der Wissensch.* **43** (1891), p. 316–393.

Capítol 12

Deuring

L'article que traduïm a continuació és un dels treballs més importants de l'extensa i imaginativa producció de Deuring. Publicat l'any 1941, té per objectiu la determinació dels possibles tipus dels anells de multiplicadors dels cossos de funcions el·líptiques.

Aquest article, que porta més enllà recerques iniciades per Abel, Kronecker i Hasse, es produeix en un moment de transició en el desenvolupament de la teoria de nombres. La branca de l'anàlisi matemàtica dedicada a les funcions especials havia assolit un grau de maduresa remarcable. Així, en el decurs d'un segle, les funcions el·líptiques (i, més generalment, les funcions hiperel·líptiques i les funcions abelianes), les funcions theta, les funcions zeta, i les sèries L s'havien convertit en instruments de domini públic entre els estudiosos de l'aritmètica. Però, al mateix temps, l'àlgebra també havia evolucionat suficientment, fins al punt de poder començar a proporcionar resultats d'algebraïcitat de valors especials de funcions analítiques i d'intuir propi-

etats aritmètics dels cossos de nombres que en resulten. Però, per a avançar cap a resultats aritmètics més profunds (relatius a solucions d'equacions diofantines, lligats a fenòmens de ramificació, o en la línia d'alguns dels problemes de Hilbert —cf. la secció 3.7—) es pot dir que la teoria era, alhora, poc fina i massa complicada, i es féu palès que calia un canvi de paradigma. Dit d'una manera poc convencional, calia arriscar-se a desenvolupar una teoria de funcions “sense funcions”. D'aquest propòsit se n'encarregaria la geometria algebraica de la segona meitat del segle XX, sorgida del creuament del pensament germànic, abstracte (analític i algebraic), amb el pensament grecollatí, concret (geomètric) —però, com dirien alguns, això són figures d'un altre paner.

12.1 El concepte de multiplicador

Abans de passar a la descripció del treball de Deuring sobre els anells de multiplicadors dels cossos de funcions el·líptiques, presentarem breument el concepte de multiplicador, tal com s'entenia a l'època, abans i després de Deuring.

Com ja ha estat esmentat més amunt (cf. la secció 2.8, p. 73), un dels treballs fonamentals de Riemann és el publicat l'any 1857 [320] sobre les funcions abelianes. La idea de Riemann en aquest treball fou estendre els resultats d'Abel i de Jacobi sobre inversió d'integrals el·líptiques (cas de gènere $g = 1$), així com també els de Weierstrass sobre la inversió d'integrals hiperel·líptiques ($g = 2$), a la inversió d'integrals abelianes de gènere qualsevol. En considerar les

integrals que s'obtenen a partir d'una base de diferencials regulars d'una superfície de Riemann compacta de gènere g , esteses a una base de $2g$ camins associats als talls canònics d'aquella (una base de l'homologia), Riemann obté unes matrius complexes $\Omega \in M(g \times 2g, \mathbb{C})$. Les matrius de Riemann, però, no són pas arbitràries, en tant que, com ell ja posa de manifest, satisfan unes relacions que provenen, essencialment, de l'aparellament d'intersecció en homologia. D'aquesta manera, una matriu $\Omega \in M(g \times 2g, \mathbb{C})$ serà anomenada una matriu de Riemann si, i només si, existeix una matriu antisimètrica $C \in M(2g, \mathbb{Q})$ tal que

$$(a) \quad \Omega C \Omega^t = 0,$$

$$(b) \quad \sqrt{-1} \Omega C \bar{\Omega}^t \text{ és una matriu hermítica definida positiva.}$$

Hem indicat per Ω^t la transposada d'una matriu Ω i per $\bar{\Omega}$, la seva conjugada complexa.

De fet, en el treball de Riemann s'investiga la varietat jacobiana d'una corba complexa no singular (superfície de Riemann), que és el primer exemple de varietat abeliana. Frobenius i Lefschetz provarien més endavant que les propietats anteriors són necessàries i suficients a fi de poder fer una immersió mitjançant funcions theta de qualsevol tor complex en un espai projectiu.

A través de la seva relació amb Betti, els treballs de Riemann mereixerien la consideració dels matemàtics italians. L'any 1916, Scorza publicà un treball sobre matrius de Riemann i l'any 1929, Rosati en publicà un altre sobre el mateix tema. Segons Scorza, un multiplicador M d'una matriu de Riemann Ω és una matriu $M \in M(g, \mathbb{C})$ per a

la qual existeix una matriu $G \in M(2g, \mathbb{Q})$ tal que

$$M\Omega = \Omega G.$$

El conjunt D de tots els multiplicadors M de Ω és una àlgebra associativa sobre el cos dels racionals. S'anomena l'àlgebra de multiplicadors de Ω . En particular, si totes les matrius no nul·les M són invertibles, D és un cos no commutatiu que té per centre un cos de nombres. En general, quan Ω és simple com a matriu de Riemann (pura, en la terminologia clàssica), és a dir, no descompon en suma directa de matrius de Riemann, l'àlgebra de multiplicadors esdevé una àlgebra simple. Quan aquesta àlgebra deixa de ser l'àlgebra de matrius sobre el cos dels racionals —que és el cas més freqüent—, ens trobem davant de fenòmens de “multiplicació complexa” —però ara, provinents del context de les varietats abelianes.

El problema principal en l'estudi de les matrius de Riemann consistí a, donada una matriu de Riemann, determinar l'àlgebra de multiplicadors que li correspon. La resolució del problema sobre $\mathbb{C}$ és de l'any 1934 i és deguda a Albert. En la resolució d'aquest problema hi jugà un paper decisiu la descoberta per part de Rosati de les involucions positives que aquestes àlgebres posseeixen.

La teoria de les matrius de Riemann estimulà l'interès per la caracterització de les classes d'isomorfia de les àlgebres simples que es poden definir sobre un cos de nombres donat i, molt especialment, el resultat que tota àlgebra simple i central sobre un cos de nombres és cíclica. Aquests problemes serien resolts per Artin, Brauer, Hasse, E. Noether i Albert, al mateix temps que es provaven els teoremes fonamentals de la teoria global de cossos de classes,

tal com s'ha exposat en la secció 3.8, relativa a l'àlgebra no commutativa.

Quan Hasse, primer, i Deuring, després, hagueren de fer front al repte de traslladar les consideracions anteriors a cossos de funcions abstractes (per tant, sense mètodos transcendents), calgué refer la noció de multiplicador de manera que fos independent dels períodes de les integrals. El mètode de Hasse i de Deuring consistí a reobtenir primer la teoria dels multiplicadors en el camp complex mitjançant altres recursos, que fossin traslladables posteriorment a qualsevol cos algebraicament tancat, de característica qualsevol.

Hasse i Deuring referen la teoria dels multiplicadors en termes de correspondències sobre els cossos de funcions abstractes i amb el suport del teorema de Riemann-Roch, que ja havia estat traslladat a característica positiva per F.K. Schmidt. En el cas clàssic, la teoria de correspondències havia estat introduïda per Hurwitz i treballada per Scorza i Severi, entre d'altres. Hasse i Deuring l'adaptaren a les seves necessitats. Més endavant, les consideracions de Hasse i de Deuring s'interpretarien en termes de la varietat jacobiana de les corbes, que, com és avui ben sabut, és una varietat abeliana de dimensió igual al gènere de la corba. Les correspondències d'una corba (cos de funcions abstracte) es llegeixen avui com els endomorfismes de la seva jacobiana. L'àlgebra dels multiplicadors de la corba és l'àlgebra de les isogènies de la jacobiana de la corba en si mateixa; l'anell dels multiplicadors és donat per l'anell dels seus endomorfismes. La noció de multiplicador clàssica, mitjançant matrius complexes o racionals, respon a representacions matricials de les àlgebres anteriors. En el

cas complex, la representació és fidel, però això no és així en el cas general. Tal com veurem, el treball de Deuring conté, a més de les representacions racionals i complexes dels multiplicadors, representacions ℓ -àdiques i p -àdiques, que són les que li permeten caracteritzar, en el cas de dimensió 1, els anells de multiplicadors dins de les àlgebres.

Totes aquestes consideracions trobarien una de les seves realitzacions més naturals en les àlgebres de multiplicadors dels cossos de funcions modulars, conegudes avui com a àlgebres de Hecke, que tenen l'atractiu impagable que tots els càlculs s'hi poden fer explícits i que han estat clau per a la demostració de la conjectura de Hasse-Weil dels cossos de funcions el·líptiques (cf. la secció 3.12).

Deuring treballa amb cossos de funcions el·líptiques abstractes, tal com ja també ho havia fet i ho feia Hasse. Per a aquests autors, les constants no cal que siguin nombres complexos sinó que pertanyen a un cos k que pot ser, fins i tot, de característica positiva —en una generalització fantàstica de les congruències, de Gauss, o de les congruències superiors, de Dedekind— i no sempre algebraicament tancat. En el llenguatge actual, nosaltres parlem de cossos de funcions de corbes el·líptiques. Si bé ni Hasse ni Deuring (ni tampoc Artin) parlen encara de corbes, és palès que en els seus cossos de funcions trobem els primers exemples d'unes funcions i d'uns divisors que transformen la seva natura i amplien (o redueixen, segons com es miri) la seva raó de ser.

12.2 1941: Aportacions a la teoria de la multiplicació complexa

Arran d'una segona demostració de la hipòtesi de Riemann per a cossos de funcions el·líptiques, Hasse havia provat, l'any 1936, i en la sèrie de tres treballs [185], [186], [187], que la classe d'isomorfia de l'àlgebra de multiplicadors $\text{End}(E|k) \otimes \mathbb{Q}$ d'una corba el·líptica E definida sobre un cos k algebraicament tancat pot ésser de tres tipus:

- (a) el cos $\mathbb{Q}$ dels nombres racionals;
- (b) un cos quadràtic imaginari; o bé
- (c) una àlgebra de quaternions definida.

Notem que avui la noció de multiplicador ha estat substituïda per la d'endomorfisme. El darrer tipus només pot tenir lloc quan el cos de constants k és de característica positiva, la qual cosa explica per què l'estructura corresponent no és present en els treballs pioners d'Abel sobre multiplicadors de diferencials el·líptiques de primera espècie (cf. la secció 2.5). Hasse i Deuring expressen els seus resultats en termes de cossos de funcions el·líptiques abstractes. La denominació d'abstractes obeeix a l'absència de veritables funcions de variable complexa, especialment quan la característica de k és positiva.

En el seu treball, Deuring va molt més enllà i determina l'estructura de l'anell $R = \text{End}(E|k)$. Aquesta estructura pot ser:

- (a) l'anell $\mathbb{Z}$ dels nombres enters;

- (b) un ordre d'un cos quadràtic imaginari el conductor del qual sigui primer amb la característica p del cos de funcions el·líptiques, on (p) , a més, és un ideal que descompon completament en el cos quadràtic de les multiplicacions; o bé
- (c) un ordre maximal de l'àlgebra de quaternions sobre $\mathbb{Q}$ de discriminant igual a $p\infty$.

A més, Deuring demostra que tots els casos anteriors es presenten. En els casos (b) i (c) l'invariant j de E és absolutament algebraic; és a dir, algebraic sobre el cos primer del cos k ; i, en el cas (c), és de grau ≤ 2 . La presència del tipus (c) també és condicionada al fet que en el grup de punts $E(k)$ no hi hagi classes de divisors d'ordre p , cas en què la corba el·líptica s'anomena supersingular i k és necessàriament un cos de característica p . Quan el cos de constants és el cos complex, l'invariant j no és cap altre que 1728 vegades el valor que pren la funció valència construïda per Dedekind en ser avaluada en el quocient d'una base de la xarxa de períodes (cf. la secció 8.1).

Per a la demostració d'aquests resultats, Deuring hagué de procedir a traduir resultats coneguts en característica zero a característica positiva. Paulatinament, es presentaren fenòmens lligats a la bona reducció de les corbes el·líptiques; i aquesta encara pot ésser ordinària o supersingular, segons hi hagi o no punts de p -torsió.

Dit així, el plantejament pot semblar molt natural i molt senzill. Però no ho és, ni de bon tros. Com que ni Hasse ni Deuring encara no utilitzaven el llenguatge geomètric —que ara hem fet servir amb tota naturalitat per a resumir el treball—, això implica que tampoc no podi-

en disposar de la intuïció geomètrica que aquest llenguatge proporciona.

De fet, tot el treball de Deuring tracta, com bé diu el títol, dels anells de multiplicadors dels *cosos de funcions el·líptiques*; i, encara, els considera sobre un cos de constants que no és necessàriament de característica zero, fet que fa més difícil la intuïció geomètrica dels resultats. Sovint, a més, suposa que el cos de constants és algebraicament tancat, de manera que tampoc no és un cos finit i ha de treballar, com a mínim, en una clausura algebraica d'aquest.

Per exemple, la definició d'invariant supersingular que dóna Deuring en el seu article es basa en les propietats de l'invariant j associat al cos de funcions el·líptiques K , que suposa que té cos de constants algebraicament tancat, k , i de característica positiva p . (En la nostra notació d'abans, K seria el cos de funcions $k(E)$ de la corba el·líptica $E|k$.) Aquest invariant $j(K)$ és supersingular si, a més de pertànyer a k , el cos K té multiplicació per una àlgebra de quaternions sobre $\mathbb{Q}$. Quan aquest és el cas, Deuring demostra que, obligatòriament, l'ordre és maximal, que l'àlgebra de quaternions només ramifica en p i ∞ , i que aquesta definició només depèn de $j(K)$, però no de K .

El fet que Deuring pugui parlar directament de l'invariant $j(K)$ independentment de K és equivalent al fet que actualment calgui demostrar que l'invariant j no correspon a la corba el·líptica individual, sinó només a la seva classe d'isomorfia.

Deuring va més enllà en les seves consideracions sobre els invariants supersingulats; ell mateix ja proporciona

l'equivalència de les dues definicions, en el llenguatge de l'època, quan prova el resultat següent (cf. més avall, a la p. 586).

Teorema. *Per a un invariant supersingular j de característica p , el cos el·líptic K d'invariant j no té cap classe de divisors d'ordre p .*

També val, recíprocament:

Si K no té cap classe de divisors d'ordre p , aleshores K té un ordre maximal de $Q_{\infty, p}$ com a anell de multiplicadors. L'invariant j corresponent és, per tant, supersingular.

Deuring pot parlar, doncs, dels invariants j supersingulars: són els elements de $\bar{k}$ que es corresponen amb les actuals classes d'isomorfisme de les corbes el·líptiques supersingulars.

Un altre dels resultats centrals de l'article de Deuring fa referència al fet que tots els invariants supersingulars en característica p són nombres algebraics absoluts sobre el cos primer $\mathbb{F}_p$, i que tots són de grau 1 o bé 2; és a dir, pertanyen a $\mathbb{F}_p$ o bé a $\mathbb{F}_{p^2}$, independentment de quin sigui el cos k de característica p considerat com a cos de constants. I, a més, si $j_0 \in \mathbb{F}_{p^2} - \mathbb{F}_p$ és un invariant supersingular, el seu altre conjugat galoisià també ho és.

Com a conseqüència, fixat un nombre primer p , només hi ha una quantitat finita d'invariants supersingulars en característica p , i té sentit que considerem el polinomi

$$ss_p(j) := \prod_{j_0 \text{ supersingular}} (j - j_0) \in \mathbb{F}_p[j],$$

que podem anomenar el polinomi supersingular en característica p . Notem que, de la seva definició es dedueix que aquest polinomi no té arrels múltiples.

Deuring també demostra que el nombre d'invariants supersingulars en característica p , o sigui, el grau del polinomi $ss_p(j)$, coincideix amb el nombre de classes de l'àlgebra de quaternions sobre $\mathbb{Q}$ que només ramifica en p i en ∞ ; i, per a aquest nombre, que prèviament havia calculat Eichler (cf. [109]), en dóna l'expressió (cf. més avall, p. 510)

$$h = \begin{cases} 1, & \text{per a } p = 2, \quad p = 3, \\ \frac{p-1}{12}, & \text{per a } p \equiv 1 \pmod{12}, \\ \frac{p-5}{12} + 1, & \text{per a } p \equiv 5 \pmod{12}, \\ \frac{p-7}{12} + 1, & \text{per a } p \equiv 7 \pmod{12}, \\ \frac{p-11}{12} + 2, & \text{per a } p \equiv 11 \pmod{12}. \end{cases}$$

Per a $p = 2$ i per a $p = 3$, l'únic invariant supersingular és $j = 0 = 1728$; en particular, els polinomis supersingulars en característica 2 i en característica 3 són

$$ss_2(j) = j \in \mathbb{F}_2[j], \quad ss_3(j) = j \in \mathbb{F}_3[j].$$

Per a $p \geq 5$, Deuring atribueix a Hasse (cf. [86], [183]) l'expressió següent per a un invariant A l'anul·lació del qual en un valor concret de j equival a dir que aquest valor de

j és supersingular (cf. més avall, p. 510):

$$A = \begin{cases} \Delta^{\frac{p-1}{12}} P(j), & \text{per a } p \equiv 1 \pmod{12}, \\ g_2 \Delta^{\frac{p-5}{12}} P(j), & \text{per a } p \equiv 5 \pmod{12}, \\ g_3 \Delta^{\frac{p-7}{12}} P(j), & \text{per a } p \equiv 7 \pmod{12}, \\ g_2 g_3 \Delta^{\frac{p-11}{12}} P(j), & \text{per a } p \equiv 11 \pmod{12}, \end{cases}$$

on g_2 i g_3 són els coeficients d'una equació de Weierstrass $y^2 = 4x^3 - g_2x - g_3$ definidora del cos K , $\Delta = g_2^3 - 27g_3^2$ és el discriminant, i $P(j)$ denota un polinomi de l'invariant j del qual Deuring diu, textualment, que “se sap com a mínim que el seu grau és com a màxim igual a l'exponent de la potència de Δ que el precedeix”. Deuring demostra que el polinomi $P(j)$ té efectivament el grau conjecturat per Hasse i, en conseqüència, que no té arrels múltiples, perquè el nombre d'arrels de A coincideix exactament amb el nombre de classes h .

No només això, Deuring també proporciona dues fórmules explícites per al càlcul de l'invariant A , invariant que, per cert, es coneix com a invariant de Hasse o, també, de Hasse-Witt. Les dues fórmules donen, en particular, una expressió concreta per al polinomi $P(j)$ que apareix a l'invariant de Hasse i estan donades en funció d'una equació de Weierstrass o de Legendre del cos de funcions el·líptiques.

Per la seva importància posterior, les reproduïm aquí (cf. més avall, p. 511):

En el cas que es disposi de l'equació de Weierstrass de més amunt,

$$A = \begin{cases} (-1)^{\frac{p-1}{4}} 3^{-\frac{p-1}{4}} \Delta^{\frac{p-1}{12}} & \left(\frac{p-1}{2}\right)! \Phi_p(j), \\ 2^2 (-1)^{\frac{p-1}{4}} 3^{-\frac{p-5}{4}} \Delta^{\frac{p-5}{12}} & g_2 \left(\frac{p-1}{2}\right)! \Phi_p(j), \\ 2^4 (-1)^{\frac{p-3}{4}} 3^{-\frac{p-7}{4}} \Delta^{\frac{p-7}{12}} & g_3 \left(\frac{p-1}{2}\right)! \Phi_p(j), \\ 2^6 (-1)^{\frac{p-3}{4}} 3^{-\frac{p-11}{4}} \Delta^{\frac{p-11}{12}} & g_2 g_3 \left(\frac{p-1}{2}\right)! \Phi_p(j), \end{cases}$$

segons que sigui $p \equiv 1, 5, 7$ o bé $11 \pmod{12}$, i on

$$\Phi_p(j) = j^{\lfloor \frac{p}{12} \rfloor} \sum_{0 \leq i < \frac{p}{12}} \frac{\left(-\frac{4}{27}\right)^i (1 - 2^6 \cdot 3^3 \cdot j^{-1})^i}{(2i)! \left(\frac{p-1}{4} - 3i\right)! \left(\frac{p-1}{4} + i\right)!},$$

si $p \equiv 1 \pmod{4}$; i

$$\Phi_p(j) = j^{\lfloor \frac{p}{12} \rfloor} \sum_{0 \leq i < \frac{p}{12}} \frac{\left(-\frac{4}{27}\right)^i (1 - 2^6 \cdot 3^3 \cdot j^{-1})^i}{(2i+1)! \left(\frac{p-7}{4} - 3i\right)! \left(\frac{p+1}{4} + i\right)!},$$

si $p \equiv -1 \pmod{4}$.

En el cas que es disposi de la forma normal de Legendre $y^2 = x(x-1)(x-\lambda)$,

$$A = (-1)^{\frac{p-1}{2}} \sum_{i=0}^{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{i} \lambda^i, \quad \text{per a } p \geq 3,$$

on λ és una qualsevol de les sis arrels de

$$j = 2^8 \frac{(1 - \lambda(1 - \lambda))^3}{\lambda^2(1 - \lambda)^2}.$$

Notem que aquí es retroba l'expressió de l'invariant modular j que hem trobat en l'article de Dedekind de més amunt (cf. p. 309). Aquest fet fa palesa la importància que té aquesta fórmula, no només per a l'estudi dels mòduls singulars, com ja sospitava Dedekind, sinó també per al dels supersingulars. Posteriorment, la fórmula també seria interpretada com a definidora d'un recobriment entre corbes modulars.

Com a conseqüència d'aquest resultat de Deuring, i si tenim en compte que els valors de j que corresponen a $g_2 = 0$ i a $g_3 = 0$ són $j = 0$ i $j = 1728$, respectivament, s'obté una expressió explícita del polinomi supersingular $ss_p(j)$ que complementa les de més amunt per a $p = 2$ i $p = 3$.

Teorema. *sigui $p \geq 5$ un nombre primer. Llavors,*

$$ss_p(j) = j^\delta(j - 1728)^\varepsilon \Phi_p(j) \in \mathbb{F}_p[j],$$

on $\delta = 0$, si $p \equiv 1 \pmod{6}$, $\delta = 1$, si $p \equiv -1 \pmod{6}$, $\varepsilon = 0$, si $p \equiv 1 \pmod{4}$, $\varepsilon = 1$, si $p \equiv -1 \pmod{4}$, i el polinomi $\Phi_p(j)$, donat més amunt, no s'anul·la per a $j = 0$ ni per a $j = 1728$.

Notem que els polinomis $\Phi_p(j)$ són, de fet, polinomis de coeficients racionals p -enters, de manera que el polinomi $ss_p(j) \in \mathbb{F}_p[j]$ és la reducció mòdul p d'un polinomi explícit de coeficients racionals p -enters, proporcionat per Deuring.

A fi de facilitar la lectura del treball, per a qui ho desitgi, oferim un petit diccionari informal entre la terminologia emprada per Deuring i l'actual.

El cos de funcions el·líptiques K_0 sobre un cos de Galois k_0 es correspon al cos de funcions d'una corba el·líptica E definida sobre un cos finit k_0 . Els divisors primers de primer grau de k_0 es corresponen amb els punts de $E(k_0)$ diferents de l'infinit. Quan Deuring empra la notació K per al cos de funcions el·líptiques sol voler dir que ha tancat algebraicament el cos residual.

El multiplicador π és l'automorfisme de Frobenius. Més generalment, un multiplicador qualsevol és un endomorfisme de la corba. El tipus d'un cos de funcions el·líptiques és la seva classe d'isomorfia.

Quan Deuring parla d'un anell de multiplicadors complex es refereix a un ordre d'un cos quadràtic imaginari i el nombre de classes és l'habitual. Recordem que el nombre de classes d'una àlgebra de quaternions és donat pel nombre de classes d'ideals bilaterals d'un ordre maximal quan aquells es classifiquen segons $I = aJ$ (o bé $I = Ja$); si se segueix la primera classificació, les classes tindran ordres per la dreta associats, i per l'esquerra, si se segueix la segona. El nombre de tipus d'una àlgebra de quaternions és el nombre de classes d'isomorfia d'ordres maximals de l'àlgebra.

Una classe de divisors d'exponent p s'ha d'entendre com un punt de p -torsió de $E(k)$; és a dir, l'exponent del divisor correspon a l'ordre del punt.

L'invariant σ de Hasse no és cap altra cosa que l'altura del grup formal dels punts de p -divisió de E , on p és la característica del cos de constants de E . Així, $\sigma = 1$ correspon al cas ordinari i $\sigma = 2$, al cas supersingular; l'invariant de Hasse-Witt és, doncs, $2 - \sigma$, en tots els casos.

Per a les corbes el·líptiques en característica $p \neq 2$ es pot prendre la forma normal de Legendre. Però quan $p = 2$ cal treballar amb la forma normal dita de Deuring, tal com es fa en el treball, que és vàlida per a tot $p \neq 3$.

En el treball hi trobem no solament corbes amb cos de constants de característica p , sinó també fenòmens de reducció de característica zero a característica p (cf. Introducció 5). Els més típics es presentaran quan k sigui un cos de nombres i $\mathfrak{p}|p$, un ideal primer del seu anell d'enters. Deuring veu que els invariants j que són $\mathfrak{p}$ -enters es corresponen exactament amb les corbes el·líptiques —que avui en diríem— de bona reducció potencial. A més, l'invariant de la corba reduïda s'obté per reducció de l'invariant de la corba en característica zero. Quan Deuring parla d'una classe d'invariants d'un ordre complex, es refereix a una classe d'ideals de l'ordre la qual conté l'invariant de la corba el·líptica.

Per a Deuring, la notació $\overline{K}$ denota la reducció mòdul $\mathfrak{p}$ de K . Deuring pot reduir tant els punts com els endomorfismes. Entre els anells d'endomorfismes d'una corba i d'una reduïda, la reducció d'endomorfismes és injectiva, però no exhaustiva. Com es posarà extensament de manifest en el decurs del treball, la no-exhaustivitat d'aquesta reducció es dona, exactament, quan la corba el·líptica en característica zero té multiplicació complexa i p és inert o ramifica en el cos de la multiplicació; en aquest cas, la corba reduïda guanya endomorfismes i es converteix en una corba el·líptica amb multiplicació quaterniònica; alhora, aquest serà exactament el cas de reducció supersingular (en el sentit que, com que encara té més endomorfismes que la corba

de partida, que és d'invariant singular, la reduïda és *més singular*).

Deuring no solament és capaç de reduir (cf. Introducció 5, resultats 1), sinó que també ho és d'aixecar: donada una corba el·líptica $\overline{E}$ en característica p i un endomorfisme $\overline{\mu}$, Deuring proporciona un aixecament del parell $(\overline{E}, \overline{\mu})$ en característica zero (cf. Introducció 5, resultats 2).

A la secció §1 trobem un cos de funcions el·líptiques K de cos residual k algebraicament tancat i un divisor primer seleccionat $\mathfrak{o}$ que li serveix per a definir el que avui coneixem com una aplicació d'Abel–Jacobi. Així, a una classe C de divisors de grau zero, Deuring fa correspondre la classe $[\mathfrak{p}]$ del divisor primer $\mathfrak{p}$ que representa $\mathfrak{o}C$. Doncs, podem interpretar $[\mathfrak{p}]$ com un punt $P \in E(k)$ i $[\mathfrak{o}]$ com l'elecció d'un origen $P_0 \in E(k)$.

Els automorfismes de reflexió i de translació dels quals ens parla tot seguit són dos elements de $\text{Aut}(K|k)$. Notem que, en ser $K|k$ una extensió de grau de transcendència 1, els automorfismes esmentats poden ser o no d'ordre finit. D'acord amb Hasse, Deuring considera automorfismes de reflexió i de translació. Els automorfismes de reflexió són associats a parells $([\mathfrak{q}_1], [\mathfrak{q}_2])$ de classes de divisors primers. Els de translació ho són a la classe $[\mathfrak{q}]$ d'un divisor primer donat. Per a definir els primers, Deuring utilitza l'existència d'una funció z amb exactament dos pols simples (Riemann–Roch) i que, a més, $K|k(z)$ és una extensió quadràtica. Si mirem l'efecte d'aquests automorfismes sobre els punts en $E(k)$, tenim, en particular, que

$$\tau_{P_0, Q}(P) = P + Q, \quad \sigma_{P_0, P_0}(P) = -P.$$

Observem que, en general, ni $\tau_{P,Q}$ ni $\sigma_{P,Q}$ respecten la llei d'addició de $E(k)$.

Els multiplicadors μ provindran de les aplicacions regulars de E en E que respecten la llei d'addició de $E(k)$; és a dir, en el llenguatge d'avui, de les *isogènies* (aplicacions que respecten l'*origen*). Deuring parla de meromorfismes normats; aquí, el concepte de normat és precisament el que ens permet mirar el seu efecte sobre els punts. Atès que el nucli $\ker(\mu) \subset E(k)$ és finit, també són finites les extensions $K|K^\mu$ que Deuring considera. Es tracta d'extensions normals, però no necessàriament separables. L'ordre del nucli de μ és $N\mu/I_\mu$, on $N\mu$, I_μ denoten la norma i el grau d'inseparabilitat de μ , respectivament; és a dir, l'ordre del nucli és donat pel grau de separabilitat de l'extensió $K|K^\mu$. La fórmula amb què Deuring defineix la imatge $\mu[\mathfrak{p}]$,

$$\mu[\mathfrak{p}] = \left[(N_{K/K^\mu} \mathfrak{p})^{\mu-1} \right],$$

no és altra que la de P interpretat com un element de $E/\ker(\mu)$, atès que K^μ és el cos de funcions de la corba $E/\ker(\mu)$, isògena a la donada. També, $\mathfrak{q}^\mu$ es pot interpretar com $Q + \ker(\mu)$.

El grup de Galois de $K|K^\mu$ (així és com parla Deuring, però, de fet, es tracta del grup de Galois de K sobre la clausura purament inseparable $K^{\mu,\text{ins}}$ de K^μ dins de K) s'identifica amb el grup de translacions $\tau_{P_0,P}$ definides pels punts $P \in \ker(\mu)$; evidentment, doncs, $K|K^{\mu,\text{sep}}$ és una extensió abeliana. En particular, si n i p són coprims, l'extensió $K|K^n$ és de Galois i, per teoria de Kummer, el seu grup de Galois consta de totes les translacions definides per punts d'ordre un divisor de n ; és, doncs, isomorf a $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. En el cas en què $n = p^f$ sigui una potència

de la característica del cos de constants k , tindrem que el grup de Galois serà isomorf a $\mathbb{Z}/p^f\mathbb{Z}$ si $\sigma = 1$, és a dir, en el cas ordinari, i trivial, si $\sigma = 2$, és a dir, en el cas supersingular. En aquests darrers dos casos, la potència de p que divideix l'ordre del grup és $p^{2f-\sigma f}$ i, en la notació de Deuring, el grup és de tipus $(n/p^f, n/p^{\sigma f-f})$.

Deuring demostra que, per a tot cos el·líptic K_0 tal que $K \supseteq K_0 \supseteq k$, el grup de Galois de $K \supseteq K_0$ (en sentit ampli) és un grup de translacions finit. És a dir, és el cos de funcions d'una corba el·líptica isògena a la de partida. Per a això utilitza que $K|K_0$ és no ramificat, la qual cosa es pot veure fent servir la fórmula de Hurwitz.

Per a relacionar els multiplicadors de E amb els de E_0 , Deuring tria com a origen de E_0 la norma de P_0 ; és a dir, el punt de $E_0(k)$ donat per la suma dels punts conjugats de P_0 . Així, el multiplicador queda ben definit a nivell de classes de divisors (és a dir, de punts). Aquí hem de fer notar que per a ajustar-nos a la notació de Deuring, nosaltres hauríem hagut d'escriure la imatge d'un punt P per μ com $(P)\mu$.

El paràgraf s'acaba amb les relacions entre els anells $\text{End}(E)$ i $\text{End}(E_0)$. Deuring veu que un multiplicador de K ho és de K_0 si, i només si, deixa invariant el nucli de la isogènia.

A la secció §2 hi trobem una construcció molt interessant, des del punt de vista històric. Deuring representa fidelment els multiplicadors del cos el·líptic K per matrius 2×2 amb entrades enters q -àdics, $S_q(\mu)$ quan $q \neq p$, o per nombres enters p -àdics, $s_p(\mu)$, quan $q = p$ i estem en el cas ordinari. La representació l'obté en fer actuar els

multiplicadors en el *mòdul de Tate* prèvia elecció d'una base (rigidificació). Aquests es representen en el text per $\mathfrak{C}_q$ (el grup de les classes de K l'ordre de les quals és una potència d'un primer q). Fem notar, aquí, el lligam amb la conjectura de Tate i el teorema de Faltings. Aquestes representacions s'estenen a les àlgebres d'endomorfismes Σ i els elements dels anells d'endomorfismes, els ordres R , són, precisament, els que tenen per imatge matrius enteres. D'aquesta manera Deuring arriba a les estructures dels possibles ordres.

A la secció §3 Deuring treballa amb cossos el·líptics de cos de constants no necessàriament algebraicament tancat i es preocupa de qüestions de cossos de definició, tant de les corbes el·líptiques com dels endomorfismes. En aquest apartat trobem la representació de l'anell d'endomorfismes de la corba que s'obté en tenir en compte la seva acció sobre les diferencials; en el nostre cas, es tracta d'una representació de dimensió 1 sobre el cos de constants k ; per tant, a diferència del cas clàssic, no pot ser fidel en característica positiva.

A la secció §4 conté el tema de les reduccions, que ja hem esmentat abans. Des d'un punt de vista tècnic, aquest és potser el paràgraf més difícil. Per a procedir a la reducció dels multiplicadors de característica zero a característica positiva, Deuring necessita treballar amb la noció de multiplicador entesa com una correspondència. Aquí fa ús de la teoria que ell mateix desenvolupà en dos articles bàsics que precediren al que ara comentem; es tracta dels publicats a la *Revista de Crelle* els anys 1937 i 1941 ([83], [85]). Un multiplicador de K en un cos isomorf K^φ és donat per una correspondència de K en K^φ , i aquesta ho és per una

classe de divisors de $KK^\varphi|K$. En les tres situacions ha de controlar que les operacions d'addició i de multiplicació són preservades i que factoritzen bé en els quocients. A més, per a procedir a l'operació de reducció li calen prèviament models locals enters. Això l'obliga a treballar amb dos conceptes de divisors, un que procedeix de la geometria, i es formula en termes de punts, i l'altre que procedeix de l'àlgebra, i es formula en termes de valoracions. Amb això aconsegueix demostrar que l'anell d'endomorfismes de K s'aplica segons un monomorfisme en el de $\overline{K}$. Després d'això està en condicions de deduir com es comporten per reducció mòdul p els punts de torsió.

A la secció §5 hi trobem el càlcul, en funció de l'invariant j de la corba el·líptica, del grup de les unitats R^* de l'anell d'endomorfismes. És en aquest paràgraf on trobem la forma normal de Deuring

$$y^2 - y + \alpha xy = x^3,$$

d'una corba el·líptica i el càlcul del seu invariant j , que satisfà $\alpha^3(\alpha^3 + 24)^3 + j(\alpha^3 + 27) = 0$. Deuring aconsegueix el càlcul de R^* en treballar amb la seva forma normal i amb la de Legendre.

A la secció §6 hi trobem la relació que satisfan els invariants j de dues corbes el·líptiques lligades per una isogènia cíclica de grau N , on es reconeixen els polinomis modulars Φ_N , definidors de les futures corbes modulars $X_0(N)$. Deuring tracta, també, com es comporten per reducció mòdul un primer p i la potència p^f d'un primer. D'aquesta manera generalitza congruències que eren conegudes per Kronecker quan $f = 1$. Calcula explícitament els polinomis Φ_2 i Φ_3 , que ja es troben en el tractat d'àlgebra de Weber. També

proporciona els primers termes de desenvolupaments de la funció j en sèries formals.

A la secció §7, i per estudi dels polinomis anteriors i de les seves reduccions, Deuring demostra que els invariants singulars, dels quals la teoria clàssica afirmava que són algebraics, són, de fet, nombres enters algebraics.

A la secció §8 Deuring calcula la llista dels polinomis supersingulars per a tots els primers $p < 100$, i en proporciona les arrels, que, com ja s'ha comentat, són, com a màxim, quadràtiques sobre el cos primer. Veu també que, per a cada classe d'isomorfia d'ordres maximals de l'àlgebra de quaternions de discriminant $p\infty$, existeix una corba el·líptica supersingular que té un d'aquells ordres com a anell d'endomorfismes.

A la secció §9 hi trobem els resultats d'aixecament d'endomorfismes que hem comentat abans. Hi demostra que, de manera similar al cas quaterniònic, ara tots els ordres quadràtics imaginaris es presenten com a anells d'endomorfismes, sempre que el seu conductor no sigui múltiple de p i p descompongui completament en el cos quadràtic.

La resta de seccions està dedicada a l'obtenció dels resultats quantitativs abans esmentats.

La llista de treballs que han sorgit directament o indirectament d'aquestes recerques de Deuring seria interminable, atès bàsicament que els seus resultats es pogueren estendre de dimensió 1 (que és el cas dels cossos de funcions el·líptiques, tractat per Deuring) a dimensió superior, en considerar la seva generalització a varietats abelianes (que sorgiren dels cossos abstractes de funcions abelianes i de l'expressió d'aquestes en termes de funcions theta).

Una possible recopilació comprendria una extensa producció relativa a fenòmens de l'aritmètica de les varietats abelianes (Lefschetz, Weil, Mumford), de reducció de varietats abelianes (Shimura–Taniyama, Serre–Tate, Grothendieck), punts de p -divisió i mòduls de Tate (Tate, Néron–Ogg–Shafarevich, Deligne), d'àlgebres d'endomorfismes d'aquestes varietats (Swinerton–Dyer, Ribet, Faltings), de multiplicitat d'intersecció de divisors (Gross–Zagier), així com també d'invariants de Hasse–Witt (Manin, Mazur–Katz, Berthelot). Com a curiositat, potser no és del tot inútil esmentar que, avui dia, la base de dades *MathSciNet*, de la Societat Matemàtica Americana (*American Mathematical Society*), ofereix gairebé 7.500 entrades sota la denominació “corba el·líptica”, 4.000 sota la denominació “varietat abeliana” i exactament dues referències d'autors que citen el treball de Deuring que ens ocupa.

Per a acabar, ens limitem a donar alguns detalls d'una ampliació d'aquest treball de Deuring realitzada a l'article [223].

Un cop els autors han introduït el polinomi supersingular en característica p , $ss_p(j)$, es plantegen com a problema donar polinomis canònics de $\mathbb{Q}[j]$ per als quals la reducció mòdul p tingui sentit i proporcionï $ss_p(j)$. Amb aquest objectiu, construeixen polinomis de tres maneres diferents i, així, obtenen:

- (a) polinomis que provenen de formes modulars;
- (b) els polinomis ortogonals d'Atkin; i
- (c) altres polinomis ortogonals que provenen de sèries hipergeomètriques.

Dels polinomis que provenen de formes modulars en donen quatre per a cada $p \geq 5$. Per a això, comencen per ensenyar com associar polinomis a formes modulars i, a continuació, es dediquen a construir quatre formes modulars, de les quals consideraran els polinomis associats.

Pel que fa als polinomis ortogonals d'Atkin, els autors els defineixen a partir del producte escalar d'Atkin, del qual donen fins a quatre descripcions diferents; això els permet donar, també, quatre descripcions diferents dels polinomis d'Atkin.

També proporcionen quatre polinomis diferents associats a sèries hipergeomètriques, la reducció mòdul p dels quals coincideix amb el polinomi supersingular.

L'article [223] conté demostracions autocontingudes de la majoria dels resultats que els autors utilitzen, de manera que aquesta exposició es pot pensar com una teoria sobre els invariants supersingulars.

Podríem dir que el Somni de Joventut de Kronecker ha derivat en unes "Variacions Zagier sobre un tema de Deuring".

ELS TIPUS D'ANELLS DE MULTIPLICADORS DELS COSSOS DE FUNCIONS ELLÍPTIQUES

Dedicat a G. HERGLOTZ en el seu 60è aniversari

per MAX DEURING

INTRODUCCIÓ

1. En una sèrie de treballs ¹⁾, H. HASSE ha desenvolupat de manera algebraica la teoria de la multiplicació de les funcions el·líptiques. Alhora, l'objectiu que ell perseguia principalment era demostrar la Hipòtesi de Riemann per a les funcions zeta de congruència de gènere 1 o bé, el que és aproximadament el mateix, l'afirmació següent sobre el nombre de solucions de congruències el·líptiques: *Sigui K_0 un cos de funcions el·líptiques sobre el cos de Galois k_0 de $q = p^f$ elements (p nombre primer). El nombre de divisors*

¹⁾ H. HASSE, Beweis des Analogons der Riemannschen Vermutung für die Artinschen und F. K. Schmidtschen Kongruenzetafunktionen in gewissen elliptischen Fällen, Nachr. Ges. d. Wiss. Göttingen, Math.-Phys. Kl. 1933, p. 253–262; 2. Abstrakte Begründung der komplexen Multiplikation und Riemannsche Vermutung in Funktionenkörpern, Abh. Math. Semin. Hamburg. Univ. **10**, p. 325–348 (1934); 3. Zur Theorie der abstrakten elliptischen Funktionenkörper, I Journ. f. d. r. u. ang. Math. **175**, p. 55–62, II, p. 69–88, III, p. 193–208 (1936). Una teoria més fàcil, a M. DEURING Arithmetische Theorie der Korrespondenzen algebraischer Funktionenkörper, I, Journ. f. d. r. u. ang. Math. **177**, p. 161–191 (1937), II **183**, p. 25–36 (1941).

primers de primer grau de K_0 o també, entesa $f(x, y) = 0$ com una equació definidora de K_0 , el nombre de solucions d'aquesta equació en k_0 augmentat amb el nombre d'ideals primers de primer grau que apareixen en el denominador de x o de y , és igual a la norma del multiplicador $\pi - 1$ de K_0 , on π és el multiplicador ²⁾ $z \rightarrow z^q$. Sembla que hagi passat per alt de l'atenció dels matemàtics que s'ocupen d'aquestes qüestions que aquest teorema sobre les congruències de gènere 1 ja era conegut per GAUSS, almenys en el cas excepcional de les funcions lemniscàtiques. Perquè l'última entrada en el diari de GAUSS no diu cap altra cosa, en tant que resa de la manera següent:

Observatio per inductionem facta gravissima theoriam residuorum biquadraticorum cum functionibus lemniscaticis elegantissime nectens. Puta si $a + bi$ est numerus primus, $a - 1 + bi$ per $2 + 2i$ divisibilis, multitudo omnium solutionum congruentiæ

$$1 \equiv xx + yy + xxyy \pmod{a + bi}$$

inclusis

$$x = \infty, \quad y = \pm i; \quad x = \pm i, \quad y = \infty$$

fit

$$= (a - 1)^2 + bb.$$

1814 Jul. 9. ³⁾

²⁾ Vegeu H. HASSE¹⁾, **3**, III, p. 206.

³⁾ (n. dels t.) Una observació molt difícil feta per inducció que relaciona d'una manera molt elegant la teoria dels residus biquadràtics amb les funcions lemniscàtiques. Si $a + bi$ és un nombre primer, $a - 1 + bi$ divisible per $2 + 2i$, la quantitat de totes les solucions de la congruència $1 \equiv xx + yy + xxyy \pmod{a + bi}$, incloses $x = \infty$, $y = \pm i$; $x = \pm i$, $y = \infty$, resulta $= (a - 1)^2 + bb$. 9 de juliol de 1814.

Per a $N(a + bi) < 100$, això ha estat provat per R. DEDEKIND, i R. FRICKE hi ha fet notar que entre

$$x = \sin \text{lemn } u \quad \text{i} \quad y = \cos \text{lemn } u$$

se satisfà precisament l'equació ⁴⁾

$$1 = x^2 + y^2 + x^2 y^2.$$

Però, finalment, G. HERGLOTZ ha demostrat aquesta afirmació de GAUSS ⁵⁾; el seu mètode, aplicar la divisió de les funcions el·líptiques per $\pi - 1 = a - 1 + bi$, és, en el fons, el mateix que H. HASSE utilitzà en el seu primer treball sobre la Hipòtesi de Riemann ⁶⁾.

2. En els treballs fets fins ara sobre la multiplicació de les funcions el·líptiques no ha estat investigat gairebé res més sobre quins són els possibles anells de multiplicadors **R** dels cossos de funcions el·líptiques K . Naturalment, per a característica zero això és conegut i s'obté de la manera més senzilla a partir de la interpretació de les funcions el·líptiques com a funcions doblement periòdiques: **R** és, o bé l'anell Γ dels nombres racionals enters o bé un ordre en un cos quadràtic imaginari, i tots aquests anells es presenten efectivament com a anells de multiplicadors. H. HASSE descobrí que, per a característica un nombre primer, encara es dona una tercera possibilitat: **R** també pot ésser, a més, un ordre en una àlgebra de quaternions definida. En aquest cas, jo he demostrat més exactament que les places

⁴⁾ Compareu GAUSS Werke X, 1. Abt., p.571–572.

⁵⁾ G.HERGLOTZ, Zur letzten Eintragung im Gausschen Tagebuch, Ber. d. Math.-Phys. Kl. d. Sächs. Ak. d. Wiss. Leipzig **73**, p. 271–276 (1921).

⁶⁾ H.HASSE ¹⁾, **1**, p. 258–259.

de ramificació d'aquesta àlgebra són ⁷⁾ ∞ i p . Designarem aquesta àlgebra amb $Q_{\infty,p}$. Però fins avui no era conegut si, per a característica un nombre primer p donat, els tres casos, a saber, 1. $\mathbf{R} = \Gamma$, 2. $\mathbf{R}$ un ordre prèviament donat en un cos quadràtic imaginari prèviament donat i 3. $\mathbf{R}$ un ordre prèviament donat en $Q_{\infty,p}$, són possibles, o bé si encara s'han de fer altres restriccions. En això que segueix, cal que ara sigui demostrat que, primerament, en el cas 2, el nombre primer p descompon en el cos quadràtic en dos ideals primers diferents i que el conductor de $\mathbf{R}$ ha d'ésser primer amb p i, segonament, que, en el cas 3, $\mathbf{R}$ ha d'ésser un ordre *maximal* de $Q_{\infty,p}$. Però tots els tipus de $\mathbf{R}$ caracteritzats d'aquesta manera es presenten realment.

3. El tipus d'un cos de funcions el·líptiques K pot ésser caracteritzat per mitjà de l'invariant j , el qual per a característica zero és simplement l'invariant absolut de la teoria de les funcions modulars, per a $p \neq 2$ es pot definir a partir de la forma normal de Legendre de la mateixa manera que per a característica zero, però per a $p = 2$ ha d'ésser introduït d'una altra manera ⁸⁾.

És conegut que, per a característica zero, els cossos el·líptics K amb $\mathbf{R}$ complex tenen com a invariants *nombres algebraics* j . I, en efecte, si h és el nombre de classes de $\mathbf{R}$, hi ha exactament h invariants j diferents que tenen $\mathbf{R}$ com a corresponent anell de multiplicadors; aquests h valors de j són nombres algebraics enters conjugats.

Per a característica un nombre primer p , val quelcom completament anàleg: sigui $\mathbf{R}$ un ordre prèviament do-

⁷⁾ M. DEURING ¹⁾ II, en particular §5, 6.

⁸⁾ M. DEURING, Invarianten und Normalformen elliptischer Funktionenkörper, Math. Zeitschr. **47**, 47–56 (1941).

nat en un cos de nombres quadràtic imaginari prèviament donat en el qual p descompongui en dos ideals primers diferents. Hi ha exactament tants invariants j diferents als quals correspon l'anell de multiplicadors $\mathbf{R}$ com comporta el nombre de classes h de $\mathbf{R}$; tots aquests j són algebraics absoluts (algebraics sobre el cos primer). Si f és l'exponent de la classe d'ideals de $\mathbf{R}$ a la qual pertany un dels dos ideals primers de $\mathbf{R}$ que divideixen p , aleshores, els j tenen grau absolut (grau sobre el cos primer) f ; per tant, descomponen en h/f grups, cadascun de f conjugats entre si.

Però, si $\mathbf{R}$ és un ordre maximal prèviament donat en $Q_{\infty,p}$ en el qual el divisor primer de p és un ideal principal, aleshores hi ha exactament un invariant j que pertany a aquest anell de multiplicadors i que és un racional absolut. Si el divisor primer de p no és cap ideal principal, aleshores hi ha dos invariants conjugats de grau absolut 2 per a aquest anell de multiplicadors. El nombre de j als quals correspon un ordre maximal de $Q_{\infty,p}$ com a anell de multiplicadors és igual al nombre de classes de $Q_{\infty,p}$.

El nombre de classes h és igual a 1 per a $p = 2$ i $p = 3$; més enllà, és ⁹⁾

$$h = \begin{cases} \frac{p-1}{12} & \text{per a } p \equiv 1 \pmod{12}, \\ \frac{p-5}{12} + 1 & \text{per a } p \equiv 5 \pmod{12}, \\ \frac{p-7}{12} + 1 & \text{per a } p \equiv 7 \pmod{12}, \\ \frac{p-11}{12} + 2 & \text{per a } p \equiv 11 \pmod{12}. \end{cases}$$

Igualment gran és, per tant, el nombre de j amb $\mathbf{R}$ no commutatiu. Demostrarem que $\mathbf{R}$ és no commutatiu si, i només si, en K no hi ha cap classe de divisors d'exponent p (és a dir, quan es presenta el cas ¹⁰⁾ $\sigma = 2$). Segons H. HASSE ¹¹⁾ això esdevé si, i només si, val zero un cert invariant A , per al qual ell dóna l'expressió

$$A = \begin{cases} \Delta^{\frac{p-1}{12}} P(j) & \text{per a } p \equiv 1 \pmod{12}, \\ g_2 \Delta^{\frac{p-5}{12}} P(j) & \text{per a } p \equiv 5 \pmod{12}, \\ g_3 \Delta^{\frac{p-7}{12}} P(j) & \text{per a } p \equiv 7 \pmod{12}, \\ g_2 g_3 \Delta^{\frac{p-11}{12}} P(j) & \text{per a } p \equiv 11 \pmod{12}, \end{cases}$$

aquí, g_2 i g_3 són els coeficients d'una equació definidora

$$y^2 = 4x^3 - g_2x - g_3$$

⁹⁾ Segons M. EICHLER, Über die Idealklassenzahl total definiter Quaternionen algebren, Math. Zeitschr. **43**, p. 102–109 (1937).

¹⁰⁾ M. DEURING ¹⁾, II, §5, 6.

¹¹⁾ H. HASSE, Existenz separabler zyklischer unverzweigter Erweiterungskörper vom Primzahlgrade p über elliptischen Funktionenkörpern der Charaktersitik p , Journal f. r. u. ang Math. **172**, p. 77–85 (1934), §1.

de K en forma normal de WEIERSTRASS, Δ és el discriminant

$$\Delta = g_2^3 - 27g_3^2,$$

i $P(j)$ denota un polinomi de l'invariant j del qual se sap, com a mínim, que el seu grau és, com a màxim, igual a l'exponent de la potència de Δ que el precedeix. Si comparem amb el nombre de classes, aleshores reconeixem que aquest grau, tal com conjecturà HASSE, és exacte, a més, que $P(j)$ no té cap arrel doble. Les arrels de $P(j)$ són els valors invariants amb anells de multiplicadors no commutatius, en correspondència amb els tipus d'ordres maximals de $Q_{\infty,p}$, per la qual cosa, es tenen $j = 0$, en el cas $p \equiv 5 \pmod{12}$; $j = 2^6 3^3$, en el cas $p \equiv 7 \pmod{12}$; i $j = 0$ i $j = 2^6 3^3$, en el cas $p \equiv 11 \pmod{12}$. Per a $p = 2$ i 3 , l'invariant amb anell de multiplicadors no commutatiu és $j = 0$.

D'altra banda, l'invariant A pot ésser calculat explícitament amb la definició donada per HASSE i WITT ¹²⁾ sense més ni més; segons que tinguem a disposició la forma normal de WEIERSTRASS o la de LEGENDRE, obtenim per a A les dues expressions que segueixen:

¹²⁾ H. HASSE und E. WITT, Zyklische unverzweigte Erweiterungskörper vom Primzahlgrade p über einem algebraischen Funktionenkörper der Charakteristik p , Mh. Math. Phys. **43**, p. 477–492 (1936).

$$a) \quad A = \begin{cases} (-1)^{\frac{p-1}{4}} 3^{-\frac{p-1}{4}} \Delta^{\frac{p-1}{12}} & \left(\frac{p-1}{2}\right)! \Phi_p(j), \\ \text{per a } p \equiv 1 \pmod{12}; \\ 2^2 (-1)^{\frac{p-1}{4}} 3^{-\frac{p-5}{4}} \Delta^{\frac{p-5}{12}} & g_2 \left(\frac{p-1}{2}\right)! \Phi_p(j), \\ \text{per a } p \equiv 5 \pmod{12}; \\ 2^4 (-1)^{\frac{p-3}{4}} 3^{-\frac{p-7}{4}} \Delta^{\frac{p-7}{12}} & g_3 \left(\frac{p-1}{2}\right)! \Phi_p(j), \\ \text{per a } p \equiv 7 \pmod{12}; \\ 2^6 (-1)^{\frac{p-3}{4}} 3^{-\frac{p-11}{4}} \Delta^{\frac{p-11}{12}} g_2 g_3 & \left(\frac{p-1}{2}\right)! \Phi_p(j), \\ \text{per a } p \equiv 11 \pmod{12}; \end{cases}$$

on

$$\Phi_p(j) = j^{\left[\frac{p}{12}\right]} \sum_{0 \leq i < \frac{p}{12}} \frac{\left(-\frac{4}{27}\right)^i (1 - 2^6 \cdot 3^3 \cdot j^{-1})^i}{(2i)! \left(\frac{p-1}{4} - 3i\right)! \left(\frac{p-1}{4} + i\right)!}$$

per a $p \equiv 1 \pmod{4}$;

i

$$\Phi_p(j) = j^{\left[\frac{p}{12}\right]} \sum_{0 \leq i < \frac{p}{12}} \frac{\left(-\frac{4}{27}\right)^i (1 - 2^6 \cdot 3^3 \cdot j^{-1})^i}{(2i+1)! \left(\frac{p-7}{4} - 3i\right)! \left(\frac{p+1}{4} + i\right)!}$$

per a $p \equiv -1 \pmod{4}$;

$$b) \quad A = (-1)^{\frac{p-1}{2}} \sum_{i=0}^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)^2 \lambda^i \text{ per a } p \geq 3;$$

aquí, λ és una de les sis arrels de

$$j = 2^8 \frac{(1 - \lambda(1 - \lambda))^3}{\lambda^2(1 - \lambda)^2}.$$

La forma a) és apropiada també per al càlcul numèric dels invariants “supersingulars” (amb $\mathbf{R}$ no commutatiu) per a valors petits de p .

4. És fàcil veure que, per a característica un nombre primer, cada cos el·líptic amb invariant algebraic absolut té multiplicadors complexos. Els p^f elements del cos de Galois G_{p^f} es divideixen, doncs, com a invariants de cossos el·líptics amb $\mathbf{R}$ complexos, i quan nosaltres investiguem quines condicions han de satisfer aquests $\mathbf{R}$, s’obté la *relació de nombres de classes* següent:

Designin $d_{n,p}$ aquells discriminants no divisibles per p de formes quadràtiques binàries definides tals que la forma principal associada representa pròpiament el nombre natural n , i $h(d_{n,p})$ el nombre de classes de $d_{n,p}$.

Aleshores, val

$$\sum h(d_{p^f,p}) + t_{p^f} = p^f,$$

on, per a f parella, t_{p^f} és el nombre de classes de $Q_{\infty,p}$ indicat a **3** i, per a f senar, la mitjana aritmètica del nombre de classes i el nombre de tipus de $Q_{\infty,p}$.

5. A fi i efecte de poder deduir els resultats esmentats, hem de poder passar de cossos el·líptics de característica 0 a aquells de característica un nombre primer i recíprocament. Sobre això, valen els dos teoremes generals següents:

1. *Sigui $\mathfrak{p}$ un divisor primer en el cos de constants k del cos de funcions el·líptiques K donat mitjançant una valoració exponencial. L'invariant j de K és $\mathfrak{p}$ -enter si, i només si, hi ha una equació definidora $f(x, y) = 0$ de K que també és irreductible i de gènere 1 mòdul $\mathfrak{p}$. Aleshores, als divisors, les classes de divisors, i els multiplicadors de K se'ls pot fer correspondre com a "residus" determinats divisors, classes de divisors, i multiplicadors del cos $\overline{K}$ de classes residuals de K mòdul $\mathfrak{p}$, de manera que les relacions entre els elements, els divisors, les classes i els multiplicadors restin inalterades per l'aplicació de classes residuals.*
2. *Si el cos $\overline{K}_0$ de característica un nombre primer p té un multiplicador $\overline{\mu}$, aleshores aquest es pot obtenir per reducció mòdul un divisor primer $\mathfrak{p}$ de p a partir d'un cos K_0 de característica 0, un dels multiplicadors del qual s'aplica mòdul $\mathfrak{p}$ en el multiplicador $\overline{\mu}$.*

El segon teorema conté el mètode de HERGLOTZ i HASSE com a cas especial.

Del primer teorema se segueix com es comporta un cos de funcions el·líptiques K de característica zero amb $\mathbf{R}$ complex per reducció en un ideal primer $\mathfrak{p}$ que divideixi p —podem prendre el cos de constants de K com un cos de nombres algebraic finit. Per aquesta reducció, $\mathbf{R}$ s'aplicarà en una part de l'anell de multiplicadors $\overline{\mathbf{R}}$ del cos de classes residuals $\overline{K}$ de K mòdul $\mathfrak{p}$. Però, en general, $\overline{\mathbf{R}}$ és més gran que $\mathbf{R}$. Si, en el cos de quocients Σ de $\mathbf{R}$, p descompon en dos ideals primers diferents, aleshores $\overline{\mathbf{R}}$ és d'aquells ordres de Σ el conductor dels quals és la part

del conductor de $\mathbf{R}$ lliure de p . Si p resta primer o bé és ramificat en Σ , aleshores $\overline{\mathbf{R}}$ és un ordre maximal de $Q_{\infty,p}$.

A partir d'aquestes consideracions, pot ésser deduïda la teoria de cossos de classes de Σ , la qual haurà d'ésser tractada amb més precisió en un treball posterior.

Atès que l'invariant $\bar{j}$ de $\overline{K}$ és la $\mathbf{p}$ -classe residual de l'invariant j de K , se segueix que j mòdul $\mathbf{p}$ és un dels h invariants supersingulars mòdul p , per a cada p que no descompon completament en Σ .

D'això se segueixen nous fets dignes de menció sobre la descomposició de nombres primers en determinats cossos de nombres algebraics que han d'ésser investigats en un treball posterior. Únicament esmentarem el cas més senzill: atès que l'invariant supersingular mòdul 2 és igual a 0, les classes invariants de cada ordre d'un cos quadràtic imaginari són senars o parelles (és a dir, primeres amb 2 o no), segons que 2 descompongui completament en Σ o no. A saber, aquest teorema és la conseqüència d'un teorema que ha estat demostrat per H. WEBER sobre la funció

$$f(\omega) = e^{-\frac{\pi i}{24}} \frac{\eta\left(\frac{\omega+1}{2}\right)}{\eta(\omega)}, \quad \eta(\omega) = e^{\frac{\pi i}{12}} \prod_{\nu=1}^{\infty} (1 - e^{2\pi i \nu})$$

per a

$$j(\omega) = \frac{(f(\omega)^{24} - 16)^3}{f(\omega)^{24}}.$$

Aquell teorema, que H. WEBER demostrà per mitjà de la fórmula límit de KRONECKER, diu: *Si ω genera un cos*

quadràtic imaginari en el qual 2 descompon completament, aleshores $f(\omega)2^{\frac{1}{2}}$ és una unitat ¹³⁾.

§1. Els subcossos d'un cos de funcions el·líptiques

1. Sigui K un cos de funcions el·líptiques de cos de constants k algebraicament tancat. Obtenim una correspondència bijectiva de les classes de grau zero C en els divisors primers de K quan, fixat un divisor primer arbitrari $\mathfrak{o}$ de K com a element normalitzador dels divisors primers, a la classe C li assignem el divisor primer $\mathfrak{p}$ de la classe $\mathfrak{o}C$ determinat unívocament d'acord amb el teorema de Riemann-Roch o bé, recíprocament, al divisor primer $\mathfrak{o}$, la classe de $\mathfrak{p}/\mathfrak{o}$. Designarem la classe de $\mathfrak{p}/\mathfrak{o}$ abreujadament per $[\mathfrak{p}]$ i escriurem additivament el grup de classes de grau zero; per tant,

$$[\mathfrak{p}_1] + [\mathfrak{p}_2] = [\mathfrak{p}_3]$$

significa simplement que

$$\frac{\mathfrak{p}_1}{\mathfrak{o}} \cdot \frac{\mathfrak{p}_2}{\mathfrak{o}} \sim \frac{\mathfrak{p}_3}{\mathfrak{o}}.$$

Ara introduïm, d'acord amb H. HASSE ¹⁴⁾, els automorfismes de reflexió i de translació de K/k . Siguin $\mathfrak{q}_1$ i $\mathfrak{q}_2$ dos divisors primers de K (iguals o diferents). Pel teorema de Riemann-Roch, hi ha un element z amb el denominador

¹³⁾H. WEBER, Lehrbuch der Algebra, III, §142, Die Normen der C Klassen-invarianten.

¹⁴⁾H. HASSE, Zur Theorie der abstrakten elliptischen Funktionenkörper, II, Journ. f. d. r. u. ang. Math., **175**, p. 69–88 (1936), §1.

exacte $\mathfrak{q}_1 \mathfrak{q}_2$. K és quadràtic i separable sobre $k(z)$ (també si la característica de K és 2, perquè l'única extensió quadràtica inseparable $k(z^{\frac{1}{2}})$ de $k(z)$ té gènere 0) i té, per tant, un automorfisme $\sigma_{\mathfrak{q}_1, \mathfrak{q}_2}$ diferent de la identitat que deixa z fix i intercanvia $\mathfrak{q}_1$ amb $\mathfrak{q}_2$.

$\sigma_{\mathfrak{q}_1, \mathfrak{q}_2}$ s'anomena un automorfisme de reflexió de K . Si $\sigma_{\mathfrak{q}_1, \mathfrak{q}_2}$ intercanvia els dos divisors primers $\mathfrak{p}_1$ i $\mathfrak{p}_2$, aleshores es té que $\sigma_{\mathfrak{p}_1, \mathfrak{p}_2} = \sigma_{\mathfrak{q}_1, \mathfrak{q}_2}$, atès que hi ha un element $\alpha z + \beta$ amb constants α, β el denominador del qual és $\mathfrak{q}_1 \mathfrak{q}_2$ i el numerador del qual és $\mathfrak{p}_1 \mathfrak{p}_2$; per tant, el cos invariant de $\sigma_{\mathfrak{p}_1, \mathfrak{p}_2}$ coincideix amb el de $\sigma_{\mathfrak{q}_1, \mathfrak{q}_2}$. És suficient, doncs, considerar les reflexions $\sigma_{\mathfrak{o}, \mathfrak{q}}$.

Atès que, entès $\mathfrak{p}$ com un divisor primer qualsevol, $\frac{\mathfrak{p}}{\mathfrak{o}} \cdot \frac{\mathfrak{p}^{\sigma_{\mathfrak{o}, \mathfrak{q}}}}{\mathfrak{o}}$ és equivalent a 1 com a divisor de $k(z)$, aleshores val

$$[\mathfrak{p}^{\sigma_{\mathfrak{o}, \mathfrak{q}}}] = [\mathfrak{q}] - [\mathfrak{p}], \quad \text{en particular, } [\mathfrak{p}^{\sigma_{\mathfrak{o}, \mathfrak{o}}}] = -[\mathfrak{p}],$$

d'on s'aclareix el nom reflexió.

Per a l'automorfisme

$$\tau_{\mathfrak{o}, \mathfrak{p}} = \sigma_{\mathfrak{o}, \mathfrak{o}} \sigma_{\mathfrak{o}, \mathfrak{q}}$$

de K/k , val

$$(1) \quad [\mathfrak{p}^{\tau_{\mathfrak{o}, \mathfrak{q}}}] = [\mathfrak{p}^{\sigma_{\mathfrak{o}, \mathfrak{o}} \sigma_{\mathfrak{o}, \mathfrak{q}}}] = [\mathfrak{q}] - [\mathfrak{p}^{\sigma_{\mathfrak{o}, \mathfrak{o}}}] = [\mathfrak{p}] + [\mathfrak{q}].$$

$\tau_{\mathfrak{o}, \mathfrak{q}}$ s'anomena una *translació* de K .

2. Passem ara a la teoria dels multiplicadors de K tal com ha estat desenvolupada en els dos treballs de M. DEURING citats a ¹⁾. Un multiplicador μ de K pot ésser pensat, d'una banda, com una aplicació homomorfa $[\mathfrak{p}] \rightarrow \mu[\mathfrak{p}]$ del

grup de classes de grau zero en si mateix, d'altra banda, com un *meromorfisme normat* $z \rightarrow z^\mu$ de K . Per a normalitzar el meromorfisme utilitzem el mateix divisor primer $\mathfrak{o}$ que en **1** per a la definició de $[\mathfrak{p}]$. Aleshores, per a la imatge de $\mu[\mathfrak{p}]$ val la *regla* següent:

$$(2) \quad \mu[\mathfrak{p}] = \left[(N_{K/K^\mu} \mathfrak{p})^{\mu^{-1}} \right].$$

Llavors μ és aplicat així a la classe de $\mathfrak{p}/\mathfrak{o}$, perquè primerament es pren la norma de $\mathfrak{p}/\mathfrak{o}$ respecte de K^μ i aquesta, després, s'aplica en K per μ^{-1} .

De (2) se segueix que:

Els divisors primers $\mathfrak{p}$ per als quals val

$$\mu[\mathfrak{p}] = \mathfrak{q}$$

són els divisors primers de $\mathfrak{q}^\mu$.

Els $[\mathfrak{p}]$ amb $\mu[\mathfrak{p}] = 0$ formen un grup de classes d'ordre $N\mu/I_\mu$, perquè el nombre dels factors primers diferents en K d'un divisor primer de K^μ és igual⁶⁾ al grau $N\mu$ dividit pel grau d'inseparabilitat I_μ de K/K^μ .

Una classe lateral del grup $\mu[\mathfrak{p}] = 0$ en el grup de classes complet consta de tots els $\mathfrak{p}$ amb $\mu[\mathfrak{p}] = \mathfrak{q}$ per a un $\mathfrak{q}$ fix. Si $\mu[\mathfrak{p}] = 0$, aleshores cada divisor primer $\mathfrak{q}^\mu$ de K^μ resta fix per la translació $\tau_{\mathfrak{o},\mathfrak{p}}$, atès que $\mathfrak{q}^\mu$ és la potència I_μ -èsima del producte de les solucions diferents $\mathfrak{x}$ de $\mu[\mathfrak{x}] = [\mathfrak{q}]$, les quals només són intercanviades entre elles per $\tau_{\mathfrak{o},\mathfrak{p}}$. D'aquí concloem que cada element de K^μ resta fix per $\tau_{\mathfrak{o},\mathfrak{p}}$, atès que val el lema següent de H. HASSE¹³⁾:

Un automorfisme τ d'un cos de funcions K que deixa fixes totes les constants i tots els divisors primers és la identitat.

Demostració: τ pot canviar cada y de K només amb un factor constant ε_y : $y^\tau = \varepsilon_y y$. Per a una constant y és $\varepsilon_y = 1$. Per a una y no constant tenim que

$$(y+1)^\tau = \varepsilon_{y+1}(y+1) = y^\tau + 1 = \varepsilon_y y + 1,$$

$$(\varepsilon_{y+1} - \varepsilon_y)y = 1 - \varepsilon_{y+1}.$$

Com que el costat dret de la darrera equació és constant, ha d'ésser $\varepsilon_{y+1} = 1$, és a dir, $y^\tau = y$, tal com s'ha afirmat.

Com que el nombre de translacions $\tau_{\mathfrak{o}, \mathfrak{p}}$ amb $\mu[\mathfrak{p}] = 0$ és igual al grau de separabilitat de K/K^μ , tenim el teorema:

K és abelià sobre K^μ i el grup de Galois de K/K^μ consta de les translacions $\tau_{\mathfrak{o}, \mathfrak{p}}$ amb $\mu[\mathfrak{p}] = 0$.

En particular, per a un multiplicador natural n , el grup de Galois de K/K^n consta de totes les translacions tals que el seu ordre divideix n . Per tant, és un grup abelià de tipus (n, n) si la característica p no divideix n , i de tipus $(n/p^f, n/p^{\sigma^f - f})$, si p^f és la potència de p que divideix n ; σ , que només depèn del cos K , és igual a 1 o 2⁶⁾.

3. Sigui ara K_0 un subcòs el·líptic qualsevol de K amb el mateix cos de constants k . K és no ramificat sobre K_0 . *Demostrem que el grup de Galois de K/K_0 és un grup de translacions finit, de tal manera que K_0 és caracteritzat dins de K pel fet de donar aquest grup de translacions i el grau d'inseparabilitat de K/K_0 .*

Manifestament, podem suposar d'entrada que K és separable sobre K_0 . Sigui K' el cos normal sobre K_0 generat per K . K' és no ramificat sobre K i, per tant, el·líptic. Sigui ϱ un automorfisme de K'/K_0 . Si provem que ϱ és una translació de K' , aleshores s'aconsegueix la demostració, perquè, a través de ρ , K' es mostra abelià sobre K_0 i,

per tant, coincideix amb K . Sigui $\mathfrak{o}'$ un divisor primer de K' , $\mathfrak{o}'^e = \mathfrak{o}^*$. $\varepsilon = \varrho\tau_{\mathfrak{o}', \mathfrak{o}^*}^{-1}$ és un automorfisme de K'/k que deixa fix $\mathfrak{o}'$; per tant, un meromorfisme de K' normat per $\mathfrak{o}'$, que representa una unitat de l'anell de multiplicadors de K' . Per a un divisor primer $\mathfrak{q}$ de K' val

$$\varepsilon^{-1}[\mathfrak{q}'] = \left[(N_{K'/K'^{\varepsilon^{-1}}} \mathfrak{q}')^{\varepsilon} \right] = [\mathfrak{q}'^{\varepsilon}].$$

Suposem que fos $\varepsilon \neq 1$. Aleshores, hi hauria una classe $[\mathfrak{q}']$ tal que

$$(1 - \varepsilon^{-1})[\mathfrak{q}'] = [\mathfrak{o}^*], \quad [\mathfrak{q}'] - [\mathfrak{q}'^{\varepsilon}] = [\mathfrak{o}^*],$$

$$[\mathfrak{q}'] = [\mathfrak{q}'^{\varepsilon}] + [\mathfrak{o}^*] = [\mathfrak{q}'^{\varepsilon\tau_{\mathfrak{o}, \mathfrak{o}^*}}] = [\mathfrak{q}'^e].$$

Per tant, ϱ seria una substitució de la inèrcia de $\mathfrak{q}'$ sobre K_0 , cosa que contradiu la no-ramificació de K'/K_0 .

4. Relacionarem els multiplicadors d'un subcòs el·líptic K_0 de K amb els del mateix K . Els multiplicadors de K_0 han d'ésser normats com a meromorfismes per la norma $\mathfrak{o}_0$ de $\mathfrak{o}$ en K_0 . $\mathfrak{o}$ s'aplica en $\mathfrak{o}_0$.

Sigui μ un multiplicador de K . *Per a les classes imatge en K^μ val la regla*

$$(3) \quad [\mathfrak{p}^\mu] = [\mathfrak{p}]^\mu.$$

Ja que $[\mathfrak{p}]^\mu$ és la classe de $\mathfrak{p}^\mu/\mathfrak{o}^\mu$, se segueix que $[\mathfrak{p}^\mu]$ també ho és com a conseqüència de la normalització fixada en $K_0 = K^\mu$.

Aquí deduïm la representació següent de les translacions de K^μ mitjançant les de K

$$\tau_{\mathfrak{o}^\mu, \mathfrak{q}^\mu} = \mu^{-1} \tau_{\mathfrak{o}, \mathfrak{q}^\mu}.$$

Val, a saber,

$$\begin{aligned} [\mathfrak{p}^{\mu\mu^{-1}\tau_{\mathfrak{o},\mathfrak{q}^\mu}}] &= [\mathfrak{p}^{\tau_{\mathfrak{o},\mathfrak{q}^\mu}}] = [\mathfrak{p}^{\tau_{\mathfrak{o},\mathfrak{q}}}]^\mu = [\mathfrak{p}]^\mu + [\mathfrak{q}]^\mu = \\ &= [\mathfrak{p}^\mu] + [\mathfrak{q}^\mu] = [\mathfrak{p}^{\mu\tau_{\mathfrak{o},\mathfrak{q}^\mu}}], \end{aligned}$$

per tant, l'automorfisme $\tau_{\mathfrak{o}^\mu,\mathfrak{q}^\mu}^{-1}\mu^{-1}\tau_{\mathfrak{o},\mathfrak{q}^\mu}$ de K^μ/k deixa fixos tots els divisors primers de K^μ i ha d'ésser la identitat.

Sigui K_0 un subcòs el·líptic qualsevol de K . Examinarem sota quina condició la imatge K_0^μ de K_0 per un meromorfisme μ de K està continguda en K_0 i, per tant, proporciona un meromorfisme de K_0 , el qual, aleshores, és normat per $\mathfrak{o}_0$. Amb aquest objectiu calculem el grup de Galois de K/K_0^μ a partir del de K/K_0 . Mostrem que

$\tau_{\mathfrak{o},\mathfrak{x}}$ és un automorfisme de K/K_0^μ si, i només si, posat $\mu[\mathfrak{x}] = \mathfrak{q}$, $\tau_{\mathfrak{o},\mathfrak{q}}$ és un automorfisme de K/K_0 .

Demostració: Siguin $\tau_{\mathfrak{o},\mathfrak{q}}, \dots, \tau_{\mathfrak{o},\mathfrak{q}_{n_0}}$ els automorfismes de K/K_0 , denoti $\mathfrak{p}_0$ un divisor primer qualsevol de K_0 i $\mathfrak{x}$ un divisor primer qualsevol de K . Calculem $\mathfrak{p}_0^{\tau_{\mathfrak{o},\mathfrak{x}}}$. Volem fer explícit el pas d'una classe $[\mathfrak{p}]$ a un divisor primer $\mathfrak{p}$ posant la classe entre parèntesis rodons: $([\mathfrak{p}]) = \mathfrak{p}$. Si $\mathfrak{p}_0$ és la norma de K sobre K_0 d'un divisor primer $\mathfrak{p}$, aleshores

$$\mathfrak{p}_0 = \prod_{i=0}^{n_0} ([\mathfrak{p}] + [\mathfrak{q}_i])^{I(K:K_0)}.$$

Per tant, tenim que

$$\mathfrak{p}_0^\mu = \prod_{i=1}^{n_0} ([\mathfrak{p}]^\mu + [\mathfrak{q}_i]^\mu)^{I(K:K_0)} = \prod_{i=1}^{n_0} ([\mathfrak{p}^\mu] + [\mathfrak{q}_i^\mu])^{I(K:K_0)}.$$

Si $([\mathfrak{p}^\mu] + [\mathfrak{q}_i^\mu])$ és la norma d'un divisor primer $\mathfrak{h}_i$ de K sobre K^μ , aleshores

$$([\mathfrak{p}^\mu] + [\mathfrak{q}^\mu]) = \left[\prod_{\mu[r]=0} ([\mathfrak{h}_i] + [\mathfrak{r}])^{I_\mu} \right].$$

D'acord amb (2), val

$$\mu[\mathfrak{h}_i] = ([\mathfrak{p}] + [\mathfrak{q}_i]).$$

Ara podem calcular $([\mathfrak{p}^\mu] + [\mathfrak{q}_i^\mu])^{\tau_0, \mathfrak{x}}$

$$\begin{aligned} ([\mathfrak{p}^\mu] + [\mathfrak{q}_i^\mu])^{\tau_0, \mathfrak{x}} &= \prod_{\mu[r]=0} ([\mathfrak{h}_i] + [\mathfrak{x}] + [\mathfrak{r}])^{I_\mu} = \\ &= N_{K/K^\mu}([\mathfrak{h}_i] + [\mathfrak{x}]) = \\ &= (\mu[\mathfrak{h}_i] + \mu[\mathfrak{x}])^\mu = \\ &= ([\mathfrak{p}] + [\mathfrak{q}_i] + \mu[\mathfrak{x}])^\mu. \end{aligned}$$

I d'això se segueix que

$$\mathfrak{p}_0^{\mu\tau_0, \mathfrak{x}} = \prod_{i=1}^{n_0} ([\mathfrak{p}] + [\mathfrak{q}_i] + \mu[\mathfrak{x}])^{\mu I(K:K_0)}.$$

A fi que s'esdevingui $\mathfrak{p}_0^{\mu\tau_0, \mathfrak{x}} = \mathfrak{p}_0^\mu$, manifestament les n_0 classes $[\mathfrak{q}_i] + \mu\mathfrak{x}$ han de coincidir amb les classes $[\mathfrak{q}_i]$ llevat de l'ordre de la sèrie, i aquest és exactament el cas quan $\mu[\mathfrak{x}]$ pertany al grup dels $[\mathfrak{q}_i]$, com hem afirmat.

A fi de determinar completament K_0^μ , encara hem d'indicar el grau d'inseparabilitat de K/K_0^μ . Però aquest és el producte dels graus d'inseparabilitat de K sobre K^μ i sobre K_0 .

A partir del teorema demostrat se segueix sense més ni més que, si $n = n_0 \cdot I(K : K_0)$ és el grau de K sobre K_0 , aleshores $K^{n\varepsilon}$ està contingut en K_0 .

A més, tenim la resposta següent a la pregunta formulada més amunt sobre quins multiplicadors de K també són multiplicadors de K_0 :

μ és un multiplicador de K_0 si, i només si, el grup de les classes $[\mathbf{q}_i]$ que corresponen als automorfismes $\tau_{\mathbf{o}, \mathbf{q}_1}, \dots, \tau_{\mathbf{o}, \mathbf{q}_{n_0}}$ de K/K_0 s'aplica per μ en si mateix:

$$\mu[\mathbf{q}_i] = [\mathbf{q}_j].$$

En particular, la n_0 -iteració de cada multiplicador de K també és un multiplicador de K_0 .

5. Ara mostrem de quina manera un multiplicador μ de K que al mateix temps és un multiplicador de K_0 es pot interpretar com un homomorfisme del grup de classes de K_0 a partir de la seva acció sobre les classes de K . Val, senzillament,

$$(4) \quad \mu[N_{K/K_0}\mathbf{p}] = [N_{K/K_0}(\mu[\mathbf{p}])].$$

Demostració:

$$\begin{aligned} \mu[N_{K/K_0}\mathbf{p}] &= [(N_{K_0/K_0^\mu}(N_{K/K_0}\mathbf{p}))^{\mu^{-1}}] = [(N_{K/K_0^\mu}\mathbf{p})^{\mu^{-1}}] = \\ &= [(N_{K^\mu/K_0^\mu}(N_{K/K_0}\mathbf{p}))^{\mu^{-1}}] = [N_{K/K_0^\mu}((N_{K/K^\mu}\mathbf{p})^{\mu^{-1}})] = \\ &= [N_{K/K_0}(\mu[\mathbf{p}])]. \end{aligned}$$

6. Mitjançant $[\mathbf{p}] \rightarrow [N_{K/K_0}\mathbf{p}]$, el grup de classes de K s'aplica homomòrficament en el de K_0 ; aquí, s'apliquen en 0 exactament les classes $[\mathbf{p}]$ per a les quals $[\tau_{\mathbf{o}, \mathbf{p}}]$ pertany al grup de Galois de K/K_0 .

7. D'això precedent se segueix que els anells de multiplicadors $\mathbf{R}$ i $\mathbf{R}_0$ de K i de K_0 tenen una intersecció no

buida. Però del que antecedeix no és clar que per als elements d'aquesta intersecció les operacions per la dreta en $\mathbf{R}_0$ coincideixin amb les de $\mathbf{R}$. Per a la multiplicació, se segueix, certament de seguida, a partir de la definició del producte de meromorfismes. Per a l'addició, ho demostrem d'aquesta manera:

Siguin μ_1, μ_2, μ_3 tres elements de la intersecció de $\mathbf{R}$ amb $\mathbf{R}_0$ la suma dels quals, presa en $\mathbf{R}$, sigui 0. Hem de mostrar que també la seva suma en $\mathbf{R}_0$ és igual a 0. A μ_i pertany un divisor primer de primer grau $\mathfrak{P}_{\mu_i}$ del doble cos KK^φ/K ¹⁵⁾, i $\mu_1 + \mu_2 + \mu_3 = 0$ significa que $\mathfrak{P}_{\mu_1} \cdot \mathfrak{P}_{\mu_2} \cdot \mathfrak{P}_{\mu_3} \sim (\mathfrak{o}^\varphi)^3$ en KK^φ . El doble cos $K_0K_0^\varphi$ que correspon a K_0 està inclòs en KK^φ , i a μ_i com a meromorfisme de K_0 li correspon manifestament el divisor primer de $K_0K_0^\varphi/K_0$ en el qual s'aplica $\mathfrak{P}_{\mu_i}$; és a dir, la norma $\mathfrak{P}_{\mu_i}^{(0)}$ de $\mathfrak{P}_{\mu_i}$ sobre $K_0K_0^\varphi$. La norma de $\mathfrak{o}^\varphi$ és $\mathfrak{o}_0^\varphi$. A partir de l'equivalència $\mathfrak{P}_{\mu_1} \cdot \mathfrak{P}_{\mu_2} \cdot \mathfrak{P}_{\mu_3} \sim (\mathfrak{o}^\varphi)^3$, se segueix doncs, a través de l'aplicació norma, l'equivalència

$$\mathfrak{P}_{\mu_1}^{(0)} \cdot \mathfrak{P}_{\mu_2}^{(0)} \cdot \mathfrak{P}_{\mu_3}^{(0)} \sim (\mathfrak{o}_0^\varphi)^3,$$

la qual ens diu que la suma dels μ_i com a meromorfismes de K_0 és 0 igualment.

§2. Els anells de multiplicadors dels subcossos

1. De nou, com en §1, sigui K un cos el·líptic amb cos de constants k algebraicament tancat. Siguí p ($= 0$ o bé

¹⁵⁾M. DEURING, Arithmetische Theorie der Korrespondenzen algebraischer Funktionenkörper, II, §5, 2. Journ. f. d. r. u. ang. Math. **183**, p. 25-36 (1941).

$\neq 0$) la característica de K . El cos de fraccions Σ de l'anell de multiplicadors $\mathbf{R}$ de K és o bé el cos P dels nombres racionals, o bé un cos de nombres quadràtic imaginari, o bé l'àlgebra de quaternions (definida) $Q_{\infty,p}$ que ramifica en 1 i p (cosa que només és possible si $p \neq 0$). $\mathbf{R}$ és un ordre de Σ .

De la mateixa manera que els elements μ de $\mathbf{R}$ deixen fixos els subcossos K^μ , també als ideals per l'esquerra $\mathbf{a}$ de $\mathbf{R}$ els podem assignar subcossos el·líptics de K .

Sigui $\mathbf{a}$ un ideal per l'esquerra de $\mathbf{R}$. La composició de tots els cossos K^α , $\alpha \equiv 0 \pmod{\mathbf{a}}$, és un subcòs el·líptic de K , que designem per $K^{\mathbf{a}}$. Si $\mathbf{a} = \mathbf{R}\alpha$ és un ideal principal, aleshores, manifestament és $K^{\mathbf{a}} = K^\alpha$. (A partir del teorema d'addició concloem fàcilment que, si val

$$\mathbf{a} = (\mathbf{R}\alpha_1, \dots, \mathbf{R}\alpha_t),$$

aleshores $K^{\mathbf{a}}$ és la composició dels cossos K^{α_i} , en nombre finit.)

El grup de Galois de K sobre $K^{\mathbf{a}}$ és, com a intersecció dels grups de Galois de K sobre tots els K^α , $\alpha \equiv 0 \pmod{\mathbf{a}}$, el grup de totes les translacions $\tau_{\mathbf{a},\mathbf{p}}$, $\mathbf{a}[\mathbf{p}] = 0$.

Si $\mathbf{a}_1 \equiv 0 \pmod{\mathbf{a}}$, aleshores val $K^{\mathbf{a}} \subseteq K^{\mathbf{a}_1}$.

2. Tal com mostràrem en §1 5, l'anell de multiplicadors de $K^{\mathbf{a}}$ té el mateix cos de fraccions Σ que $\mathbf{R}$. Però, a més, val:

L'anell de multiplicadors $\mathbf{R}_0$ de $K^{\mathbf{a}} = K_0$ és l'ordre per la dreta de $\mathbf{a}$ en Σ .

Demostració. En el que segueix demostrem únicament que $\mathbf{R}_0$ conté l'ordre per la dreta de $\mathbf{a}$; que $\mathbf{R}_0$ no és més gran ho demostrem més tard (9).

Explicuem de quina manera un element μ_0 de l'ordre per la dreta de $\mathbf{a}$ s'aplica als elements de K_0 . Un element z de K_0 és una funció racional $z = R(z_1^{\alpha_1}, \dots, z_t^{\alpha_t})$ d'uns elements $z_i^{\alpha_i}$ dels cossos K^{α_i} , $\alpha_i \equiv 0 \pmod{\mathbf{a}}$, z_i de K . Els $\alpha_i \mu_0$ estan en $\mathbf{a}$ i, per tant, mitjançant

$$z^{\mu_0} = R(z_1^{\alpha_1 \mu_0}, \dots, z_t^{\alpha_t \mu_0}),$$

és definit un element de $K^{\mathbf{a}}$. És fàcil adonar-se que z^{μ_0} no depèn de la manera en què l'element z es representa mitjançant els elements z^{α_i} , expressat d'una altra manera, que

$$R(z_1^{\alpha_1 \mu_0}, \dots, z_t^{\alpha_t \mu_0}) = 0$$

sempre que val

$$R(z_1^{\alpha_1}, \dots, z_t^{\alpha_t}) = 0 :$$

existeix un nombre natural n tal que $n\mu_0$ és de $\mathbf{R}$. A partir de

$$R(z_1^{\alpha_1}, \dots, z_t^{\alpha_t}) = 0$$

se segueix que

$$0 = R(z_1^{\alpha_1}, \dots, z_t^{\alpha_t})^{\mu_0 n} = R(z_1^{\alpha_1 \mu_0}, \dots, z_t^{\alpha_t \mu_0})^{n\varepsilon}$$

i, per tant, que

$$R(z_1^{\alpha_1 \mu_0}, \dots, z_t^{\alpha_t \mu_0}) = 0.$$

A partir de la definició de l'acció de μ_0 en K_0 se segueix immediatament que μ_0 és un meromorfisme de K_0 .

μ_0 és normat per $\mathfrak{o}_0 = N_{K/K_0}\mathfrak{o}$; és a dir, és $\mathfrak{o}_0^{\mu_0} = N_{K/K_0^{\mu_0}}\mathfrak{o}_0$; dit d'una altra manera, $\mathfrak{o}_0$ s'aplica en $\mathfrak{o}_0^{\mu_0}$. Per a demostrar-ho, sigui α un element qualsevol de $\mathbf{a}$. $\mathfrak{o}_0$, $\mathfrak{o}^\alpha$ i $\mathfrak{o}^{\alpha\mu_0}$ són divisibles per $\mathfrak{o}$; en conseqüència, el divisor primer del cos intermedi $K^{\mathbf{a}\mu_0}$ entre $K_0 = K^{\mathbf{a}}$ i $K^{\alpha\mu_0}$, que és divisible per $\mathfrak{o}$ i també per $\mathfrak{o}_0$, és igual a $\mathfrak{o}_0^{\mu_0}$.

En el cas en què $\mathbf{a}$ és un ideal amb ordre maximal, l'anell de multiplicadors de $K^{\mathbf{a}}$ naturalment no pot ésser més gran que l'ordre per la dreta de $\mathbf{a}$, cosa que aleshores fa innecessaris complements en la demostració.

3. És $(K : K^{\mathbf{a}}) = N\mathbf{a}$.

A continuació, demostrem aquest teorema únicament per al cas en què $\mathbf{R}$ és maximal, i ajornem la demostració general a **9**.

Sigui $\mathbf{R}_1$ l'ordre per l'esquerra de $\mathbf{a}$, sigui $\mathbf{R}_2$ l'ordre per la dreta de $\mathbf{a}$, és a dir, l'anell de multiplicadors de $K^{\mathbf{a}}$. Designarem per $\mathbf{a}_{ij}$ un ideal amb ordre per l'esquerra $\mathbf{R}_i$ i ordre per la dreta $\mathbf{R}_j$ i, d'acord amb això, escriurem $\mathbf{a}_{12}$ en lloc de $\mathbf{a}$. Sigui ara $\mathbf{a}_{23}$ un ideal per l'esquerra enter de $\mathbf{R}_2$ coprimer amb $(K : K^{\mathbf{a}})$ per al qual $\mathbf{a}_{12}\mathbf{a}_{23} = \mathbf{R}_1\alpha$ és un ideal principal ¹⁶⁾. Atès que $K^\alpha \leq K^{\mathbf{a}_{12}}$, és $(K : K^\alpha) \equiv 0 \pmod{(K : K^{\mathbf{a}_{12}})}$; a partir de

$$(K : K^{\mathbf{a}}) = N\alpha = N\mathbf{a}_{12} \cdot N\mathbf{a}_{23}$$

¹⁶⁾Per a Σ commutatiu, això és conegut. Que també valgui per a $Q_{\infty,p}$, fou provat per NEHRKORN: H. NEHRKORN, Über absolute Idealklassengruppe und Einheiten in algebraischen Zahlkörpern, en aquest treball: **9**, p. 318–334 (1933). Vegeu també M. DEURING, Algebren, Ergebn. der Math. IV, 1, p. 106, Satz 27.

se segueix, per tant,

$$N\mathbf{a}_{12} \equiv 0 \pmod{(K : K^{\mathbf{a}})};$$

sigui, doncs,

$$N\mathbf{a}_{12} = t(K : K^{\mathbf{a}}).$$

De la mateixa manera val

$$N\mathbf{a}_{23} = t'(K^{\mathbf{a}_{12}} : K^{\mathbf{a}_{12}\mathbf{a}_{23}})$$

amb t' enter. Però ja que és $N\mathbf{a}_{12}N\mathbf{a}_{23} = N\alpha = (K : K^{\mathbf{a}}) = (K : K^{\mathbf{a}_{12}})(K^{\mathbf{a}_{12}} : K^{\mathbf{a}_{12}\mathbf{a}_{23}})$, se segueix que ha d'ésser $t = t' = 1$, $(K : K^{\mathbf{a}}) = N\mathbf{a}$, com s'ha afirmat.

4. Si Σ és l'àlgebra de quaternions $Q_{\infty,p}$, aleshores $\mathbf{R}$ és un ordre maximal de Σ .

Demostració. Per a un ideal per l'esquerra $\mathbf{a}$ de $\mathbf{R}$ d'ordre maximal, l'anell de multiplicadors de $K_0 = K^{\mathbf{a}}$ és maximal. Com que el subcòs $K^{N\mathbf{a}\varepsilon}$ isomorf a K està contingut en K_0 , aleshores n'hi ha prou amb suposar que $\mathbf{R}$ és maximal i demostrar que tots els subcossos el·líptics de K tenen igualment anells de multiplicadors *maximals*. D'aquí deduirem, per tant, que cada subcòs el·líptic K_0 de K pertany a un ideal per l'esquerra $\mathbf{a}$ de $\mathbf{R}$: $K_0 = K^{\mathbf{a}}$. D'això se segueix novament que hi ha tants subcossos el·líptics de K , sobre els quals K té un grau prèviament donat n , com ideals per l'esquerra enters de $\mathbf{R}$ de norma n . Descomponguem n en una potència p^f de la característica i en un producte de potències de primers $n_0 = \prod q_i^{f_i}$ coprimes amb aquella. Cada ideal per l'esquerra enter de $\mathbf{R}$ de norma n és la intersecció d'ideals per l'esquerra de normes $p^f, q_1^{f_1}, q_2^{f_2}, \dots$ unívocament determinats. S'obté fàcilment que el nombre d'ideals per l'esquerra enters de norma $q_i^{f_i}$

és igual a $1 + q_i + q_i^2 + \cdots + q_i^{f_i}$, en canvi, hi ha solament un ideal per l'esquerra enter de norma p^f . En conseqüència, hi ha

$$\prod (1 + q_i + q_i^2 + \cdots + q_i^{f_i})$$

ideals per l'esquerra enters de norma n .

Atès que en K no hi ha cap classe de divisors d'ordre p , aleshores el grup de Galois de K sobre un subcòs K_0 amb $(K : K_0) = n$ és d'ordre n_0 i K_0 és la potència p^f -èsima del cos d'invariants d'aquest grup de Galois. Com a conseqüència d'això, hi ha tants cossos K_0 com grups de classes d'ordre n_0 -èsim de K . Atès que el grup de totes les classes amb ordre divisible per n_0 és el producte directe de dos cíclics d'ordre n_0 , aleshores aquest nombre esdevé precisament igual a

$$\prod (1 + q_i + q_i^2 + \cdots + q_i^{f_i}),$$

com s'havia de demostrar.

5. El grup $\mathfrak{C}_q$ de les classes de K l'ordre de les quals és una potència d'un nombre primer q és, per a $q \neq p$, isomorf al grup additiu de les classes de residus mòdul 1 de tots els parells (r_1, r_2) de nombres racionals el denominador dels quals és potència de q ; en canvi, per a $q = p$, o bé és isomorf al grup de les classes de residus mòdul 1 de tots els racionals el denominador dels quals és potència de p —en el cas $\sigma = 1$ —, o bé consisteix únicament en la classe $0 = [\mathfrak{o}]$ —en el cas $\sigma = 2$.

Si $q \neq p$ [i $[\mathfrak{p}]$ és de $\mathfrak{C}_q$], aleshores designarem per $r[\mathfrak{p}]$ el parell de classes de residus associats a la classe $[\mathfrak{p}]$. Per a un multiplicador μ val

$$r\mu[\mathfrak{p}] \equiv r[\mathfrak{p}]S_q(\mu) \pmod{1},$$

on $S_q(\mu)$ designa una matriu q -àdica entera determinada. $\mu \rightarrow S_q(\mu)$ és una representació fidel de $\mathbf{R}$ ¹⁷⁾.

Per a $q = p$, $\sigma = 1$, denotem per $r_1[\mathfrak{p}]$ la classe de residus associada a $[\mathfrak{p}]$. Aleshores, esdevé

$$r_1\mu[\mathfrak{p}] \equiv r_1[\mathfrak{p}]s_p(\mu) \pmod{1}$$

amb un nombre p -àdic enter $s_p[\mu]$. De nou $\mu \rightarrow s_p(\mu)$ és una representació fidel de $\mathbf{R}$.

La representació $S_q(\mu)$ o bé $s_p(\mu)$ pot ésser estesa de manera única a una representació fidel de Σ . *Per a elements μ de $\mathbf{R}$, totes les $S_q(\mu)$ i $s_p(\mu)$ són enteres. Demostrem que, recíprocament, l'element μ de Σ és de $\mathbf{R}$ quan totes les $S_q(\mu)$ i $s_p(\mu)$ són enteres i, en el cas $p \neq 0$, a més, μ és p -entera.*

Demostració. Sigui n un nombre natural per al qual la potència n -èsima de μ és de $\mathbf{R}$. El propi μ pertany a $\mathbf{R}$ quan cada automorfisme $\tau_{\sigma, \mathfrak{p}}$ de $K/K^{n\epsilon}$ també deixa fix $K^{n\mu}$ element a element i si, a més, el grau d'inseparabilitat $I(K : K^{n\epsilon})$ divideix $I(K : K^{n\mu})$. La primera [afirmació] s'obté així: podem suposar que l'ordre de $\tau_{\sigma, \mathfrak{p}}$ és potència d'un nombre primer q . Segons §1 2, per a $q \neq p$ esdevé $n \cdot r[\mathfrak{p}] \equiv 0 \pmod{1}$; en conseqüència,

$$n \cdot r\mu[\mathfrak{p}] \equiv n \cdot r[\mathfrak{p}]S_q(\mu) \equiv 0 \pmod{1};$$

i per a $q = p$, $\sigma = 1$, atès que per a μ p -enter, $s_p(\mu)$ és enter,

$$n \cdot r_1[\mathfrak{p}] \equiv 0 \pmod{1},$$

¹⁷⁾M. DEURING, Arithmetische Theorie der Korrespondenzen algebraischer Funktionenkörper, II §5, 6, Journ. f. d. r. u. ang. Math. **183**, p. 25–36 (1941).

$$n \cdot r_1 \mu[\mathfrak{p}] \equiv n \cdot r_1[\mathfrak{p}] s_p(\mu) \equiv 0 \pmod{1};$$

per tant, segons §1 **2**, $\tau_{\mathfrak{o}, \mathfrak{p}}$ és un automorfisme de $K/K^{n\mu}$.

Demostrem que $I(K : K^{n\varepsilon}) | I(K : K^{n\mu})$ de la manera següent: sigui p^f la potència de p que divideix n i p^λ la que divideix $N\mu$. Es té que

$$I(K : K^{n\varepsilon}) = p^{f\sigma} \quad \text{i} \quad I(K : K^{n\mu}) = p^{f\sigma+\lambda},$$

però, atès que μ és p -enter, λ és no negatiu.

6. Sigui $\mathfrak{K}$ un grup de classes finit de K . Denoti $\mathfrak{K}_q$ el subgrup dels elements de $\mathfrak{K}$ l'ordre dels quals és una potència d'un nombre primer q . Per a $q \neq p$, les matrius q -àdiques racionals

$$R = \begin{pmatrix} r_{11} & r_{12} \\ r_{21} & r_{22} \end{pmatrix},$$

tals que les dues files (r_{i1}, r_{i2}) , preses mod 1, són associades a classes contingudes en $\mathfrak{K}_q$ formen un ideal per l'esquerra $\mathfrak{l}_q$ en l'anell de les matrius q -àdiques enteres. Com que la diferència de dues matrius R és de nou una matriu R , perquè $\mathfrak{K}_q$ és un grup, el producte GR d'una matriu entera G amb una matriu R té com a files combinacions lineals enteres de files de R , i, per tant, ella mateixa és una matriu R ; en conclusió, el producte de cada matriu R amb el denominador principal d'un nombre finit de $r[\mathfrak{p}]$, $[\mathfrak{p}]$ en $\mathfrak{K}_q$, és enter. Atès que totes les matrius enteres estan contingudes en $\mathfrak{l}_q$, $\mathfrak{r}_q = \mathfrak{l}_q^{-1}$ és un ideal per la dreta enter. L'ideal $\mathfrak{r}_q$ estarà generat per una matriu q -àdica entera C_q , determinada unívocament a menys d'un factor per la dreta unimodular. La matriu R pertany a $\mathfrak{l}_q$ exactament quan RC_q és entera. *Doncs, els elements $[\mathfrak{p}]$ del grup $\mathfrak{K}_q$ són*

caracteritzats per

$$(5) \quad r[\mathfrak{p}]C_q \equiv 0 \pmod{1},$$

i l'ordre de $\mathfrak{K}_q$ és la potència de q continguda en el determinant de C_q . Gairebé totes les C_q són unimodulars i poden ser preses iguals a la matriu unitat E .

En el cas $p \neq 0$, $\sigma = 1$, $\mathfrak{K}$ també pot tenir un p -subgrup $\mathfrak{K}_p$. Aquells elements associats a les classes de residus $r_1[\mathfrak{p}]$ tenen un denominador principal c_p , que és unívocament determinat a menys d'un factor unitari p -àdic. *Aleshores, els elements de $\mathfrak{K}_p$ són caracteritzats per*

$$(6) \quad r_1[\mathfrak{p}]c_p \equiv 0 \pmod{1}$$

i l'ordre de $\mathfrak{K}_p$ és la potència de p continguda en c_p .

El grup $\mathfrak{K}$ queda determinat per tots els C_q i c_p .

Si, recíprocament, per a cada nombre primer $q \neq p$ són donats una matriu q -àdica entera C_q , que no és unimodular únicament per a un nombre finit de q i, a més, en el cas $p \neq 0$, $\sigma = 1$, un nombre p -àdic enter c_p , aleshores a ells els pertany un grup de classes finit $\mathfrak{K}$.

7. Siguin K_0 un subcòs el·líptic de K i $\mathfrak{K}$ el grup de classes que és isomorf al grup de Galois de K/K_0 mitjançant $[\mathfrak{p}] \rightarrow \tau_{\mathfrak{o}, \mathfrak{p}}$. Dins de K , K_0 és determinat per $\mathfrak{K}$ i $I(K : K_0)$ o, allò que és el mateix, per les matrius C_q , c_p i $I(K : K_0)$.

A partir de la representació $[\mathfrak{p}] \rightarrow r[\mathfrak{p}]$ del q -grup de classes $\mathfrak{C}_q$ de K , pot ésser deduïda una representació associada del q -grup de classes de K_0 , per a la qual s'ha posat

$$(7) \quad r[N_{K/K_0}\mathfrak{p}] \equiv r[\mathfrak{p}]C_q \pmod{1}.$$

Llavors, l'homomorfisme $r[\mathfrak{p}] \rightarrow r[\mathfrak{p}]C_q$ aplica en 0 exactament els $[\mathfrak{p}]$ per als quals $\tau_{\sigma, \mathfrak{p}}$ és un automorfisme de K/K_0 (§1 6). De la mateixa manera, en el cas $p \neq 0$, $\sigma = 1$, per al p -grup de classes es posarà

$$(8) \quad r_1[N_{K/K_0}\mathfrak{p}] \equiv r_1[\mathfrak{p}]c_p \pmod{1}.$$

Si μ és un multiplicador comú de K i de K_0 , aleshores per a cada element $[\mathfrak{p}]$ de $\mathfrak{C}_q$ val

$$(9) \quad \begin{aligned} r\mu[N_{K/K_0}\mathfrak{p}] &\equiv r[N_{K/K_0}(\mu[\mathfrak{p}])] \equiv r\mu[\mathfrak{p}]C_q \equiv r[\mathfrak{p}]S_q(\mu)C_q \\ &\equiv r[N_{K/K_0}\mathfrak{p}]C_q^{-1}S_q(\mu)C_q \pmod{1} \end{aligned}$$

i de la mateixa manera, en el cas $p \neq 0$, $\sigma = 1$, per a un element $[\mathfrak{p}]$ de $\mathfrak{C}_p$,

$$(10) \quad \begin{aligned} r_1\mu[N_{K/K_0}\mathfrak{p}] &\equiv r_1[N_{K/K_0}(\mu[\mathfrak{p}])] \equiv r_1\mu[\mathfrak{p}]c_p \equiv \\ &\equiv r_1[\mathfrak{p}]s_p(\mu)c_p \equiv r_1[N_{K/K_0}\mathfrak{p}]s_p(\mu) \pmod{1}. \end{aligned}$$

En altres paraules:

La matriu C_q transforma la representació q -àdica de Σ que correspon a K en la que correspon a K_0 mentre que en el cas $p \neq 0$, $\sigma = 1$ a K i K_0 els correspon la mateixa representació p -àdica de Σ .

8. Ara determinem més exactament les representacions $S_q(\mu)$, $s_p(\mu)$.

Atès que el multiplicador natural n no és més gran que la imatge de la potència n -èsima en el grup de classes, val:

Si Σ és el cos dels racionals, aleshores
 $S_q(n) = \begin{pmatrix} n & 0 \\ 0 & n \end{pmatrix}$ *és la representació idèntica de Σ presa dues vegades i $s_p(n) = n$.*

Si $\Sigma = Q_{\infty,p}$, aleshores $S_q(\mu)$ és la representació q -àdica irreductible de segon grau de Σ .

Perquè no hi ha cap altra representació q -àdica irreductible de $Q_{\infty,p}$.

Resta investigar de més a prop el cas en què Σ és un cos quadràtic imaginari. *Afirmem que, aleshores, per a $q \neq p$, $S_q(\mu)$ és la representació regular de Σ i, en el cas $p \neq 0$, $\sigma = 1$, $s_p(\mu)$ és la representació $\mathbf{p}_1$ -àdica de Σ , on $\mathbf{p}_1$ denota un dels dos ideals primers diferents de Σ que divideixen p .*

L'afirmació sobre $s_p(\mu)$ és palesa, perquè no es poden donar altres representacions p -àdiques de primer grau de Σ . De la mateixa manera, és palesa l'afirmació sobre cada $q \neq p$ que a Σ no descompon completament. Sigui $q \neq p$ el producte en Σ de dos ideals primers $\mathbf{q}_1$ i $\mathbf{q}_2$ diferents. Aleshores, hi ha dues representacions q -àdiques racionals no equivalents de primer grau Δ_1 i Δ_2 de Σ i cal mostrar que $S_q(\mu)$ és equivalent a la suma $\Delta_1 + \Delta_2$. La representació Δ_i aplica els μ divisibles per $\mathbf{q}_i$ exactament en els nombres divisibles per q . Atès que, d'acord amb 7, l'afirmació necessita ésser demostrada només per als subcossos el·líptics arbitraris de K , podem suposar que $\mathbf{R}$ és l'ordre maximal de Σ . Suposem que $S_q(\mu)$ no fos equivalent a $\Delta_1 + \Delta_2$ sinó que ho fos a $2\Delta_1$. Per a un element μ de $\mathbf{R}$ divisible per $\mathbf{q}_2$ però no per $\mathbf{q}_1$, el determinant $|S_q(\mu)|$ aleshores no seria divisible per q , i, per tant, no hi hauria cap classe d'ordre q amb $r\mu[\mathbf{p}] \equiv 0 \pmod{1}$ o $\mu[\mathbf{p}] = 0$. Doncs, el grup de Galois de K/K^μ no contindria cap element d'ordre q , la qual cosa contradiu que $(K : K^\mu) = N\mu$ és divisible per q .

9. Examinem ara més exactament el cas en què Σ és un cos de nombres quadràtic imaginari.

Els nombres μ_q de les extensions q -àdiques Σ_q de Σ per a les quals $S_q(\mu_q)$ és una matriu q -àdica entera formen un ordre $\mathbf{R}_q$ de Σ_q ($\mu_q[\mathfrak{p}]$ es defineix per

$$r\mu_q[\mathfrak{p}] = \lim_{i \rightarrow \infty} r\mu_i[\mathfrak{p}],$$

per a una successió de nombres μ_i de $\mathbf{R}$ convergents a μ_q). Si designem encara en el cas $p \neq 0$ per $\mathbf{R}_p$ l'ordre maximal de Σ_p , aleshores $\mathbf{R}$ és la intersecció de tots els $\mathbf{R}_q$ i $\mathbf{R}_p$, i $\mathbf{R}_q$ ($q \neq p$ o bé $= p$) és el completat q -àdic de $\mathbf{R}$.

Per a $\mathbf{R}$ complexos i commutatius procurem ara demostracions pendents del fet que l'ordre $\mathbf{R}'$ d'un ideal $\mathbf{a}$ de $\mathbf{R}$ és l'anell de multiplicadors de $K^{\mathbf{a}}$ i que és $(K : K^{\mathbf{a}}) = N\mathbf{a}$.

Mitjançant una base escaient $\omega_1(q)$, $\omega_2(q)$ de $\mathbf{R}_q$, la representació $S_q(\mu)$ és generada per:

$$\mu(\omega_1(q), \omega_2(q)) = (\omega_1(q), \omega_2(q))S_q(\mu).$$

Sigui α_1 , α_2 una base de $\mathbf{a}$,

$$(\alpha_1, \alpha_2) = (\omega_1(q), \omega_2(q))A_q.$$

De

$$\alpha(\omega_1(q), \omega_2(q)) = (\alpha_1, \alpha_2)A_q^{-1}S_q(\alpha)$$

se segueix que $A_q^{-1}S_q(\alpha)$ és entera per a α de $\mathbf{a}$, A_q és, per tant, un divisor comú per l'esquerra de totes les matrius $S_q(\alpha)$, $\alpha \equiv 0 \pmod{\mathbf{a}}$. D'altra banda, A_q es pot expressar per mitjà de dues matrius q -àdiques enteres H_1 i H_2 en la forma

$$A_q = S_q(\alpha_1)H_1 + S_q(\alpha_2)H_2,$$

únicament necessitem determinar els H_i mitjançant

$$(\omega_1(q), \omega_2(q))H_1 = (1, 0),$$

$$(\omega_1(q), \omega_2(q))H_2 = (0, 1).$$

Doncs, A_q és un màxim comú divisor per l'esquerra de totes les $S_q(\alpha)$, $\alpha \equiv 0 \pmod{\mathfrak{a}}$.

Per a un element $\tau_{\mathfrak{o}, \mathfrak{p}}$ del grup de Galois de $K/K^{\mathfrak{a}}$, l'ordre del qual és una potència de q , val $\mathfrak{a}[\mathfrak{p}] = 0$; per tant, $r\alpha[\mathfrak{p}] \equiv 0 \pmod{1}$, si $\alpha \equiv 0 \pmod{\mathfrak{a}}$ o bé $r[\mathfrak{p}]S_q(\alpha) \equiv 0 \pmod{1}$, i, per tant, $r[\mathfrak{p}]A_q \equiv 0 \pmod{1}$. Recíprocament, si $r[\mathfrak{p}]A_q \equiv 0 \pmod{1}$ per a una classe $[\mathfrak{p}]$, l'ordre de la qual és una potència de q , aleshores es té que

$$r\alpha[\mathfrak{p}] \equiv r[\mathfrak{p}]S_q(\alpha) \equiv 0 \pmod{1} \text{ per a tot } \alpha \equiv 0 \pmod{\mathfrak{a}}$$

i, per tant, $\tau_{\mathfrak{o}, \mathfrak{p}}$ és un automorfisme de $K/K^{\mathfrak{a}}$. Això significa que per al subcòs $K_0 = K^{\mathfrak{a}}$ podem suposar que la matriu S_q és igual a A_q . Doncs, a $K^{\mathfrak{a}}$ correspon la representació q -àdica $A_q^{-1}S_q(\mu)A_q$, el completat q -àdic $\mathbf{R}'_q$ de l'anell de multiplicadors $\mathbf{R}'$ de $K^{\mathfrak{a}}$ és l'ordre del mòdul $\mathfrak{a}_q$, el completat q -àdic de $\mathfrak{a}$ i $\mathbf{R}'$ és la intersecció de tots els $\mathbf{R}'_q$ amb $\mathbf{R}_p$, però aquest és l'ordre de $\mathfrak{a}$.

Podem demostrar ara que $(K : K^{\mathfrak{a}}) = N\mathfrak{a}$ literalment com per als $\mathbf{R}$ maximals. De fet, només cal remarcar que $\mathbf{R}_2$ és l'anell de multiplicadors de $\mathfrak{a}_{12}$; i que també per als $\mathbf{R}_2$ no maximals pot ésser escollit un ideal $\mathfrak{a}_{23}$ primer amb $(K : K^{\mathfrak{a}})$, de manera que $\mathfrak{a}_{12}\mathfrak{a}_{23}$ sigui un ideal principal ¹⁸⁾.

¹⁸⁾W. WEBER, Bemerkungen zur arithmetischen Theorie der binären quadratischen Formen, Nachr. Ges. d. Wiss. Göttingen, 1929, p. 116–130; Satz 1.

10. Del que precedeix se'n dedueixen condicions restrictives per als tipus dels anells de multiplicadors. Mentre deixem de banda el cas de multiplicadors únicament racionals, afirmem:

Tingui K un anell de multiplicadors complexos $\mathbf{R}$ de cos de quocients Σ . Si la característica de K és 0, aleshores Σ és un cos de nombres quadràtic imaginari. Si la característica és $p \neq 0$ i $\sigma = 1$, aleshores Σ és un cos de nombres quadràtic imaginari, en el qual p descompon en dos ideals primers diferents i $\mathbf{R}$ és un ordre de Σ de conductor no divisible per p . Per contra, si $\sigma = 2$, aleshores és $\Sigma = Q_{\infty,p}$ i $\mathbf{R}$, un ordre maximal de $Q_{\infty,p}$.

L'afirmació per a $p = 0$ ja ha estat demostrada. Sigui $p \neq 0$ i $\sigma = 1$. Atès que hi ha una representació p -àdica $\mu \rightarrow s_p(\mu)$ de Σ , p descompon en dos ideals primers diferents de Σ . Atès que $\mathbf{R}$ és la intersecció de tots els $\mathbf{R}_q$, la potència de p continguda en el conductor de $\mathbf{R}$ és el conductor de $\mathbf{R}_p$; però $\mathbf{R}_p$ és l'ordre maximal de Σ_p (9), per tant, el seu conductor, 1. En el cas $p \neq 0$, $\sigma = 2$, és $K^{p^\varepsilon} = K^{p^2}$ i, per tant, $j^{p^2} = j$, en conseqüència, hi ha únicament un nombre finit de tipus de cossos no isomorfs d'aquesta forma, en particular el K donat té únicament un nombre finit de subcossos el·líptics no isomorfs. Si Σ fos un cos de nombres quadràtic imaginari i no $Q_{\infty,p}$, aleshores, entesos $q_1, q_2, \dots$ pels nombres primers que resten primers en Σ , els termes d'una successió $K = K_1, K_2, \dots$ de subcossos de K , on cadascun dels K_i és cíclic sobre K_{i+1} de grau q_i , tindrien invariants completament diferents, perquè altrament hi hauria en Σ nombres enters de norma $q_i q_{i+1} \cdots q_{i+h}$.

§3. Multiplicadors en el cas de cos de constants no algebraicament tancat. La representació dels anells de multiplicadors per mitjà de les diferencials enteres associades

1. Considerem, com en les seccions anteriors, un cos de funcions el·líptiques K de cos de constants k algebraicament tancat. Si x, y són un parell d'elements generadors de K/k i els coeficients de l'equació irreductible $f(x, y) = 0$ pertanyen a un subcòs $k^{(0)}$ de k , aleshores hi ha un subcòs $K^0 = k^{(0)}(x, y)$ de K de cos de constants $k^{(0)}$ a partir del qual K resulta per extensió de constants. $k^{(0)}$ conté sempre l'invariant j de K . D'altra banda, x, y poden ésser escollits de manera que $k^{(0)} = P(j)$ i que $K^{(0)} = P(j; x, y)$ sigui un cos de funcions el·líptiques amb almenys un divisor primer de primer grau (P denota el cos primer)¹⁹. Per tant, $P(j)$ és el cos de constants més petit possible per a un cos de funcions K^0 , a partir del qual K pot ésser obtingut per extensió de constants, $K^{(0)}k = K$.

2. Sigui $K^{(0)} = k^{(0)}(x, y)$ un cos el·líptic amb $K^{(0)}k = K$. Ens preguntem a continuació per a quins cossos $k^{(1)}$ continguts entre $k^{(0)}$ i k un multiplicador donat μ de K/k ja es troba en $k^{(1)}(x, y) = K^{(1)}$, és a dir, quan el doble cos $K^{(1)}K^{(1)\varphi}$ format amb un dels cossos $K^{(1)\varphi}/k^{(1)}$ isomorfs a $K^{(1)}/k^{(1)}$ mitjançant $x \rightarrow x^\varphi, y \rightarrow y^\varphi$, té com a cos de funcions de x^φ sobre K un divisor $\mathfrak{D}$ que defineix el multiplicador μ .

¹⁹) Cf. M. DEURING: Invarianten und Normalformen elliptischer Funktionenöper un Zur Theorie der Moduln algebraischer Funktionenkörper, Math. Zeitschr. **47**, p. 34–56 (1941).

Atès que només volem arribar al tipus, suposem que $K^{(0)}$ té un divisor primer $\mathfrak{o}$ de primer grau. Com per a k , podem aleshores determinar unívocament per $\mathfrak{P}_\mu \sim \mathfrak{D}\mathfrak{o}^\varphi / \mathfrak{D}(\mathfrak{o})^\varphi$ un divisor primer de primer grau, $\mathfrak{P}_\mu$, que defineixi el multiplicador μ i per al qual se satisfaci ²⁰⁾ $\mathfrak{P}_\mu(\mathfrak{o}) = \mathfrak{o}$. L'element z^μ de $K^{(1)}$ determinat unívocament per

$$z^\varphi \equiv z^\mu \pmod{\mathfrak{P}_\mu}$$

per a cada z de $K^{(1)}$, proporciona un meromorfisme $z \rightarrow z^\mu$ de $K^{(1)}/k^{(1)}$ normat per $\mathfrak{o}$; per tant, *si el multiplicador μ és possible en $K^{(1)}$, llavors també el corresponent meromorfisme normat per $\mathfrak{o}$.*

Els multiplicadors de $K^{(1)}/k^{(1)}$ constitueixen un subanell $\mathbf{R}_1$ de l'anell de multiplicadors complet $\mathbf{R}$ de K/k .

Signi *du* una diferencial entera de $K^{(0)}$. Mitjançant

$$(11) \quad (du)^\mu = \mu' du$$

es defineix una aplicació homomorfa $\mu \rightarrow \mu'$ de $\mathbf{R}$ en el cos de constants k .

Si la característica p és igual a 0, aleshores per a $\mu \neq 0$ també val $\mu' \neq 0$ i, per tant, en aquest cas, la representació $\mu \rightarrow \mu'$ és fidel. Si, en canvi, és $p \neq 0$, aleshores no pot ésser fidel, perquè com que k i $\mathbf{R}$ tenen característiques diferents, aquesta ha d'aplicar fidelment l'anell de classes de residus de $\mathbf{R}$ segons un ideal primer $\mathfrak{p}$ que divideix p . Atès que $\mu \neq 0$ i $\mu' = 0$ només es pot donar si K sobre K^μ és inseparable, *aleshores $\mathfrak{p}$ consta, a més dels $\mu = 0$, de tots els $\mu \neq 0$ per als quals K sobre K^μ té un grau d'inseparabilitat I_μ diferent de 1. Si $\Sigma = P_0$, aleshores és*

²⁰⁾ Loc. cit. ¹⁴⁾.

$\mathbf{p} = \mathbf{R}p$; si Σ és un cos de nombres quadràtic imaginari, aleshores segons §2 10, p descompon en dos ideals primers diferents de $\mathbf{R}$, un dels quals és $\mathbf{p}$; si $\Sigma = Q_{\infty, p}$, aleshores $\mathbf{p}$ és l'únic ideal primer de $\mathbf{R}$ que divideix p .

3. A partir de la definició de la representació $\mu \rightarrow \mu'$ se segueix immediatament:

Si μ ja és possible en $K^{(1)}$ aleshores μ' es troba en $k^{(1)}$.

D'això, val el recíproc següent:

Si $\mathbf{R}$ és commutatiu, aleshores μ és possible en $K^{(1)}$, en el cas en què μ' es troba en $k^{(1)}$. Per a la demostració no suposem d'entrada que μ' es troba en k .

Per a fer possible μ en $K^* = k^*(x, y)$, n'hi ha prou amb una extensió algebraica finita k^* de k . Si n és el grau de y en $k^{(1)}(x)$ i

$$x^\mu = \sum_{i=0}^{n-1} A_i(x)y^i, \quad y^\mu = \sum_{i=0}^{n-1} B_i(x)y^i,$$

n'hi ha prou d'adjuntar els coeficients de les funcions racionals A_i i B_i , unívocament determinades, però aquests són algebraics sobre $k^{(1)}$, perquè un coeficient transcendent, especialitzat algebraicament, donaria lloc a una infinitat de nous multiplicadors la norma dels quals estaria per sota d'una fita fixada. *Els coeficients de A_i i B_i són fins i tot separables sobre $k^{(1)}$.* Si μ és enter racional, aleshores es troben en $k^{(1)}$, perquè els multiplicadors racionals enters poden ésser obtinguts a partir del multiplicador unitat $x \rightarrow x$, $y \rightarrow y$ per addició. Per a $p = 0$ no hi ha res més a demostrar. Però, per a $p \neq 0$ i $\mathbf{R}$ complex, l'invariant j de K és algebraic absolut, de la qual cosa se'n segueix la separabilitat dels coeficients de A_i i B_i , perquè $k^{(1)}$ és complet: per

a $\sigma = 2$ és $K^{\varepsilon p} = K^{p^2}$ i, per tant, $j^{p^2} = j$; per a $\sigma = 1$, segons §2 10, p descompon en dos ideals primers diferents de $\mathbf{R}$ i per a un dels quals, $\mathbf{p}$, ha d'ésser $K^{\mathbf{p}} = K^p$, perquè segons 2, val $N\mathbf{p} = p$. Si $\mathbf{p}^h = (\pi)$ és un ideal principal, aleshores és $K^{p^h} = K^\pi \simeq K$ i, per tant, $j^{p^h} = j$.

Prendrem k^* com una extensió normal, separable i finita de $k^{(1)}$. Sigui ϱ un automorfisme de $k^*/k^{(1)}$. Ens el pensarem en $K^* = K^{(1)}k^*$ en tant que posem $x^\varrho = x$, $y^\varrho = y$, la qual cosa és possible perquè els coeficients de l'equació $f(x, y) = 0$ entre x i y es troben en k_0 i, amb més motiu, en $k^{(1)}$. Igualment, x^μ i y^μ satisfan l'equació

$$f(x^\mu, y^\mu) = 0,$$

de la qual se segueix

$$f((x^\mu)^\varrho, (y^\mu)^\varrho) = 0.$$

En conseqüència, $z \rightarrow (z^\mu)^\varrho$ és un meromorfisme μ^ϱ de K^*/k^* . Si μ^ϱ és normat per $\mathfrak{o}$, aleshores de $\mathfrak{o}|\mathfrak{o}^{\mu^\varrho}$ se segueix $\mathfrak{o}^\varrho|\mathfrak{o}^{\mu^\varrho}$ o bé $\mathfrak{o}|\mathfrak{o}^{\mu^\varrho}$. Es té que $\mu \rightarrow \mu^\varrho$ és un automorfisme de $\mathbf{R}$.

$$(\mu\nu)^\varrho = \mu^\varrho\nu^\varrho$$

se segueix immediatament de la definició de ϱ . Demostrem que

$$(\mu + \nu)^\varrho = \mu^\varrho + \nu^\varrho,$$

mentre estenem ϱ a $K^*K^{*\varphi}$ mitjançant $(x^\varphi)^\varrho = x^\varphi$, $(y^\varphi)^\varrho = y^\varphi$, i després mostrem que $\mathfrak{P}_{\mu^\varrho} = \mathfrak{P}_\mu^\varrho$. Aleshores, de $\mu + \nu + \lambda = 0$ se segueix primerament que $\mathfrak{P}_\mu\mathfrak{P}_\nu\mathfrak{P}_\lambda \sim \text{const.}$, d'on, per aplicació de ϱ ,

$$\mathfrak{P}_{\mu^\varrho}\mathfrak{P}_{\nu^\varrho}\mathfrak{P}_{\lambda^\varrho} \sim \text{const.},$$

i això significa que $\mu^{\varrho} + \nu^{\varrho} + \lambda^{\varrho} = 0$. Atès que és

$$x^{\varphi} \equiv x^{\mu}, \quad y^{\varphi} \equiv y^{\mu} \quad \text{mod } \mathfrak{P}_{\mu},$$

se satisfà que

$$x^{\varphi} \equiv x^{\mu^{\varrho}}, \quad y^{\varphi} \equiv y^{\mu^{\varrho}} \quad \text{mod } \mathfrak{P}_{\mu}^{\varrho},$$

però això significa que $\mathfrak{P}_{\mu^{\varrho}} = \mathfrak{P}_{\mu}^{\varrho}$, atès que $\mathfrak{P}_{\mu^{\varrho}}$ és determinat pels residus de x^{φ} i y^{φ} . De

$$(du)^{\mu} = \mu' du$$

se segueix que

$$(du)^{\mu^{\varrho}} = \mu'^{\varrho} du;$$

per tant, la representació $\mu \rightarrow \mu'$ es transforma per ϱ de la mateixa manera que el mateix $\mathbf{R}$.

Si ara suposem que μ' es troba en $k^{(1)}$, aleshores val

$$(du)^{\mu^{\varrho}} = \mu' du.$$

Si la característica és $p = 0$, aleshores se segueix immediatament que $\mu^{\varrho} = \mu$ atesa la fidelitat de la representació $\mu = \mu'$; en conseqüència, els coeficients de A_i i B_i són invariants per a cada ϱ i per tant s'han de trobar en $k^{(1)}$, com s'ha afirmat. En el cas $p \neq 0$, no ho podem concloure tan fàcilment. Atès que hem suposat $\mathbf{R}$ commutatiu, p descompon, com ja s'ha dit, en dos ideals primers diferents $\mathbf{p}_1$ i $\mathbf{p}_2$ de $\mathbf{R}$. L'únic automorfisme de $\mathbf{R}$ diferent de la identitat intercanvia $\mathbf{p}_1$ i $\mathbf{p}_2$. Si ara no fos $\mu^{\varrho} = \mu$, un multiplicador μ divisible per $\mathbf{p}_1$ però no per $\mathbf{p}_2$ seria aplicat en un multiplicador μ^{ϱ} i, d'una banda, seria $\mu' = 0$ perquè μ es troba en $\mathbf{p}_1$, i, d'altra banda, $\mu' \neq 0$, perquè μ^{ϱ} no es troba en

p₁. Amb això, $\mu = \mu^\varrho$, i concloem com més amunt que μ és possible en $K^{(1)}$.

4. No totes les translacions $\tau_{\mathfrak{o}, \mathfrak{q}}$ de K són ja possibles en $K^{(0)}$, és a dir, transformen $K^{(0)}$ en ell mateix, sinó exactament aquelles per a les quals $\mathfrak{q}$ ja és un divisor primer de $K^{(0)}$. En conseqüència s'obté el cos de constants més petit $k^{(1)}$ per al qual $\tau_{\mathfrak{o}, \mathfrak{q}}$ és possible, a partir de $k^{(0)} = P(j)$, per adjunció de residus mòdul $\mathfrak{q}$ d'elements d'un cos

$$K^{(0)} = k^{(0)}(x, y) = P(j; x, y),$$

quan $\mathfrak{o}$ és un divisor de primer grau en aquest cos $K^{(0)}$. Aquest cos $k^{(1)}$ és algebraic finit sobre $k^{(0)} = P(j)$, si $\mathfrak{q}$ s'aplica en un divisor primer $\mathfrak{q}^*$ de $K^{(0)}$, per tant, en particular, per a les úniques translacions importants aquí d'ordre finit. Si $\tau_1, \dots, \tau_{n_0}$ són totes les translacions l'ordre de les quals divideix n , aleshores $\left(\mathfrak{o}^{\sum_{i=1}^{n_0} \tau_i}\right)^{p^{f\sigma}}$ és el divisor primer de $K^{n\varepsilon}$ divisible per $\mathfrak{o}$, que ja és un divisor primer en $K^{(0)n\varepsilon}$; aquí p^f és la potència de la característica p que divideix n i $n_0 = n^2/p^{\sigma f}$. D'això se segueix, a més, que $k^{(1)}$ és separable sobre $P(j)$ per a n no divisibles per p i per a $\sigma = 1$ té un grau d'inseparabilitat $\leq p^f$; per a $\sigma = 2$ no existeix cap translació d'ordre divisible per p .

§4. El comportament dels multiplicadors per reducció en un divisor primer del cos de constants

1. Del cos de funcions el·líptiques K no suposem ara altra cosa que el seu cos de constants k és algebraicament tancat. Sigui $\mathfrak{p}$ un divisor primer de k donat mitjançant una valoració exponencial discreta. Pel que fa a $\mathfrak{p}$ li és

transferit un element no constant ²¹⁾ x de K . Si suposem que 1. $\mathfrak{p}$ roman primer en K , 2. el cos de classes de residus $\overline{K}$ de K mòdul $\mathfrak{p}$ també és el·líptic, i 3. $\overline{K}$ té cos de constants $\overline{k}$, aleshores podem associar a cada divisor $\mathfrak{a}$ de K un divisor $\overline{\mathfrak{a}}$ de $\overline{K}$ com a classe de residus mòdul $\mathfrak{p}$, de tal manera que totes les relacions entre divisors, elements i classes de divisors es mantenen ²¹⁾ per reducció mòdul $\mathfrak{p}$.

2. Examinarem com es comporten els multiplicadors de K per reducció segons $\mathfrak{p}$ i per a aquest fi considerem com en §3, juntament amb K , el doble cos KK^φ . En prendre com a base x^φ , $\mathfrak{p}$ pot ésser transferit de la mateixa manera de K a KK^φ com pel que fa a x , de k a K . Aleshores, el cos de classes de residus $\overline{KK^\varphi} = \overline{K} \overline{K^\varphi}$ és l'extensió de constants corresponent de $\overline{K}/\overline{k}$ i $\overline{z} \rightarrow \overline{z}^\varphi$ és una aplicació isomorfa de $\overline{K}/\overline{k}$ en $\overline{K^\varphi}/\overline{k}$. Aleshores se satisfan de la mateixa manera, per a KK^φ com a cos de funcions de x^φ amb cos de constants K , les hipòtesis 1. 1, 2, 3, per a l'aplicabilitat de la teoria de la reducció. Doncs, els residus mòdul $\mathfrak{p}$ també estan explicats per als divisors de KK^φ/K . Els divisors constants s'apliquen mòdul $\mathfrak{p}$ sobre divisors constants.

Un multiplicador μ de K serà definit mitjançant una classe de residus del grup de divisors de KK^φ/K pel subgrup dels divisors constants. Mòdul $\mathfrak{p}$, aquesta classe s'aplica sobre una corresponent classe de residus per a $\overline{KK^\varphi}/\overline{K}$. D'aquesta manera s'associa unívocament a μ un multiplicador $\overline{\mu}$ de $\overline{K}$. En particular podem representar μ a través d'un meromorfisme μ normat per un divisor primer fixat

²¹⁾ Compareu per a això el treball publicat en Math. Zeitschr.: M. DEURING, Reduktion algebraischer Funktionenkörper nach Primdivisoren des Konstantenkörpers.

de primer grau $\mathfrak{o}$, o bé pel divisor primer associat de primer grau $\mathfrak{P}_\mu$ de KK^φ/K .

Demostrem que $\mu \rightarrow \bar{\mu}$ és una aplicació isomorfa de l'anell de multiplicadors $\mathbf{R}$ de K en una part de l'anell de multiplicadors de $\bar{K}$.

En primer lloc, demostrem que $\mu \rightarrow \bar{\mu}$ és fidel per a la suma: $\mu + \nu + \lambda = 0$ significa que $\mathfrak{P}_\mu \mathfrak{P}_\nu \mathfrak{P}_\lambda \sim \text{const.}$, de la qual cosa se segueix que $\overline{\mathfrak{P}_\mu} \overline{\mathfrak{P}_\nu} \overline{\mathfrak{P}_\lambda} \sim \text{const.}$, i de la qual cosa que

$$\bar{\mu} + \bar{\nu} + \bar{\lambda} = 0.$$

En segon lloc, mostrem que $\mu \rightarrow \bar{\mu}$ està inversament determinat. Ja que $\overline{\mu + \nu} = \bar{\mu} + \bar{\nu}$, n'hi ha prou amb concloure que $\bar{\mu} \neq 0$ a partir de $\mu \neq 0$. $\mu \neq 0$ significa que $\mathfrak{P}_\mu$ no és constant. Per a cada z de K val

$$z^\varphi \equiv z^\mu \pmod{\mathfrak{P}_\mu}$$

i, en particular,

$$x^\varphi \equiv x^\mu \pmod{\mathfrak{P}_\mu}.$$

Hi ha un element z^μ de K^μ que mòdul $\mathfrak{p}$ no és constant. Com que els coeficients de l'equació irreductible de x en K^μ són $\mathfrak{p}$ -enters, però no la totalitat divisibles per $\mathfrak{p}$, no poden ésser tots constants mòdul $\mathfrak{p}$, perquè altrament $\bar{x}$ seria constant. Segons que x sigui $\mathfrak{p}$ -enter o no, escrivim z com a quocient d'elements s i t , els dos x -enters o bé els dos $\frac{1}{x}$ -enters, $z = s/t$. Podem suposar que $\bar{t} \neq 0$. De

$$s^\varphi \equiv s^\mu, \quad t^\varphi \equiv t^\mu \pmod{\mathfrak{P}_\mu}$$

se segueix²¹⁾ que

$$\overline{s^\varphi} \equiv \overline{s^\mu}, \quad \overline{t^\varphi} \equiv \overline{t^\mu} \pmod{\overline{\mathfrak{P}_\mu}},$$

per tant, ja que $\overline{t^\varphi} \neq 0$, que

$$\overline{z^\varphi} = \overline{s^\varphi} / \overline{t^\varphi} \equiv \overline{s^\mu} / \overline{t^\mu} = \overline{z^\mu} \pmod{\overline{\mathfrak{P}_\mu}}.$$

Atès que també el K -element z^φ té el residu $\overline{z^\mu} \pmod{\overline{\mathfrak{P}_\mu}}$ no constant, aleshores $\overline{\mathfrak{P}_\mu}$ no és constant, com s'ha afirmat.

Demostrem a continuació la següent *regla sobre l'intercanvi de l'aplicació de classes de residus mod $\mathfrak{p}$ amb el meromorfisme μ* :

$$(12) \quad \overline{z^\mu} = \overline{z^\mu}$$

per a cada $\mathfrak{p}$ -enter z . Aleshores val també per a divisors

$$(13) \quad \overline{\mathfrak{a}^\mu} = \overline{\mathfrak{a}^\mu}$$

i per a la totalitat de K

$$(14) \quad \overline{K^\mu} = \overline{K^\mu}.$$

N'hi ha prou de demostrar (12) per a z x -enter, perquè cada z és quocient de dos elements x -enters. A continuació mostrem que x^μ és $\mathfrak{p}$ -enter i que $\overline{x^\mu}$ és no constant. Altrament, donat que $1/\overline{x^\varphi} \equiv 0 \pmod{\overline{\mathfrak{P}_\mu}}$ o bé $\overline{x^\varphi} \equiv \overline{x^\mu} \pmod{\overline{\mathfrak{P}_\mu}}$, el divisor $\overline{\mathfrak{P}_\mu}$ seria constant. Per a cada z x -enter, de la congruència $z^\varphi \equiv z^\mu \pmod{\mathfrak{P}_\mu}$ se segueix ara la congruència $\overline{z^\varphi} \equiv \overline{z^\mu} \pmod{\overline{\mathfrak{P}_\mu}}$ i, doncs, $\overline{z^\mu} = \overline{z^\mu}$.

Atès que la normalització de μ s'expressa per $\mathfrak{o}|\mathfrak{o}^\mu$, aleshores és $\overline{\mathfrak{o}}|\overline{\mathfrak{o}^\mu}$ o bé $\overline{\mathfrak{o}}|\overline{\mathfrak{o}^\mu}$; és a dir, $\overline{\mu}$ és normalitzat per $\overline{\mathfrak{o}}$.

Finalment mostrem ara que $\mu \rightarrow \overline{\mu}$ és fidelment multiplicativa; és a dir, $\overline{\mu\nu} = \overline{\mu} \overline{\nu}$. Si μ o bé ν és igual a 0, aleshores és $\overline{\mu\nu} = 0$, i $\overline{\mu} \overline{\nu} = 0$. Si $\mu \neq 0$ i $\nu \neq 0$, aleshores per a cada z de K $\mathfrak{p}$ -enter val

$$\overline{z^\mu}^\nu = (\overline{z^\mu})^\nu = \overline{(z^\mu)^\nu} = \overline{(z^\mu)^\nu} = \overline{z^{\mu\nu}} = \overline{z^{\mu\nu}},$$

però això significa que $\overline{\mu} \overline{\nu} = \overline{\mu\nu}$, com s'ha afirmat.

3. Si són donats K i el divisor primer $\mathfrak{p}$ en el seu cos de constants k , aleshores el tipus del cos de classes de residus $\overline{K}$ depèn encara del x de K en què hem basat l'expressió de $\mathfrak{p}$; intentarem escollir x de manera que se satisfacin les condicions 1, 2, 3, de 1. Sobre això val el teorema següent:

Sota la suposició que j és $\mathfrak{p}$ -enter, x pot ésser escollit de manera que $\mathfrak{p}$ romangui primer en K i $\overline{K}$ esdevingui el·líptic de cos de constants $\overline{k}$. L'invariant de $\overline{K}$ és el $\mathfrak{p}$ -residu $\overline{j}$ de j . Per a obtenir un x apropiat, s'ha d'estendre eventualment k circumstancial algebraicament i finitament i, després, substituir $\mathfrak{p}$ per un dels seus divisors primers en l'extensió.

Demostració. Atès que cal donar una extensió algebraica finita de k , podem fer servir de base una equació definidora de K en la forma normal

$$y^2 = x(x-1)(x-\lambda) \quad \text{o bé} \quad y^2 - y + \alpha xy = x^3,$$

segons que la característica p de K sigui diferent de 2 o bé de 3 ²²⁾. Aquí és

$$2^8(1-\lambda(1-\lambda))^3 = j\lambda^2(1-\lambda)^2, \quad (\alpha^3+24)^3 + j(\alpha^3+27) = 0,$$

$$\text{i} \quad \lambda \neq 0, 1,$$

$$\text{i} \quad \alpha^3 + 27 \neq 0.$$

De la suposició que j és $\mathfrak{p}$ -enter, se segueix que λ és $\mathfrak{p}$ -enter i que $\overline{\lambda} \neq 0, 1$ o bé que α és $\mathfrak{p}$ -enter i $\overline{\alpha}^3 + 27 \neq 0$. Amb això, si x esdevé l'extensió del $\mathfrak{p}$ de K , pres per base,

$$\overline{y}^2 = \overline{x}(\overline{x}-1)(\overline{x}-\overline{\lambda}) \quad \text{o bé} \quad \overline{y}^2 - \overline{y} + \overline{\alpha} \overline{x} \overline{y} = \overline{x}^3$$

²²⁾ Loc. cit. ¹⁹⁾

és irreductible i defineix un cos el·líptic $\overline{K}$ de cos de constants $\overline{k}$.

Del teorema que acabem de demostrar val el recíproc següent:

Si x pot ésser escollit en K de manera que $\mathfrak{p}$ romangui primer en K i $\overline{K}$ esdevingui el·líptic de cos de constants $\overline{k}$, aleshores j és $\mathfrak{p}$ -enter i $\overline{K}$ té invariant $\overline{j}$.

Demostració. De nou prenem per base una equació definidora de $\overline{K}$ en la forma

$$\overline{y}^2 = \overline{x}(\overline{x} - 1)(\overline{x} - \overline{\lambda}) \quad \text{o bé} \quad \overline{y}^2 - \overline{y} + \overline{\alpha x y} = \overline{x}^3,$$

atès que no depèn d'una extensió de constants finita. El denominador de $\overline{x}$ és un divisor primer quadrat $\overline{\sigma}^2$. Podem suposar que $\overline{\sigma}$ és el $\mathfrak{p}$ -residu d'un divisor primer σ de K , en tot cas després d'una extensió algebraica finita escaient de constants. Sigui $\mathfrak{q}$ un divisor primer de primer grau de K que mòdul $\mathfrak{p}$ no es transforma en $\overline{\sigma}$, i x_1 un múltiple de $\mathfrak{q}\sigma^{-2}$. Podem suposar que x_1 és primer amb $\mathfrak{p}$. Aleshores $\overline{x}_1$ és un múltiple no constant de $\overline{\sigma}^{-2}$, per tant, $\overline{x}_1 = \overline{\varepsilon} \overline{x} + \overline{\delta}$ amb constants $\overline{\varepsilon}, \overline{\delta}$ i, doncs, igualment podem suposar $\overline{x}_1 = \overline{x}$. De la mateixa manera trobem un element y_1 de K de denominador $\overline{\sigma}^3$, que mòdul $\mathfrak{p}$ s'aplica en $\overline{y}$. Els elements x_1 i y_1 generen el cos K i entre ells se satisfà una equació

$$(15) \quad gy_1^2 + hy_1 + ax_1y_1 = c_0x_1^3 + c_1x_1^2 + c_2x_1 + c_3 = c_0\varphi(x_1),$$

que igualment podem suposar $\mathfrak{p}$ -primitiva. Atès que aquesta mòdul $\mathfrak{p}$ s'ha d'aplicar en l'equació entre x i y , en el primer cas és

$$h \equiv a \equiv 0, \quad g \equiv c_0 \not\equiv 0 \pmod{\mathfrak{p}}$$

i

$$\overline{\varphi(x_1)} = \overline{x}(\overline{x} - 1)(x - \overline{\lambda}).$$

Doncs, $\varphi(x_1)$ té tres arrels ξ_1, ξ_2, ξ_3 amb

$$\overline{\xi_1} = 0, \quad \overline{\xi_2} = 1 \quad \text{i} \quad \overline{\xi_3} = \overline{\lambda}.$$

Si posem

$$\begin{aligned} \frac{x_1 - \xi_1}{\xi_2 - \xi_1} &= x, & \frac{\xi_3 - \xi_1}{\xi_2 - \xi_1} &= \lambda, \\ \left(y_1 + \frac{ax_1 + h}{2} \right) (\xi_2 - \xi_1)^{-\frac{3}{2}} &= y, \end{aligned}$$

aleshores esdevé

$$y^2 = x(x - 1)(x - \lambda),$$

i x, y, λ s'apliquen mòdul $\mathfrak{p}$ en $\overline{x}, \overline{y}, \overline{\lambda}$, de la qual cosa l'afirmació del teorema se segueix immediatament.

En el segon cas és

$$g \equiv -h \equiv c_0 \not\equiv 0 \pmod{\mathfrak{p}}$$

i

$$\overline{\varphi(x_1)} = \overline{x}^3.$$

Apliquem una transformació lineal

$$(16) \quad x_1 = Ax + B, \quad y_1 = Fy + Cx + D$$

tal que transformi

$$(17) \quad gy_1^2 + hy_1 + ax_1y_1 = c_0x_1^3 + c_1x^2 + c_2x + c_3$$

en la forma normal

$$(18) \quad y^2 - y + \alpha xy = x^3.$$

De primer, suposem que la característica de K no és 2, aleshores podem escriure (17) en la forma

$$(19) \quad \begin{aligned} & (gy_1 + \tfrac{1}{2}(ax_1 + h))^2 = gc_0x_1^3 + \\ & + \left(gc_1 + \frac{a^2}{4}\right)x_1^2 + (gc_2 + \tfrac{1}{2}ah)x_1 + \left(gc_3 + \frac{h^2}{4}\right) \end{aligned}$$

i (18) en la forma

$$(20) \quad \left(y + \frac{1}{2}(\alpha x - 1)\right)^2 = x^3 + \frac{\alpha^2}{4}x^2 - \frac{\alpha}{2}x + \frac{1}{4}.$$

El polinomi cúbic de la dreta de (19) s'ha de transformar mitjançant (16) en el polinomi cúbic de la dreta de (20) llevat del factor gc_0A^3 . Això proporciona les dues equacions següents

$$(21) \quad \begin{aligned} gc_0A^3 &= 4gc_0B^3 + (4gc_1 + a^2)B^2 + (4gc_2 + 2ah)B + \\ &+ (4gc_3 + h^2) = \\ &= 4g(c_0B^3 + c_1B^2 + c_2B + c_3) + (aB + h)^2, \end{aligned}$$

$$(22) \quad \begin{aligned} (6gc_0B^2 + (4gc_1 + a^2)B + (2gc_2 + ah))^2 &= \\ &= gc_0A^3(12B + (4gc_1 + a^2)); \end{aligned}$$

a més, per a α , l'expressió

$$(23) \quad \alpha = -\frac{6gc_0B^2 + (4gc_1 + a^2)B + (2gc_2 + ah)}{gc_0A^2}.$$

L'eliminació de A a partir de (21) i (22) proporciona l'equació biquadràtica següent per a B

$$(24) \quad \begin{aligned} 3g^2c_0^2B^4 &+ gc_0(4gc_1 + a^2)B^3 + 3gc_0(2gc_2 + ah)B^2 + \\ &+ 3gc_0(4gc_3 + h^2)B + \\ &+ (4gc_1c_3 + gc_3a^2 + gc_1h^2 - gc_2^2 - ghc_2a) = 0. \end{aligned}$$

Tots els coeficients d'aquesta equació són $\mathfrak{p}$ -enters, el darrer és divisible per $\mathfrak{p}$, però el primer no, atès que la característica és diferent de 3. En conseqüència, (24) té una arrel B divisible per $\mathfrak{p}$ —aquí suposem que (24) té totes les arrels en k , això ja només depèn d'una extensió algebraica finita de k que és determinable. Aleshores de (22) s'obtenen tres valors de A , un dels quals, A , és congru a 1 mod $\mathfrak{p}$.

Ara substituïm (16) immediatament en (17) i comparem els coeficients amb els de (18). El terme constant proporciona

$$(25) \quad gD^2 + (aB + h)D = c_0B^3 + c_1B^2 + c_2B + c_3,$$

aquesta equació té una arrel D divisible per $\mathfrak{p}$. El coeficient de x proporciona

$$(aB + h + 2gD)C = 3c_0AB^2 + 2c_1AB + c_2A.$$

El factor de C a l'esquerra és congru a h mòdul $\mathfrak{p}$; per tant, és no divisible per $\mathfrak{p}$ i, amb més motiu, diferent de 0. Doncs, s'esdevé

$$(26) \quad C = A \frac{3c_0B^2 + 2c_1B + c_2}{aB + h + 2gD},$$

i és palès que C és divisible per $\mathfrak{p}$. Finalment comparem el coeficient de y amb el de x^3

$$2gFD + hF + aBF = -c_0A^3$$

o bé

$$(27) \quad F = -\frac{c_0A^3}{aB + h + 2gD};$$

com que $h + 2gD \equiv h \not\equiv 0 \pmod{\mathfrak{p}}$, és $h + 2gD \neq 0$.

S'esdevé $F \equiv 1 \pmod{\mathfrak{p}}$. A continuació se segueix de (23) que el $\mathfrak{p}$ -residu de α és igual al de a , per tant, igual al del $\bar{\alpha}$ donat. Amb això s'ha trobat una transformació de (17) en la forma normal (18) que és còngrua a la identitat mòdul $\mathfrak{p}$. Aquesta també roman vàlida per a característica 2, perquè el càlcul de B, A, D, C, F a partir de la llista (24), (22), (25), (26) i (27) també val per a característica 2, perquè cap dels denominadors que hi surten s'anul·la per a $2 = 0$.

Amb això s'ha demostrat el teorema enunciat però, a més, el refinament següent:

Si la contribució de $\mathfrak{p}$ en K pot ésser escollida de manera que $\mathfrak{p}$ romangui primer en K i K sigui el·líptic de cos de constants k , i si

$$\bar{y}^2 = \bar{x}(\bar{x} - 1)(\bar{x} - \bar{\lambda}) \quad \text{o bé} \quad \bar{y}^2 - \bar{y} + \bar{\alpha} \bar{x} \bar{y} = \bar{x}^3$$

és una equació definidora de $\bar{K}$, aleshores hi ha un parell d'elements generadors x, y de K que mòdul $\mathfrak{p}$ s'aplica en $\bar{x}, \bar{y}$, i que satisfà una equació

$$y^2 = x(x-1)(x-\lambda) \quad \text{o bé} \quad y^2 - y + \alpha xy = x^3.$$

Aleshores $\bar{\lambda}$ també és el $\mathfrak{p}$ -residu de λ o bé $\bar{\alpha}$ el de α . Eventualment, és necessària una extensió algebraica finita de k .

4. Ara examinarem com es comporten els subcossos el·líptics de K mòdul $\mathfrak{p}$. Siguin $\mathfrak{G}$ un grup d'automorfismes finit de K/k , K^* el seu cos d'invariants i $\mathfrak{p}^*$ el divisor primer de K^* divisible per $\mathfrak{p}$. El grup de Galois de $\bar{K}/\bar{K}^*$ és el grup quocient $\bar{\mathfrak{G}} = \mathfrak{Z}/\mathfrak{I}$ del grup de descomposició $\mathfrak{Z}$ pel grup d'inèrcia $\mathfrak{I}$ de $\mathfrak{p}$ respecte de K^* . D'entrada, apliquem això en el cas en què $\mathfrak{G}$ és generat per una reflexió $\sigma_{\mathfrak{o}, \mathfrak{q}}$. Atès que

K^* és de gènere 0, no pot ésser $\overline{K^*} = \overline{K}$, en conseqüència, és $\mathfrak{Z} = \mathfrak{G}$ i $\mathfrak{T} = 1$, $\mathfrak{p}^* = \mathfrak{p}$ i $\sigma_{\mathfrak{o},q}$ aplica elements $\mathfrak{p}$ -enters en $\mathfrak{p}$ -enters. La reflexió $\sigma_{\mathfrak{o},q}$ indueix en $\overline{K}$ la reflexió $\sigma_{\overline{\mathfrak{o}},\overline{q}}$; doncs, volem dir *que $\sigma_{\mathfrak{o},q} \bmod \mathfrak{p}$ s'aplica en $\sigma_{\overline{\mathfrak{o}},\overline{q}}$* .

D'això se segueix, a més, que la translació $\tau_{\mathfrak{o},q}$ de K s'aplica mòdul $\mathfrak{p}$ en la translació $\tau_{\overline{\mathfrak{o}},\overline{q}}$ de $\overline{K}$. Certament, aquesta aplicació del grup de translacions de K en el de $\overline{K}$ no és necessàriament fidel, sinó que totes les $\tau_{\mathfrak{o},q}$ amb la mateixa $\overline{q}$ van a parar sobre una mateixa translació $\tau_{\overline{\mathfrak{o}},\overline{q}}$. Atès que per a nosaltres només són importants les translacions d'ordre finit, examinarem si, i quines d'aquestes, poden aplicar-se en la identitat.

En primer lloc, considerem el grup de totes les translacions l'ordre de les quals s'aixeca a un nombre natural n no divisible per la característica p . Per a un cos de constants suficientment gran, constitueixen un grup $\mathfrak{G}$ de tipus (n, n) de cos d'invariants $K^* = K^{n\varepsilon}$. D'acord amb §3 2, (14), $K^{n\varepsilon}$ mòdul $\mathfrak{p}$ s'aplica sobre $\overline{K}^{n\varepsilon}$. Per tant, s'esdevé novament que $\mathfrak{Z} = \mathfrak{G}$ (de la qual cosa també se segueix que totes les translacions d'amplituds $\mathfrak{p}$ -enteres es transformen en $\mathfrak{p}$ -enteres), i $\mathfrak{T} = 1$ i totes les n^2 translacions $\tau_{\mathfrak{o},q}$ tals que $n[\mathfrak{q}] = 0$ van a unes altres tantes translacions diferents $\tau_{\overline{\mathfrak{o}},\overline{q}}$ de $\overline{K}$ amb $n[\overline{q}] = 0$, dit d'una altra manera, el grup de les classes de K d'ordre divisible per n s'aplica de manera isomorfa en el corresponent grup de $\overline{K}$. Finalment, també podem formular això com:

Si el nombre primer q és diferent de la característica de $\overline{K}$, aleshores el grup $\mathfrak{C}_q$ de totes les classes de K l'ordre de les quals és una potència de q s'aplica mòdul $\mathfrak{p}$ de manera isomorfa sobre el corresponent grup $\overline{\mathfrak{C}}_q$ de $\overline{K}$.

A continuació, en el cas en què K i $\overline{K}$ tenen característica el mateix nombre primer p , considerem el grup $\mathfrak{C}_p$ de K . Les $p^{f(2-\sigma(K))}$ translacions de K d'ordre divisible per p^f deixen $K^{p^f\varepsilon}$ invariant, però, a més, K té grau d'inseparabilitat $p^{\sigma f}$ sobre $K^{p^f\varepsilon}$. Atès que $K^{p^f\varepsilon}$ s'aplica mòdul $\mathfrak{p}$ en $\overline{K}^{p^f\varepsilon}$, tenim que

Si $\sigma(\overline{K}) = \sigma(K)$, aleshores $\mathfrak{C}_p$ s'aplica de manera isomorfa en $\overline{\mathfrak{C}}_p$, en canvi, per a $\sigma(K) = 1$ i $\sigma(\overline{K}) = 2$ el grup $\mathfrak{C}_p$ diferent de 1 s'aplica sobre $\overline{\mathfrak{C}}_p = 1$.

Finalment, en el cas $Ch.(K) = 0$, $Ch.(\overline{K}) = p \neq 0$, val:

Per a $\sigma(\overline{K}) = 2$, tot $\mathfrak{C}_p$ s'aplica sobre 1; per a $\sigma(\overline{K}) = 1$, solament un subgrup, el qual és isomorf al grup additiu de totes les classes de residus mod 1 dels nombres racionals de denominadors potències de p .

A partir del comportament del grup $\mathfrak{C}_q$, es pot deduir fàcilment com es comporten mòdul $\mathfrak{p}$ els subcossos el·líptics de K . En cada cas és $(\overline{K} : \overline{K}_0) = (K : K_0)$, perquè això val per al subcòs $K^{n\varepsilon}$. El grup de Galois de K/K_0 s'aplica sobre el de $\overline{K}/\overline{K}_0$ i $\overline{K}_0$ és el·líptic. El grau d'inseparabilitat creix conforme a l'empetitiment del grup. A continuació considerem solament aquells K_0 sobre els quals K és cíclic; això és suficient perquè el cos $K^{m\varepsilon}$ isomorf a K és cíclic sobre K_0 , per al nombre natural m més gran per al qual K_0 està contingut en $K^{m\varepsilon}$.

Si n no és divisible per la característica de K , aleshores hi ha

$$(28) \quad \mu(n) = n \prod_{q|n} (1 + q^{-1})$$

cossos K_0 sobre els quals K és cíclic de grau n ; aquests s'apliquen sobre altres tants cossos diferents $\overline{K}_0$ sobre els quals $\overline{K}$ és cíclic de grau n .

Anàlogament és en el cas $Ch.(K) = Ch.(\overline{K}) = p \neq 0$, $\sigma(K) = \sigma(\overline{K}) = 1$ per a $n = p^f$ (i doncs per a tots els n). Aleshores hi ha exactament un subcòs K_0 de K sobre el qual K té un grup cíclic d'ordre p^{f_1} i grau d'inseparabilitat p^{f-f_1} , $0 \leq f_1 \leq f$; aquest cos s'aplica mòdul $\mathfrak{p}$ sobre el subcòs corresponent de $\overline{K}$. Per a $\sigma(K) = \sigma(\overline{K}) = 2$, hi ha un cos K_0 amb $(K : K_0) = p^f$, només la potència K^{p^f} del qual s'aplica mòdul $\mathfrak{p}$ en $\overline{K}^{p^f}$. En canvi, si $\sigma(K) = 1$ i $\sigma(\overline{K}) = 2$, aleshores els $f + 1$ cossos K_0 sobre els quals K té grau p^f s'apliquen tots sobre l'únic cos K^{p^f} .

Resta examinar el cas $Ch.(K) = 0, Ch.(\overline{K}) = p \neq 0$. Si $\sigma(\overline{K}) = 2$, aleshores la totalitat dels cossos K_0 amb $(K : K_0) = p^f$ (no solament aquells sobre els quals K és cíclic) s'apliquen sobre l'únic cos $\overline{K}_0 = \overline{K}^{p^f}$.

Si $\sigma(\overline{K}) = 1$, aleshores dels $p^f + p^{f-1}$ subcossos sobre els quals K és cíclic de grau p^f , p^f s'apliquen en el cos $\overline{K}_0$ sobre el qual $\overline{K}$ és cíclic de grau p^f , un en $\overline{K}^{p^f}$ i de cadascun dels $p^{f-i} - p^{f-i-1}$ de la resta, en cossos $\overline{K}_i$ sobre els quals K és cíclic de grau p^{f-i} i inseparable de grau p^i , $i = 1, 2, \dots, f - 1$.

A saber, sigui τ_1, τ_2 una base del grup de totes les translacions de K d'ordre divisible per p^f i tal que $\tau_2 \pmod{\mathfrak{p}}$ s'apliqui en 1. Llavors, els p^f cossos invariants per les translacions $\tau_1 \tau_2^h$, $h = 1, \dots, p^f$, s'apliquen sobre $\overline{K}_0$, els cossos invariants per les $p^{f-i} - p^{f-i-1}$ translacions $\tau_1^{p^i} \tau_2^h$, $h \pmod{p^{f-i}}$, $(h, p) = 1$, en $\overline{K}_i$, i els cossos invariants de τ_2 ,

en $\overline{K}^{p^f}$. Però en aquest cas també s'apliquen encara altres subcossos de K sobre $\overline{K}_i$, és a dir, els cossos invariants d'aquells grups de translacions no cíclics d'ordre p^f que mòdul $\mathfrak{p}$ s'apliquen en els grups cíclics generats per $\tau_1^{p^i}$.

§5. Els automorfismes de les formes normals uniparamètriques i les unitats dels anells de multiplicadors

1. Sigui K un cos el·líptic d'invariant j . Per a un cos de constants k algebraicament tancat, el podem generar mitjançant l'equació

$$(29) \quad y^2 = x(x-1)(x-\lambda)$$

si la característica és $p \neq 2$, i mitjançant

$$(30) \quad y^2 - y + \alpha xy = x^3,$$

si és $p \neq 3$. Aquí és

$$(31) \quad 2^8(1 - \lambda(1 - \lambda))^3 = j\lambda^2(1 - \lambda)^2,$$

$$(32) \quad \alpha^3(\alpha^3 + 24)^3 + j(\alpha^3 + 27) = 0.$$

Alhora, el divisor primer $\mathfrak{o}$ del denominador de x i y pot ésser prescrit arbitràriament.

2. Considerem primerament el cas $p \neq 2$. Siguin $\lambda_1, \dots, \lambda_6$ les sis arrels de (31). Per a cada λ_ν cal que existeixi una equació generadora

$$(33) \quad y_\nu^2 = x_\nu(x_\nu - 1)(x_\nu - \lambda)$$

de K , que pertanyi al mateix divisor primer $\mathfrak{o}$, com a (29). Si x_ν és una combinació lineal d'ambdós múltiples linealment independents, 1, x de $\mathfrak{o}^{-2}$ i y_μ ha d'ésser un múltiple constant de y

$$(34) \quad x = a_\mu x_\mu + b_\mu, \quad y = c_\nu y_\nu, \quad a_\mu, b_\mu, c_\mu \text{ de } k.$$

Aleshores se satisfà que

$$\begin{aligned} y^2 &= c_\nu^2 y_\nu^2 = x(x-1)(x-\lambda) = \\ &= (a_\nu x_\nu + b_\nu)(a_\nu x_\nu + b_\nu - 1)(a_\nu x_\nu + b_\nu - \lambda_\nu) = \\ &= a_\nu^3 (x_\nu + b_\nu/a_\nu)(x + (b_\nu - 1)/a_\nu)(x + (b_\nu - \lambda_\nu)/a_\nu) = \\ &= c_\nu^2 x_\nu (x_\nu - 1)(x_\nu - \lambda_\nu), \end{aligned}$$

i d'entrada se segueix que

$$c_\nu^2 = a_\nu^3$$

i a continuació les sis possibilitats següents per a $a_\nu, b_\nu, \lambda_\nu, x_\nu$

$$\begin{array}{llll} a_1 = 1, & b_1 = 0, & \lambda_1 = \lambda, & x_1 = x, \\ a_2 = \lambda, & b_2 = 0, & \lambda_2 = \frac{1}{\lambda}, & x_2 = \frac{x}{\lambda}, \\ a_3 = -1, & b_3 = 1, & \lambda_3 = 1 - \lambda, & x_3 = 1 - x, \\ a_4 = \lambda - 1, & b_4 = 1, & \lambda_4 = \frac{1}{1 - \lambda}, & x_4 = \frac{1 - x}{1 - \lambda}, \\ a_5 = -\lambda, & b_5 = \lambda, & \lambda_5 = 1 - \frac{1}{\lambda}, & x_5 = \frac{\lambda - x}{\lambda}, \\ a_6 = 1 - \lambda, & b_6 = \lambda, & \lambda_6 = \frac{\lambda}{\lambda - 1}, & x_6 = \frac{\lambda - x}{\lambda - 1}. \end{array}$$

A cadascun d'aquests sistemes de valors pertanyen dos parells de valors de c_ν i y_ν

$$\begin{array}{ll} c_1 = \pm 1, & y_1 = \pm y, \\ c_2 = \pm(\sqrt{\lambda})^3, & y_2 = \pm(\sqrt{\lambda})^{-3}y, \\ c_3 = \pm i, & y_3 = \mp i y, \\ c_4 = \pm i(\sqrt{1-\lambda})^3, & y_4 = \mp i(\sqrt{1-\lambda})^{-3}y, \\ c_5 = \pm i(\sqrt{\lambda})^3, & y_5 = \mp i(\sqrt{\lambda})^{-3}y, \\ c_6 = \pm(\sqrt{1-\lambda})^3, & y_6 = (\sqrt{1-\lambda})^{-3}y. \end{array}$$

Doncs, en total hi ha 12 transformacions biracionals de la forma normal (29) en una altra, si es requereix que $\mathfrak{o}$ resti invariant. Entre aquestes han d'aparèixer les unitats dels anells de multiplicadors associades als meromorfismes normalitzats per $\mathfrak{o}$; a saber, són exactament aquelles que transformen λ en si mateix. D'aquesta manera obtenim per a cada j el grup d'unitats de l'anell de multiplicadors:

En general hi ha únicament el parell d'unitats

$$x \rightarrow x, \quad y \rightarrow \pm y,$$

per tant ± 1 .

A fi que hi hagi més unitats, han d'ésser iguals dos λ d'índexs diferents. Això proporciona les possibilitats següents:

1. $\lambda = \frac{1}{\lambda}$, $\lambda = -1$, $j = 2^6 3^3$ ($\lambda = 1$ proporcionaria $j = \infty$). En aquest cas és $\lambda_1 = \lambda_2 = -1$, $\lambda_3 = \lambda_5 = 2$, $\lambda_4 = \lambda_6 = \frac{1}{2}$. Per a $p \neq 3$ això proporciona les quatre unitats

$$x \rightarrow x, \quad y \rightarrow \pm y; \quad x \rightarrow -x, \quad y \rightarrow \mp i y,$$

que formen un grup cíclic. Però si és $p = 3$, aleshores és $j = 0$, tots sis valors λ_ν esdevenen -1 i, doncs, hi ha dotze unitats

$$\begin{array}{ll} x \rightarrow x, & y \rightarrow \pm y, \\ x \rightarrow x - 1, & y \rightarrow \pm y, \\ x \rightarrow x + 1, & y \rightarrow \pm y, \\ x \rightarrow -x, & y \rightarrow \mp iy, \\ x \rightarrow 1 - x, & y \rightarrow \mp iy, \\ x \rightarrow -x - 1, & y \rightarrow \mp iy. \end{array}$$

$\mathbf{R}$ és l'ordre maximal de $Q_{\infty,3}$ (únic d'acord amb el tipus).

2. $\lambda = 1 - \lambda$, $\lambda = \frac{1}{2}$. Això proporciona de nou $j = 2^6 3^3$.

3. $\lambda = \frac{1}{1 - \lambda}$, $\lambda = -\varepsilon$, ε una arrel primitiva tercera de la unitat, $j = 0$. Per a $p \neq 3$ s'esdevé $\lambda_1 = \lambda_4 = \lambda_5 = -\varepsilon$, $\lambda_2 = \lambda_3 = \lambda_6 = -\varepsilon^2$, i tenim sis unitats

$$\begin{array}{ll} x \rightarrow x, & y \rightarrow \pm y, \\ x \rightarrow \varepsilon(x - 1), & y \rightarrow \pm y, \\ x \rightarrow \varepsilon^2(x + \varepsilon), & y \rightarrow \pm y, \end{array}$$

que formen un grup cíclic. Per a $p = 3$ s'esdevé novament $j = 0$.

En el cas $p \neq 3$, $j = 2^6 3^3$, es tracta de l'equació definidora

$$y^2 = x^3 - x,$$

el multiplicador $x \rightarrow -x$, $y \rightarrow iy$, que designarem per ι , forma conjuntament amb 1 una base de l'ordre maximal del cos de nombres de Gauss $P(\sqrt{-1})$, que està contingut en l'anell de multiplicadors.

En el cas $p = 3$, $j = 0$, es tracta igualment de l'equació definidora

$$y^2 = x^3 - x.$$

Sigui ι novament el multiplicador $x \rightarrow -x$, $y \rightarrow iy$ i sigui η el multiplicador $x \rightarrow x + 1$, $y \rightarrow y$. L'element ι és una arrel quarta primitiva i η una arrel tercera primitiva de la unitat. Se satisfà, com es repassa fàcilment, la regla de commutació

$$\iota\eta = \eta^2\iota,$$

d'on, a més, s'obtenen les relacions additives

$$\iota^2 + 1 = 0, \quad \eta^2 + \eta + 1 = 0.$$

Totes les dotze unitats són

$$\begin{array}{cccc} 1, & \iota, & -1, & -\iota, \\ \eta, & \eta\iota, & -\eta, & -\eta\iota, \\ \eta^2, & \eta^2\iota, & -\eta^2, & -\eta^2\iota. \end{array}$$

Les unitats $\pm\iota$, $\pm\eta\iota$, $\pm\eta^2\iota$ tenen ordre 4, η , η^2 , ordre 3, i $-\eta$, $-\eta^2$, ordre 6. Una base de $\mathbf{R}$ és 1, η , ι , $\eta\iota$, ja que el discriminant Δ d'aquestes quatre quantitats és

$$\Delta = \begin{vmatrix} +2 & -1 & 0 & 0 \\ -1 & -1 & 0 & 0 \\ 0 & 0 & -2 & 1 \\ 0 & 0 & 1 & -2 \end{vmatrix} = -9,$$

perquè és

$$\text{Traça}(\pm 1) = \pm 2,$$

$$\text{Tr}(\pm\iota) = \text{Tr}(\pm\eta\iota) = \text{Tr}(\pm\eta^2\iota) = 0,$$

$$\text{Tr}(\eta) = \text{Tr}(\eta^2) = -1,$$

$$\text{Tr}(\eta) = \text{Tr}(-\eta^2) = 1.$$

En el cas $p \neq 3$, $j = 0$, transformem la forma normal $y^2 = x(x-1)(x+\varepsilon)$ mitjançant $x = \frac{z-\varepsilon}{1-\varepsilon}$, $y = u(1-\varepsilon)^{-\frac{3}{2}}$ en

$$u^2 = z^3 - 1.$$

Aleshores les sis unitats es diuen

$$z \rightarrow z, \quad u \rightarrow \pm u; \quad z \rightarrow \varepsilon^h z, \quad u \rightarrow \pm u.$$

El multiplicador $z \rightarrow \varepsilon z$, $u \rightarrow u$ és una arrel tercera primitiva de la unitat i forma juntament amb 1 una base de l'ordre maximal del cos de les arrels terceres de la unitat, que està contingut en l'anell de multiplicadors.

3. Amb l'ajut de la forma normal (30) tractem el cas $p \neq 3$ de manera completament semblant. Per a un j donat hi ha dotze arrels $\alpha_1, \dots, \alpha_{12}$ de (32) i per a cadascuna d'aquestes arrels almenys una transformació lineal

$$(35) \quad \begin{aligned} x &= a_\nu x_\nu + b_\nu, \\ y &= f_\nu y_\nu + c_\nu x_\nu + d_\nu, \end{aligned}$$

que transforma (30) en

$$y_\nu^2 - y_\nu + \alpha_\nu x_\nu y_\nu = x_\nu^3.$$

Per al càlcul d'aquestes transformacions podem intercalar en la forma normal (30) les transformacions de $gy_1^2 + hy_1 + \alpha x_1 y_1 = c_0 x_1^3 + c_1 x_1^2 + c_2 x_1 + c_3$ com ho hem tractat en §4

3. Per al càlcul de b obtenim com en (24) l'equació

$$(36) \quad 3b^4 + \alpha^2 b^3 - 3\alpha b^2 + 3b = 0.$$

Aquesta equació té una arrel $b = 0$. A partir de (22), (23), (25), (26), (27) obtenim els valors corresponents a , f , c , d , α ; això dona sis transformacions:

$$a_\nu = \varepsilon^\nu, \quad b_\nu = 0, \quad f_\nu = \begin{cases} +1 \\ -1 \end{cases},$$

$$c_\nu = \begin{cases} 0 \\ -\varepsilon^\nu \alpha \end{cases}, \quad d_\nu = \begin{cases} 0 \\ 1 \end{cases}, \quad \alpha_\nu = \varepsilon^\nu \alpha,$$

ε denota una arrel tercera primitiva de la unitat.

Per als b restants tenim l'equació cúbica

$$(37) \quad b^3 + \frac{\alpha^2}{3}b^2 - \alpha b + 1 = 0,$$

les arrels de la qual són

$$(38) \quad b = -\frac{\alpha^2}{9} - \varepsilon^h \sqrt[3]{\left(\frac{\alpha}{3}\right)^3 + \left(\frac{\alpha}{3}\right)^6} - \varepsilon^{2h} \sqrt[3]{\left(1 + \left(\frac{\alpha}{3}\right)^3\right)^2},$$

$h = 1, 2, 3$, segons les fórmules de Cardano. (D'entrada únicament per a $p \neq 2$. Atès que la fórmula final no conté cap divisió per 2, també val per a $p = 2$.)

Si β és una arrel tercera escollida i fixada de $\alpha^3 + 3^3$, a partir de (32) s'obté l'expressió

$$\beta = -\frac{\alpha(\alpha^3 + 24)}{\sqrt[3]{j}}$$

en el cas $j \neq 0$, de manera que podem escriure

$$b = -\frac{1}{9}(\alpha^2 + \alpha\beta\varepsilon^h + \beta^2\varepsilon^{2h}), \quad h = 1, 2, 3.$$

Atès que a cada b pertanyen tres valors a , posarem

$$b_4 = b_5 = b_6 = -\frac{1}{9}(\alpha^2 + \alpha\beta + \beta^2),$$

$$b_7 = b_8 = b_9 = -\frac{1}{9}(\alpha^2 + \alpha\beta\varepsilon + \beta^2\varepsilon^2),$$

$$b_{10} = b_{11} = b_{12} = -\frac{1}{9}(\alpha^2 + \alpha\beta\varepsilon^2 + \beta^2\varepsilon),$$

abreujadament

$$b_{3h+\mu} = -\frac{1}{9}(\alpha^2 + \alpha\beta\varepsilon^h + \beta^2\varepsilon^{2h}) \quad h = 1, 2, 3, \quad \mu = 1, 2, 3.$$

A partir de (22), per als corresponents a tenim que

$$\begin{aligned} a_{3h+\mu}^3 = & -\frac{4}{3^6}(\alpha^2 + \alpha\beta\varepsilon^h + \beta^2\varepsilon^{2h})^3 + \\ & + \frac{1}{3^4}\alpha^2(\alpha^2 + \alpha\beta\varepsilon^h + \beta^2\varepsilon^{2h})^2 + \\ & + \frac{2}{3^2}\alpha(\alpha^2 + \alpha\beta\varepsilon^h + \beta^2\varepsilon^{2h}) + 1 \end{aligned}$$

Atès que ara és

$$(39) \quad \alpha^2 + \alpha\beta\varepsilon^h + \beta^2\varepsilon^{2h} = \frac{\alpha^3 - \beta^3}{\alpha - \beta\varepsilon^h} = -\frac{3^3}{\alpha - \beta\varepsilon^h},$$

esdevé

$$\begin{aligned} a_{3h+\mu}^3 = & (\alpha^2 + \alpha\beta\varepsilon^h + \beta^2\varepsilon^{2h})^2 \times \\ & \times \left[-\frac{4}{3^6}(\alpha^2 + \alpha\beta\varepsilon^h + \beta^2\varepsilon^{2h}) + \frac{1}{3^4}\alpha^2 - \right. \end{aligned}$$

$$\begin{aligned} & -\frac{2}{3^2}\alpha\frac{\beta\varepsilon^h}{3} + \frac{1}{3^6}(\alpha - \beta\varepsilon^h)^2 \Big] = \\ & = -\frac{1}{3^5}\beta^2\varepsilon^{2h}(\alpha^2 + \alpha\beta\varepsilon^h + \beta^2\varepsilon^{2h}). \end{aligned}$$

Per γ_h entenem una arrel cúbica escollida i fixada de

$$9\beta\varepsilon^h(\alpha^2 + \alpha\beta\varepsilon^h + \beta^2\varepsilon^{2h});$$

d'acord amb (39), γ_h és diferent de 0. Amb aquesta abreviatura podem posar

$$(40) \quad a_{3h+\mu} = -\frac{\varepsilon^\mu \gamma_h^2}{27}.$$

D'acord amb (25), tenim per a d l'equació quadràtica

$$d^2 + (\alpha b - 1)d = b^3.$$

La resollem primerament sota el supòsit que és $p \neq 2$:

$$2d = 1 - \alpha b \pm \sqrt{(1 - \alpha b)^2 + 4b^3}.$$

D'acord amb (37), per al radical tenim que

$$\begin{aligned} (1 - \alpha b)^2 + 4b^3 &= 1 - 2\alpha b + \alpha^2 b^2 - \frac{4}{3}\alpha^2 b^2 + 4\alpha b - 4 = \\ &= -\frac{1}{3}(\alpha^2 b^2 - 6\alpha b + 9) = -\frac{1}{3}(\alpha b - 3)^2, \end{aligned}$$

per tant, és $2d = 1 - \alpha b \pm \frac{\sqrt{-3}}{3}(\alpha b - 3)$.

Per $\sqrt{-3}$ podem prendre $2\varepsilon + 1$, amb la qual cosa obtenim per a $d_{3h+\mu}$ els dos valors següents

$$(41) \quad d_{3h+\mu} = \begin{cases} -\varepsilon + \frac{\varepsilon - 1}{3}\alpha b_{3h+\mu} & = -\varepsilon - \frac{\varepsilon - 1}{27}\alpha(\alpha^2 + \alpha\beta\varepsilon^h + \beta^2\varepsilon^{2h}), \\ -\varepsilon^2 + \frac{\varepsilon^2 - 1}{3}\alpha b_{3h+\mu} & = -\varepsilon^2 - \frac{\varepsilon^2 - 1}{27}\alpha(\alpha^2 + \alpha\beta\varepsilon^h + \beta^2\varepsilon^{2h}), \end{cases}$$

els quals també valen per a $p = 2$, perquè no hi entra cap denominador que s'anul·li per a $2 = 0$.

(26) proporciona

$$(42) \quad c_{3h+\mu} = \begin{cases} \frac{\varepsilon^{\mu-h}}{27(2\varepsilon+1)} \frac{\gamma_h^2}{\beta} (\alpha^2 + \alpha\beta\varepsilon^h + \beta^2\varepsilon^{2h}), \\ \frac{\varepsilon^{\mu-h}}{27(2\varepsilon^2+1)} \frac{\gamma_h}{\beta} (\alpha^2 + \alpha\beta\varepsilon^h + \beta^2\varepsilon^{2h}). \end{cases}$$

(27) dóna f

$$(43) \quad f_{3h+\mu} = \begin{cases} -\frac{\varepsilon^h}{9(2\varepsilon+1)} \beta (\alpha^2 + \alpha\beta\varepsilon^h + \beta^2\varepsilon^{2h})^2, \\ -\frac{\varepsilon^h}{9(2\varepsilon^2+1)} \beta (\alpha^2 + \alpha\beta\varepsilon^h + \beta^2\varepsilon^{2h})^2 \end{cases}$$

i (23)

$$(44) \quad \alpha_{3h+\mu} = -\frac{3\varepsilon^\mu(\alpha + 2\beta\varepsilon^h)}{\gamma_h}.$$

Amb aquestes fórmules, les unitats de l'anell de multiplicadors es poden calcular de la mateixa manera que més amunt. Únicament per a $p = 2$ obtenim un resultat nou, sobre el qual doncs ens restringim. En aquest cas les fórmules per a α_ν resen

$$\alpha_\nu = \varepsilon^\nu \alpha; \quad \nu = 1, 2, 3;$$

$$\alpha_{3h+\mu} = \varepsilon^\mu \alpha / \gamma_\mu; \quad h = 1, 2, 3; \quad \mu = 1, 2, 3.$$

L'únic valor de α per al qual els dos α_ν d'índexs diferents esdevenen iguals és $\alpha = 0$ (a partir de la segona

fórmula encara s'obté la solució $\gamma_\mu = \varepsilon^\mu$, però que condueix a $j = \infty$). Per tant, únicament en el cas $j = 0$ s'obté per a $p = 2$ un grup d'unitats diferent de ± 1 , atès que, llavors, tots els α_ν esdevenen iguals a 0; per tant, llavors hi ha 24 unitats i $\mathbf{R}$ ha d'ésser l'ordre quaterniònic maximal. Les 24 unitats s'obtenen per mitjà de

$$x \rightarrow \varepsilon^h x, \quad y \rightarrow y + \begin{cases} 0 \\ 1 \end{cases}, \quad h \pmod{3},$$

$$x \rightarrow \varepsilon^s x + \varepsilon^t, \quad y \rightarrow y + \varepsilon^{s-t} x + \begin{cases} \varepsilon \\ \varepsilon^2 \end{cases}, \quad s, t \pmod{3}.$$

Les primeres sis unitats formen un grup cíclic, generat pel multiplicador $x \rightarrow \varepsilon x$, $y \rightarrow 1 + y$, que designarem per $-\eta$. Per tant, η és una arrel tercera primitiva de la unitat.

$$\begin{aligned} \iota_1 : \quad & x \rightarrow x + 1, \quad y \rightarrow y + x + \varepsilon, \\ \iota_2 : \quad & x \rightarrow x + \varepsilon, \quad y \rightarrow y + \varepsilon^2 x + \varepsilon, \\ \iota_3 : \quad & x \rightarrow x + \varepsilon^2, \quad y \rightarrow y + \varepsilon x + \varepsilon \end{aligned}$$

són unitats quaterniòniques ja que val

$$\begin{aligned} \iota_1 \iota_2 &= -\iota_2 \iota_1 = \iota_3, \\ \iota_2 \iota_3 &= -\iota_3 \iota_2 = \iota_1, \\ \iota_3 \iota_1 &= -\iota_1 \iota_3 = \iota_2. \end{aligned}$$

A més, és

$$\begin{aligned} \eta \iota_1 &= \iota_2 \eta, \\ \eta \iota_2 &= \iota_3 \eta, \\ \eta \iota_3 &= \iota_1 \eta, \end{aligned}$$

η cal que s'expressi amb coeficients racionals a mitjançant ι

$$\eta = a_0 + a_1 \iota_1 + a_2 \iota_2 + a_3 \iota_3.$$

A partir de

$$\begin{aligned}\eta\iota_1 &= a_0\iota_1 - a_1 - a_2\iota_3 + a_3\iota_2, \\ \iota_2\eta &= a_0\iota_2 - a_1\iota_3 - a_2 + a_3\iota_1, \\ \eta\iota_2 &= a_0\iota_2 + a_1\iota_3 - a_2 - a_3\iota_1, \\ \iota_3\eta &= a_0\iota_3 + a_1\iota_2 - a_2\iota_1 - a_3, \\ \eta\iota_3 &= a_0\iota_3 - a_1\iota_2 + a_2\iota_2 - a_3, \\ \iota_1\eta &= a_0\iota_1 - a_1 + a_2\iota_3 - a_3\iota_2,\end{aligned}$$

se segueixen les igualtats

$$\begin{aligned}a_0 &= a_3, & a_1 &= a_2, \\ a_0 &= a_1, & a_2 &= a_3, \\ a_0 &= a_2, & a_3 &= a_1;\end{aligned}$$

en conseqüència, totes les a són iguals entre si i com que la traça de l'arrel tercera de la unitat η és igual a -1 , esdevé

$$\eta = -\frac{1}{2}(1 + \iota_1 + \iota_2 + \iota_3).$$

Amb això, juntament amb

$$\iota_1^2 = \iota_2^2 = \iota_3^2 = -1; \quad \eta^2 + \eta + 1 = 0,$$

també són exposades totes les relacions additives entre les unitats.

§6. Equacions invariants

1. *Sigui K un cos de funcions el·líptiques d'invariant transcendent absolut j . Entre j i l'invariant j_0 d'un subcòs el·líptic K_0 de K se satisfà una equació algebraica*

$$\Phi(j, j_0) = 0$$

de coeficients enters racionals, en la qual les potències més altes de j i j_0 tenen el coeficient ± 1 .

Demostració. Podem suposar que el cos de constants k de K és la clausura algebraica de $P(j)$, P el cos primer. Ja que un cos de constants encara més gran no pot aportar cap més subcòs el·líptic nou. En conseqüència, j_0 depèn algebraicament de $P(j)$, això significa que se satisfà una equació algebraica irreductible en P ,

$$\Phi(j, j_0) = 0,$$

de coeficients de P , que en el cas de característica 0 poden ésser presos com a nombres enters coprimers. Demostrem ara que Φ com a polinomi de j_0 té un coeficient més alt constant 0, el que és el mateix, que j_0 és una funció algebraica entera de j . Per a tal cosa restringim k a una extensió algebraica finita escaient de $P(j)$, la qual cosa és manifestament possible. D'acord amb §4 3, podem reduir aleshores K segons un divisor primer $\mathfrak{p}$ de k que no entri en el denominador de j , a un cos $\overline{K}$ d'invariant $\overline{j}$. D'acord amb §4 4, K_0 s'aplica sobre un subcòs el·líptic $\overline{K}_0$ de $\overline{K}$. En conseqüència, l'invariant j_0 de K_0 , d'acord §4 3, ha d'ésser $\mathfrak{p}$ -enter. Atès que la situació és simètrica respecte de j i j_0 —el cos $K^{n\varepsilon}$ d'invariant j , $(K : K_0) = n$ està contingut en K_0 —, aleshores Φ com a polinomi en j també té un coeficient més alt constant.

De manera completament semblant demostrem que per a característica 0 els coeficients més alts de j i j_0 en Φ són iguals a ± 1 . Un divisor primer $\mathfrak{p}$ de P (donat mitjançant un nombre primer) l'estenem pel que fa a j a $P(j)$ i a k . La mateixa conclusió que més amunt mostra que j_0 ha de dependre $\mathfrak{p}$ -enterament de j , i això és possible per a tots els p únicament quan el coeficient més alt de j_0 és ± 1 .

2. Investiguem més de prop el polinomi $\Phi(t, t_0)$ i aquí podem suposar que k és algebraic i finit sobre $P(j)$. Si m és el nombre enter més gran per al qual $K^{m\varepsilon}$ encara està contingut en K_0 , aleshores $K^{m\varepsilon}$ és cíclic sobre K_0 . Atès que $K^{m\varepsilon}$ és isomorf a K , podem suposar des del principi que K és cíclic sobre K_0 .

Segui n un nombre no divisible per la característica p . Els $\mu(n)$ subcossos $K_1, \dots, K_{\mu(n)}$, sobre els quals K és cíclic de grau n , tenen, d'acord amb §3 4, invariants separables $j_1, \dots, j_{\mu(n)}$ sobre $P(j)$. Demostrem que

$$(45) \quad \Phi_n(t, j) = \prod_{h=1}^{\mu(n)} (t - j_h)$$

és un polinomi de t i j de coeficients racionals enters. Per a això considerem un parell d'elements x, y de K entre els quals se satisfaci una equació irreductible de coeficients en $P(j)$, i estenem un isomorfisme ϱ de $k/P(j)$ a K mitjançant l'assignació $x^\varrho = x, y^\varrho = y$. Aleshores, ϱ transforma el cos K corresponent al grup de translacions $1, \tau, \dots, \tau^{n-1}$, sobre el corresponent al grup $1, \varrho^{-1}\tau\varrho, \dots, \varrho^{-1}\tau^{n-1}\varrho$, per tant, commuta entre si els cossos K_h i doncs també els invariants $j_{(h)}$. Per tant, els coeficients de $\Phi_n(t, j)$ com a polinomi en t són invariants per a tots els isomorfismes de $k/P(j)$; són enters separables, funció algebraica numèrica entera de j , és a dir, polinomis en j de coeficients racionals enters, com s'ha afirmat. $\Phi_n(t, j)$ és un producte de polinomis irreductibles de la classe considerada en 1. *Designem*

$$\Phi_n(t, j) = 0$$

l'equació invariant d'ordre n de la característica en qüestió.

Abans que entrem en el cas $n \equiv 0 \pmod{p}$, fem notar:

Si $\Phi_n(t, j) = 0$ és l'equació invariant d'ordre n per a la característica 0, aleshores la mateixa equació considerada mòdul el nombre primer p és l'equació invariant d'ordre n per a la característica p , suposat que p no divideix n .

Això proporciona immediatament que K mòdul p s'aplica en un cos $\overline{K}$ d'invariant transcendent absolut $\bar{j}$ mentre que aleshores els subcossos K_h s'apliquen en els corresponents subcossos de $\overline{K}$.

A causa d'aquests fets, per a tots els n , entendrem l'equació invariant d'ordre n per a característica un nombre primer p com l'equació invariant d'ordre n en característica 0 presa mòdul p , encara que entre els zeros de $\Phi_n(t, j)$ a més dels subcossos invariants sobre els quals K és cíclic de grau n , també poden aparèixer altres subcossos.

Podem exposar fàcilment l'equació invariant d'ordre p^f en característica p . El cos sobre el qual K és cíclic i separable de grau p^f té l'invariant $j^{p^{-f}}$ ja que la seva potència p^f és el cos $K^{p^f\varepsilon}$, isomorf a K . Per contra, K^{p^f} té l'invariant j^{p^f} . D'acord amb §4 4, l'equació invariant d'ordre p^f mòdul p esdevé

$$\begin{aligned}
 (46) \quad & (t - j^{p^{-f}})^{p^f} (t - j^{p^f}) \prod_{\substack{i=1 \\ f-1}}^{f-1} (t - j^{p^{2i-f}})^{p^{f-i} - p^{f-i-1}} = \\
 & = (t^{p^f} - j)(t - j^{p^f}) \prod_{i=1}^{f-1} (t^{p^{f-i-1}} - j^{p^{i-1}})^{p-1} = 0,
 \end{aligned}$$

per a $f = 1$, simplement

$$(47) \quad (t^p - j)(t - j^p) = 0.$$

3. *Siguin n' i n'' dos nombres enters primers entre si. Aleshores és*

$$(48) \quad \Phi_{n'n''}(t, j) = \prod_{h=1}^{\psi(n'')} \Phi_{n'}(t, j_h),$$

quan val

$$\Phi_{n''}(t, j) = \prod_{h=1}^{\psi(n'')} (t - j_h).$$

Demostració. Sigui K_h el cos d'invariant j_h sobre el qual K és cíclic de grau n'' . En ell estan continguts $\psi(n')$ cossos K_{hl} , sobre els quals K_h és cíclic de grau n'' . Si j_{hl} són els invariants corresponents, val

$$\Phi(t, j_h) = \prod_{l=1}^{\psi(n')} (t - j_{hl}).$$

Sobre tots els cossos K_{hl} el cos K és cíclic de grau $n'n''$ i no hi ha altres cossos amb aquesta propietat. Amb això és

$$\Phi_{n'n''}(t, j) = \prod_{h,l} (t - j_{hl}) = \prod_h \Phi_{n'}(t, j_h).$$

De manera anàloga s'obté

$$(49) \quad \Phi^{pf}(t, j) = \prod_{h=1}^{p+1} \frac{\Phi^{pf-1}(t, j_h)}{t - j}, \quad \Phi_p(t, j) = \prod_{h=1}^{p+1} (t - j_h);$$

només cal observar que un cop s'ha tret el factor $t - j$ de $\Phi_{p^{f-1}}(t, j_h)$, per al cos contingut en K^{p^e} sobre el qual K_h és cíclic, el grau és p^{f-1} .

El càlcul del polinomi $\Phi_n(t, j)$ es remet al càlcul del polinomi $\Phi_p(t, j)$, p un nombre primer.

Per a $n \not\equiv 0 \pmod{p}$, $\Phi_n(t, j) = 0$ té totes les arrels diferents j_h .

N'hi ha prou de demostrar això per a característica un nombre primer p , perquè un factor lineal múltiple de $\Phi_n(t, j)$ roman per reducció mòdul p . Suposem que j_1 i j_2 fossin iguals. Aleshores el subcòs K_1 d'invariant j_1 contindria els dos subcossos $K^{n\varepsilon}$ i $K_2^{n\varepsilon}$, igualment tots dos tindrien els invariants $j_1 = j_2$ i, doncs, els dos, no solament llevat del signe, donarien lloc a multiplicadors diferents de K_1 de la mateixa norma. D'acord amb §3 **3**, j_1 seria algebraic absolut, i amb més motiu l'invariant j del subcòs $K^{n\varepsilon}$ de K_1 , en contra del que hem suposat.

$$(50) \quad \text{Per a } n > 1 \text{ és } \Phi_n(t, j) = \Phi_n(j, t).$$

Demostració. Per a cada arrel j_h de $\Phi_n(t, j) = 0$ val $\Phi_n(j, j_h) = 0$, perquè K_h és cíclic de grau n sobre el cos $K^{n\varepsilon}$ d'invariant j . Atès que els j_h són diferents dos a dos $\Phi_n(j, t)$ és divisible per $\Phi_n(t, j)$:

$$\Phi_n(j, t) = \Phi_n(t, j)\psi(t, j).$$

D'això se segueix

$$\Phi_n(t, j) = \Phi_n(t, j)\psi(j, t),$$

$$\Phi_n(t, j) = \Phi_n(t, j)\psi(t, j)\psi(j, t),$$

$$\psi(t, j)\psi(j, t) = 1.$$

Doncs, $\psi(t, j)$ és una constant i, a continuació, esdevé que $\psi(j, t) = \pm 1$. Excepte per a $n = 1$, que val

$$\Phi(t, j) = t - j = -\Phi(j, t),$$

és $\psi(t, j) = 1$, ja que altrament seria

$$\Phi(t, j) = -\Phi(j, t), \quad \Phi(j, j) = 0$$

i K tindria un subcòs K_h isomorf a ell mateix, per tant, un multiplicador complex, la qual cosa, d'acord amb §3 3, no és possible per a $p \neq 0$.

4. Les $p + 1$ arrels j_h de $\Phi_p(t, j) = 0$ són funcions algebraiques enteres de j , que poden ésser desenvolupades en potències de $u = 1/j$. Escrivim només el primer terme del desenvolupament en cada cas

$$j_h = \varrho_h u^{e_h} + \cdots, \quad \varrho_h \neq 0.$$

Els primers exponents e_h són no positius. Atès que cap j_h pot ser independent de j —altrament amb més motiu serien independents els invariants j dels subcossos K^{p^e} continguts en K_h —, els primers exponents e_h són de fet negatius.

D'acord amb (47) i (50) és

$$\Phi_p(t, j) = (t^p - j)(t - j^p) + \sum_{\nu=0}^p \sum_{\mu=0}^p p c_{\nu\mu} t^\nu t^\mu$$

amb nombres enters $c_{\nu\mu}$. Atès que d'això se segueix que

$$\prod_{h=1}^{p+1} j_h = (-1)^{p-1} j^{p+1} + \sum_{\mu=0}^p p c_{0\mu} j^\mu,$$

val

$$\prod_{h=1}^{p+1} \varrho_h = (-1)^{p-1}, \quad -\sum_{h=1}^{p+1} e_h = p+1.$$

Si substituïm en el desenvolupament en sèrie obtenim

$$(51) \quad \varrho_h^{p+1} u^{+e_h(p+1)} + (p c_{pp} - 1) \varrho_h^p u^{+p(e_h+1)} + u^{-p+1} + \dots = 0,$$

on els termes en punts denoten que en ells u intervé amb exponents més alts que $-p(e_h+1)$. Doncs, dos dels nombres

$$e_h(p+1), \quad p(e_h+1), \quad -p+1$$

han d'ésser iguals i no més petits que el tercer. Això se satisfà únicament per a $e_h = -p$ i $e_h = -1/p$. Com que $-\sum e_h = 1+p$, com a molt un e_h pot ésser igual a $-p$. Per a cadascuna de les arrels j_h de $\Phi_p(t, j) = 0$ també val l'equació $\Phi_p(j, j_h) = 0$. Per tant, val un desenvolupament en sèrie

$$j = \varrho_h^* u_h^{e_h^*} + \dots$$

de j en potències de

$$u_h = 1/j_h = \frac{1}{\varrho_h} u^{-e_h} + \dots,$$

i d'això se segueix $e_h e_h^* = 1$. Per tant, en la sèrie $e_1, \dots, e_{p+1}$, amb l'exponent e_h es presenta també l'exponent $1/e_h$. Doncs, almenys un e_h és igual a $-p$ i almenys un igual a $-1/p$, i això passa únicament si un e_h , eventualment e_{p+1} , és igual a $-p$, i els restants $e_1, \dots, e_p$ són iguals a $-1/p$. (Els exponents $-1/p$ han d'aparèixer en grups per a cada p .)

A continuació podem calcular els primers coeficients, en els quals tenim en compte que en (51) els termes amb els

exponents més petits han de tenir suma 0. Això dona per a $h = p + 1$

$$\varrho_{p+1}^{p+1} + (p c_{pp} - 1) \varrho_{p+1}^p = 0, \quad \varrho_{p+1} = 1 - p c_{pp},$$

i per a $h = 1, 2, \dots, p$,

$$(p c_{pp} - 1) \varrho_h^p + 1 = 0,$$

conseqüència d'una numeració convenient,

$$\varrho_h = \frac{\zeta_p^h}{\sqrt[p]{1 - p c_{pp}}},$$

ζ_p arrel p -èsima primitiva de la unitat,

$$j_h = \frac{\zeta_p^h}{\sqrt[p]{1 - p c_{pp}}} u^{-\frac{1}{p}} + \dots; \quad h = 1, 2, \dots, p;$$

$$j_{p+1} = (1 - p c_{pp}) u^{-p} + \dots.$$

A continuació demostrarem que

$$(52) \quad c_{pp} = 0$$

és a dir, val

$$(53) \quad \begin{cases} j_h = \zeta_p^h u^{-\frac{1}{p}} + \dots; & h = 1, 2, \dots, p; \\ j_{p+1} = u^{-p} + \dots. \end{cases}$$

Amb aquesta finalitat prenem un nombre primer q diferent de p i calculem mitjançant (48) els primers termes del u -

desenvolupament de les arrels j_{hl} de $\Phi_{pq}(t, j) = 0$:

$$j_{hl} = \frac{\zeta_q^l \zeta_p^{hq}}{\sqrt[q]{1 - qc_{qq}^{(q)}} \left(\sqrt[p]{1 - pc_{pp}^{(p)}} \right)^q} u^{-\frac{1}{pq}} + \dots ;$$

$$j_{p+1,l} = \frac{\zeta_q^l}{\sqrt[q]{1 - qc_{qq}^{(q)}}} (1 - pc_{pp}^{(p)})^q u^{-\frac{p}{q}} + \dots ;$$

$$j_{h,q+1} = (1 - qc_{qq}^{(q)}) \frac{\zeta_p^{hq}}{(\sqrt[p]{1 - pc_{pp}^{(p)}})^q} u^{-\frac{q}{p}} + \dots ;$$

$$j_{p+1,q+1} = (1 - qc_{qq}^{(q)}) (1 - pc_{pp}^{(p)})^q u^{-pq} + \dots ;$$

$h = 1, 2, \dots, p, l = 1, 2, \dots, q$.

(Hem diferenciat els c que pertanyen a p i q amb superíndexs.) Si intercanviem els papers de p i q , obtenim del desenvolupament de $j_{p+1,q+1}$

$$(1 - qc_{qq}^{(q)})^{p-1} = (1 - pc_{pp}^{(p)})^{q-1}.$$

D'aquí se segueix que $1 - pc_{pp}^{(p)}$ no és divisible per cap nombre primer q diferent de p . Atès que tampoc no és divisible per p , és $1 - pc_{pp}^{(p)} = \pm 1$. En el cas $p > 2$ s'obté fins i tot que $1 - pc_{pp}^{(p)} = 1$, per tant, $c_{pp}^{(p)} = 0$. El signe que precedeix $1 - 2c_{22}^{(2)}$ roman encara dubtós. El determinem mitjançant el càlcul complet de $\Phi_2(t, j)$.

Un mètode per al càlcul de $\Phi_n(t, j)$ que en principi condueix a l'objectiu és el següent. Generem K mitjançant una equació de la forma $y^2 = f(x)$, tal vegada en la forma

normal de Legendre

$$y^2 = x(x-1)(x-\lambda).$$

Una base linealment independent de múltiples de $\mathfrak{o}^{-n}$ és, per a n parell,

$$1, x, y, x^2, xy, x^3, x^2y, \dots, x^{\frac{1}{2}n-1}y, x^{\frac{1}{2}n},$$

i per a n senar,

$$1, x, y, x^2, xy, \dots, x^{\frac{1}{2}(n-1)}, x^{\frac{1}{2}(n-1)}y.$$

A partir d'aquí es poden trobar, segons HASSE ²³⁾, representants $\mathfrak{p}_1/\mathfrak{o}, \dots, \mathfrak{p}_{n^2}/\mathfrak{o}$ de les n^2 classes de divisors, les potències n -èsimes dels quals són 1, i a més en resulten elements $y_i \cong (\mathfrak{p}_i/\mathfrak{o})^n$. Si $\mathfrak{p}_1/\mathfrak{o}, \dots, \mathfrak{p}_{\psi(n)}/\mathfrak{o}$ són les classes d'ordre exactament n , aleshores

$$k(x, y, \sqrt[n]{y_1}), \dots, k(x, y, \sqrt[n]{y_{\psi(n)}})$$

són les $\psi(n)$ extensions de cossos no ramificades cícliques de grau n de K i els seus invariants són les arrels de $\Phi_n(t, j)$. Per a $p = 2$ l'algoritme és força fàcil de dur a terme. Prenem la forma normal de Legendre

$$y^2 = x(x-1)(x-\lambda).$$

Els tres elements y_1, y_2, y_3 són manifestament $y_1 = x, y_2 = x-1, i y_3 = x-\lambda$.

És

$$y^2 = (\sqrt{x})^2(\sqrt{x^2-1})(\sqrt{x^2-\lambda}),$$

²³⁾ H. HASSE, Zur Theorie der abstrakten elliptischen Funktionenkörper, I, Journ. f. d. r. u. ang. Math. **175**, p. 55-62 (1936), p. 57.

$$\left(\frac{y}{\sqrt{x}}\right)^2 = (\sqrt{x} - 1)(\sqrt{x} + 1)(\sqrt{x} - \sqrt{\lambda})(\sqrt{x} + \sqrt{\lambda}).$$

A partir d'aquestes equacions definidores de K_1 podem calcular el valor λ_1 del paràmetre λ corresponent a K_1

$$\lambda_1 = \frac{1 - \sqrt{\lambda}}{1 + \sqrt{\lambda}} : \frac{-1 - \sqrt{\lambda}}{-1 + \sqrt{\lambda}} = \left(\frac{1 - \sqrt{\lambda}}{1 + \sqrt{\lambda}}\right)^2,$$

i d'això se segueix que

$$j_1 = 2^8 \frac{(1 - \lambda_1(1 - \lambda_1))^3}{\lambda_1^2(1 - \lambda_1)^2} = 2^4 \frac{((1 - \lambda)^2 + 16\lambda)^3}{\lambda(1 - \lambda)^4}.$$

De manera anàloga s'obté que

$$j_2 = 2^4 \frac{(\lambda^2 + 16(1 - \lambda))^3}{\lambda^4(1 - \lambda)},$$

$$j_3 = 2^4 \frac{(16\lambda(1 - \lambda) - 1)^3}{\lambda(1 - \lambda)}.$$

Sigui

$$\begin{aligned} \Phi_2(t, j) &= t^3 + j^3 + at^2j^2 + bt^2j + btj^2 + ct^2 + cj^2 + \\ &+ dtj + et + ej + f = 0 \end{aligned}$$

l'equació invariant de segon ordre. Aleshores és

$$(54) \quad aj^2 + bj + c = -(j_1 + j_2 + j_3),$$

$$(55) \quad bj^2 + dj + e = j_1j_2 + j_2j_3 + j_3j_1,$$

$$(56) \quad j^3 + cj^2 + ej + f = -j_1j_2j_3.$$

Ara donem valors especials a λ i d'aquesta manera obtenim equacions lineals per al càlcul dels coeficients a , b , c , d , e , f . $\lambda = -\varepsilon$ (ε arrel primitiva tercera de la unitat) dóna $j = 0$, $j_1 = j_2 = j_3 = 2^4 3^3 5^3$, en conseqüència, és

$$c = -2^4 3^4 5^3, \quad e = 2^8 3^7 5^6, \quad f = -2^{12} 3^9 5^9.$$

A continuació posem $\lambda = 0$ després d'haver multiplicat prèviament per una potència escaient de λ . S'esdevé que

$$\lambda^2 j|_{\lambda=0} = 2^8, \quad \lambda j_1|_{\lambda=0} = 2^4, \quad \lambda^4 j_2|_{\lambda=0} = 2^{16}, \quad \lambda j_3|_{\lambda=0} = -2^4.$$

Multipliquem (54) per λ^4 , posem $\lambda = 0$ i trobem que

$$a = -1.$$

Igualment multipliquem (55) per λ^4 i posem $\lambda = 0$. Al costat esquerre hi ha aleshores $2^{16}b$, al costat dret esdevé $\lambda^4 j_1 j_3 = 0$, però per a

$$\lambda^4(j_1 j_2 + j_2 j_3) = \lambda^4 j_2(j_1 + j_3)$$

s'obté que

$$\lambda^4(j_1 j_2 + j_2 j_3)|_{\lambda=0} = 2^{20} \cdot 3 \cdot 31,$$

en conseqüència, és

$$b = 2^4 \cdot 3 \cdot 31.$$

Finalment fem $\lambda = 2$, això dóna

$$j = 2^6 \cdot 3^3, \quad j_1 = 2^3 3^3 11^3, \quad j_2 = 2^6 3^3, \quad j_3 = 2^3 3^3 11^3.$$

Substituït a (55), obtenim una equació per a d , la qual, llavors, condueix a

$$d = 3^3 \cdot 5^3 \cdot 4027.$$

En conseqüència, l'equació invariant de segon ordre és ²⁴⁾

$$(57) \quad \begin{aligned} \Phi_2(t, j) = & t^3 + j^3 - t^2 j^2 + 2^4 3 \cdot 31(t^2 j + t j^2) - \\ & - 2^4 3^4 5^3(t^2 + j^2) + 3^3 5^3 \cdot 4027 t j + \\ & + 2^8 3^5 5^6(t + j) - 2^{12} 3^9 5^9 = 0. \end{aligned}$$

O bé

$$\begin{aligned} \Phi_2(t, j) = & (t^2 - j)(t - j^2) + 2^4 3 \cdot 31(t^2 j + t j^2) - \\ & - 2^4 3^4 5^3(t^2 + j^2) + 2 \cdot 6795563 t j + \\ & + 2^8 3^5 5^6(t + j) - 2^{12} 3^9 5^9 = 0. \end{aligned}$$

Per tant, de fet, també és $c_{22}^{(2)} = 0$.

Podem calcular ara els termes inicials del u -desenvolupament per a les arrels d'una equació invariant $\Phi_n(t, j) = 0$ qualsevol. D'entrada, considerem el cas $n = p^2$. Sigui j_h una arrel de $\Phi_p(t, j) = 0$. Els desenvolupaments de les arrels j_{hl} de $\Phi_p(t, j_h)$ són, per a $l = 1, 2, \dots, p$,

$$j_{hl} = \zeta_p^l u_h^{-\frac{1}{p}} + \dots, \quad u_h = 1/j_h,$$

per tant,

$$j_{hl} = \zeta_{p^2}^{h+lp} u_h^{-\frac{1}{p^2}} + \dots, \quad \text{per a } h = 1, 2, \dots, p,$$

aquí ζ_{p^2} denota una arrel p -èsima fixada de ζ_p , i

$$j_{p+1,l} = \zeta_p^l u_{p+1}^{-\frac{1}{p}} + \dots = \zeta_p^l u^{-1} + \dots;$$

per a $l = p + 1$ en canvi

$$\begin{aligned} j_{h,p+1} &= u_h^{-p} + \dots = u^{-1} + \dots; \quad h = 1, 2, \dots, p; \\ j_{p+1,p+1} &= u_{p+1}^{-p} + \dots = u^{-p^2} + \dots. \end{aligned}$$

²⁴⁾ Cf. tal vegada H. WEBER, Lehrbuch der Algebra III, p. 248. L'equació (5) d'allí és l'equació invariant de segon ordre per a $\gamma_2(\omega) = \sqrt[3]{j(\omega)}$.

En aquestes fórmules es pot reconèixer sense més ni més quina arrel de $\Phi_p(t, j_h)$ és igual a j , a saber, $j_{h,p+1}$ per a $h = 1, 2, 3, \dots, p$ i $j_{p+1,p}$ per a $h = p + 1$. D'acord amb (33), doncs, totes les arrels de $\Phi_{p^2}(t, j)$ són

$$\begin{aligned} j_{hl} &= \zeta_{p^2}^{h+lp} u^{-\frac{1}{p^2}} + \dots, & h, l &= 1, 2, \dots, p, \\ j_{p+1,l} &= \zeta_p^l u^{-1} + \dots, & l &= 1, 2, \dots, p-1, \\ j_{p+1,p+1} &= u^{-p^2} + \dots. \end{aligned}$$

Prosseguint d'aquesta manera, obtenim els inicis dels desenvolupaments de les arrels de $\Phi_{p^f}(t, j)$

$$\begin{aligned} j_h &= \zeta_{p^f}^h u^{-\frac{1}{p^f}}, & h &\pmod{p^f}, \\ j_{h,1} &= \zeta_{p^{f-1}}^h u^{-\frac{1}{p^{f-2}}}, & h &\pmod{p^{f-1}}, & (h, p) &= 1, \\ j_{h,2} &= \zeta_{p^{f-2}}^h u^{-\frac{1}{p^{f-4}}}, & h &\pmod{p^{f-2}}, & (h, p) &= 1, \\ j_{h,f-1} &= \zeta_p^h u^{-p^{f-1}} + \dots, & h &\pmod{p}, & (h, p) &= 1, \\ j_{h,f} &= u^{-p^f} + \dots. \end{aligned}$$

En cada cas aquí ζ_{p^i} és una arrel p -èsima fixada de $\zeta_{p^{i-1}}$, $i = 1, 2, \dots, f$.

Finalment, amb l'ajut de (48) podem donar els termes inicials dels u -desenvolupaments de les arrels de $\Phi_n(t, j) = 0$ per a un n compost qualsevol i trobem sense esforç

$$(58) \quad j_{s,h} = \zeta_s^h u^{-n/s^2} + \dots, \quad s|m, \quad h \pmod{s}, \quad (h, s, n/s) = 1;$$

per a les arrels $j_{s,h}$ numerades de nou, on s descriu tots els divisors de n i h per a un s fix tots els residus mòdul s primers amb $\left(s, \frac{n}{s}\right)$, per ζ_s s'entén una arrel primitiva s -èsima de la unitat.

Finalment, encara demostrarem:

Els coeficients de la sèrie (58) per a característica 0 són nombres enters del cos de les arrels s -èsimes de la unitat. Doncs, obtenim les sèries corresponents per a característica un nombre primer q quan reduïm segons un factor primer de q en el cos de les arrels n -èsimes de la unitat.

La deducció de la sèrie (58) mostra que només cal provar aquesta afirmació per a $n = p =$ nombre primer. Aquí n'hi ha prou de considerar la sèrie

$$j_p = u^{-p} + \cdots,$$

perquè a causa de la simetria de $\Phi_p(t, j)$, les altres p -sèries $j_h = \zeta_p^h u^{-\frac{1}{p}} + \cdots$ són recíproques d'aquesta sèrie.

Escrivim per raó de claredat $\Phi_p(t, j)u^{p^2+p}$ com a polinomi de $z = tu^p$ i $1/j = u$ i hi denotem els termes en potències positives de u mitjançant punts

$$z^{p+1} - z^p + \cdots = \Phi_p(t, j)u^{p^2+p}.$$

Els coeficients d'aquests polinomis són nombres enters. Els coeficients d_i de la sèrie

$$z = 1 + d_1 u + \cdots,$$

que fa 0 aquest polinomi, com és sabut, es calculen a partir dels coeficients dels polinomis mitjançant addicions, subtraccions, multiplicacions i a més divisions pel valor de la derivada parcial del polinomi respecte a z , per a $z = 1$, $u = 0$. Però manifestament aquest és igual a 1.

Els u -desenvolupaments presentats d'aquesta manera per a les arrels dels polinomis invariants fan, per a la teoria de la multiplicació complexa, el mateix paper que els

q -desenvolupaments (desenvolupaments en $q = e^{2\pi\omega i}$) en la teoria analítica. No importa en absolut la convergència dels q -desenvolupaments. La teoria de Galois de les equacions invariants es pot tractar igualment amb l'ajut dels u -desenvolupaments com per mitjà dels q -desenvolupaments; no hi entrem més a prop perquè gairebé no proporciona canvis (cf. WEBER Lehrbuch der Algebra III, capítol vuit).

§7. Invariants singulars i supersingulars

Atès que el tipus d'un cos de funcions el·líptiques és completament determinat mitjançant el seu invariant j , en particular l'estructura del corresponent anell de multiplicadors s'ha de poder expressar mitjançant j . La resta d'aquest treball s'ocupa de la investigació d'aquesta relació.

Anomenem un invariant j *singular* si l'anell de multiplicadors és complex i commutatiu; *supersingular*, si és no commutatiu.

Els invariants singulars i els supersingulars són algebraics absoluts (algebraics sobre el cos primer), els invariants supersingulars fins i tot tenen com a molt grau 2 sobre el cos primer.

Demostració. Ja hem utilitzat dues vegades l'afirmació sobre els invariants supersingulars, sens dubte se segueix immediatament del fet que com que $\sigma = 2$, és $K^{\varepsilon p} = K^{p^2}$ i, per tant, $j^{p^2} = j$.

Igualment, per als invariants singulars de característica un nombre primer ja hem demostrat l'afirmació en §3 3, però en el que segueix s'obté encara una altra vegada.

Sigui $K = k(x, y)$ un cos d'invariant transcendent absolut j i k una extensió algebraica finita de cos de constants $P(j)$. Suposem que l'anell de multiplicadors $\mathbf{R}$ de K fos complex. També per a característica un nombre primer hauria d'ésser commutatiu, perquè és $\sigma = 1$. Sigui q un nombre primer que roman primer en el cos de quocients Σ de $\mathbf{R}$ i j^* un zero de l'equació

$$\Phi_q(j, j) = 0.$$

Si reduïm K segons un divisor primer de $j - j^*$, aleshores obtenim, d'acord amb §4 **2, 3**, un cos el·líptic $\overline{K}$ d'invariant j^* . L'anell de multiplicadors $\overline{\mathbf{R}}$ de $\overline{K}$ conté d'una banda $\mathbf{R}$ però d'altra banda contindria també un multiplicador de norma q perquè un dels subcossos de $\overline{K}$, sobre el qual $\overline{K}$ és cíclic de grau q , seria isomorf a K , ja que $\Phi_q(j^*, j^*) = 0$. Atès que Σ no conté cap nombre de norma q , $\mathbf{R}$ hauria d'ésser no commutatiu, la qual cosa no és possible per a $p = 0$, però tampoc per a $p \neq 0$, perquè Σ no pot ésser immers en $Q_{\infty, p}$.

Si K té multiplicadors complexos, aleshores es troben altres multiplicadors tals que no són múltiple enter de cap altre, però tenen norma > 1 . Si n és la norma d'un tal multiplicador μ , aleshores K és cíclic sobre K^μ de grau n i, doncs, l'invariant j de K satisfà l'equació

$$\Phi_n(j, j) = 0.$$

Els invariants singulars de característica 0 són nombres algebraics enters.

A fi de demostrar això, calcularem el coeficient més alt d'una equació

$$\Phi_n(j, j) = 0$$

que satisfaci l'invariant singular j . El coeficient més alt de $\Phi_n(j, j) = 0$ és el coeficient de la potència més baixa de u en el desenvolupament de $\Phi_n(j, j) = 0$ en potències de u . Descompongum $\Phi_n(t, j)$ en factors lineals

$$\Phi_n(t, j) = \prod_{\substack{s|n \\ h \bmod s \\ (h, s, \frac{n}{s}) = 1}} (t - j_{s,h})$$

i substituïm per als $j_{s,h}$ els desenvolupaments en sèrie (58)

$$\Phi_n(j, j) = \prod_{\substack{s|n \\ h \bmod s, (h, s, \frac{n}{s}) = 1}} (u^{-1} - \zeta_s^h u^{-n/s^2} + \dots).$$

El terme més baix del factor (s, h) és

$$\begin{aligned} & u^{-1} \quad \text{per a } s^2 > n, \\ & (1 - \zeta_s^h) u^{-1} \quad \text{per a } s^2 = n, \\ & -\zeta_s^h u^{-n/s^2} \quad \text{per a } s^2 < n. \end{aligned}$$

En conseqüència, el terme més alt de $\Phi_n(j, j)$ s'anomena

$$\begin{aligned} & j^{\sum_{s|n, s^2 > n} s \frac{\varphi(s, n/s)}{(s, n/s)} + \sum_{s|n, s^2 > n} \frac{n}{s} \frac{\varphi(s, n/s)}{(s, n/s)}} = \\ (59) \quad & = j^{2 \sum_{s|n, s^2 > n} s \frac{\varphi(s, n/s)}{(s, n/s)}}, \end{aligned}$$

en cas que n no sigui cap nombre quadrat, i

$$\begin{aligned} (60) \quad & \prod_{\substack{h \bmod m \\ (h, m) = 1}} (1 - \zeta_m^h) j^{\sum_{s|m^2, s > m} s \frac{\varphi(s, m^2/s)}{(s, m^2/s)} + \varphi(m)} \end{aligned}$$

per a un nombre quadrat $n = m^2$.

Atès que en un anell de multiplicadors complexos sempre hi ha elements de norma no quadrat, un invariant singular j de característica 0 satisfà una equació

$$\Phi_n(j, j) = 0$$

de coeficients racionals enters i de coeficient més alt 1; doncs, és un nombre algebraic enter ²⁵⁾.

§8. Existència i càlcul d'invariants supersingulars

1. Per a un invariant supersingular de característica p el corresponent σ és igual a 2, és a dir, el cos el·líptic K d'invariant j no té cap classe de divisors d'ordre p . Però també val, recíprocament:

Si és $\sigma = 2$, K tampoc no té cap classe de divisors d'ordre p , aleshores K té un ordre maximal de $Q_{\infty, p}$ com a anell de multiplicadors, l'invariant corresponent j és, per tant, supersingular.

D'acord amb §2 10, és suficient provar que K té multiplicadors complexos. Els invariants de K satisfan l'equació $j^{p^2} = j$. El mateix val, per q entès un nombre primer $\neq p$, per als $q + 1$ subcossos el·líptics $K_{q, i}$ de K sobre els quals K és cíclic de grau q . Atès que $j^{p^2} = j$ té únicament p^2 solucions hi ha d'haver dos nombres primers diferents q_1, q_2 tals que un dels cossos K_{q_1, i_1} té el mateix invariant que un dels cossos K_{q_2, i_2} . Però d'això se segueix que K_{q_1, i_1} té

²⁵⁾ Aquesta és la demostració clàssica, cf. H. WEBER, Lehrbuch der Algebra III, p. 422.

un multiplicador de norma $q_1 q_2$, que no pot ésser racional. Però amb això s'ha demostrat tot.

2. Atès que, recíprocament, segons §1, els grups de classes de divisors d'ordre p es corresponen unívocament amb les extensions de cossos cíclics no ramificades de grau p de K , aleshores l'existència d'invariants supersingulars se segueix de l'existència de cossos el·líptics sense extensions cíclics de grau p . Però això ho podem exposar fàcilment d'acord amb una investigació de HASSE ²⁶⁾.

D'acord amb HASSE, fem correspondre a un cos el·líptic K de característica un nombre primer p un *invariant* A , unívocament determinat llevat d'un factor s^{1-p} , $s \neq 0$, de la manera següent: sigui $\mathfrak{o}$ un divisor primer de K , ω un element primer corresponent i v el múltiple de $\mathfrak{o}^{-p}$, unívocament determinat llevat d'una constant additiva, que satisfà la congruència

$$v \equiv \omega^{-p} \pmod{\mathfrak{o}^{-1}}.$$

Aleshores, val una congruència

$$v \equiv \omega^{-p} - A/\omega \pmod{\mathfrak{o}^0}$$

amb una constant A . Aquesta A és l'invariant; és, com s'ha dit, independent de l'elecció de $\mathfrak{o}$ i ω llevat d'un factor constant s^{1-p} , $s \neq 0$. El cos K té extensions cíclics no ramificades, o no en té, segons que sigui $A \neq 0$ o bé $A = 0$. Doncs, els invariants supersingulars són aquells valors de j que fan 0 l'invariant A dels cossos K d'invariant transcendent absolut j . Per tant, calculem A per a aquests cossos.

²⁶⁾H. HASSE, loc. cit. ²³⁾, Nr. 1.

a) $p = 2$. Partim de la forma normal

$$y^2 - y + \alpha xy = x^3.$$

L'element $x/y = \omega$ és primer per al divisor primer $\mathfrak{o}$ del denominador de x i y . Els múltiples enters de $\mathfrak{o}^{-2}$ tenen la forma

$$\xi + \eta x.$$

Per tant, hem de determinar

$$v = \eta x$$

a partir de

$$\eta x \equiv y^2/x^2 \pmod{\mathfrak{o}^{-1}}$$

o bé de

$$\frac{\eta}{(1 + \alpha x)yx^{-3} + 1} \equiv 1 \pmod{\mathfrak{o}}.$$

Això dona $\eta = 1$, $v = x$. Aleshores, trobem A a partir de

$$x \equiv y^2/x^2 - Ay/x \pmod{\mathfrak{o}^0}$$

o bé

$$x^3/y^2 \equiv 1 - Ax/y \pmod{\mathfrak{o}^2}$$

o bé

$$(1 + \alpha x)y^{-1} + 1 \equiv 1 - Ax/y \pmod{\mathfrak{o}^2},$$

que significa el mateix, ja que $1/y \equiv 0 \pmod{\mathfrak{o}^3}$ amb

$$\alpha x/y \equiv Ax/y \pmod{\mathfrak{o}^2}.$$

En conseqüència, és simplement

$$A = \alpha,$$

i l'únic invariant supersingular de característica 2 és

$$j = 0,$$

la qual cosa coincideix amb el resultat de §5 **3**, que $j = 0$ és l'únic invariant al qual correspon un grup d'unitats multiplicatives més gran que ± 1 .

b) $p \neq 2$. Generem K mitjançant una equació

$$y^2 = f(x),$$

on $f(x) = a_0x^3 + a_1x^2 + a_2x + a_3$ denota un polinomi cúbic i prenem per a $\mathfrak{o}$ el divisor primer del denominador de x i y . Aleshores x/y és un element primer corresponent i

$$1, x, x^2, \dots, x^{\frac{1}{2}(p-1)}, y, xy, \dots, x^{\frac{1}{2}(p-3)}y$$

és una base dels múltiples de $\mathfrak{o}^{-p}$. Doncs, podem posar v unívocament en la forma

$$v = \alpha_1x + \dots + \alpha_{\frac{p-1}{2}}x^{\frac{1}{2}(p-1)} + y \left(\beta_0 + \beta_1x + \dots + \beta_{\frac{p-3}{2}}x^{\frac{1}{2}(p-3)} \right).$$

L'automorfisme de $K/k(x)$ produeix a partir de la congruència

$$\begin{aligned} & \left(\alpha_1x + \dots + \alpha_{\frac{p-1}{2}}x^{\frac{1}{2}(p-1)} \right) + \\ & + y \left(\beta_0 + \beta_1x + \dots + \beta_{\frac{1}{2}(p-3)}x^{\frac{1}{2}(p-3)} \right) \equiv y^p/x^p \pmod{\mathfrak{o}^{-1}}, \end{aligned}$$

l'altra

$$\begin{aligned} & \left(\alpha_1x + \dots + \alpha_{\frac{p-1}{2}}x^{\frac{1}{2}(p-1)} \right) - \\ & - y \left(\beta_0 + \beta_1x + \dots + \beta_{\frac{1}{2}(p-3)}x^{\frac{1}{2}(p-3)} \right) \equiv -y^p/x^p \pmod{\mathfrak{o}^{-1}}, \end{aligned}$$

de manera que

$$2 \left(\alpha_1x + \dots + \alpha_{\frac{p-1}{2}}x^{\frac{1}{2}(p-1)} \right) \equiv 0 \pmod{\mathfrak{o}^{-1}},$$

és a dir, val

$$\alpha_1 = \alpha_2 = \cdots = \alpha_{\frac{p-1}{2}} = 0.$$

Per a la determinació de A tenim la congruència

$$y \left(\beta_0 + \beta_1 x + \cdots + \beta_{\frac{1}{2}(p-3)} x^{\frac{1}{2}(p-3)} \right) \equiv y^p / x^p - Ay / x \pmod{\mathfrak{o}^0}.$$

La multipliquem per x/y i substituïm per a y^{p-1} l'expressió $f(x)^{\frac{1}{2}(p-1)}$

$$A \equiv f(x)^{\frac{1}{2}(p-1)} x^{1-p} - x \left(\beta_0 + \beta_1 x + \cdots + \beta_{\frac{p-3}{2}} x^{\frac{1}{2}(p-3)} \right) \pmod{\mathfrak{o}}.$$

Atès que y no es presenta més, la congruència també pot ésser presa mòdul $\mathfrak{o}^2$, o bé x^{-1} , o finalment posada en la forma

$$(f(x)/x^3)^{\frac{1}{2}(p-1)} \equiv Ax^{-\frac{1}{2}(p-1)} + \beta_0 x^{-\frac{1}{2}(p-3)} + \cdots + \beta_{\frac{p-3}{2}} \pmod{x^{-\frac{p+1}{2}}}.$$

En conseqüència, A no és altra cosa que el coeficient de $x^{-\frac{1}{2}(p-1)}$ en el polinomi en x^{-1}

$$(f(x)/x^3)^{\frac{1}{2}(p-1)} = (a_3 x^{-3} + a_2 x^{-2} + a_1 x^{-1} + a_0)^{\frac{1}{2}(p-1)}.$$

Prenem primerament la forma normal de Legendre

$$f(x) = x(x-1)(x-\lambda).$$

A és el coeficient de $x^{-\frac{1}{2}(p-1)}$ en

$$((1-x^{-1})(1-\lambda/x))^{\frac{1}{2}(p-1)},$$

és a dir,

$$(61) \quad A = (-1)^{\frac{1}{2}(p-1)} \sum_{i=1}^{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{i}^2 \lambda^i = s_p(\lambda).$$

Manifestament val

$$s_p(1/\lambda) = \lambda^{-\frac{1}{2}(p-1)} s_p(\lambda).$$

Atès que $1-\lambda$ correspon al mateix invariant que λ , $s_p(1-\lambda)$ s'ha de diferenciar de $s_p(\lambda)$ en un factor independent de λ . Això dona

$$s_p(1-\lambda) = (-1)^{\frac{1}{2}(p-1)} s_p(\lambda).$$

Per a $p = 3$ tenim

$$A = -1 - \lambda,$$

en conseqüència,

$$j = 0$$

és l'únic invariant supersingular mòdul 3, de conformitat amb §5 2.

Per a $p > 3$, (61) proporciona com a mínim l'existència d'invariants supersingulats, per a això només cal que ens convencem que les arrels de $s_p(\lambda) = 0$ no són 0 o bé 1 ($j = \infty$):

$$s_p(0) = 1, \quad s_p(1) = \sum_{i=0}^{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{i}^2 = \binom{p-1}{\frac{p-1}{2}} \neq 0.$$

Per al càlcul dels invariants supersingulats és avantatjós partir de la forma normal de Weierstrass, per tant, prendre $f(x) = 4x^3 - g_2x - g_3$. A és el coeficient de $x^{-\frac{1}{2}(p-1)}$ en

$$(-g_3x^{-3} - g_2x^{-2} + 4)^{\frac{1}{2}(p-1)},$$

per tant,

(62)

$$A = \sum_{3i+2h=\frac{p-1}{2}} \frac{\left(\frac{p-1}{2}\right)!}{i!h!\left(\frac{p-1}{2} - i - h\right)!} (-g_3)^i (-g_2)^h 4^{\frac{p-1}{2}-i-h}.$$

Es té que

$$j = 2^6 3^3 g_2^3 / \Delta \text{ amb } \Delta = g_2^3 - 27 g_3^2,$$

doncs,

$$g_2 = j^{\frac{1}{3}} \Delta^{\frac{1}{3}} / 12, \quad g_3 = (j - 2^6 3^3)^{\frac{1}{2}} \Delta^{\frac{1}{2}} / 216.$$

Si substituïm aquest valor en (62), aleshores obtenim
per a $p \equiv 1 \pmod{12}$

$$(63.1) \quad \begin{aligned} A &= (-1)^{\frac{p-1}{4}} \frac{\left(\frac{p-1}{2}\right)!}{3^{\frac{p-1}{4}}} \Delta^{\frac{p-1}{12}} \times \\ &\times \sum_{i=0}^{\frac{p-1}{12}} \frac{\left(-\frac{4}{27}\right)^i}{(2i)! \left(\frac{p-1}{4} - 3i\right)! \left(\frac{p-1}{4} + i\right)!} j^{\frac{p-1}{12}-i} (j - 2^6 3^3)^i, \end{aligned}$$

per a $p \equiv 5 \pmod{12}$

$$(63.5) \quad \begin{aligned} A &= 4 (-1)^{\frac{p-1}{4}} \frac{\left(\frac{p-1}{2}\right)!}{3^{\frac{p-5}{4}}} \Delta^{\frac{p-5}{12}} g_2 \times \\ &\times \sum_{i=0}^{\frac{p-5}{12}} \frac{\left(-\frac{4}{27}\right)^i}{(2i)! \left(\frac{p-1}{4} - 3i\right)! \left(\frac{p-1}{4} + i\right)!} j^{\frac{p-5}{12}-i} (j - 2^6 3^3)^i, \end{aligned}$$

per a $p \equiv 7 \pmod{12}$
(63.7)

$$A = 16(-1)^{\frac{p-3}{4}} \frac{\left(\frac{p-1}{2}\right)!}{3^{\frac{p-7}{4}}} \Delta^{\frac{p-7}{12}} g_3 \times \\ \times \sum_{i=0}^{\frac{p-7}{4}} \frac{\left(-\frac{4}{27}\right)^i}{(2i+1)! \left(\frac{p-7}{4} - 3i\right)! \left(\frac{p+1}{4} + i\right)!} j^{\frac{p-7}{12}-i} (j - 2^6 3^3)^i,$$

i per a $p \equiv 11 \pmod{12}$
(63.11)

$$A = 64(-1)^{\frac{p-3}{4}} \frac{\left(\frac{p-1}{2}\right)!}{3^{\frac{p-11}{4}}} \Delta^{\frac{p-11}{12}} g_2 g_3 \times \\ \times \sum_{i=0}^{\frac{p-11}{12}} \frac{\left(-\frac{4}{27}\right)^i}{(2i+1)! \left(\frac{p-7}{4} - 3i\right)! \left(\frac{p+1}{4} + i\right)!} j^{\frac{p-11}{12}-i} (j - 2^6 3^3)^i.$$

Les sumes del costat dret d'aquestes fórmules són, llevat d'un factor constant, els polinomis designats per HASSE²⁷⁾ amb $P(j)$. Reconeixem que el grau numèric $[p/12]$ conjecturat per HASSE és correcte.

Si introduïm

$$t = -4(j - 2^6 3^3)/27j$$

com una nova variable, esdevé

$$\text{const. } j^{-[\frac{p}{12}]} P(j) = \\ (64.1) \quad = \sum_{0 \leq i < \frac{p}{12}} \frac{t^i}{(2i)! \left(\frac{p-1}{4} - 3i\right)! \left(\frac{p-1}{4} + i\right)!},$$

²⁷⁾ H. HASSE. Existenz separabler zyklischer unverzweigter Erweiterungskörper vom Primzahlgrade p über elliptischen Funktionenkörper der Charakteristik p . Journ. f. d. r. u. ang. Math **172**, p. 77–85, (1934), p. 81.

si $p \equiv 1 \pmod{4}$, i

$$\begin{aligned} & \text{const. } j^{-[\frac{-p}{12}]} P(j) = \\ (64. - 1) \quad &= \sum_{0 \leq i < \frac{p}{12}} \frac{t^i}{(2i+1)! \left(\frac{p-7}{4} - 3i\right)! \left(\frac{p+1}{4} + i\right)!}, \end{aligned}$$

si $p \equiv -1 \pmod{4}$.

Amb aquesta aparença es deixen calcular amb relativa comoditat. Proporcionem una taula dels polinomis $P(j)$ i dels invariants supersingulars per a $p < 100$.

Invariants supersingulars mòdul p (65)

p	$P_p(j)$	arrels de $P_p(j)$	$2^6 3^3$	0
2	*	*	0	0
3	*	*	0	0
5	1	*	*	0
7	1	*	6	*
11	1	*	1	0
13	$j - 5$	5	*	*
17	$j - 8$	8	*	0
19	$j - 7$	7	18	*
23	$j - 19$	19	3	0
29	$j^2 + 2j + 21$	2,25	*	0
31	$j^2 + 25j + 8$	2,4	23	*
37	$j^3 + 23j^2 + 5j + 11$	$8, 3 \pm 10\sqrt{2}$	*	*
41	$j^3 + 19j^2 + 10j + 18$	3, 28, 32	*	0
43	$j^3 + 21j^2 + 11j + 32$	$41, 12 \pm 8\sqrt{2}$	8	*
47	$j^3 + 31j^2 + 33j + 35$	9, 10, 44	36	0
53	$j^4 + 7j^3 + 30j^2 + 9j + 24$	$46, 50, 28 \pm 9\sqrt{2}$	*	0
59	$j^4 + 39j^3 + 35j^2 + 31j + 39$	15, 28, 47, 48	17	0
61	$j^5 + 60j^4 + 8j^3 + 27j^2 + 21j + 60$	$9, 41, 50, 42 \pm 4\sqrt{2}$	*	*
67	$j^5 + 53j^4 + 4j^3 + 47j^2 + 36j + 8$	$66, 45 \pm 30\sqrt{2}, 63 \pm 32\sqrt{2}$	53	*
71	$j^5 + j^4 + 33j^3 + 28j^2 + 54j + 18$	17, 40, 41, 48, 66	24	0
73	$j^6 + 19j^5 + 18j^4 + 34j^3 + 31j^2 + 67j + 7$	$9, 56, 39 \pm 5\sqrt{5}, 8 \pm 37\sqrt{5}$	*	*
79	$j^6 + 55j^5 + 57j^4 + 63j^3 + j^2 + 25j + 10$	$15, 17, 21, 64, 72 \pm 38\sqrt{3}$	69	*
83	$j^6 + 11j^5 + 62j^4 + 81j^3 + 81j^2 + 72j + 43$	$17, 28, 50, 67, 38 \pm 35\sqrt{2}$	68	0
89	$j^7 + 60j^6 + 86j^5 + 37j^4 + 22j^3 + 23j^2 + 79j + 42$	$6, 7, 13, 52, 66, 76 \pm 39\sqrt{3}$	*	0
97	$j^8 + 60j^7 + 10j^6 + 96j^5 + 2j^4 + 74j^3 + 3j^2 + 69j + 78$	$1, 20, 45 \pm 28\sqrt{5}, 76 \pm 3\sqrt{5}, 81 \pm 22\sqrt{5}$	*	*

Com a resultat general de les consideracions precedents constatem:

Per a cada tipus d'ordre maximal en $Q_{\infty,p}$ hi ha invariants supersingulars mòdul p .

Atès que hi ha un cos K supersingular mòdul p , entre els seus subcossos n'hi haurà algun amb un ordre maximal de $Q_{\infty,p}$ donat per endavant com a anell de multiplicadors.

§9. Existència d'invariants singulars

1. L'existència d'invariants singulars de característica 0, i certament, per a cada ordre en un cos de nombres quadràtic imaginari donat per endavant, en quantitat exacta com el nombre de classes d'aquest ordre, se sap que és una conseqüència directa de la teoria analítica de les funcions el·líptiques. Atès que aquests invariants singulars són nombres algebraics enters, poden ésser presos, segons §4 **2**, **3**, per reducció segons ideals primers dels cossos de nombres generats pels invariants singulars de característica un nombre primer p , i certament, com ens convencem de manera fàcil, per a cada ordre de conductor no divisible per p d'un cos de nombres quadràtic imaginari donat per endavant, n'hi ha tants com el nombre de classes de l'ordre.

Però és manifest que resta [estudiar] si no n'hi ha encara d'altres que no poden ésser obtinguts per reducció. A fi de decidir això i deduir-ho tot d'una manera algebraica, necessitem el lema següent:

Si el cos $\overline{K_0}$ de característica un nombre primer p té un multiplicador $\bar{\mu}$, aleshores es pot obtenir per reducció mòdul

un divisor primer $\mathbf{p}$ de p d'un cos K_0 de característica 0 un dels multiplicadors del qual s'aplica en el multiplicador $\bar{\mu}$ de $\bar{K}_0$ donat per endavant.

Ens permet, a partir dels invariants supersingulars mòdul p exposats en l'apartat anterior, aconseguir els invariants singulars en característica 0 i llavors a partir d'aquí els invariants singulars mòdul p .

Demostració del lema. Podem suposar des del principi que $\bar{\mu}$ és complex; atès que el teorema és obvi per a $\bar{\mu}$ racional. A continuació, podem suposar que la norma n de $\bar{\mu}$ no és divisible per p i que $\bar{\mu}$ no és cap múltiple d'un multiplicador racional m , llavors podem substituir $\bar{\mu}$ per $m^{-1}\bar{\mu}$ o bé $m^{-1}\bar{\mu} + 1$. Si suposem el cos de constants com un cos de Galois suficientment gran, aleshores $\bar{K}_0$ també és cíclic sobre $\bar{K}_0^{\bar{\mu}}$, de grau n no divisible per p . Sigui Σ un cos de nombres algebraics finit que posem encara a la nostra disposició. Adjuntem a Σ una indeterminada j i una arrel λ de

$$2^8(1 - \lambda(1 - \lambda))^3 = j\lambda^2(1 - \lambda)^2$$

o bé una arrel α de

$$\alpha^3(\alpha^3 + 24)^3 + j(\alpha^3 + 27) = 0$$

segons sigui $p \neq 2$ o bé $p \neq 3$. Sobre el cos de constants $\Sigma(j, \lambda)$ o bé $\Sigma(j, \alpha)$ construïm un cos de funcions el·líptiques $\Sigma(j, \lambda; x, y)$ o bé $\Sigma(j, \alpha; x, y)$ d'invariant j , mitjançant l'equació definidora

$$y^2 = x(x - 1)(x - \lambda)$$

o bé

$$y^2 - y + \alpha xy = x^3.$$

Estenem el cos de constants $\Sigma(j, \lambda)$ o bé $\Sigma(j, \alpha)$ de manera algebraica i finita a un cos k tal que els $\mu(n)$ subcossos $K_1, \dots, K_{\mu(n)}$, sobre els quals K és no ramificada i cíclica de grau n , estiguin continguts en $k(x, y) = K$; els invariants d'aquests cossos són les arrels $j_1, \dots, j_{\mu(n)}$ de l'equació invariant $\Phi_n(t, j) = 0$, d'ordre n . Els j_i es troben doncs en k ; suposarem, a més, que per a cada i totes les arrels $\lambda_i^{(h)}$ de l'equació

$$2^8(1 - \lambda_i(1 - \lambda_i))^3 = j_i \lambda_i^2(1 - \lambda_i)^2$$

o bé totes les arrels $\alpha_i^{(h)}$ de l'equació

$$\alpha_i^3(\alpha_i^3 + 24)^3 + j_i(\alpha_i^3 + 27) = 0$$

són contingudes en k .

Estenem la valoració corresponent a un ideal primer de Σ que divideix p pel que fa j a $\Sigma(j)$ i entenem per $\mathbf{p}$ un dels seus divisors primers en k . Designem mitjançant un supratallat l'aplicació de classes de residus mòdul $\mathbf{p}$. Pel que fa a x , $\mathbf{p}$ serà transferit a $k(x)$; atès que $\bar{\lambda}$ és transcendent sobre $\bar{\Sigma}$, aleshores $\mathbf{p}$ roman primer en K i $\bar{K} = \bar{k}(\bar{x}, \bar{y})$ és el·líptic amb invariant $\bar{j}$ transcendent absolut sobre el cos de constants $\bar{k}$. Els cossos $K_1, \dots, K_{\mu(n)}$ s'apliquen mòdul $\mathbf{p}$ sobre els corresponents subcossos $\bar{K}_1, \dots, \bar{K}_{\mu(n)}$ de $\bar{K}$ d'invariants $\bar{j}_1, \dots, \bar{j}_{\mu(n)}$.

Tornem al cos donat $\bar{K}_0$ de característica p . Siguin $\bar{j}_0$ el seu invariant i $\bar{\lambda}_0$ una arrel de l'equació

$$2^8(1 - \bar{\lambda}_0(1 - \bar{\lambda}_0))^3 = \bar{j}_0 \bar{\lambda}_0^2(1 - \bar{\lambda}_0)^2$$

o bé $\bar{\alpha}_0$ una arrel de l'equació

$$\bar{\alpha}_0^3(\bar{\alpha}_0^3 + 24)^3 + \bar{j}_0(\bar{\alpha}_0^3 + 27) = 0.$$

Ara escollim el cos Σ de manera que contingui un nombre $\lambda_0(\alpha_0)$ el residu del qual mòdul $\mathbf{p}$ pugui ésser identificat amb aquest $\overline{\lambda_0(\alpha_0)}$. A més, exigim de Σ que els divisors de les funcions algebraïques enteres $j - j_0$ i $\lambda - \lambda_i^{(h)}$, $i = 1, \dots, \mu(n)$; $h = 1, \dots, 6$, o bé $\alpha - \alpha_i^{(h)}$, $i = 1, \dots, \mu(n)$; $h = 1, \dots, 12$ de j tinguin en el numerador únicament divisors primers de primer grau. Sigui k_j l'anell de funcions algebraïques enteres de j en k . Llavors, $\overline{k_j}$ consta de funcions algebraïques enteres de $\bar{j}$, possiblement, però, no totes contingudes en $\overline{k}$, la qual cosa fa una mica complicats els raonaments següents.

Sigui $\overline{\wp}$ un ideal primer de $\overline{k_j}$ que divideixi $\bar{j} - \bar{j}_0$. Hi ha almenys un divisor primer de $\overline{k}$ amb la propietat que tots els elements de $\overline{k_j}$ divisibles per aquest formen un ideal primer $\overline{\wp}$, igualment el designem per $\overline{\wp}$. Llavors, $\overline{K}$ s'aplica mòdul $\overline{\wp}$ sobre un cos d'invariant $\bar{j}_0$ donat per endavant; podem suposar, atès que això no depèn del cos de constants exacte, que és el cos donat $\overline{K_0}$. Si s'escull Σ suficientment gran, aleshores el multiplicador $\overline{\mu}$ donat per endavant és de $\overline{K_0}$. Per reducció mòdul $\overline{\wp}$, $\overline{K_0}^{\overline{\mu}}$ ha de resultar un dels cossos $\overline{K_i}$, tal vegada $\overline{K_1}$.

El parell d'elements generadors $\overline{x}, \overline{y}$ de $\overline{K}$ amb

$$\overline{y}^2 = \overline{x}(\overline{x} - 1)(\overline{x} - \overline{\lambda}) \quad [\overline{y}^2 - \overline{y} + \overline{\alpha} \overline{x} \overline{y} = \overline{x}^3]$$

s'aplica mòdul $\overline{\wp}$ sobre un parell d'elements generadors $\overline{x}_0, \overline{y}_0$ de $\overline{K_0}$ amb

$$\overline{y}_0^2 = \overline{x}_0(\overline{x}_0 - 1)(\overline{x}_0 - \overline{\lambda}_0) \quad [\overline{y}_0^2 - \overline{y}_0 + \overline{\alpha}_0 \overline{x}_0 \overline{y}_0 = \overline{x}_0^3].$$

El parell d'elements generadors $\overline{x}_0^{\overline{\mu}}, \overline{y}_0^{\overline{\mu}}$ de $\overline{K_0}^{\overline{\mu}}$ amb

$$\overline{y}_0^{\overline{\mu}^2} = \overline{x}_0^{\overline{\mu}}(\overline{x}_0^{\overline{\mu}} - 1)(\overline{x}_0^{\overline{\mu}} - \overline{\lambda}_0) \quad [\overline{y}_0^{\overline{\mu}^2} - \overline{y}_0^{\overline{\mu}} + \overline{\alpha}_0 \overline{x}_0^{\overline{\mu}} \overline{y}_0^{\overline{\mu}} = \overline{x}_0^{3\overline{\mu}}]$$

s'obté, d'acord amb la secció §4 **3**, a partir d'un parell d'elements generadors $\bar{x}_1, \bar{y}_1$ de $\bar{K}_1$ amb

$$\bar{y}_1^2 = \bar{x}_1(\bar{x}_1 - 1)(\bar{x}_1 - \bar{\lambda}_1) \quad [\bar{y}_1^2 - \bar{y}_1 + \bar{\alpha}_1 \bar{x}_1 \bar{y}_1 = \bar{x}_1^3],$$

on $\lambda_1 [\alpha_1]$ és una arrel determinada de

$$2^8(1 - \bar{\lambda}_1(1 - \bar{\lambda}_1))^3 = \bar{j}_1 \bar{\lambda}_1^2(1 - \bar{\lambda}_1)^2$$

$$[\text{de } \bar{\alpha}_1^3(\bar{\alpha}_1^3 + 24)^3 + \bar{j}_1(\bar{\alpha}_1^3 + 27) = 0]$$

que satisfà la congruència

$$\bar{\lambda}_1 \equiv \bar{\lambda} \pmod{\bar{\wp}}, \quad [\bar{\alpha}_1 \equiv \bar{\alpha} \pmod{\bar{\wp}}]$$

tal vegada $\lambda_1^{(1)} [\alpha_1^{(1)}]$. A continuació, d'acord amb §4 **3**, $\bar{x}_1, \bar{y}_1$ són els **p**-residus d'un parell d'elements generadors x_1, y_1 de K_1 amb

$$y_1^2 = x_1(x_1 - 1)(x_1 - \lambda_1) \quad [y_1^2 - y_1 + \alpha_1 x_1 y_1 = x_1^3].$$

Per tant, tenen lloc les aplicacions següents

$$\begin{array}{c} x, y, \lambda[\alpha] \xrightarrow{\text{mòdul } \mathbf{p}} \bar{x}, \bar{y}, \bar{\lambda} [\bar{\alpha}] \xrightarrow{\text{mòdul } \bar{\wp}} \bar{x}_0, \bar{y}_0, \bar{\lambda}_0[\bar{\alpha}_0] \\ \downarrow \\ x_1, y_1, \lambda_1[\alpha_1] \xleftarrow{\text{mòdul } \mathbf{p}} \bar{x}_1, \bar{y}_1, \bar{\lambda}_1[\bar{\alpha}_1] \xleftarrow{\text{mòdul } \bar{\wp}} \bar{x}_0^\mu, \bar{y}_0^\mu, \bar{\lambda}_0[\bar{\alpha}_0]. \end{array}$$

Les fletxes indiquen la successió en la qual aquestes termes s'han obtingut les unes de les altres.

A continuació, mostrarem que hi ha un ideal primer $\wp$ de k_j que divideix $\lambda - \lambda_1 [\alpha - \alpha_1]$ i que mòdul $\mathbf{p}$ s'aplica en l'ideal $\bar{\wp}$ de $\bar{k}_j$. Estenem a K el corresponent divisor

primer $\wp$ respecte de x , llavors, K s'aplica mòdul $\wp$ en un cos $K_0 = k_0(x_0, y_0)$; designem la reducció mòdul $\wp$ afegint un índex 0. Atès que $\lambda_0 = \lambda_{10}$, K_0 té un multiplicador μ donat mitjançant $x_0 \rightarrow x_{10}$, $y_0 \rightarrow y_{10}$. Com a conseqüència de la regla d'intercanvi (12), §4 **2**, x, y mòdul $\mathbf{p}$ s'apliquen sobre $\overline{x_0}$, $\overline{y_0}$ i x_{10}, y_{10} sobre $\overline{x_0^\mu}$, $\overline{y_0^\mu}$. En conseqüència, μ proporciona per reducció el multiplicador donat $\overline{\mu}$ de K_0 .

Resta encara demostrar l'afirmació sobre $\overline{\wp}$ i $\wp$; per a aquesta finalitat, investiguem quelcom més general, com es comporten els ideals de $\overline{k_j}$ respecte dels de k_j .

Per a cada ideal $\mathfrak{a}$ de k_j , el conjunt $\overline{\mathfrak{a}}$ dels residus mòdul $\mathbf{p}$ dels elements $\mathbf{p}$ -enters continguts en $\mathfrak{a}$ és un ideal de $\overline{k_j}$.

Manifestament, per a dos ideals $\mathfrak{a}$ i $\mathfrak{b}$ val

$$\overline{\mathfrak{a}\mathfrak{b}} \supseteq \overline{\mathfrak{a}} \cdot \overline{\mathfrak{b}}$$

$$\overline{\mathfrak{a} \cap \mathfrak{b}} \subseteq \overline{\mathfrak{a}} \cap \overline{\mathfrak{b}},$$

i $\overline{\mathfrak{a}} \subseteq \overline{\mathfrak{b}}$, si $\mathfrak{a} \subseteq \mathfrak{b}$.

De la descomposició en factors primers d'un ideal de k_j

$$\mathfrak{a} = \wp_1^{e_1} \cdots \wp_h^{e_h}$$

se segueix, per tant,

$$\overline{\wp_1^{e_1}} \overline{\wp_2^{e_2}} \cdots \overline{\wp_h^{e_h}} \subseteq \overline{\mathfrak{a}} \subseteq \overline{\wp_1^{e_1}} \cap \cdots \cap \overline{\wp_h^{e_h}}.$$

Un ideal primer $\overline{\wp}$ de $\overline{\mathfrak{a}}$ s'aplica, doncs, en un dels ideals $\overline{\wp_i^{e_i}}$, ja que $\overline{\wp_i^{e_i}} \supseteq \overline{\wp_i^{e_i}}$ també en un dels ideals $\overline{\wp_i}$. D'altra banda, un ideal primer $\overline{\wp}$ divisor de $\overline{\wp_i}$ s'aplica en un $\overline{\wp_i^{e_i}}$ i, doncs, en $\overline{\mathfrak{a}}$. Per tant, els ideals primers divisors de $\overline{\mathfrak{a}}$ són exactament els de $\overline{\wp_i}$.

Mostrem ara que, per a un ideal primer de primer grau $\wp$, o bé $\overline{\wp} = \overline{k_j}$, o bé és de nou un ideal primer de primer grau de k_j , de tal manera que per a $\mathfrak{a} = (\lambda - \lambda_1)$, com més amunt, $\mathfrak{a}$ conté únicament factors primers de primer grau, cada factor primer $\overline{\wp}$ de $\overline{\mathfrak{a}}$ s'aplica en un factor primer $\wp$ de $\mathfrak{a}$ que té grau 1. Considerem per a cada z $\mathbf{p}$ -enter de k_j el seu residu constant ζ mòdul $\wp$. Si per a un tal z el residu ζ no és $\mathbf{p}$ -enter, aleshores és $\overline{\wp} = \overline{k_j}$, llavors esdevé $1 - z/\zeta \equiv 0 \pmod{\wp}$, per tant, atès que $z/\zeta = 0$, $1 \equiv 0 \pmod{\overline{\wp}}$. Si $\overline{\wp}$ no esdevé igual a $\overline{k_j}$, aleshores totes les ζ són $\mathbf{p}$ -enteres i de $z \equiv \zeta \pmod{\wp}$ se segueix que $\overline{z} \equiv \overline{\zeta} \pmod{\overline{\wp}}$, doncs, $\overline{\wp}$ és un ideal primer de primer grau.

3. *Per a cada ordre $\mathbf{R}$ d'un cos de nombres quadràtic imaginari hi ha invariants singulars de característica 0 que tenen associat aquest $\mathbf{R}$ com a anell de multiplicadors.*

Demostració. N'hi ha prou d'indicar un cos el·líptic K_0 de característica 0 l'anell de multiplicadors $\mathbf{R}_0$ del qual tinguí igual cos de quocients Σ que el $\mathbf{R}$ donat per endavant. Llavors per a cada nombre primer q sigui $(\omega_{01}(q), \omega_{02}(q))$ una base de $\mathbf{R}_{0q}$ que proporcioni la representació $S_q(\mu)$ (§2 5) de $\mathbf{R}_0$ i C_q una matriu q -àdica entera que la transformi en una base $\omega_1(q), \omega_2(q)$ d'un mòdul de l'ordre $\mathbf{R}_q$. Aquestes matrius C_q , d'acord amb §2 6, poden ésser escollides quasi totes unimodulars; fixen un subcòs K de K_0 l'anell de multiplicadors del qual és $\mathbf{R}$.

Sigui p un nombre primer que romanguí primer en Σ . Aleshores $Q_{\infty, p}$ conté un subcòs isomorf a Σ , l'anell de multiplicadors d'un cos $\overline{K}$ de característica p , doncs, amb invariant supersingular un element $\overline{\mu}$ que genera aquest cos. D'acord amb el lema demostrat a 2, $\overline{K}$ pot ésser obtingut per reducció mòdul un divisor primer contingut en p

d'un cos K de característica 0, un multiplicador μ del qual s'aplica en $\bar{\mu}$. Però μ satisfà la mateixa equació quadràtica que $\bar{\mu}$ i, per tant, genera Σ , amb la qual cosa tot és demostrat.

Sigui Σ un cos de nombres quadràtic imaginari en el qual el nombre primer p descompongui en dos ideals primers diferents, i $\mathbf{R}$ un ordre de Σ , el conductor del qual no sigui divisible per p . Hi ha invariants singulars de característica p als quals pertany l'anell de multiplicadors $\mathbf{R}$.

Demostració. Partim d'un cos K_0 de característica 0, l'anell de multiplicadors $\mathbf{R}_0$ del qual té cos de quocients Σ . Atès que el seu invariant j és un nombre algebraic enter, podem prendre com a cos de constants un cos de nombres algebraics finit, i si nosaltres proporcionem una variable x escaient, i transferim a K un factor primer de p en aquest cos, aleshores, d'acord amb §4 3, obtenim per reducció segons aquest factor primer un cos el·líptic $\bar{K}$ de característica p amb invariant $\bar{j}$, l'anell de multiplicadors $\mathbf{R}_{00}$ del qual és un ordre de Σ . Com més amunt, prenem per a cada nombre primer $q \neq p$ una matriu q -àdica entera C_q , que mitjançant la representació S_q de $\mathbf{R}_{00}$ transforma la base $(\omega_1(q), \omega_2(q))$ de $\mathbf{R}_{00q}$ en una base d'un mòdul de $\mathbf{R}_q$. D'acord amb §2 6, juntament amb c_p i $I(K_0 : K)$ qualssevol, fixen un subcòs K de K_0 d'anell de multiplicadors $\mathbf{R}$.

4. Per a concloure remarquem encara que, per a cada característica, també hi ha cossos el·líptics que tenen únicament multiplicadors racionals: aquells d'invariant absolut transcendent.

§10. Els sistemes complets d'invariants singulars. Relacions entre nombres de classes

1. Investigarem les relacions que existeixen entre invariants singulars amb anells de multiplicadors del mateix cos de quocients.

Primer considerarem un cos el·líptic K l'anell de multiplicadors $\mathbf{R}$ del qual és un ordre en un cos de nombres quadràtic imaginari Σ . Si la característica p de K no és 0, aleshores descompon en Σ en dos ideals primers diferents $\mathbf{p}_1$ i $\mathbf{p}_2$. Si $\mathbf{a}$ és un ideal de $\mathbf{R}$, aleshores $K^{\mathbf{a}}$ té l'ordre $\mathbf{R}_1$ de $\mathbf{a}$ com a anell de multiplicadors (§2 2, 9). Els ideals *propis* de $\mathbf{R}$ que tenen l'ordre $\mathbf{R}$ condueixen a subcossos $K^{\mathbf{a}}$ amb el mateix anell de multiplicadors $\mathbf{R}$ de K . Dos d'aquests, $K^{\mathbf{a}_1}$ i $K^{\mathbf{a}_2}$, són isomorfs, tenen doncs el mateix invariant si, i només si, $\mathbf{a}_1$ i $\mathbf{a}_2$ són equivalents. *Doncs, entre els subcossos K n'hi ha tants no isomorfs com classes d'ideals en $\mathbf{R}$, sempre que demostrem a més que cada subcòs K_0 de K l'anell de multiplicadors del qual és igual a $\mathbf{R}$ pot ésser escrit en la forma $K_0 = K^{\mathbf{a}}$ amb un ideal $\mathbf{a}$ de $\mathbf{R}$. Aleshores apareix associat a cada classe d'ideals de $\mathbf{R}$ un invariant singular.* A fi de mostrar $K_0 = K^{\mathbf{a}}$ considerem per a cada $q \neq p$ la representació S_q de Σ corresponent a K (§2 5) i les matrius C_q corresponents a K_0 , a més, per a $p \neq 0$ la representació s_p i el c_p corresponent a K_0 . Sigui $\omega_1(q), \omega_2(q)$ una base de $\mathbf{R}_q$, proporcionada per S_q . Aleshores $(\omega_1(q), \omega_2(q)) C_q$ ha d'ésser base d'un mòdul $\mathbf{a}_q$ de l'ordre $\mathbf{R}_q$ (§2 7). A continuació, per a $p \neq 0$, si s_p és la representació $\mathbf{p}_1$ -àdica de Σ i K té el grau d'inseparabilitat p^f sobre K_0 , substituïm $\mathbf{a}_p = \mathbf{R}_p \mathbf{p}_1^h \mathbf{p}_2^f$, on h denota l'exponent de la potència de p continguda en c_p . Només per a una quantitat finita de q , $\mathbf{a}_q$ no és igual a $\mathbf{R}_q$ i, per

tant, hi ha un ideal $\mathbf{a}$ de $\mathbf{R}$ els components q -àdics del qual són aquests $\mathbf{a}_q$. Mostrem que $K_0 = K^{\mathbf{a}}$. D'entrada, els graus d'inseparabilitat $I(K : K_0)$ i $I(K : K^{\mathbf{a}})$ coincideixen per tot, són tots dos iguals a p^f . A continuació, atès que la potència de p continguda tant en $(K : K_0)$ com també en $(K : K^{\mathbf{a}})$ és igual a p^{h+t} , coincideixen també per tot les potències de p contingudes en els graus de separabilitat de K sobre K_0 i de K sobre $K^{\mathbf{a}}$. Finalment, d'acord amb (§2 9), les matrius C_q tenen per a $K^{\mathbf{a}}$ el mateix significat que per a K_0 . Per tant, d'acord amb §2 6, efectivament és $K^{\mathbf{a}} = K_0$.

Anomenarem la totalitat dels invariants dels subcossos de K *un sistema complet d'invariants singulars del cos Σ* . En aquesta, per a cada classe d'un ordre de Σ hi ha un invariant, per tant, tants invariants als quals pertany aquest ordre com a anell de multiplicadors com classes en l'ordre. Hem demostrat l'existència *d'un sistema complet d'invariants* per a Σ . Però n'hi podria haver més.

2. Podem formular els raonaments corresponents per als invariants supersingulars de característica p . Sigui K un cos el·líptic de característica p , l'anell de multiplicadors $\mathbf{R}_i$ del qual és un ordre maximal de $Q_{\infty,p}$. Si $\mathbf{a}_{ih}$ és un ideal per l'esquerra de $\mathbf{R}_i$, aleshores l'anell de multiplicadors de $\mathbf{K}^{\mathbf{a}_{ih}}$ és l'ordre per la dreta $\mathbf{R}_h$ de $\mathbf{a}_{ih}$. Atès que dos cossos $K^{\mathbf{a}_{ih}}$ i $K^{\mathbf{a}_{il}}$ són isomorfs si, i només si, $\mathbf{a}_{ih}$ i $\mathbf{a}_{il}$ són equivalents, entre els subcossos de K n'hi ha tants no isomorfs com classes d'ideals en $Q_{\infty,p}$. Igualment gran és el nombre d'invariants supersingulars de característica p , que es presenten generalment a causa dels subcossos de K . De nou anomenarem la seva totalitat *un sistema complet d'invariants supersingulars de característica p* .

A dos invariants supersingulars j_1 i j_2 del sistema complet corresponen anells de multiplicadors isomorfs $\mathbf{R}_{h_1}$ i $\mathbf{R}_{h_2}$ si els cossos corresponents $K^{\mathbf{a}_{ih_1}}$ i $K^{\mathbf{a}_{ih_2}}$ mantenen una relació $\mathbf{a}_{ih_2} = \mathbf{c}_{ii}\mathbf{a}_{ih_1}\gamma$, $\mathbf{c}_{ii}$ ideal bilateral de $\mathbf{R}_i$, per tant si, i només si, $\mathbf{a}_{ih_1}$ i $\mathbf{a}_{ih_2}$ tenen ordres per la dreta $\mathbf{R}_{h_1}$ i $\mathbf{R}_{h_2}$ isomorfs (o bé que pertanyen al mateix tipus)²⁸⁾. En lloc de $\mathbf{a}_{ih_2} = \mathbf{c}_{ii}\mathbf{a}_{ih_1}\gamma$, podem també escriure $\mathbf{a}_{ih_2} = \mathbf{a}_{ih_1}\mathbf{c}_{h_1h_1}\gamma$. Sigui $\mathbf{p}_{h_1h_1}$ l'ideal bilateral primer de $\mathbf{R}_{h_1}$ de quadrat p . Aleshores un ideal bilateral de $\mathbf{R}_{h_1}$ és, o bé igual a $\mathbf{R}_{h_1}n$, o bé igual a $\mathbf{p}_{h_1h_1}n$, on per n entenem un nombre racional. *En conseqüència, hi ha un o bé dos invariants supersingulars en el sistema complet dels quals els corresponents anells de multiplicadors són del mateix tipus segons que $\mathbf{p}$ sigui o no en aquest tipus un ideal principal. En el primer cas, l'invariant és manifestament racional, en el segon, els dos invariants són del mateix grau i conjugats entre si.* La taula (65) mostra que es presenten tots dos casos.

3. *Per a cada possible domini de divisió Σ hi ha únicament un sistema complet d'invariants singulars o bé supersingulars.*

Demostració. Considerem, primerament, el cas en què $\Sigma = Q_{\infty,p}$. D'acord amb **2**, el nombre de tots els invariants supersingulars de característica p és un múltiple del nombre de classes de $Q_{\infty,p}$. Però el nombre de classes de $Q_{\infty,p}$ calculat per EICHLER²⁹⁾, és

²⁸⁾Cf. M. DEURING, *Algebren*, Ergebn. der Math. IV,₁, p. 89.

²⁹⁾M. EICHLER, *Über die Idealklassenzahl total definierter Quaternionalgebren*, Math. Zeitschr. **43**, p. 102–109 (1937)

$$\begin{aligned}
 & \frac{p-1}{12} \quad \text{per a } p \equiv 1 \pmod{12}, \\
 & \frac{p-5}{12} + 1 \quad \text{per a } p \equiv 5 \pmod{12}, \\
 & \frac{p-7}{12} + 1 \quad \text{per a } p \equiv 7 \pmod{12}, \\
 & \frac{p-11}{12} + 2 \quad \text{per a } p \equiv 11 \pmod{12},
 \end{aligned}
 \tag{66}$$

d'acord amb (63) en general coincideix per tot amb el nombre de tots els invariants supersingulars de característica p , quan suposem que el polinomi $P(j)$ té totes les arrels diferents $P(j)$. *Amb això s'ha demostrat la unicitat del sistema complet d'invariants i , al mateix temps, que efectivament el polinomi $P(j)$ té totes les arrels diferents.* No sembla fàcil veure-ho directament a partir de l'expressió (63) (o bé (61) o també (64)) per a $P(j)$.

Demostrarem la unicitat del sistema d'invariants supersingulars per al cas $p \not\equiv 1 \pmod{12}$ sense recolzar-nos en les fórmules del nombre de classes d'Eichler. Per a $p = 2$ i $p = 3$ ja hem demostrat en §8 **2** que només hi ha un invariant supersingular. Sigui ara $p \equiv 2 \pmod{3}$. Atès que en aquest cas $Q_{\infty, p}$ conté el cos de les arrels terceres de la unitat, hi ha almenys un ordre maximal en el qual es troben les arrels terceres de la unitat. D'acord amb §5 **2**, això és únicament possible per a l'invariant $j = 0$. Però mitjançant un invariant es determina el sistema d'invariants supersingulars complet. Per tant, només n'hi ha un. Exactament de la mateixa manera concloem per a $p \equiv -1 \pmod{4}$. En $Q_{\infty, p}$ hi ha un ordre maximal amb les arrels quartes de la unitat, al qual, segons §5 **2** pertany l'invariant $j = 2^6 3^3$ i

d'aquesta manera és fixat el sistema complet. Els nombres primers $p \equiv 1 \pmod{12}$ se sostreuen d'aquesta conclusió.

D'entrada considerem doncs el cas de característica 0. Si volem recolzar-nos en la teoria analítica, és natural no demostrar res més. Si hi renunciem, podem avançar de la manera següent. Sigui Σ el cos de nombres quadràtic imaginari donat. Siguin S_1 i S_2 dos sistemes complets d'invariants de Σ , que volem reconèixer com a iguals. Considerem únicament els h invariants $j_{i,1}, \dots, j_{i,h}$ dels sistemes S_i que pertanyen a l'ordre *maximal* $\mathbf{R}$ de Σ . Considerem un cos el·líptic K_1 d'invariant $j_{1,1}$ i un cos K_2 d'invariant $j_{2,1}$. Si suposem que el cos de constants k comú dels dos conté el cos Σ , aleshores d'acord amb §3 3, tots els multiplicadors que pertanyen a $j_{i,1}$, per tancament algebraic del cos de constants, ja són possibles en K_i . Sigui q un nombre primer $\equiv 2 \pmod{3}$ que roman primer en Σ , $\mathfrak{q}$ un factor primer de q en k , i $\bar{k}$ el cos de classes de residus de k mòdul $\mathfrak{q}$. Sigui $\overline{K^*}$ un cos el·líptic de característica 0 d'invariant supersingular i de cos de constants $\bar{k}$. D'acord amb §4 3, estenem $\mathfrak{q}$ a K_i de manera que $\overline{K_i}$ mòdul $\mathfrak{q}$ s'apliqui en un cos el·líptic $\overline{K_i}$ d'invariant $\bar{j}_{i,1}$ amb cos de constants $\bar{k}$. D'acord amb §4 2 i §2 10, l'anell de multiplicadors de $\overline{K_i}$ és un ordre maximal $\overline{\mathbf{R}_i}$ de $Q_{\infty,p}$ que conté un subanell $\overline{\mathbf{o}_i}$ isomorf a un dels ordres maximals de Σ .

Per causa de la unicitat dels sistemes d'invariants supersingulars mòdul q , $\overline{K_i}$ pot ésser aplicat de manera isomorfa en un subcòs $\overline{K_i^*}$ de $\overline{K^*}$, on $\bar{k}$ cal que s'apliqui en ell mateix element a element. Hi ha un element $\bar{\xi}$ de $\overline{\mathbf{R}_2}$ que transforma $\overline{\mathbf{o}_2}$ en $\overline{\mathbf{o}_1}$, $\overline{\mathbf{o}_1} = \bar{\xi}^{-1} \overline{\mathbf{o}_2} \bar{\xi}$. L'anell de multiplicadors $\bar{\xi}^{-1} \overline{\mathbf{R}_2} \bar{\xi}$ de $\overline{K_i^*}$ conté, de la mateixa manera que $\overline{\mathbf{R}_1}$, l'anell $\overline{\mathbf{o}_1}$. Però d'això se segueix que hi ha un ideal

$\bar{\mathbf{a}}$ de $\bar{\mathbf{o}}_1$ per al qual val $\bar{\xi}^{-1}\bar{\mathbf{R}}_2\bar{\xi} = \bar{\mathbf{a}}^{-1}\bar{\mathbf{R}}_1\bar{\mathbf{a}}$ ³⁰⁾. $K_1^{\mathbf{a}}$ s'aplica mòdul $\mathfrak{q}$ sobre un subcòs $\bar{K}_1^{\mathbf{a}}$ de $\bar{K}_1$, la imatge del qual en $\bar{K}_1^*$, $\bar{K}_1^{*\bar{\mathbf{a}}}$ té l'ordre maximal $\bar{\mathbf{a}}^{-1}\bar{\mathbf{R}}_1\bar{\mathbf{a}} = \bar{\xi}^{-1}\bar{\mathbf{R}}_2\bar{\xi}$ com a anell de multiplicadors. Doncs $\bar{K}_1^{\mathbf{a}}$ té els mateixos invariants que $\bar{K}_2$, i això significa que té lloc una congruència

$$j_{2,1} \equiv j_{1,l(q)} \pmod{\mathfrak{q}},$$

on $l(q)$ designa un dels índexs $1, \dots, h$. Ara els nombres primers q poden ésser caracteritzats com aquells nombres primers que en els subcossos quadràtics diferents de Σ i $P(\sqrt{-3})$ del cos biquadràtic $\Sigma(\sqrt{-3})$ descomponen en factors primers de primer grau, els quals, per la seva banda, romanen primers en $\Sigma(\sqrt{-3})$. Però, d'acord amb el teorema de BAUER ³¹⁾, d'aquests nombres primers q n'hi ha una infinitat. Per a una infinitat d'ells, $l(q)$ té el mateix valor l . Atès que $j_{2,1}$ és congru a $j_{1,l}$ segons una infinitat d'ideals primers de k , val $j_{2,1} = j_{1,l}$ i amb això queda demostrada la unicitat dels sistemes complets d'invariants singulars de característica 0 del cos Σ .

En aquest moment resta encara per demostrar que també són únics els sistemes d'invariants singulars de característica un nombre primer i els invariants supersingulars de característica $q \equiv 1 \pmod{12}$. Per a això, escollim dos sistemes d'invariants de característica q , que reconeixem com iguals, l'un $\bar{j}_1$ i l'altre $\bar{j}_2$, on podem suposar que en l'anell de multiplicadors $\bar{\mathbf{R}}_i$ que pertany a $\bar{j}_1$ està contingut un

³⁰⁾ VL. KOŘÍNEK, Maximale kommutative Körper in einfachen Systemem von hyperkomplexen Zahlen, Mém. Soc. Roy. Sci. Bohême 1932, p. 1-24 (1933); §3, Satz 3.

³¹⁾ Cf. tal vegada M. DEURING, Neuer Beweis des Bauerschen Satzes, Journ. f. d. r. u. ang. Math.

subanell $\overline{\mathbf{o}}_i$ que és isomorf a l'ordre maximal $\mathbf{o}$ d'un determinat cos de nombres quadràtic imaginari Σ . Sigui $1, \omega$, una base de $\mathbf{o}$. D'acord amb el lema 2, per reducció mòdul un divisor primer $\mathfrak{q}$ que divideix q , podem obtenir $\overline{K}_i$ a partir d'un cos K_i de característica 0, l'anell de multiplicadors del qual conté ω i, per tant, és l'ordre maximal de Σ . Aquí K_1 i K_2 cal que tinguin un cos de nombres algebraics finit k com a cos de constants comú, el qual mòdul $\mathfrak{q}$ s'aplica en el cos de constants comú $\overline{k}$ de $\overline{K}_1$ i $\overline{K}_2$. Fins i tot podem interpretar K_2 com a subcòs de K_1 , atès que només hi ha un sistema d'invariants singulars per a Σ de característica 0. Així $\overline{K}_2$ esdevé un subcòs de $\overline{K}_1$; en conseqüència, $\overline{j}_1$ i $\overline{j}_2$ pertanyen al mateix sistema d'invariants, com calia demostrar.

4. Després que s'ha demostrat la unicitat del sistema d'invariants singulars de característica 0 podem deduir les relacions clàssiques entre nombres de classes de KRONECKER ³²⁾ de la manera habitual. No tractem aquest tema.

De manera semblant, però, podem deduir noves relacions entre nombres de classes a partir dels sistemes d'invariants singulars i supersingulars de característica un nombre primer. Demostrem per endavant:

Cada invariant algebraic absolut j de característica un nombre primer p és singular o bé supersingular.

Sigui $j^{p^f} = j$. Si j no és supersingular, aleshores val $\sigma = 1$ per a un cos K d'invariant j . K és isomorf a un dels seus subcossos K^{p^f} (suposat un cos de constants suficientment gran), atès que té el mateix invariant. En conseqüència,

³²⁾ Cf. tal vegada H. WEBER, Lehrbuch der Algebra III, p. 423.

K té un multiplicador π de norma p^f el qual, però, no pot ésser cap potència de p , perquè K^{p^e} no és purament inseparable sota K ja que $\sigma = 1$. Doncs, π és complex, amb la qual cosa és demostrat el teorema.

D'acord amb §3 **2**, per a un dels dos ideals primers en què p descompon en l'anell de multiplicadors $\mathbf{R}$ de K , tal vegada per a $\mathbf{p}_1$, val $K^{\mathbf{p}_1} = K^p$. Llavors, $\mathbf{p}_1^f = (\pi)$ és un ideal principal de $\mathbf{R}$. Podem expressar això també d'una altra manera: sigui d el discriminant de l'ordre $\mathbf{R}$. Considerem les formes quadràtiques binàries de discriminant d . $\mathbf{p}_1^f =$ ideal principal significa que p^f permet una representació *pròpia* per mitjà de la forma principal de discriminant d , és a dir, mitjançant $x^2 - y^2 d/4$ o bé $x^2 + xy - y^2(d-1)/4$, segons que sigui $d \equiv 0$ o bé $d \equiv 1 \pmod{4}$.

El nombre d'invariants singulars j de característica p amb el mateix anell de multiplicadors és igual al nombre de classes $h(d)$ de d .

De manera semblant tractem també els invariants supersingulars j .

Si és $j^p = j$, d'acord amb **2**, en el corresponent anell de multiplicadors hi ha un element de norma p , és a dir, p és representable (pròpiament) per mitjà de la forma nòrmica quaternària de discriminant $-p^2$ de l'anell de multiplicadors. Si, en canvi, és $j^p \neq j$, però $j^{p^2} = j$, aleshores, per la forma nòrmica no és representable p , sinó p^2 . En el primer cas, totes les potències de p són representables per la forma nòrmica; en el segon, únicament les d'exponent parell.

Si ara reflexionem sobre com es reparteixen tots els p^f elements del cos de Galois de grau f en invariants singulars

i supersingulars, obtenim la relació de nombres de classes següent:

Val

$$(67) \quad \sum h(d_{p^f}) + t_{p^f} = p^f.$$

Aquí d_{p^f} recorre tots els discriminants no divisibles per p de les formes quadràtiques binàries definides per a les quals p^f és representable pròpiament per la forma principal corresponent, i t_{p^f} denota el nombre d'aquelles classes d'ideals en un ordre maximal donat $\mathbf{R}$ de $Q_{\infty,p}$, tals que la seva forma nòrmica quaternària representa p^f , qualsevol $\mathbf{R}$ que es transformi en aquests ordres maximals.

D'acord amb **2**, també podem dir:

Per a f parell, t_{p^f} és el nombre de classes de $Q_{\infty,p}$ donat per mitjà de (66), i, per a f senar, és el nombre de tipus d'ordres maximals de $Q_{\infty,p}$ en els quals l'ideal primer que divideix p és principal, per tant, les formes nòrmiques del qual també representen p ; o també

$$t_{p^2} = t_{p^4} = \cdots = h, \quad t_p = t_{p^3} = \cdots = \frac{h+t}{2},$$

on h denota el nombre de classes, i t el de tipus de $Q_{\infty,p}$.

§11. Relacions de congruència per als invariants singulars

1. El pas dels cossos el·líptics de característica 0 a aquells de característica un nombre primer, que ja hem

aplicat repetidament, proporciona relacions de congruència notables entre els invariants singulars.

Segui K un cos el·líptic de característica 0 amb invariant singular j i cos de constants un cos de nombres algebraic [de grau] finit, k , del qual suposem que conté j i el cos de nombres quadràtic imaginari Σ en el qual el cos de quocients Σ de l'anell de multiplicadors $\mathbf{R}$ de K s'aplica isomòrficament mitjançant la diferencial entera de K (§3 2). Llavors, tots els multiplicadors són possibles en K (§3 3).

Segui $\mathfrak{p}$ un ideal primer de k , que d'acord amb §4 3 estenem a K , que apliqui K mòdul $\mathfrak{p}$ en un cos el·líptic $\overline{K}$ d'invariant $\overline{j}$ amb cos de constants $\overline{k}$. Investigarem com es relaciona l'anell de multiplicadors de $\overline{K}$ amb el de K . En aquest treball ens restringirem al cas en què el nombre primer p divisible per $\mathfrak{p}$ no descompon completament en Σ , de tal manera que $\overline{j}$ és supersingular; l'altre cas és tractat en un treball ulterior sobre els cossos de classes de multiplicació complexa.

Afirmem: L'anell de multiplicadors $\overline{\mathbf{R}}$ de $\overline{K}$ és un ordre maximal de $Q_{\infty, \mathfrak{p}}$, que té en comú amb el cos Σ aquells ordres el conductor dels quals, privat del conductor de $\overline{\mathbf{R}}$, conté la potència de p corresponent.

Per a demostrar-ho necessitem considerar que, segons §4 4, la representació $S_q(\mu)$ de Σ per a $\overline{K}$ introduïda en §2 5, té el mateix significat que per a K en el cas en què q és un nombre primer diferent de p ; mentre $\mathbf{R}$ és la intersecció de totes les complecions q -àdiques $\mathbf{R}_q$ de $\mathbf{R}$ amb $\mathbf{R}_p$, la part de Σ que es troba en $\overline{\mathbf{R}}$ és la intersecció de tots els $\mathbf{R}_q$ en tant que consisteix en nombres p -enters i, per tant, el conductor d'aquestes parts és el producte dels conductors

de tots els $\mathbf{R}_q$, però el de $\mathbf{R}$, és el producte dels conductors de tots els $\mathbf{R}_q$ amb el de $\mathbf{R}_p$.

Considerem primerament el cas $p = 2$. Atès que només hi ha un invariant supersingular 0, aleshores val:

Un invariant singular j de característica 0 o bé no és divisible per cap factor primer de 2, o bé per tots, segons que 2 descompongui completament en el cos quadràtic imaginari Σ corresponent o no.

Aquest resultat és remarcable, perquè està relacionat amb un teorema demostrat d'una manera sorprenent per H. WEBER per mitjà de la fórmula límit de KRONECKER. Aquest teorema ³³⁾ diu així:

Sigui

$$f(\omega) = \frac{e^{-\frac{\pi i}{24}} \eta\left(\frac{\omega + 1}{2}\right)}{\eta(\omega)},$$

on

$$\eta(\omega) = e^{\frac{2\pi i}{24}} \prod_{n=1}^{\infty} \left(1 - e^{\frac{2\pi i n}{24}}\right)$$

denota la funció η de DEDEKIND; l'invariant absolut $j(\omega)$ pot ésser expressat de la manera següent per mitjà de f :

$$j(\omega) = \frac{(f(\omega)^{24} - 16)^3}{f(\omega)^{24}}.$$

Sigui $\omega = \omega_1/\omega_2$ el quocient de dos nombres ω_1, ω_2 que formin una base d'un ideal d'un ordre arbitrari en un cos de nombres quadràtic imaginari Σ , llavors,

$$f(\omega)/\sqrt{2}$$

³³⁾ H. WEBER, Lehrbuch der Algebra III, p. 540–541.

és una unitat si 2 descompon completament en Σ ; altrament, el producte de $f(\omega)/\sqrt{2}$ amb una potència donada de 2 d'exponent positiu és una unitat.

La conseqüència que d'això hem d'extreure per a $j(\omega)$ és el teorema demostrat més amunt: $j(\omega)$ o bé no és divisible per cap factor primer de 2, o bé per tots, segons que 2 descompongui completament en Σ o no.

Únicament el primer cas requereix el mètode transcendent de WEBER; en el segon cas, la potència de 2 continguda en $f(\omega)$ pot ésser determinada de manera algebraica. Si un es limita a la pregunta corresponent per a j , aleshores poden aparèixer les equacions invariants de segon ordre calculades mitjançant les de §6 4. No hi insistim més.

Obtenim afirmacions semblantment afinades com per a $p = 2$ per a la resta de nombres primers per als quals $Q_{\infty,p}$ té únicament una classe, és a dir, per a $p = 3, 5, 7, 13$. Per a 3 i 5 les afirmacions, en completa correspondència, són:

j o bé no és divisible per cap factor primer de 3 o 5, o bé per tots, segons que 3 (5) descompongui completament en Σ o no.

A més,

$j - 2^6 3^3 \equiv j + 1$ o bé no és divisible per cap factor primer de 7, o bé per tots, segons que 7 descompongui completament en Σ o no.

$j - 5$ o bé no és divisible per cap factor primer de 13, o bé per tots, segons que 13 descompongui completament en Σ o no.

Per als p restants, caldria conèixer exactament com es reparteixen els invariants supersingulars en els diferents tipus d'ordres maximals; d'altra banda, donat un ordre de Σ , caldria conèixer en quin tipus d'ordre maximal està contingut.

2. Exemples.

$j(\sqrt{-1}) = 2^6 \cdot 3^3$ és divisible per 2 i per 3, perquè 2 i 3 no descomponen completament en $P(\sqrt{-1})$. $j - 5 \equiv 7 \pmod{13}$ no és divisible per 13, 13 esdevindria descompost completament. Però $2^6 \cdot 3^3 - 2^6 \cdot 3^3 = 0$ és divisible per 7, perquè 7 no descompon completament.

En general, atès que $p \equiv 7$ o bé $11 \pmod{12}$, $2^6 \cdot 3^3$ esdevé supersingular per a cada nombre primer p que no descompongui completament en $P(\sqrt{-1})$.

Per contra, considerem $j(\sqrt{-4}) = 2^3 \cdot 3^3 \cdot 11^3$, que pertany al mateix sistema singular que $j(\sqrt{-1})$. De nou $j(\sqrt{-4})$ és divisible per 2, 3. A continuació és

$$2^3 \cdot 3^3 \cdot 11^3 - 2^6 \cdot 3^3 \equiv 2^3 \cdot 3^3 (1331 - 2^3) \equiv 0 \pmod{7}$$

però

$$2^3 \cdot 3^3 \cdot 11^3 \equiv 0 \pmod{11},$$

per tant, per a 11 es presenta un altre invariant supersingular més que per a $j(\sqrt{-1})$.

De la mateixa manera, per a 19:

$$2^3 \cdot 3^3 \cdot 11^3 = 66^3 \equiv 9^3 = 9 \cdot 81 \equiv 9 \cdot 5 = 45 \equiv 7 \pmod{19},$$

$$23 : \quad 2^3 \cdot 3^3 \cdot 11^3 = 66^3 \equiv 20^3 \equiv -3^3 = -27 \equiv 19 \pmod{23},$$

$$31 : \quad 2^3 \cdot 3^3 \cdot 11^3 = 66^3 \equiv 4^3 \equiv 2 \pmod{31},$$

$$\begin{aligned}
43 : \quad 2^3 \cdot 3^3 \cdot 11^3 &= 66^3 \equiv -20^3 = -8000 \equiv 41 \pmod{43}, \\
47 : \quad 2^3 \cdot 3^3 \cdot 11^3 &= 66^3 \equiv 44 \pmod{47}.
\end{aligned}$$

En $P\sqrt{-3}$ amb $j(-\frac{1}{2} + \frac{1}{2}\sqrt{-3}) = 0$ descomponen els nombres primers $\equiv -1 \pmod{3}$, per tant, no completament $\equiv 5, 11 \pmod{12}$, per als quals en efecte $j = 0$ és supersingular. Per a $j(\sqrt{-3}) = 2^4 \cdot 3^3 \cdot 5^3$ tenim que

$$\begin{aligned}
2^4 \cdot 3^3 \cdot 5^3 &\equiv 0 \pmod{5}, \\
&\equiv 2^6 \cdot 3^3 \pmod{11}, \\
&\equiv 8 \pmod{17}, \\
&\equiv 19 \pmod{23}, \\
&\equiv 2 \pmod{29}, \\
&\equiv 3 \pmod{41}, \\
&\equiv 44 \pmod{47}.
\end{aligned}$$

En $P(\sqrt{-5})$ amb $j(\sqrt{-5}) = 2^6 \cdot 5\sqrt{5}(16 + 7\sqrt{5})^3(9 - 4\sqrt{5})$ no descomponen completament 11, 13, 17, 19, 31, 37. Esdevé

$$j(\sqrt{-5}) \equiv \begin{cases} 0 & \text{quan } \sqrt{5} \equiv 4 \\ 1 \equiv 2^6 \cdot 3^3 & \text{quan } \sqrt{5} \equiv -4 \end{cases} \pmod{11},$$

$$\begin{aligned}
j(\sqrt{-5}) &\equiv 5\sqrt{5}(3 + 7\sqrt{5})^3(4 + 4\sqrt{5}) \\
&\equiv 5\sqrt{5}(-4 + 6\sqrt{5})(4 + 4\sqrt{5}) \\
&\equiv \sqrt{5}(-2 + 3\sqrt{5})(1 + \sqrt{5}) \\
&= \sqrt{5}(13 + \sqrt{5}) \equiv 5 \pmod{13},
\end{aligned}$$

$$j(\sqrt{-5}) \equiv -3\sqrt{5}(-1 + 7\sqrt{5})^3(9 - 4\sqrt{5}) \equiv 8 \pmod{17},$$

$$j(\sqrt{-5}) \equiv \begin{cases} 2^6 \cdot 3^3 & \text{quan } \sqrt{5} \equiv 9 \\ 7 & \text{quan } \sqrt{5} \equiv -9 \end{cases} \pmod{19},$$

$$j(\sqrt{-5}) \equiv \begin{cases} 2 & \text{quan } \sqrt{5} \equiv 6 \\ 4 & \text{quan } \sqrt{5} \equiv -6 \end{cases} \pmod{31},$$

$$j(\sqrt{-5}) \equiv 3 \pm 2\sqrt{13} \pmod{37}.$$

Referències de l'article

Recollim totes juntes les referències citades en aquest article.

Deuring, M.: *Algebren*. Springer, Ergebnisse der Mathematik und ihre Grenzgebiete, vol. IV, 1935.

Deuring, M.: Neuer Beweis des Bauerschen Satzes. *J. reine u. angew. Math.* **173** (1935), p. 1–4.

Deuring, M.: Arithmetische Theorie der Korrespondenzen algebraischer Funktionenkörper, I. *J. reine u. angew. Math.* **177** (1937), p. 161–191.

Deuring, M.: Arithmetische Theorie der Korrespondenzen algebraischer Funktionenkörper, II. *J. reine u. angew. Math.* **183** (1941), p. 25–36.

Deuring, M.: Zur Theorie der Moduln algebraischer Funktionenkörper. *Math. Zeitschr.* **47** (1941), p. 34–46.

Deuring, M.: Invarianten und Normalformen elliptischer Funktionenkörper. *Math. Zeitschr.* **47** (1941), p. 47–56.

Deuring, M.: Reduktion algebraischer Funktionenkörper nach Primdivisorem des Konstantenkörpers. *Math. Zeitschr.* **47** (1941), p. 643–654.

Eichler, M.: Über die Idealklassenzahl total definiter Quaternionen algebren. *Math. Zeitschr.* **43** (1937), p. 102–109.

Gauss, C. F.: Werke, Zehnten Bandes Erste Abteilung. Herausgegeben von der Königlichen Gesellschaft der Wissenschaften zu Göttingen, Leipzig, Teubner, 1917. Tagebuch mit Erläuterungen [146], p. 571–572.

Hasse, H.: Beweis des Analogons der Riemannschen Vermutung für die Artinschen und F. K. Schmidtschen Kongruenzzetafunktionen in gewissen elliptischen Fällen. *Nachr. Ges. d. Wiss. Göttingen Math.-Phys. Kl. I*, **42** (1933), p. 253–262.

Hasse, H.: Abstrakte Begründung der komplexen Multiplikation und Riemannsche Vermutung in Funktionenkörpern. *Abh. Math. Semin. Hamburg. Univ.*, **10** (1934) p. 325–348.

Hasse, H.: Existenz separabler zyklischer unverzweigter Erweiterungskörper vom Primzahlgrade p über elliptischen Funktionenkörpern der Charaktersitik p . *J. reine u. angew. Math.* **172** (1934), p. 77–85.

Hasse, H.: Zur Theorie der abstrakten elliptischen Funktionenkörper, I. *J. reine u. angew. Math.* **175** (1936), p. 55–62.

Hasse, H.: Zur Theorie der abstrakten elliptischen Funktionenkörper, II. *J. reine u. angew. Math.* **175** (1936), p. 69–88.

Hasse, H.: Zur Theorie der abstrakten elliptischen Funktionenkörper, III. *J. reine u. angew. Math.* **175** (1936), p. 193–208.

Hasse, H.; Witt, E.: Zyklische unverzweigte Erweiterungskörper vom Primzahlgrade p über einem algebraischen Funktionenkörper der Charakteristik p , *Mh. Math. Phys.* **43** (1936) p. 477–492.

Herglotz, G.: Zur letzten Eintragung im Gausschen Tagebuch. *Ber. d. Math.-Phys. Kl. d. Sächs. Ak. d. Wiss. Leipzig*, **73** (1921), p. 271–276.

Koříněk, V.: Maximale kommutative Körper in einfachen Systemem von hyperkomplexen Zahlen. *Mém. Soc. Roy. Sci. Bohême*, **1932** (1933), p. 1–24.

Nehrkorn, H.: Über absolute Idealklassengruppe und Einheiten in algebraischen Zahlkörpern. *Abh. Math. Sem. Univ. Hamburg*, **9** (1933), p. 318–334.

Weber, H.: *Lehrbuch der Algebra*, vol. III. Brunswick, Friedrich Vieweg und Sohn, segona edició, 1908. La primera edició, de 1891, duia el títol *Elliptischen Funktionen und algebraischen Zahlen*.

Weber, W.: Bemerkungen zur arithmetischen Theorie der binären quadratischen Formen, *Nachr. Ges. d. Wiss. Göttingen Math. Phys. Kl. I*, **1929** (1929), p. 116–130.

Capítol 13

Sprague i Richert

Els dos darrers articles que traduïm han arribat a les nostres mans a partir de les nostres tasques de docència en cursos d'aritmètica bàsica de la llicenciatura; no cal cercar-hi, doncs, relacions profundes amb la recerca.

Amb eines elementals, els seus autors presenten resultats d'aritmètica a l'abast de la comprensió de qualsevol estudiant de matemàtiques, sense necessitat de cap especialització concreta ni de cap tècnica sofisticada. (I la seva presentació al grup classe es pot fer de manera prou còmoda en una sola sessió.)

13.1 1948–1949: Aportació a la teoria additiva de nombres

L'origen dels treballs de Sprague i de Richert dels quals presentem la traducció no es pot desvincular de la teoria matemàtica de jocs.

Sembla que l'interès de Sprague per la teoria de jocs es remunta als anys de la Primera Guerra Mundial. En aquella època s'aficionà a diferents jocs i, en particular, esdevingué un admirador i seguidor del matemàtic i gran mestre d'escacs alemany Emanuel Lasker. Més endavant, l'any 1930, Sprague seria un dels millors jugadors alemanys de go.

Aquest interès de Sprague el conduí a l'estudi matemàtic de diferents problemes combinatoris (cf. [372]), o jocs que tenen estratègia guanyadora com el nim (cf. [365]); i també a la creació d'una teoria matemàtica de jocs, que publicà l'any 1936 a la revista japonesa *Tôhoku Math. J.* (cf. [362]). La teoria, descoberta independentment i publicada per Grundy l'any 1939, és coneguda actualment com la teoria de Sprague i Grundy i és àmpliament utilitzada en ciències econòmiques.

En aquesta època, Sprague també s'interessà pel problema de descompondre un quadrat en altres quadrats més petits, tots diferents. Sembla que aquest problema, que es coneixeria més endavant com “quadrar un quadrat”, ja havia estat esmentat l'any 1902 pel matemàtic britànic i creador de trencaclosques, lògics i matemàtics, Henry Dudeney en el trencaclosques anomenat *La caixeta de Lady Isabel* (*Lady Isabel's Casket*). Aquest entreteniment consistia a

calcular la mida d'una caixeta quadrada de fusta sabent que la tapa contenia un rectangle d'or, del qual es coneixia la mida dels costats, i una sèrie de quadrats més petits, tots diferents i també de fusta, dels quals no se'n sabien les arestes. (El problema, doncs, no era ben bé quadrar un quadrat.)

El problema es relaxà de seguida a la consideració de disseccions de rectangles en quadrats diferents. En un article publicat als *Mathematischen Annalen* (cf. [73]), Dehn, que ja havia fet contribucions al problema 3 de Hilbert, hi féu avenços l'any 1903. Més endavant, l'any 1925, aparegueren alguns exemples concrets de descomposicions de rectangles en quadrats diferents en un article en polonès de Moroń (cf. [277]). Reproduïm dos d'aquests rectangles en aquesta pàgina i la següent.

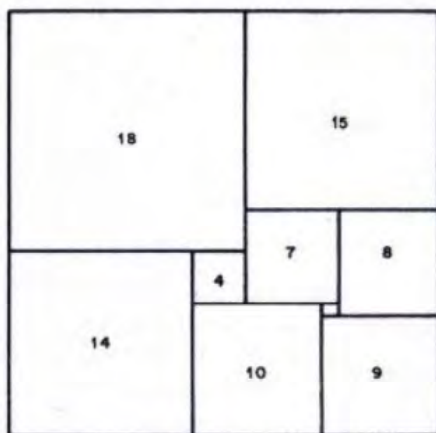
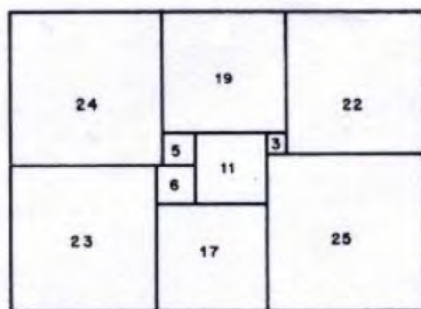


Figura 5. Rectangle 32×33

Figura 6. Rectangle 47×65

El primer exemple d'un quadrat descompost en quadrats tots diferents fou publicat per Sprague l'any 1939 (cf. [369]), poc després que Stöhr hagués presentat la seva tesi (cf. [375]) sobre descomposicions de rectangles. Sprague utilitzà alguns dels exemples dels rectangles descompostos l'any 1925, que ja havia citat en [221]. El quadrat de Sprague és d'aresta 4205 i la seva descomposició consta de 55 quadrats diferents. A la pàgina següent reproduïm l'esquema del quadrat de Sprague. Consta de cinc quadrats, de costats $29 \cdot 33$, $5 \cdot 13 \cdot 29$, $13 \cdot 33$, $13 \cdot 80$ i $29 \cdot 80$; de dues còpies escalades de la parella anterior de rectangles, una multiplicada per 29 (retolada com 29·I, 29·II) i l'altra per 13 (sense retolar en el dibuix), i d'un rectangle (retolat com 5·III) descompost en 12 quadrats, les mides dels quals són unívocament determinades. Es deixa com a exercici la determinació del costat de cadascun dels quadrats que formen el quadrat de Sprague i la comprovació que tots són diferents.

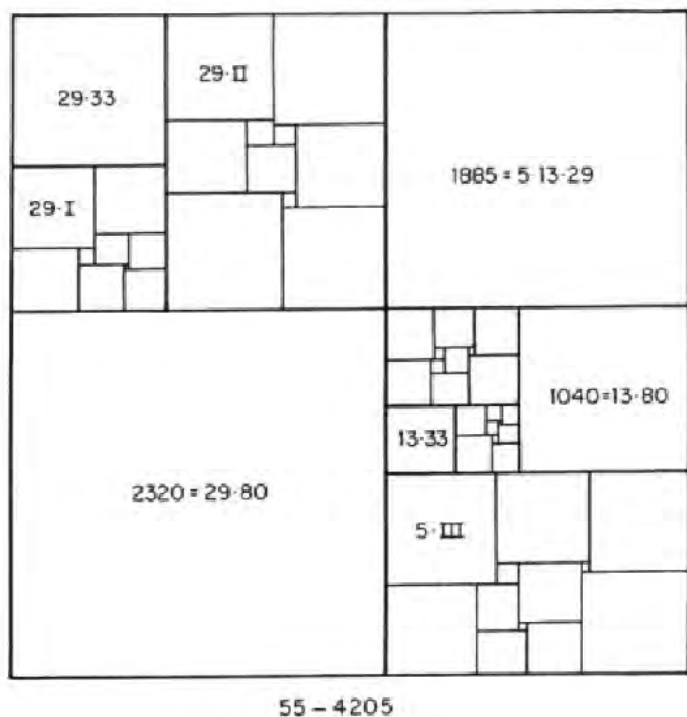


Figura 7. Quadrat de costat 4205

El problema també fou tractat per un grup de matemàtics britànics autoanomenat *Blanche Descartes*, que formaren Brooks, Smith, Stone i Tutte, i que també es conegueren com “els quatre del Trinity”. Posteriorment a Sprague, i com a conseqüència d’un estudi més profund, aquests també publicaren solucions al problema (cf. [49]).

Sembla que Sprague no publicà res més sobre el problema de quadrar quadrats. Però l’any 1946, poc després de la Segona Guerra Mundial, envià a la revista *Mathematische Zeitschrift* l’article del qual presentem una traducció, i que fou publicat l’any 1948. Com diu el mateix autor en l’arti-

cle, el problema que hi tracta sorgeix de manera natural en considerar l'anàleg aritmètic del problema geomètric i, tot i que la demostració és elemental, el resultat sembla nou. Sprague hi demostra el teorema següent.

Teorema. *Tot nombre natural més gran que 128 es pot expressar com a suma de quadrats tots diferents.*

El mateix any, ell mateix tractaria el cas de potències n -èsimes, en lloc de quadrats (cf. [374]).

Al cap de poc temps de l'aparició de l'article de Sprague, Richert presentà a la mateixa revista l'article del qual també oferim una traducció. En aquest article, per causa de la seva dedicació a la teoria analítica de nombres, i probablement esperonat per la senzillesa del mètode de demostració de Sprague, Richert canvia la successió de quadrats, o la de potències n -èsimes, per la successió dels nombres primers, i demostra el resultat següent.

Teorema. *Tot nombre natural més gran que 6 es pot expressar com a suma de primers tots diferents.*

Richert demostra el seu resultat emprant el mètode de Sprague i amb la consideració addicional del teorema de Txebychev.

Per a acabar, podem afegir que aquests resultats de Sprague i de Richert, juntament amb altres d'enunciat i demostració igualment senzills d'altres autors, foren generalitzats per Brown en [51].

Math. Z. **51** (1948), 289–290

SOBRE DESCOMPOSICIONS EN NOMBRES QUADRATS DIFERENTS

de R. SPRAGUE a Berlín–Charlottenburg ¹⁾

Una dissertació Schmidiana, la del Sr. STÖHR, tingué com a tema descomposicions de rectangles en quadrats incongrus dos a dos.

En certa analogia amb la pregunta geomètrica, es planteja la de teoria de nombres sobre quins nombres naturals són descomponibles en suma de quadrats dos a dos diferents.

No obstant la simplicitat de la idea de la demostració, el resultat mostrat aquí sembla que és nou.

Per a una sèrie de n_0 nombres consecutius, considerem obtingudes a partir de quadrats $\leq q_0^2$ representacions del tipus desitjat, de manera que valgui

$$\sqrt{n_0} - q_0 \geq 1.$$

Aleshores existeix com a mínim un nombre q_1^2 amb la propietat que

$$q_0^2 < q_1^2 \leq n_0,$$

el qual, afegit als q_1^2 nombres més grans, allarga immediatament la sèrie fins a

$$n_1 = n_0 + q_1^2$$

termes.

¹⁾ En el setantè aniversari d'E. SCHMIDT

Aquest procediment pot ésser iterat il·limitadament.

Ja que, a partir de

$$q_{k-1}^2 < q_k^2 \leq n_{k-1}$$

se segueix que

$$\sqrt{n_k} - q_k = \sqrt{n_{k-1} + q_k^2} - q_k \geq q_k(\sqrt{2} - 1);$$

per tant, com que evidentment ja ha d'ésser $q_0 > 2$, s'obté que

$$\sqrt{n_k} - q_k \geq 1$$

i el nombre dels valors permesos per a q_{k+1} creix amb k il·limitadament.

La taula següent pertoca a una sèrie que s'inicia en 129. Les seves llacunes fins a 192 són fàcils de completar per addició d'un o més dels nombres 1^2 , 2^2 , 3^2 a descomposicions escaients sense els sumands en qüestió. Per als nombres del 193 al 256, s'obtenen aleshores descomposicions a partir de les de 192 fins a 129 per pas als conjunts complementaris corresponents dels primers deu nombres quadrats. D'aquesta manera, amb $n_0 = 128$ i $q_0 = 10$ ens assegurem que

$$\sqrt{n_0} - q_0 \geq 1.$$

$$129 = 10^2 + 5^2 + 2^2$$

$$130 = 9^2 + 7^2$$

$$132 = 9^2 + 5^2 + 4^2 + 3^2 + 1^2$$

$$133 = 9^2 + 6^2 + 4^2$$

$$138 = 8^2 + 7^2 + 5^2$$

$$141 = 10^2 + 5^2 + 4^2$$

$$149 = 10^2 + 7^2$$

$$152 = 10^2 + 6^2 + 4^2$$

$$155 = 9^2 + 7^2 + 5^2$$

$$166 = 9^2 + 7^2 + 6^2$$

$$171 = 9^2 + 7^2 + 5^2 + 4^2$$

$$173 = 10^2 + 8^2 + 3^2$$

$$174 = 10^2 + 7^2 + 5^2$$

$$182 = 9^2 + 7^2 + 6^2 + 4^2$$

$$189 = 10^2 + 8^2 + 5^2.$$

Resultat: Cada nombre més gran que 128 és representable com a suma de termes dos a dos diferents d'una successió parcial de nombres quadrats; d'aquestes successions parcials n'hi ha infinites.

(Lliurat el 24 d'abril de 1946)

Referències de l'article

En aquest article, l'autor només fa una cita, i encara de manera implícita; sembla que es refereix a la memòria següent:

Stöhr, A.: Über Zerlegungen von Rechtecken in inkongruente Quadrate. *Schriften d. Math. Sem. u. d. Inst. f. angew. Math. d. Univ. Berlin* **4**, Part 5 (1939), p. 118–140.

Math. Z. **52** (1949), 342–343

SOBRE DESCOMPOSICIONS EN NOMBRES PRIMERS DIFERENTS

de HANS-EGON RICHERT a Hamburg

El senyor R. SPRAGUE ²⁾ demostrà per mitjà d'un mètode molt senzill la possibilitat de la descomposició de tots els nombres naturals > 128 en nombres quadrats diferents.

Si a la idea principal de la seva demostració s'afegeix el teorema de TXEBIXEV segons el qual entre els extrems $n > 3$ i $2n - 2$ es troba com a mínim un nombre primer, s'obté aleshores el teorema de descomposició següent:

Cada nombre natural $n > 6$ és representable com a suma de nombres primers diferents.

Demostració. Disposem una sèrie de s_0 nombres consecutius representats com a suma de primers diferents d'entre els k primers nombres primers $p_1, p_2, \dots, p_k$, de manera que sigui

$$s_0 \geq p_{k+1}.$$

Per addició de p_{k+1} als darrers p_{k+1} nombres de la s_0 -sèrie, aquesta és allargada en una s_1 -sèrie, on

$$s_1 = s_0 + p_{k+1},$$

²⁾R. SPRAGUE, Über Zerlegungen in ungleiche Quadratzahlen, *Math. Z.* **51**, 289–290 (1948). Cf. a més la nota del mateix autor, Über Zerlegungen in n -te Potenzen mit lauter verschiedenen Grundzahlen, *idem*, 466–468 (1948).

en la qual, de nou, tots els s_1 nombres consecutius són representats com a suma de nombres primers diferents.

D'aquesta manera es pot procedir il·limitadament, ja que a partir de

$$s_{r-1} \geq p_{k+r} \quad \text{i} \quad s_r = s_{r-1} + p_{k+r},$$

se segueix sempre novament que

$$s_r \geq 2p_{k+r}$$

i atès que, pel teorema de TXEBIXEV, per a $p_\ell > 3$ és

$$2p_\ell - 2 > p_{\ell+1} > p_\ell,$$

també és

$$s_r \geq p_{k+r+1}.$$

Atès que, com a inici de la inducció, és palès que en la taula següent és representada una s_0 -sèrie del tipus desitjat formada a partir dels nombres primers

$$p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7, p_5 = 11,$$

on

$$s_0 \geq p_6 = 13 (> 3),$$

amb això el teorema és demostrat completament.

$7 = 7$	$12 = 7 + 5$	$16 = 11 + 5$
$8 = 5 + 3$	$13 = 11 + 2$	$17 = 7 + 5 + 3 + 2$
$9 = 7 + 2$	$14 = 11 + 3$	$18 = 11 + 7$
$10 = 7 + 3$	$15 = 7 + 5 + 3$	$19 = 11 + 5 + 3.$
$11 = 11$		

(Lliurat el 18 d'octubre de 1948)

Referències de l'article

Recollim totes juntes les referències citades en aquest article.

Sprague, R. P.: Über Zerlegungen in ungleiche Quadratzahlen. *Math. Z.* **51** (1948), p. 289–290.

Sprague, R. P.: Über Zerlegungen in n -te Potenzen mit lauter verschiedenen Grundzahlen. *Math. Z.* **51** (1948), p. 466–468.

Part III

Referències

Cronologia

A continuació, fem una llista de les persones que se citen en algun lloc o altre del text i de les quals coneixem el lloc i la data de naixement, ordenades cronològicament. Una relació alfabètica d'aquestes s'inclou a l'índex antroponímic.

Aristòtil

Ἀριστοτέλης

(Estagira, *Στάγिरα*, península Calcídica, *Χαλκιδική*, Grècia, 384 a. de la n. e.; Eubea, *Εὔβοια*, Grècia, 322 a. de la n. e.)

Arquimedes de Siracusa

Αρχιμήδης

(Siracusa, Sicília, 287 a. de la n. e.; Siracusa, Sicília, 212 a. de la n. e.)

Eratòstenes de Cirene

Ερατοσθένης

(Cirene, Líbia, 276 a. de la n. e.; Egipte, 194 a. de la n. e.)

Diofant d'Alexandria

Διόφαντος ὁ Ἀλεξανδρεύς

(Alexandria, Egipte, Imperi Romà, entre 200 i 214; Alexandria, Egipte, Imperi Romà, entre 284 i 298)

Ramon Llull

(Palma, Mallorca, Corona d'Aragó, 1232; Palma, Mallorca, Regne de Mallorca, 29 de juny de 1315)

Alexandre V

Pietro Philargi de Candia

(Creta, Venècia, 1340; Bolonya, Estats Papals, 3 de maig de 1410)

Frederic I Elector de Saxònia

o bé, Friedrich IV der Streitbare

o sigui, Frederic IV el Belligerant

(Dresden, Saxònia, Sacre Imperi, 11 d'abril de 1370; Altenburg, Saxònia, Sacre Imperi, 4 de gener de 1428)

Guillem II el Ric

Wilhelm II der Reiche

(Dresden, Saxònia, Sacre Imperi, 23 d'abril de 1371; Altenburg, Saxònia, Sacre Imperi, 30 de març de 1425)

Pere Posa

(Sant Joan d'Avinyonet, bisbat de Vic, s. XV; Barcelona, 1506)

Francesc Santcliment

(Barcelona, s. XV; Barcelona, s. XVI)

Albert de Prússia

Albrecht von Brandenburg-Ansbach,

també Albrecht von Preussen, o Albrecht von Hohenzollern,

(Ansbach, Baviera, Sacre Imperi, 17 de maig de 1490; Burg Tapiau, Königsberg, Ducat de Prússia, 20 de març de 1568)

Girolamo Cardano

Hieronimus Cardanus

(Pavia, Ducat de Milà, Sacre Imperi, 24 de setembre de 1501; Roma, Estats Papals, 21 de setembre de 1576)

Francisco **Suárez**

(Granada, Corona de Castella, 5 de gener de 1548; Lisboa, Portugal, 25 de setembre de 1617)

Johannes **Kepler**

(Weil der Stadt, Württemberg, Sacre Imperi, 27 de desembre de 1571; Regensburg, Baviera, Sacre Imperi, 15 de novembre de 1630)

Marin **Mersenne**

(Oizé, França, 8 de setembre de 1588; París, França, 1 de setembre de 1648)

René **Descartes**

(Descartes, França, 31 de març de 1596; Estocolm, Suècia, 11 de febrer de 1650)

Friedrich **Leibniz**

(Leipzig, Saxònia, Sacre Imperi, 1597; Leipzig, Saxònia, Sacre Imperi, 1652)

Pierre de **Fermat**

(Beaumont de Lomagne, França, 17 d'agost de 1601; Castres, França, 12 de gener de 1665)

John **Pell**

(Southwick, Sussex, Anglaterra, 1 de març de 1611; Londres, Anglaterra, 12 de desembre de 1685)

Antoine **Arnauld**

(París, França, 6 de febrer de 1612; Brusselles, Països Baixos, 8 d'agost de 1694)

Frans van **Schooten**

(Leiden, Països Baixos, 15 de maig de 1615; Leiden, Països Baixos, 29 de maig de 1660)

William Brouncker

(Castlelyons, Cork, Irlanda, 1620; Westminster, Anglaterra, 5 d'abril de 1684)

Catherina Schmuck

(Leipzig, Saxònia, Sacre Imperi, 1621; Leipzig, Saxònia, Sacre Imperi, 1664)

Jakob Thomasius

(Leipzig, Saxònia, Sacre Imperi, 27 d'agost de 1622; Leipzig, Saxònia, Sacre Imperi, 9 de setembre de 1684)

Blaise Pascal

(Clermont-Ferrand, França, 19 de juny de 1623; París, França, 19 d'agost de 1662)

Robert Boyle

(Lismore, Irlanda, 25 de gener de 1627; Londres, Anglaterra, 31 de desembre de 1691)

Christiaan Huygens

(L'Haia, Països Baixos, 14 d'abril de 1629; L'Haia, Països Baixos, 8 de juliol de 1695)

Nicolas Malebranche

(París, França, 6 d'agost de 1638; París, França, 13 d'octubre de 1715)

Lluís XIV de França

(Saint Germain en Laye, França, 5 de setembre de 1638; Versailles, França, 10 de setembre de 1715)

Isaac Newton

(Woolfsthorne by Colsterworth, Anglaterra, 25 de desembre de 1642 (Ju), 4 de gener de 1643 (Gr); Kensington, Anglaterra, 20 de març de 1717 (Ju), 31 de març de 1717 (Gr))

Otto Mencke

(Oldenburg, Baixa Saxònia, Sacre Imperi, 22 de març de 1644; Leipzig, Saxònia, Sacre Imperi, 18 de gener de 1717)

Gottfried Wilhelm von Leibniz

(Leipzig, Saxònia, Sacre Imperi, 1 de juliol de 1646; Hannover, Baixa Saxònia, Sacre Imperi, 14 de novembre de 1716)

Ehrenfried Walther von Tschirnhaus

(Kieslingswalde, ara, Sławnikowice, Silèsia, Sacre Imperi, ara, Polònia, 10 d'abril de 1651; Dresden, Saxònia, Sacre Imperi, 11 d'octubre de 1708)

Jakob Bernoulli

també conegut per Jacques i per Jakob I

(Basilea, Suïssa, 27 de desembre de 1654; Basilea, Suïssa, 16 d'agost de 1705)

Christian Thomasius

(Leipzig, Saxònia, Sacre Imperi, 1 de gener de 1655; Halle, Saxònia Anhalt, Sacre Imperi, 23 de setembre de 1728)

Frederic I de Prússia

o també **Frederic III** de Brandenburg

(Königsberg, Prússia, 11 de juliol de 1657; Berlín, Prússia, 25 de febrer de 1713)

Johann Christoph Wichmannshausen

(Ilseburg, Saxònia Anhalt, Sacre Imperi, 3 d'octubre de 1663; Wittenberg, Saxònia Anhalt, Sacre Imperi, 17 de gener de 1727)

Johann Bernoulli

(Basilea, Suïssa, 27 de juliol de 1667; Basilea, Suïssa, 1 de gener de 1748)

Pere I el Gran

Pere Aleksèievitx Romànov

(Moscou, Rússia, 30 de maig de 1672 (Ju), 9 de juny de 1672)

(Gr); Sant Petersburg, Rússia, 28 de gener de 1725 (Ju), 8 de febrer de 1725 (Gr))

Giulio Carlo **Fagnano** dei Toschi

(Sinigaglia, Estats Papals, 6 de desembre de 1682; Sinigaglia, Estats Papals, 26 de setembre de 1766)

Georg August Elector de Hannover

George II, Rei de Gran Bretanya i Irlanda

(Hannover, Baixa Saxònia, Sacre Imperi, 30 d'octubre de 1683 (Ju), 10 de novembre de 1683 (Gr); Londres, Anglaterra, 25 d'octubre de 1760)

Felip V

Felip V de Castella, Felip IV d'Aragó, o Felip d'Anjou

(Versalles, França, 19 de desembre de 1683; Madrid, 9 de juliol de 1746)

Brook **Taylor**

(Edmonton Middlesex, Anglaterra, 18 d'agost de 1685; Somerset House, Londres, Anglaterra, 29 de desembre de 1731)

Carles VI d'Àustria

Karl Franz Joseph Wenceslau Balthasar Johann Anton Ignatius (Viena, Àustria, Sacre Imperi, 1 d'octubre de 1685; Viena, Àustria, Sacre Imperi, 20 d'octubre de 1740)

Gerlach **Adolph** Freiherr von Münchhausen

(Berlín, Brandenburg, Sacre Imperi, 14 d'octubre de 1688; Hannover, Baixa Saxònia, Sacre Imperi, 26 de novembre de 1770)

Christian **Goldbach**

(Königsberg, Prússia, 18 de març de 1690; Moscou, Rússia, 20 de novembre de 1764 (Ju), 1 de desembre de 1764 (Gr))

Elisabet Cristina de Brunsvic-Wolfenbüttel

Elisabeth Christinne von Braunschweig-Wolfenbüttel

(Brunsvic, Baixa Saxònia, Sacre Imperi, 28 d'agost de 1691; Viena, Àustria, Sacre Imperi, 21 de desembre de 1750)

Christian August **Hausen**

(Dresden, Saxònia, Sacre Imperi, 19 de juny de 1693; Leipzig, Saxònia, Sacre Imperi, 1743)

François Marie Arouet, **Voltaire**

(París, França, 21 de novembre de 1694; París, França, 30 de maig de 1778)

Colin **Maclaurin**

(Kilmodan, Tighnabruaich, Cowal, Argyllshire, Escòcia, febrer de 1698; Edimburg, Escòcia, 14 de juny de 1746)

Jan Andrej **Segner**

o bé János András Segner,

o també Johann Andreas Segner

(Pozsony, Hongria, ara Bratislava, Eslovàquia, 9 d'octubre de 1704; Halle, Saxònia Anhalt, Sacre Imperi, 5 d'octubre de 1777)

Leonhard **Euler**

(Basilea, Suïssa, 15 d'abril de 1707; Sant Petersburg, Rússia, 7 de setembre de 1783 (Ju), 18 de setembre de 1783 (Gr))

Carl von **Linné**

Carl Nilsson von Linnæus

(Råshult, Suècia, 23 de maig de 1707; Uppsala, Suècia, 10 de gener de 1778)

Frederic II el Gran

Friedrich von Hohenzollern die Grosse

(Berlín, Prússia, 24 de gener de 1712; Potsdam, Prússia, 17 d'agost de 1786)

Pere II

Piotr II Alekseievitx Romanov, Tsar de Rússia

(Sant Petersburg, Rússia, 23 d'octubre de 1715; Moscou, Rússia, 30 de gener de 1730)

Maria Teresa d'Àustria

Maria Theresa Walburga Amalia Christina

(Viena, Àustria, Sacre Imperi, 13 de maig de 1717; Viena, Àustria, Sacre Imperi, 29 de novembre de 1780)

Abraham Gotthelf **Kästner**

(Leipzig, Saxònia, Sacre Imperi, 27 de setembre de 1719; Göttingen, Baixa Saxònia, Sacre Imperi, 20 de juny de 1800)

Alexander Georg von **Humboldt**

(Pomerània, Prússia, aprox. 1720; Prússia, 6 de gener de 1779)

Giuseppe **Torelli**

(Verona, Venècia, 3 de novembre de 1721; Verona, Venècia, 18 d'agost de 1781)

Tobias **Mayer**

(Marbach am Neckar, Baden Württemberg, Sacre Imperi, 17 de febrer de 1723; Göttingen, Baixa Saxònia, Sacre Imperi, 20 de febrer de 1762)

Immanuel **Kant**

(Königsberg, Prússia, 22 d'abril de 1724; Königsberg, Prússia, 12 de febrer de 1804)

Gotthold Ephraim **Lessing**

(Kamenz, Saxònia, Sacre Imperi, 22 de gener de 1729; Brunsvic, Baixa Saxònia, Sacre Imperi, 15 de febrer de 1781)

Moses **Mendelssohn**

Moisès Mendelssohn

(Dessau, Saxònia Anhalt, Sacre Imperi, 6 de setembre de 1729; Berlín, Prússia, 4 de gener de 1786)

Carles Guillem Ferran de Brunsvic–Wolfenbüttel

Karl Wilhelm Ferdinand von Braunschweig–Wolfenbüttel

(Wolfenbüttel, Baixa Saxònia, Sacre Imperi, 9 d'octubre de 1735; Ottensen, Hamburg, Sacre Imperi, 16 d'octubre de 1806)

Joseph Louis **Lagrange**

Giuseppe Lodovico Lagrangia,

o bé Giuseppe Luigi Lagrangia

(Torí, Regne de Sardenya, 25 de gener de 1736; París, França, 10 d'abril de 1813)

Elisabeth von Holwede

nascuda Marie Elisabeth Colomb,

després, Marie Elisabeth von Humboldt

(Berlín, Prússia, 8 de desembre de 1741; Tegel, Prússia, 19 de novembre de 1796)

Frederic Guillem II de Prússia

Friedrich Wilhelm II von Preussen

(Berlín, Prússia, 25 de setembre de 1744; Potsdam, Prússia, 16 de novembre de 1797)

Elisabet Cristina

Elisabeth Christine Ulrike von Braunschweig–Wolfenbüttel

(Wolfenbüttel, Baixa Saxònia, Sacre Imperi, 18 de novembre de 1746; Stettin, Pomerània, Prússia, 18 de febrer de 1840)

Pierre Simon de **Laplace**

(Beaumont en Auge, França, 23 de març de 1749; París, França, 5 de març de 1827)

Johann Wolfgang von **Goethe**

(Frankfurt am Main, Hessen, Sacre Imperi, 28 d'agost de 1749; Weimar, Turíngia, Confederació Germànica, 22 de març de 1832)

Lorenzo **Mascheroni**

(Bèrgam, Venècia, 13 de maig de 1750; París, França, 14 de juliol de 1800)

Johann Tobias Mayer

(Göttingen, Baixa Saxònia, Sacre Imperi, 5 de maig de 1752; Göttingen, Baixa Saxònia, Prússia, 30 de novembre de 1830)

Adrien Marie Legendre

(París, França, 18 de setembre de 1752; París, França, 10 de gener de 1833)

Maria Antonieta

Maria Antonia Josepha Johanna

(Viena, Àustria, Sacre Imperi, 2 de novembre de 1755; París, França, 16 d'octubre de 1793)

Wolfgang Amadeus Mozart

Johannes Chrysostomus Wolfgangus Theophilus Mozart

(Salzbug, Àustria, Sacre Imperi, 27 de gener de 1756; Viena, Àustria, Sacre Imperi, 5 de desembre de 1791)

Gottlob Johann Christian Kunth

(Baruth, Prússia, 12 de juny de 1757; Berlín, Prússia, 22 de novembre de 1829)

Heinrich Wilhelm Matthias Olbers

(Arbergen, Bremen, Baixa Saxònia, Sacre Imperi, 11 d'octubre de 1758; Bremen, Baixa Saxònia, Prússia, 2 de març de 1840)

Johann Christoph Friedrich von Schiller

(Marbach am Neckar, Baden Württemberg, Sacre Imperi, 10 de novembre de 1759; Weimar, Turíngia, Sacre Imperi, 9 de maig de 1805)

Siméon Denis Poisson

(Pithiviers, França, 21 de juny de 1761; Sceaux, França, 25 d'abril de 1840)

Johann Friedrich Pfaff

(Stuttgart, Baden Württemberg, Sacre Imperi, 22 de desembre de 1765; Halle, Saxònia Anhalt, Prússia, 21 d'abril de 1825)

Wilhelm von **Humboldt**

Friedrich Wilhelm Christian Carl Ferdinand von Humboldt
(Potsdam, Prússia, 22 de juny de 1767; Tegel, Prússia, 8 d'abril de 1835)

Jean Baptiste Joseph **Fourier**

(Auxerre, França, 21 de març de 1768; París, França, 16 de maig de 1830)

Napoleó

Napoleone Bonaparte

(Ajaccio, Còrsega, França, 15 d'agost de 1769; Longwood, Santa Helena, Imperi Britànic, 1821)

Alexander von **Humboldt**

Friedrich Wilhelm Heinrich Alexander von Humboldt
(Berlín, Prússia, 14 de setembre de 1769; Berlín, Prússia, 6 de maig de 1859)

Joseph **Mendelssohn**

(Berlín, Prússia, 11 d'agost de 1770; Berlín, Prússia, 24 de novembre de 1848)

Georg Wilhelm Friedrich **Hegel**

(Stuttgart, Baden Württemberg, Sacre Imperi, 27 d'agost de 1770; Berlín, Prússia, 14 de novembre de 1831)

Ludwig van **Beethoven**

(Bonn, Rin del Nord Westfàlia, Sacre Imperi, 16 de desembre de 1770; Viena, Àustria, Imperi Austríac, 26 de març de 1827)

Jean Baptiste **Biot**

(París, França, 21 d'abril de 1774; París, França, 3 de febrer de 1862)

Farkas Wolfgang **Bolyai**

(Bolya, Transilvània, Monarquia Austríaca, ara Sibiu, Romania, 9 de febrer de 1775; Marosvásárhely, Transilvània, Monar-

quia Austríaca, ara Tirgu Mures, Romania, 20 de novembre de 1856)

Abraham Ernst **Mendelssohn** Bartholdy

nascut Abraham Mendelssohn

(Berlín, Prússia, 10 de desembre de 1776; Berlín, Prússia, 19 de novembre de 1835)

Johann Carl Friedrich **Gauss**

(Brunsvic, Baixa Saxònia, Sacre Imperi, 30 d'abril de 1777; Göttingen, Baixa Saxònia, Prússia, 23 de febrer de 1855)

August Leopold **Crelle**

(Eichwerder, Wriezen, Prússia, 11 de març de 1780; Berlín, Prússia, 6 d'octubre de 1855)

Heinrich Christian **Schumacher**

(Bad Bramstedt, Imperi Danès, actualment a Schleswig Holstein, Alemanya, 3 de setembre de 1780; Altona, Imperi Danès, actualment a Hamburg, Baixa Saxònia, Alemanya, 28 de desembre de 1850)

Friedrich Wilhelm **Bessel**

(Minden, Rin del Nord Westfàlia, Prússia, 22 de juliol de 1784; Königsberg, Prússia, 17 de març de 1846)

Enno Heeren **Dirksen**

(Eilsum, Frísia, Prússia, 3 de gener de 1788; París, França, 16 de juliol de 1850)

Cristian Ludwig **Gerling**

(Hamburg, 10 de juliol de 1788; Marburg, Hessen, 15 de gener de 1864)

Augustin Louis **Cauchy**

(París, França, 21 d'agost de 1789; Sceaux, França, 23 de maig de 1857)

August Ferdinand **Möbius**

(Schulpforta, Saxònia Anhalt, Sacre Imperi, 17 de novembre de 1790; Leipzig, Saxònia, Confederació Germànica, 26 de setembre de 1868)

Johann Franz Friedrich **Encke**

(Hamburg, Sacre Imperi, 23 de setembre de 1791; Spandau, Berlín, Prússia, 26 d'agost de 1865)

Charles **Babbage**

(Londres, Anglaterra, 26 de desembre de 1791; Londres, Anglaterra, 18 d'octubre de 1871)

George **Green**

(Sneinton, Nottingham, Anglaterra, juliol de 1793; Sneinton, Nottingham, Anglaterra, 31 de maig de 1841)

Friedrich Wilhelm IV

Frederic Guillem IV de Prússia

(Berlín, Prússia, 15 d'octubre de 1795; Potsdam, Prússia, 2 de gener de 1861)

Jakob **Steiner**

(Utzenstorf, Suïssa, 18 de març de 1796; Berna, Suïssa, 1 d'abril de 1863)

Christoph **Gudermann**

(Vienenburg, Hildesheim, Baixa Saxònia, Sacre Imperi, 25 de març de 1798; Münster, Rin del Nord Westfàlia, Prússia, 25 de setembre de 1852)

George Karl Justus **Ulrich**

(Göttingen, Baixa Saxònia, Sacre Imperi, 29 d'abril de 1798; Göttingen, Baixa Saxònia, Imperi Alemany, 1879)

Franz Ernst **Neumann**

(Joachimsthal, Brandenburg, Prússia, 11 de setembre de 1798; Königsberg, Prússia, Imperi Alemany, 23 de maig de 1895)

Heinrich Ferdinand **Scherk**

(Posen, Prússia, ara Poznań, Polònia, 27 d'octubre de 1798; Bremen, Baixa Saxònia, Imperi Alemany, 4 d'octubre de 1885)

Julius **Plücker**

(Elberfeld, ara Wuppertal, Rin del Nord Westfàlia, Prússia, 16 de juny de 1801; Bonn, Rin del Nord Westfàlia, Prússia, 22 de maig de 1868)

Niels Henrik **Abel**

(Frindøe, Noruega, 5 d'agost de 1802; Froland, Noruega, 6 d'abril de 1829)

Moritz Wilhelm **Drobisch**

(Leipzig, Saxònia, Sacre Imperi, 16 d'agost de 1802; Leipzig, Saxònia, Alemanya, 30 de setembre de 1896)

János **Bolyai**

(Koložsvár, Transilvània, Monarquia Austríaca, ara Cluj, Romania, 15 de desembre de 1802; Marosvásárhely, Transilvània, Monarquia Austríaca, ara Tirgu Mures, Romania, 27 de gener de 1860)

Whilhelm Eduard **Weber**

(Wittenberg, Saxònia Anhalt, Sacre Imperi, 4 d'octubre de 1804; Göttingen, Baixa Saxònia, Imperi Alemany, 23 de juny de 1891)

Carl Gustav Jacob **Jacobi**

(Potsdam, Prússia, 10 de desembre de 1804; Berlín, Prússia, 18 de febrer de 1851)

Johann Peter Gustav Lejeune **Dirichlet**

(Düren, Rin del Nord Westfàlia, Prússia, 13 de febrer de 1805; Göttingen, Baixa Saxònia, Prússia, 5 de maig de 1859)

William Rowan **Hamilton**

(Dublín, Irlanda, 4 d'agost de 1805; Dublín, Irlanda, 2 de setembre de 1865)

Fanny Cäcilie **Mendelssohn** Bartholdy

nascuda Fanny Zippora Mendelssohn,
després Fanny Hensel

(Hamburg, Sacre Imperi, 14 de novembre de 1805; Berlín, Prússia, 14 de maig de 1847)

Moritz Abraham **Stern**

algunes vegades, Moriz Abraham Stern

(Frankfurt am Main, Hessen, Confederació del Rin, 29 de juny de 1807; Zuric, Suïssa, 30 de gener de 1894)

Charles Louis **Napoléon** Bonaparte

Napoléó III

(París, França, 20 d'abril de 1808; Chislehurst, Kent, Anglaterra, 9 de gener de 1873)

Johann Benedict **Listing**

(Frankfurt am Main, Hessen, Confederació del Rin, 25 de juliol de 1808; Göttingen, Baixa Saxònia, Imperi Alemany, 24 de desembre de 1882)

Friedrich Julius **Richelot**

(Königsberg, Prússia, 6 de novembre de 1808; Königsberg, Prússia, Imperi Alemany, 31 de març de 1875)

Jakob Ludwig Felix **Mendelssohn** Bartholdy

nascut Felix Mendelssohn

(Hamburg, Ocupació francesa, 3 de febrer de 1809; Leipzig, Saxònia, Confederació Germànica, 4 de novembre de 1847)

Benjamin **Peirce**

(Salem, Massachusetts, Estats Units, 4 d'abril de 1809; Cambridge, Massachusetts, Estats Units, 6 d'octubre de 1880)

Ernst Eduard **Kummer**

(Sorau, Brandenburg, Prússia, 29 de gener de 1810; Berlín, Prússia, Imperi Alemany, 14 de maig de 1893)

Rebecka Henriette **Mendelssohn**

nascuda Rebecka Mendelssohn,
després, Rebecka Henriette Mendelssohn Bartholdy,
i després, Rebecka Henriette Dirichlet
(Hamburg, Ocupació francesa, 11 d'abril de 1811; Göttingen, Baixa Saxònia, Confederació Germànica, 1 de desembre de 1858)

Ludwig Otto **Hesse**

(Königsberg, Prússia, 22 d'abril de 1811; Munic, Baviera, Imperi Alemany, 4 d'agost de 1874)

Évariste **Galois**

(Bourg la Reine, París, França, 25 d'octubre de 1811; París, França, 31 de maig de 1832)

Gustav Adolph **Göpel**

(Rostock, Mecklenburg, Prússia, 29 de setembre de 1812; Berlín, Imperi Alemany, 7 de juny de 1847)

Pierre Alphonse **Laurent**

(París, França, 18 de juliol de 1813; París, França, 2 de setembre de 1854)

James Joseph **Sylvester**

(Londres, Anglaterra, 3 de setembre de 1814; Londres, Anglaterra, 15 de març de 1897)

Otto Eduard Leopold von **Bismarck**

Comte de Bismarck-Schönhausen, Duc de Lauenburg i Príncep de Bismarck

(Schönhausen, Saxònia, Prússia, 1 d'abril de 1815; Friedrichsruh Lauenburg, Schleswig-Holstein, Imperi Alemany, 30 de juliol de 1898)

Karl Theodor Wilhelm **Weierstrass**

(Ostenfelde, Ennigerloh, Westfàlia, Prússia, 31 d'octubre de 1815; Berlín, Prússia, Imperi Alemany, 19 de febrer de 1897)

Ada **Lovelace**

Augusta Ada King, Comtessa de Lovelace,
nascuda Augusta Ada Byron

(Picadilly, Londres, Anglaterra, 10 de desembre de 1815; Marylebone, Londres, Anglaterra, 27 de novembre de 1852)

Heinrich Wilhelm Feodor **Deahna**

(Prússia, 1815; Prússia, 1844)

Johann Georg **Rosenhain**

(Königsberg, Prússia, 10 de juny de 1816; Berlín, Prússia, Imperi Alemany, 14 de maig de 1887)

Paul Julius **Reuter**

nascut Israel Bere **Josafat**

(Kassel, Hessen, Prússia, 21 de juny de 1816; Niça, França, 25 de febrer de 1899)

Karl Wilhelm **Borchardt**

(Berlín, Prússia, 22 de febrer de 1817; Rüdersdorf, Brandenburg, Prússia, Imperi Alemany, 27 de juny de 1880)

Julius **Springer**

(Berlín, Prússia, 10 de maig de 1817; Berlín, Prússia, Imperi Alemany, 17 d'abril de 1877)

Charles Auguste **Briot**

(Saint Hippolyte, Doubs, França, 19 de juliol de 1817; Bourg-d'Ault, França, 20 de setembre de 1882)

Heinrich Richard **Baltzer**

(Meissen, Saxònia, Confederació Germànica, 27 de gener de 1818; Giessen, Hessen, Imperi Alemany, 7 de novembre de 1887)

Ferdinand **Joachimsthal**

(Goldberg, ara Złotoryja, Silèsia, Prússia, 9 de març de 1818; Breslau, Silèsia, Prússia, ara Wroclaw, Polònia, 5 d'abril de 1861)

Otilie Ernestine Françoise **Mendelssohn**

després Otilie Ernestine Kummer

(Neisse, Silèsia, Prússia, 14 de juliol de 1819; Breslau, Silèsia, Prússia, ara Wroclaw, Polònia, 30 de juliol de 1848)

Jean Claude **Bouquet**

(Morteau, Doubs, França, 7 de setembre de 1819; París, França, 9 de setembre de 1885)

Narcís **Monturiol** i Estarriol

(Figueres, 28 de setembre de 1819; Sant Martí de Provençals, Barcelona, 6 de setembre de 1885)

Victor Alexandre **Puiseux**

(Argenteuil, França, 16 d'abril de 1820; Frontenay, França, 9 de setembre de 1883)

Heinrich Eduard **Heine**

(Berlín, Prússia, 16 de març de 1821; Halle, Saxònia Anhalt, Imperi Alemany, 21 d'octubre de 1881)

Pafnuty Lvovich **Txebixev**

també Chebyshev

(Okatovo, Rússia, 16 de maig de 1821; Sant Petersburg, Rússia, 8 de desembre de 1894)

Arthur **Cayley**

(Richmond, Surrey, Anglaterra, 16 d'agost de 1821; Cambridge, Anglaterra, 26 de gener de 1895)

Hermann Ludwig Ferdinand von **Helmholtz**

(Potsdam, Prússia, 31 d'agost de 1821; Berlín, Prússia, Imperi Alemany, 8 de setembre de 1894)

Philipp Ludwig von **Seidel**

(Zweibrücken, Prússia, 24 d'octubre de 1821; Munic, Baviera, Imperi Alemany, 13 d'agost de 1896)

Charles **Hermite**

(Dieuze, França, 24 de desembre de 1822; París, França, 14 de gener de 1901)

Ferdinand Gotthold Max **Eisenstein**

(Berlín, Prússia, 16 d'abril de 1823; Berlín, Prússia, 11 d'octubre de 1852)

Enrico **Betti**

(Pistoia, Toscana, Imperi Autríac, 21 d'octubre de 1823; Soiana, Pisa, Toscana, Itàlia, 11 d'agost de 1892)

Leopold **Kronecker**

(Liegnitz, Silèsia, Prússia, 7 de desembre de 1823; Berlín, Prússia, Imperi Alemany, 29 de desembre de 1891)

Georg Friedrich Bernhard **Riemann**

(Breselenz, Hannover, 17 de setembre de 1826; Selasca, Piemont, Itàlia, 20 de juliol de 1866)

Heinrich Eduard **Schröter**

(Königsberg, Prússia, 8 de gener de 1829; Breslau, Silèsia, Prússia, Imperi Alemany, ara Wroclaw, Polònia, 3 de gener de 1892)

Moritz Benedikt **Cantor**

(Mannheim, Baden Württemberg, Confederació Germànica, 23 d'agost de 1829; Heidelberg, Baden Württemberg, Alemanya, 10 d'abril de 1920)

Elwin Bruno **Christoffel**

(Montjoie, ara Monschau, Aachen, Rin del Nord Westfàlia, Prússia, 10 de novembre de 1829; Estrasburg, França, 15 de març de 1900)

Julius Wilhelm Richard **Dedekind**

(Brunsvic, Baixa Saxònia, Prússia, 6 d'octubre de 1831; Brunsvic, Baixa Saxònia, Imperi Alemany, 12 de febrer de 1916)

Charles Lutwidge **Dodgson**

també conegut com a Lewis Carroll,

(Daresbury, Anglaterra, 27 de gener de 1832; Guilford, Anglaterra, 14 de gener de 1898)

Carl Gottfried **Neumann**

(Königsberg, Prússia, 7 de maig de 1832; Leipzig, Saxònia, Alemanya, 27 de març de 1925)

Rudolf Otto Sigismund **Lipschitz**

(Königsberg, Prússia, 14 de maig de 1832; Bonn, Rin del Nord Westfàlia, Prússia, Imperi Alemany, 7 d'octubre de 1903)

Eugène **Rouché**

(Sommières, Languedoc, França, 18 d'agost de 1832; Lunel, Languedoc, França, 19 d'agost de 1910)

Peter Ludwig Mejdell **Sylov**

(Christiania, ara Oslo, Noruega, 12 de desembre de 1832; Christiania, ara Oslo, Noruega, 7 de setembre de 1918)

Rudolf Friedrich Alfred **Clebsch**

(Königsberg, Prússia, 19 de gener de 1833; Göttingen, Baixa Saxònia, Imperi Alemany, 7 de novembre de 1872)

Lazarus Immanuel **Fuchs**

(Moschin, Posen, Prússia, ara Poznań, Polònia, 5 de maig de 1833; Berlín, Prússia, Imperi Alemany, 26 d'abril de 1902)

Ernst Christian Julius **Schering**

(Forsthaus Sandbergen, Bleckede, Baixa Saxònia, Confederació Germànica, 13 de juliol de 1833; Göttingen, Baixa Saxònia, Imperi Alemany, 2 de novembre de 1897)

Edmond Nicolas **Laguerre**

(Bar le Duc, França, 9 d'abril de 1834; Bar le Duc, França, 14 d'agost de 1886)

Eugenio **Beltrami**

(Cremona, Llombardia, Imperi Austríac, ara Itàlia, 16 de novembre de 1835; Roma, Itàlia, 18 de febrer de 1900)

Paul Albert **Gordan**

(Breslau, Silèsia, Prússia, ara Wroclaw, Polònia, 27 d'abril de 1837; Erlangen, Baviera, Imperi Alemany, 21 de desembre de 1912)

Marie Ennemond Camille **Jordan**

(La Croix Rousse, Lió, França, 5 de gener de 1838; París, França, 22 de gener de 1922)

John Davison **Rockefeller**

(Richford, Nova York, Estats Units, 8 de juliol de 1839; The Casements, Ormond Beach, Florida, Estats Units, 23 de maig de 1937)

Charles Sanders **Peirce**

(Cambridge, Massachusetts, Estats Units, 10 de setembre de 1839; Milford, Pensilvània, Estats Units, 19 d'abril de 1914)

Gustav **Roch**

(Leipzig, Saxònia, Confederació Germànica, 9 de desembre de 1839; Venècia, Itàlia, 21 de novembre de 1866)

Franz Carl Joseph **Mertens**

(Schroda, Posen, Prússia, ara Środa Wielkopolska, Polònia, 20 de març de 1840; Viena, Àustria, 5 de març de 1927)

Karl Johannes **Thomae**

(Laucha an der Unstrut, Saxònia Anhalt, Prússia, 11 de desembre de 1840; Jena, Turíngia, Alemanya, 1 d'abril de 1921)

Friedrich Emil Fritz **Prym**

(Düren, Rin del Nord Westfàlia, Prússia, 28 de setembre de 1841; Bonn, Rin del Nord Westfàlia, Prússia, Imperi Alemany, 15 de desembre de 1915)

Heinrich Martin **Weber**

(Heidelberg, Baden Württemberg, Confederació Germànica, 5 de maig de 1842; Estrasburg, Imperi Alemany, 17 de maig de 1913)

Alexander Wilhelm von **Brill**

(Darmstadt, Hessen, Prússia, 20 de setembre de 1842; Tübingen, Baden Württemberg, Alemanya, 8 de juny de 1935)

Marie Elisabeth **Schwarz**

nascuda Marie Elisabeth Kummer

(Breslau, Silèsia, Prússia, ara Wroklaw, Polònia, 13 de novembre de 1842; Berlín, Alemanya, 22 d'abril de 1921)

Marius Sophus **Lie**

(Nordfjordeide, Noruega, 17 de desembre de 1842; Christiania, ara Oslo, Noruega, 18 de febrer de 1899)

Karl Hermann Amandus **Schwarz**

(Hermsdorf, Silèsia, Prússia, 25 de gener de 1843; Berlín, Alemanya, 30 de novembre de 1921)

Max **Noether**

(Mannheim, Baden Württemberg, Confederació Germànica, 24 de setembre de 1844; Erlangen, Baviera, Alemanya, 13 de desembre de 1921)

Albert Victor **Bäcklund**

(Väsby, Malmöhus, Suècia, 11 de gener de 1845; Lund, Suècia, 23 de febrer de 1922)

Georg Ferdinand Ludwig Philipp **Cantor**

(Sant Petersburg, Rússia, 3 de març de 1845; Halle, Saxònia Anhalt, Imperi Alemany, 6 de gener de 1918)

Wilhelm Karl Joseph **Killing**

(Burbach, Siegen, Rin del Nord Westfàlia, Prússia, 10 de maig de 1847; Münster, Rin del Nord Westfàlia, Alemanya, 11 de febrer de 1923)

Diederik Johannes **Korteweg**

(s'Hertogenbosch, Holanda, 31 de març de 1848; Amsterdam, Holanda, 10 de maig de 1941)

Hermann Cäsar Hannibal **Schubert**

(Potsdam, Prússia, 22 de maig de 1848; Hamburg, Imperi Alemany, 20 de juliol de 1911)

Eugen Otto Erwin **Netto**

(Halle, Saxònia Anhalt, Prússia, 30 de juny de 1848; Giessen, Hessen, Alemanya, 13 de maig de 1919)

Friedrich Ludwig Gottlob **Frege**

(Wismar, Mecklenburg Schwerin, Prússia, 8 de novembre de 1848; Bad Kleinen, Mecklenburg, Alemanya, 26 de juliol de 1925)

Georges **Fontené**

(França, 1848; França, 1928)

Felix Christian **Klein**

(Düsseldorf, Rin del Nord Westfàlia, Prússia, 25 d'abril de 1849; Göttingen, Baixa Saxònia, Alemanya, 22 de juny de 1925)

Ferdinand Georg **Frobenius**

(Berlín-Charlottenburg, Prússia, 26 d'octubre de 1849; Berlín, Prússia, Imperi Alemany, 3 d'agost de 1917)

Sofia Vasilyevna **Kovalevskaya**

(Moscou, Rússia, 15 de gener de 1850; Estocolm, Suècia, 10 de febrer de 1891)

Ludwig **Stickelberger**

(Buch, Schaffhausen, Suïssa, 18 de maig de 1850; Basilea, Suïssa, 11 d'abril de 1936)

Jorgen Pedersen **Gram**

(Nustrup, Haderslev, Dinamarca, 27 de juny de 1850; Copenhagen, Dinamarca, 29 d'abril de 1916)

Carl Gustav Axel **Harnack**

(Tartu, Estònia, Rússia, 25 d'abril de 1851 (Ju), 7 de maig de 1851 (Gr); Dresden, Saxònia, Imperi Alemany, 3 d'abril de 1888)

Friedrich Hermann **Schottky**

(Breslau, Silèsia, Prússia, ara Wroclaw, Polònia, 24 de juliol de 1851; Berlín, Alemanya, 12 d'agost de 1935)

Carl Louis Ferdinand von **Lindemann**

(Hannover, 12 d'abril de 1852; Munic, Baviera, Alemanya, 6 de març de 1939)

William **Burnside**

(Paddington, Londres, Anglaterra, 2 de juliol de 1852; Cotleigh, West Wickham, Kent, Anglaterra, 21 d'agost de 1927)

Arthur Moritz **Schönflies**

(Landsberg an der Warthe, Prússia, 17 d'abril de 1853; Frankfurt am Main, Hessen, Alemanya, 27 de maig de 1928)

Hendrik Antoon **Lorentz**

(Arnhem, Holanda, 18 de juliol de 1853; Haarlem, Holanda, 4 de febrer de 1928)

Heinrich **Maschke**

(Breslau, Silèsia, Prússia, ara Wroclaw, Polònia, 24 d'octubre de 1853; Chicago, Illinois, Estats Units, 1 de març de 1908)

Jules Henry **Poincaré**

(Nancy, França, 29 d'abril de 1854; París, França, 17 de juliol de 1912)

Hans Karl Friedrich von **Mangoldt**

(Weimar, Turíngia, Prússia, 18 de maig de 1854; Danzig Langfuhr, Ciutat lliure de Danzig, ara Gdańsk, Polònia, 27 d'octubre de 1925)

Robert Hjalmar **Mellin**

(Liminka, Northern Ostrobothnia, Finlàndia, 19 de juny de 1854; Hèlsinki, Finlàndia, 5 d'abril de 1933)

Alfredo **Capelli**

(Milà, Regne de Llombardia i Venècia, Imperi Austríac, ara Itàlia, 5 d'agost de 1855; Nàpols, Itàlia, 28 de gener de 1910)

Johannes **Knoblauch**

(Halle, Saxònia Anhalt, Prússia, 27 d'agost de 1855; Berlín, Prússia, Imperi Alemany, 22 de juliol de 1915)

Luigi **Bianchi**

(Parma, Emília Romanya, Ducat de Parma, ara Itàlia, 18 de gener de 1856; Pisa, Toscana, Itàlia, 6 de juny de 1928)

Sigmund **Freud**

(Freiberg, Prússia, 6 de maig de 1856; Londres, Anglaterra, 23 de setembre de 1939)

Andrei Andreyevich **Markov**

(Ryazan, Rússia, 14 de juny de 1856; Sant Petersburg, Rússia, 20 de juliol de 1922)

Charles Émile **Picard**

(París, França, 24 de juliol de 1856; París, França, 11 de desembre de 1941)

Carl David Tolmé **Runge**

(Bremen, Baixa Saxònia, Prússia, 30 d'agost de 1856; Göttingen, Baixa Saxònia, Alemanya, 3 de gener de 1927)

Walther Franz Anton von **Dyck**

(Munic, Baviera, Confederació Germànica, 6 de desembre de 1856; Munic, Baviera, Alemanya, 5 de novembre de 1934)

Henry Ernest **Dudeney**

(Mayfield, Sussex, Anglaterra, 10 d'abril de 1857; Lewes, Sussex, Anglaterra, 24 d'abril de 1930)

Oskar **Bolza**

(Bergzabern, Renània Palatinat, Confederació Germànica, 12 de maig de 1857; Freiburg im Breisgau, Baden Württemberg, Alemanya, 5 de juliol de 1942)

Adolf **Krazer**

(Zusmarshausen, Augsburg, Baviera, Confederació Germànica, 15 d'abril de 1858; Karlsruhe, Baden Württemberg, Alemanya, 7 d'agost de 1926)

Max Karl Ernst Ludwig **Planck**

(Kiel, Schleswig Holstein, Prússia, 23 d'abril de 1858; Göttingen, Baixa Saxònia, Alemanya, 4 d'octubre de 1947)

Charlotte Angas **Scott**

(Lincoln, Anglaterra, 8 de juny de 1858; Cambridge, Anglaterra, 10 de novembre de 1931)

Giuseppe **Peano**

(Cuneo, Regne de Sardenya, ara Itàlia, 27 d'agost de 1858; Torí, Itàlia, 20 d'abril de 1932)

Guillem II Kàiser

nascut Friedrich Wilhelm Viktor Albrecht

(Berlín, Prússia, 27 de gener de 1859; Doom, Holanda, 4 de juny de 1941)

Adolf Hurwitz

(Hildesheim, Baixa Saxònia, Prússia, 26 de març de 1859; Zuric, Suïssa, 18 de novembre de 1919)

Karl Heun

(Wiesbaden, Hessen, Prússia, 3 d'abril de 1859; Karlsruhe, Baden Württemberg, Alemanya, 10 de gener de 1929)

Otto Ludwig Hölder

(Stuttgart, Baden Württemberg, Confederació Germànica, 22 de desembre de 1859; Leipzig, Saxònia, Alemanya, 29 d'agost de 1937)

Mathias Lerch

(Milínov, Sušice, Bohèmia, Imperi Austríac, ara Txèquia, 20 de febrer de 1860; Sušice, Bohèmia, Txecoslovàquia, ara Txèquia, 3 d'agost de 1922)

Theodor Molien

(Riga, Letònia, Rússia, 10 de setembre de 1861; Tomsk, Sibèria, Rússia, 25 de desembre de 1941)

Robert Karl Emanuel Fricke

(Helmstedt, Baixa Saxònia, Prússia, 24 de setembre de 1861; Bad Harzburg, Baixa Saxònia, Alemanya, 18 de juliol de 1930)

Friedrich Engel

(Lugau, Chemnitz, Saxònia, Confederació Germànica, 26 de desembre de 1861; Giessen, Hessen, Alemanya, 29 de setembre de 1941)

Kurt Hensel

(Königsberg, Prússia, 29 de desembre de 1861; Marburg, Hessen, Alemanya, 1 de juny de 1941)

David Hilbert

(Königsberg, Prússia, 23 de gener de 1862; Göttingen, Baixa Saxònia, Alemanya, 14 de febrer de 1943)

Adolf Kneser

(Grüssow, Mecklenburg, Prússia, 19 de març de 1862; Breslau, Silèsia, Alemanya, ara Wroclaw, Polònia, 24 de gener de 1930)

Philbert Maurice d'Ocagne

(París, França, 26 de març de 1862; Le Havre, França, 23 de setembre de 1938)

Walter de Gruyter

(Duisburg, Westfàlia del Nord, Prússia, 10 de maig de 1862; Berlín, Alemanya, 6 de setembre de 1923)

Otilie Bertha Augusta Schwarz,

posteriorment, Schwartz

(Berlín, Prússia, 9 d'agost de 1862; Marienfelde, Berlín, Alemanya, 30 d'abril de 1945)

Paul Painlevé

(París, França, 5 de desembre de 1863; París, França, 29 d'octubre de 1933)

William Fogg Osgood

(Boston, Massachusetts, Estats Units, 10 de març de 1864; Belmont, Massachusetts, Estats Units, 22 de juliol de 1943)

Hermann Minkowski

(Alexotas, Imperi Rus, ara Kaunas, Lituània, 22 de juny de 1864; Göttingen, Baixa Saxònia, Imperi Alemany, 12 de gener de 1909)

Ludwig **Schlesinger**

(Nagyszombat, Hongria, Imperi Austríac, ara Trnava, Eslovàquia, 1 de novembre de 1864; Giessen, Hessen, Alemanya, 16 de desembre de 1933)

Wilhelm **Wirtinger**

(Ybbs an der Donau, Àustria, 15 de juliol de 1865; Ybbs an der Donau, Àustria, 15 de gener de 1945)

Guido **Castelnuovo**

(Venècia, Regne de Llombardia i Venècia, Imperi Austríac, ara Itàlia, 14 d'agost de 1865; Roma, Itàlia, 27 d'abril de 1952)

Jacques Salomon **Hadamard**

(Versalles, França, 8 de desembre de 1865; París, França, 17 d'octubre de 1963)

Gustav de **Vries**

(Amsterdam, Holanda, 22 de gener de 1866; Haarlem, Holanda, 16 de desembre de 1934)

Charles Jean Gustave Nicolas de la **Vallée Poussin**

(Lovaina, Bèlgica, 14 d'agost de 1866; Lovaina, Bèlgica, 2 de març de 1962)

Ernst **Ritter**

(Waltershausen, Turíngia, Prússia, 9 de gener de 1867; Ithaca, Nova York, Estats Units, 23 de setembre de 1895)

John Irwin **Hutchinson**

(Bangor, Maine, Estats Units, 12 d'abril de 1867; Ithaca, Nova York, Estats Units, 1 de desembre de 1935)

Grace Chisholm **Young**

(Haslemere, Londres, Anglaterra, 15 de març de 1868; Croydon, Surrey, Anglaterra, 29 de març de 1944)

Felix Hausdorff

(Breslau, Silèsia, Prússia, ara Wroclaw, Polònia, 8 de novembre de 1868; Bonn, Rin del Nord Westfàlia, Alemanya, 26 de gener de 1942)

Emanuel Lasker

(Berlinchen, Prússia, ara Barlinek, Polònia, 24 de desembre de 1868; Nova York, Estats Units, 11 de gener de 1941)

Else Lasker-Schüler

(Elberfeld, ara Wuppertal, Rin del Nord Westfàlia, Prússia, 11 de febrer de 1869; Jerusalem, Palestina, ara Israel, 22 de gener de 1945)

Élie Joseph Cartan

(Dolomieu, Chambéry, França, 9 d'abril de 1869; París, França, 6 de maig de 1951)

Philipp Furtwängler

(Elze, Baixa Saxònia, Prússia, 21 d'abril de 1869; Viena, Àustria, 19 de maig de 1940)

Karl Theodor Vahlen

(Viena, Àustria, Imperi Austrohongarès, 30 de juny de 1869; Praga, Txecoslovàquia, 16 de novembre de 1945)

Louis Jean-Baptiste Alphonse Bachelier

(Le Havre, França, 11 de març de 1870; Saint Servan sur Mer, França, 26 d'abril de 1946)

Virginia Ragsdale

(Jamestown, Carolina del Nord, Estats Units, 13 de desembre de 1870; Greensboro, Carolina del Nord, Estats Units, 4 de juny de 1945)

Federigo Enriques

(Leghorn, ara Livorno, Toscana, Itàlia, 5 de gener de 1871; Roma, Itàlia, 14 de juny de 1946)

Ernst **Steinitz**

(Laurahütte, Silèsia, Prússia, ara Huta Laura, Polònia, 13 de juny de 1871; Kiel, Schleswig Holstein, Alemanya, 29 de setembre de 1928)

Paul **Epstein**

(Frankfurt, Hessen, Prússia, Imperi Alemany, 24 de juliol de 1871; Dornbusch, Hessen, Alemanya, 11 d'agost de 1939)

Ernst Friedrich Ferdinand **Zermelo**

(Berlín, Prússia, Imperi Alemany, 27 de juliol de 1871; Freiburg, Baden Württemberg, Alemanya, 21 de maig de 1953)

Rudolf Ernst **Rothe**

(Berlín, Prússia, Imperi Alemany, 15 d'octubre de 1873; Berlín, Alemanya, 26 d'octubre de 1942)

Maximilian Ernst Richard **Fuchs**

(Greifswald, Mecklenburg, Prússia, Imperi Alemany, 5 de desembre de 1873; Doberan, Rostock, Mecklenburg, Alemanya, 28 de desembre de 1944)

Leonard Eugene **Dickson**

(Independence, Iowa, Estats Units, 22 de gener de 1874; Harlingen, Texas, Estats Units, 17 de gener de 1954)

Arnold Franz Walter **Schönberg**

(Viena, Àustria, Imperi Austrohongarès, 13 de setembre de 1874; Los Angeles, Califòrnia, Estats Units, 13 de juliol de 1951)

Mihály **Bauer**

(Budapest, Hongria, Imperi Austrohongarès, 20 de setembre de 1874; Budapest, Hongria, 2 de març de 1945)

Winston Leonard Spencer **Churchill**

(Woodstock, Oxfordshire, Anglaterra, 30 de novembre de 1874; Londres, Anglaterra, 24 de gener de 1965)

Issai Schur

(Mogilyov, Rússia, 10 de gener de 1875; Tel Aviv, Palestina, ara Israel, 10 de gener de 1941)

Teiji Takagi

(Kazuya, Gifu, Japó, 21 d'abril de 1875; Tòquio, Japó, 29 de febrer de 1960)

Erhard Schmidt

(Dorpat, Estònia, Rússia, 13 de gener de 1876; Berlín, Alemanya, 6 de desembre de 1959)

Bernardino Gaetano Scorza

(Morano Calabro, Itàlia, 29 de setembre de 1876; Roma, Itàlia, 6 d'agost de 1939)

Carlo Rosati

(Livorno, Itàlia 1876; Pisa, Itàlia, 1929)

Godfrey Harold Hardy

(Cranleigh, Surrey, Anglaterra, 7 de febrer de 1877; Cambridge, Anglaterra, 1 de desembre de 1947)

Edmund Georg Hermann Landau

(Berlín, Prússia, Imperi Alemany, 14 de febrer de 1877; Berlín, Alemanya, 19 de febrer de 1938)

Georg Karl Wilhelm Hamel

(Düren, Rin del Nord Westfàlia, Prússia, Imperi Alemany, 12 de setembre de 1877; Landshut, Baviera, Alemanya, 4 d'octubre de 1954)

Felix Bernstein

(Halle, Saxònia Anhalt, Prússia, Imperi Alemany, 24 de febrer de 1878; Zuric, Suïssa, 3 de desembre de 1956)

Max Wilhelm **Dehn**

(Hamburg, Imperi Alemany, 13 de novembre de 1878; Black Mountain, Carolina del Nord, Estats Units, 27 de juny de 1952)

Otto **Hahn**

(Frankfurt, Hessen, Prússia, Imperi Alemany, 8 de març de 1879; Göttingen, Baixa Saxònia, Alemanya, 28 de juliol de 1968)

Albert **Einstein**

(Ulm, Württemberg, Imperi Alemany, 14 de març de 1879; Princeton, New Jersey, Estats Units, 18 d'abril de 1955)

Francesco **Severi**

(Arezzo, Itàlia, 13 d'abril de 1879; Roma, Itàlia, 8 de desembre de 1961)

Sergei Natanovich **Bernstein**

(Odessa, Ucraïna, Rússia, 5 de març de 1880; Moscou, Rússia, 26 d'octubre de 1968)

Oskar **Perron**

(Frankenthal, Pfalz, Renània Palatinat, Imperi Alemany, 7 de maig de 1880; Munic, Baviera, Alemanya, 22 de febrer de 1975)

Karl Rudolf **Fueter**

(Basilea, Suïssa, 30 de juny de 1880; Brunnen, Suïssa, 9 d'agost de 1950)

Gustav **Herglotz**

(Wallern, Bohèmia, Imperi Austrohongarès, 2 de febrer de 1881; Göttingen, Baixa Saxònia, Alemanya, 22 de març de 1953)

Luitzen Egbertus Jan **Brouwer**

(Overschie, Rotterdam, Holanda, 27 de febrer de 1881; Blaricum, Holanda, 2 de desembre de 1966)

Otto Toeplitz

(Breslau, Silèsia, Prússia, Imperi Alemany, ara Wroclaw, Polònia, 1 d'agost de 1881; Jerusalem, Palestina, ara Israel, 15 de febrer de 1940)

Franklin Delano Roosevelt

(Hyde Park, Nova York, Estats Units, 30 de gener de 1882; Warm Springs, Geòrgia, Estats Units, 12 d'abril de 1945)

Joseph Henry Maclagen Wedderburn

(Forfar, Angus, Escòcia, 2 de febrer de 1882; Princeton, New Jersey, Estats Units, 9 d'octubre de 1948)

Paul Koebe

(Luckenwalde, Brandenburg, Prússia, Imperi Alemany, 15 de febrer de 1882; Leipzig, Saxònia, Alemanya, 6 d'agost de 1945)

Emmy Amalie Noether

(Erlangen, Baviera, Imperi Alemany, 23 de març de 1882; Bryn Mawr, Pensilvània, Estats Units, 14 d'abril de 1935)

Max Born

(Breslau, Silèsia, Prússia, Imperi Alemany, ara Wroclaw, Polònia, 11 de desembre de 1882; Göttingen, Baixa Saxònia, Alemanya, 5 de gener de 1970)

Richard von Mises

(Lemberg, Imperi Austrohongarès, ara Lvov, Ucraïna, 19 d'abril de 1883; Boston, Massachusetts, Estats Units, 4 de juliol de 1953)

Petrus Josephus Wilhelmus Debye

nascut Petrus Josephus Wilhelmus Debije,
conegut per Peter Debye

(Maastricht, Holanda, 24 de març de 1884; Ithaca, Nova York, Estats Units, 2 de novembre de 1966)

Solomon **Lefschetz**

(Moscou, Rússia, 3 de setembre de 1884; Princeton, Nova Jersey, Estats Units, 5 d'octubre de 1972)

John Edensor **Littlewood**

(Rochester, Kent, Anglaterra, 9 de juny de 1885; Cambridge, Anglaterra, 6 de setembre de 1977)

Andreas **Speiser**

(Basilea, Suïssa, 10 de juny de 1885; Basilea, Suïssa, 12 d'octubre de 1970)

Theodor Franz Eduard **Kaluza**

(Opeln, ara Opole, Alta Silèsia, Prússia, Imperi Alemany, ara Polònia, 9 de novembre de 1885; Göttingen, Baixa Saxònia, Alemanya, 19 de gener de 1954)

Hermann Klaus Hugo **Weyl**

(Elmshorn, Hamburg, Imperi Alemany, 9 de novembre de 1885; Zuric, Suïssa, 9 de desembre de 1955)

Marcel **Riesz**

(Győr, Hongria, Imperi Austrohongarès, 16 de novembre de 1886; Lund, Suècia, 4 de setembre de 1969)

Ludwig Georg Elias Moses **Bieberbach**

(Goddelau, Darmstadt, Hessen, Imperi Alemany, 4 de desembre de 1886; Oberaudorf, Oberbayern, Baviera, Alemanya, 1 de setembre de 1982)

Thoralf Albert **Skolem**

(Sandsvaer, Buskerud, Noruega; 23 de maig de 1887; Oslo, Noruega, 23 de març de 1963)

Erwin Rudolf Josef Alexander **Schrödinger**

(Erdberg, Viena, Àustria, Imperi Austrohongarès, 12 d'agost de 1887; Viena, Àustria, 4 de gener de 1961)

Adriaan Daniël **Fokker**

(Buitenzorg, Índies Holandeses, ara Bogor, Indonèsia, 17 d'agost de 1887; Beekbergen, Holanda, 24 de setembre de 1972)

Erich **Hecke**

(Buk, Posen, Prússia, Imperi Alemany, ara Poznań, Polònia, 20 de setembre de 1887; Copenhaguen, Dinamarca, 13 de febrer de 1947)

George **Pólya**

(Budapest, Hongria, Imperi Austrohongarès, 13 de desembre de 1887; Palo Alto, Califòrnia, Estats Units, 7 de setembre de 1985)

Srinivasa Aiyangar **Ramanujan**

(Erode, Tamil Nadu, Índia, 22 de desembre de 1887; Kumbakonam, Tamil Nadu, Índia, 26 d'abril de 1920)

Richard **Courant**

(Lublinitz, Prússia, Imperi Alemany, ara Polònia, 8 de gener de 1888; New Rochelle, Nova York, Estats Units, 27 de gener de 1972)

Julio **Rey** Pastor

(Logronyo, Espanya, 16 d'agost de 1888; Buenos Aires, Argentina, 21 de febrer de 1962)

Isaak Paul **Bernays**

(Londres, Anglaterra, 17 d'octubre de 1888; Zuric, Suïssa, 18 de setembre de 1977)

Adolf **Hitler**

(Braunau am Inn, Àustria, Imperi Austrohongarès, 20 d'abril de 1889; Berlín, Alemanya, 30 d'abril de 1945)

Jakob **Nielsen**

(Mjels, Als, Schleswig, ara Dinamarca, 15 d'octubre de 1890; Elsinore, Dinamarca, 3 d'agost de 1959)

Fritz Anton Christian **Lang**

(Viena, Àustria, Imperi Austrohongarès, 5 de desembre de 1890; Los Angeles, Califòrnia, Estats Units, 2 d'agost de 1976)

Adolf Abraham Halevi **Fraenkel**

(Munic, Baviera, Imperi Alemany, 17 de febrer de 1891; Jerusalem, Israel, 15 d'octubre de 1965)

Walter **Gordon**

(Apolda, Turíngia, Imperi Alemany, 13 d'agost de 1893; Estocolm, Suècia, 24 de desembre de 1939)

Alexander Markowich **Ostrowski**

(Kiev, Ucraïna, Rússia, 25 de setembre de 1893; Montagnola, Lugano, Suïssa, 20 de novembre de 1986)

Satyendra Nath **Bose**

(Calcuta, Índia, 1 de gener de 1894 Calcuta, Índia, 4 de febrer de 1974)

Nikolai Grigorievich **Txebotarev**

o bé Chebotaryov

(Kamenets Podolsk, Ucraïna, Rússia, 15 de juny de 1894; Moscou, Rússia, 2 de juliol de 1947)

Roland Percival **Sprague**

(Unterliederbach, Hoechst, Hessen, Imperi Alemany, 11 de juliol de 1894; 1967)

Wilhelm **Ackermann**

(Schönebeck, Saxònia Anhalt, Imperi Alemany, 29 de març de 1896; Lüdenscheid, Rin del Nord Westfàlia, Alemanya, 24 de desembre de 1962)

Carl Ludwig **Siegel**

(Berlín, Prússia, Imperi Alemany, 31 de desembre de 1896; Göttingen, Baixa Saxònia, Alemanya, 4 d'abril de 1981)

Emil Artin

(Viena, Àustria, Imperi Austrohongarès, 3 de març de 1898; Hamburg, Alemanya, 20 de desembre de 1962)

Chiungtze Chiung Tsen

també Zeng Jiongzhi,

també Tseng Chiung-chih

(Hsienkien, Xinjian, Nanchang, Xina, 2 d'abril de 1898; Xichang, Xina, novembre de 1940)

Hellmuth Kneser

(Dorpat, Rússia, ara Tartu, Estònia, 16 d'abril de 1898; Tübingen, Baden Württemberg, Alemanya, 23 d'agost de 1973)

Alwin Oswald Walther

(Dresden, Saxònia, Imperi Alemany, 6 de maig de 1898; Darmstadt, Hessen, Alemanya, 4 de gener de 1967)

Helmut Hasse

(Kassel, Hessen, Imperi Alemany, 25 d'agost de 1898; Ahrensburg, Hamburg, Alemanya, 26 de desembre de 1979)

Vladimír Koříněk

(Praga, Imperi Austrohongarès, ara Txèquia, 18 d'abril de 1899; Praga, Txecoslovàquia, ara Txèquia, 2 de juny de 1981)

Oscar Zariski

(Kobrin, Bielorússia, Rússia, 24 d'abril de 1899; Brookline, Massachusetts, Estats Units, 4 de juliol de 1986)

Otto Neugebauer

(Innsbruck, Àustria, Imperi Austrohongarès, 26 de maig de 1899; Princeton, New Jersey, Estats Units, 19 de febrer de 1990)

Edward Charles Titchmarsh

(Newbury, Berkshire, Anglaterra, 1 de juny de 1899; Oxford, Oxfordshire, Anglaterra, 18 de gener de 1963)

Wolfgang **Krull**

(Baden–Baden, Baden Württemberg, Imperi Alemany, 26 d'agost de 1899; Bonn, Rin del Nord Westfàlia, Alemanya, 12 d'abril de 1971)

Öystein **Ore**

(Cristiania, ara Oslo, Noruega, 7 d'octubre de 1899; Oslo, Noruega, 13 d'agost de 1968)

Kurt Julian **Weill**

(Dessau, Saxònia Anhalt, Imperi Alemany, 2 de març de 1900; Nova York, Estats Units, 3 d'abril de 1950)

Richard Dagobert **Brauer**

(Berlín–Charlottenburg, Prússia, Imperi Alemany, 10 de febrer de 1901; Belmont, Massachusetts, Estats Units, 17 d'abril de 1977)

Friedrich Karl **Schmidt**

(Düsseldorf, Rin del Nord Westfàlia, Prússia, Imperi Alemany, 22 de setembre de 1901; Heidelberg, Baden Württemberg, Alemanya, 25 de gener de 1977)

Werner Karl **Heisenberg**

(Würzburg, Baviera, Imperi Alemany, 5 de desembre de 1901; Munic, Baviera, Alemanya, 1 de febrer de 1976)

Lady **Isabel** de FitzArnulph

personatge de ficció de Henry Dudeney

(Strand Magazine, Londres, Anglaterra, 7 de gener de 1902)

Eberhard Frederich Ferdinand **Hopf**

(Salzburg, Àustria, Imperi Austrohongarès, 4 d'abril de 1902; Bloomington, Indiana, Estats Units, 24 de juliol de 1983)

Stephan **Cohn Vossen**

(Breslau, Silèsia, Prússia, Imperi Alemany, ara Wroclaw, Polònia, 28 de maig de 1902; Moscou, Rússia, 25 de juny de 1936)

Paul Adrien Maurice **Dirac**

(Bristol, Anglaterra, 8 d'agost de 1902; Tallahassee, Florida, Estats Units, 20 d'octubre de 1984)

Bartel Leendert van der **Waerden**

(Amsterdam, Holanda, 2 de febrer de 1903; Zuric, Suïssa, 12 de gener de 1996)

Andrey Nikolaevich **Kolmogorov**

(Tambov, Rússia, 25 d'abril de 1903; Moscou, Rússia, 20 d'octubre de 1987)

William Vallance Douglas **Hodge**

(Edimburg, Escòcia, 17 de juny de 1903; Cambridge, Cambridgeshire, Anglaterra, 7 de juliol de 1975)

John von **Neumann**

(Budapest, Imperi Austrohongarès, ara Hongria, 28 de desembre de 1903; Washington, Estats Units, 8 de febrer de 1957)

Henri Paul **Cartan**

(Nancy, França, 8 de juliol de 1904; París, França, 13 d'agost de 2008)

Zbigniew **Moroń**

(Wracław, Prússia, Imperi Alemany, ara Polònia, 1904; Wracław, Polònia, 1971)

Käte **Hey**

(1904; 1990)

Leo **Zippin**

(Nova York, Estats Units, 25 de gener de 1905; Manhattan, Nova York, Estats Units, 11 de maig de 1995)

Derrick Henry **Lehmer**

(Berkeley, Califòrnia, Estats Units, 23 de febrer de 1905; Berkeley, Califòrnia, Estats Units, 22 de maig de 1991)

Abraham Adrian **Albert**

(Chicago, Illinois, Estats Units, 9 de novembre de 1905; Chicago, Illinois, Estats Units, 6 de juny de 1972)

Gottfried Maria Hugo **Köthe**

(Graz, Àustria, Imperi Austrohongarès, 25 de desembre de 1905; Frankfurt, Hessen, Alemanya, 30 d'abril de 1989)

Werner Ludwig Eduard **Weber**

(Oberstein an der Nahe, Renània Palatinat, Imperi Alemany, 3 de gener de 1906; Hamburg, Alemanya, 2 de febrer de 1975)

Kurt **Gödel**

(Brün, Imperi Austrohongarès, ara Brno, Txèquia, 28 d'abril de 1906; Princeton, New Jersey, Estats Units, 14 de gener de 1978)

André **Weil**

(París, França, 6 de maig de 1906; Princeton, New Jersey, Estats Units, 6 d'agost de 1998)

Olga **Taussky-Todd**

(Olmütz, Imperi Austrohongarès, ara Txèquia, 30 d'agost de 1906; Pasadena, Califòrnia, Estats Units, 7 d'octubre de 1995)

Aleksandr Osipovich **Gelfond**

(Sant Petersburg, Rússia, 24 d'octubre de 1906; Moscou, Rússia, 7 de novembre de 1968)

Hans **Fitting**

(Mönchengladbach, Rin del Nord Westfàlia, Prússia, Imperi Alemany, 13 de novembre de 1906; Königsberg, Prússia, Alemanya, 15 de juny de 1938)

Lars Valerian **Ahlfors**

(Helsingfors, ara Hèlsinki, Finlàndia, 18 d'abril de 1907; Pittsfield, Massachusetts, Estats Units, 11 d'octubre de 1996)

John Barkley **Rosser Sr.**

(Jacksonville, Florida, Estats Units, 6 de desembre de 1907;
Madison, Wisconsin, Estats Units, 5 de setembre de 1989)

Max Friedrich **Deuring**

(Göttingen, Baixa Saxònia, Imperi Alemany, 9 de desembre de 1907;
Göttingen, Baixa Saxònia, Alemanya, 20 de desembre de 1984)

Leonard **Carlitz**

(Filadèlfia, Pensilvània, Estats Units, 26 de desembre de 1907;
Pittsburgh, Pensilvània, Estats Units, 17 de setembre de 1999)

Alexander **Dinghas**

(Esmirna, Turquia, 9 de febrer de 1908; Berlín, Alemanya, 19
d'abril de 1974)

Jacques **Herbrand**

(París, França, 12 de febrer de 1908; La Bérarde, França, 27 de
juliol de 1931)

Marceli **Stark**

(Lemberg, Imperi Austrohongarès, ara Lvov, Ucraïna, 19 de
setembre de 1908; Varsòvia, Polònia, 4 de maig de 1974)

Sergei Lvovich **Sobolev**

(Sant Petersburg, Rússia, 6 d'octubre de 1908; Moscou, Rússia,
3 de gener de 1989)

Hans Arnold **Heilbronn**

(Berlín, Prússia, Imperi Alemany, 8 d'octubre de 1908; Toronto,
Canadà, 28 d'abril de 1975)

Claude **Chevalley**

(Johannesburg, Transvaal, Sud-àfrica, 11 de febrer de 1909; Pa-
rís, França, 28 de juny de 1984)

Deane Montgomery

(Weaver, Minnesota, Estats Units, 2 de setembre de 1909; Chapel Hill, Carolina del Nord, Estats Units, 15 de març de 1992)

Konrad Zuse

(Berlín, Prússia, Imperi Alemany, 22 de juny de 1910; Hünfeld, Fulda, Hessen, Alemanya, 18 de desembre de 1995)

Harald Nehrkorn

(9 de juliol de 1910)

Ruth Stauffer

després, Ruth McKee

(Harrisburg, Pensilvània, Estats Units, 16 de juliol de 1910; Pensswood Village, Newtown, Pensilvània, Estats Units, 9 de gener de 1993)

Nathan Jacobson

(Varsòvia, Rússia, ara Polònia, 8 de setembre de 1910; Hamden, Connecticut, Estats Units, 5 de desembre de 1999)

Theodor Schneider

(Frankfurt am Main, Hessen, Imperi Alemany, 7 de maig de 1911; Zähringen, Freiburg, Baden Württemberg, Alemanya, 31 d'octubre de 1988)

Hans Maass

(Hamburg, Imperi Alemany, 17 de juny de 1911; Heidelberg, Baden Württemberg, Alemanya, 15 d'abril de 1992)

Ernst Witt

(Alsen, Imperi Alemany, ara Als, Dinamarca, 26 de juny de 1911; Hamburg, Alemanya, 3 de juliol de 1991)

Otto Franz Georg Schilling

(Apolda, Turíngia, Imperi Alemany, 3 de novembre de 1911; Highland Park, Illinois, Estats Units, 20 de juny de 1973)

Wernher Magnus Maximilian von **Braun**

(Wyrzysk, Prússia, Imperi Alemany, ara Polònia, 23 de març de 1912; Alexandria, Virgínia, Estats Units, 6 de juny de 1977)

Martin **Eichler**

(Pinnow, Brandenburg, Prússia, Imperi Alemany, 29 de març de 1912; Basilea, Suïssa, 7 d'octubre de 1992)

Alan Mathison **Turing**

(Maida Vale, Londres, Anglaterra, 23 de juny de 1912; Wilmslow, Cheshire, Anglaterra, 7 de juny de 1954)

Paul **Erdős**

(Budapest, Imperi Austrohongarès, ara Hongria, 26 de març de 1913; Varsòvia, Polònia, 20 de setembre de 1996)

Paul Julius Oswald **Teichmüller**

(Nordhausen im Harz, Turíngia, Imperi Alemany, 18 de juny de 1913; regió del Dnieper, Rússia, 11 de setembre de 1943)

Kunihiko **Kodaira**

(Tòquio, Japó, 16 de març de 1915; Kofu, Japó, 26 de juliol de 1997)

Rowland Leonard **Brooks**

(Lincolnshire, Anglaterra, 6 de febrer de 1916; Londres, Anglaterra, 18 de juny de 1993)

Alfred Max Helmut **Stöhr**

(Berlín Karlshorst, Prússia, Imperi Alemany, 4 de març de 1916; Berlín, Alemanya, 10 d'octubre de 1973)

Claude Elwood **Shannon**

(Gaylord, Michigan, Estats Units, 30 d'abril de 1916; Medford, Massachusetts, Estats Units, 24 de febrer de 2001)

Arthur Harold **Stone**

(Islington, Londres, Anglaterra, 30 de setembre de 1916; Nort-

heastern, Boston, Massachusetts, Estats Units, 6 d'agost de 2000)

Cedric Austen Bardell **Smith**

(Leicester, Anglaterra, 5 de febrer de 1917; Londres, Anglaterra, 10 de gener de 2002)

William Thomas **Tutte**

(Newmarket, Suffolk, Anglaterra, 14 de maig de 1917; Kitchener, Ontario, Canadà, 2 de maig de 2002)

Atle **Selberg**

(Langesund, Noruega, 14 de juny de 1917; Princeton, New Jersey, Estats Units, 6 d'agost de 2007)

Kenkichi **Iwasawa**

(Shinshuku-mura, Kiryu, Gumma, Japó, 11 de setembre de 1917; Tòquio, Japó, 26 d'octubre de 1998)

Patrick Michael **Grundy**

(Yarmouth, Illa de Wight, Anglaterra, 16 de novembre de 1917; Anglaterra, 1959)

Julia Hall Bowman **Robinson**

(Sant Lluís, Missouri, Estats Units, 8 de desembre de 1919; Oakland, Califòrnia, Estats Units, 30 de juliol de 1985)

Andrew Mattei **Gleason**

(Fresno, Califòrnia, Estats Units, 4 de novembre de 1921; Cambridge, Massachusetts, Estats Units, 17 d'octubre de 2008)

Roger **Godement**

(Le Havre, França, 1921)

Chen-Ning Franklin **Yang**

(Hefei, Anhui, Xina, 1 d'octubre de 1922)

André **Néron**

(La Clayette, França, 30 de novembre de 1922; París, França, 5 d'abril de 1985)

Igor Rostislavovich **Shafarevich**

(Zhytomyr, Rússia, 3 de juny de 1923)

Hans-Egon **Richert**

(Hamburg, Alemanya, 1924; Blaustein, Baden Württemberg, Alemanya, 25 de novembre de 1993)

Jun-Ichi **Igusa**

(Maebashi, Gunma, Japó, 1924)

John Torrence **Tate**

(Minneapolis, Minnesota, Estats Units, 13 de març de 1925)

Arthur Oliver Lonsdale **Atkin**

(31 de juliol de 1925; Maywood, Illinois, Estats Units, 28 de desembre de 2008)

Martin C. **Gutzwiller**

(Basilea, Suïssa, 12 d'octubre de 1925)

Tsuneo **Tamagawa**

(Tòquio, Japó, 1925)

John Lawrence **Brown Jr.**

(Ellenville, Nova York, Estats Units, 1925; State College, Pensilvània, Estats Units, 20 de febrer de 2011)

Hilary Whitehall **Putnam**

(Chicago, Illinois, Estats Units, 31 de juliol de 1926)

Jean-Pierre **Serre**

(Bages, França, 15 de setembre de 1926)

Griselda **Pascual** i Xufré

(Barcelona, 1926; Barcelona, 9 de juny de 2001)

Masayoshi **Nagata**

(Obu, Aichi, Japó, 9 de febrer de 1927; Kyoto, Japó, 27 d'agost de 2008)

Robert L. **Mills**

(Englewood, New Jersey, Estats Units, 15 d'abril de 1927; Echo Lake, Vermont, Estats Units, 27 d'octubre de 1999)

Serge **Lang**

(Saint Germain en Laye, París, 19 de maig de 1927; Berkeley, Califòrnia, Estats Units, 12 de setembre de 2005)

Henry Peter Francis **Swinerton-Dyer**

(Ponteland, Northumberland, Anglaterra, 2 d'agost de 1927)

Heinrich Wolfgang **Leopoldt**

(Alemanya 22 d'agost de 1927; Alemanya, 28 de juliol de 2011)

Peter Jaques **Roquette**

(Königsberg, Prússia, Alemanya, 8 d'octubre de 1927)

Friedrich Ernst Peter **Hirzebruch**

(Hamm, Rin del Nord Westfàlia, Alemanya, 17 d'octubre de 1927)

Yutaka **Taniyama**

(Kisai, Tòquio, Japó, 12 de novembre de 1927; Tòquio, Japó, 17 de novembre de 1958)

Heini **Halberstam**

(Txecoslovàquia, 1927)

Ennio **De Giorgi**

(Lecce, Puglia, Itàlia, 8 de febrer de 1928; Pisa, Itàlia, 25 d'octubre de 1996)

Alexander **Grothendieck**

(Berlín, Alemanya, 28 de març de 1928)

John Forbes **Nash**

(Bluefield, Virgínia Occidental, Estats Units, 13 de juny de 1928)

Jürgen Kurt **Moser**

(Königsberg, Prússia, Alemanya, 4 de juliol de 1928; Schwerzenbach, Zuric, Suïssa, 17 de desembre de 1999)

Boris Borisovich **Kadomstev**

(Rússia, 9 de novembre de 1928; Rússia, 19 d'agost de 1998)

Martin David **Davis**

(Nova York, Estats Units, 1928)

Goro **Shimura**

(Hamamatsu, Japó, 23 de febrer de 1930)

Stephen **Smale**

(Flint, Michigan, Estats Units, 15 de juliol de 1930)

Donald Joseph **Newman**

(Brooklin, Nova York, Estats Units, 27 de juliol de 1930; Filadèlfia, Estats Units, 28 de març de 2007)

Richard Gordon **Swan**

(Nova York, Estats Units, 21 de desembre de 1933)

Paul Joseph **Cohen**

(Long Branch, New Jersey, Estats Units, 2 d'abril de 1934; Palo Alto, Califòrnia, Estats Units, 23 de març de 2007)

Andrew Pollard **Ogg**

(Bowling Green, Ohio, Estats Units, 9 d'abril de 1934)

Albrecht **Pfister**

(Munic, Baviera, Alemanya, 30 de juliol de 1934)

Arnold **Schönhage**

(Lockhausen, estat lliure de Lippe, ara Bad Salzuflen, Rin del Nord Westfàlia, 1 de desembre de 1934)

Francesco **Calogero**

(Fiesole, Itàlia, 6 de febrer de 1935)

David Pierre **Ruelle**

(Ghent, Bèlgica, 20 d'agost de 1935)

Nicolas **Bourbaki**

(Besse et Chandesse, ara Besse et Saint Anastaise, Auvergne, França, 1935)

Blanche **Descartes**

Pseudònim del grup format pels quatre matemàtics Brooks, Smith, Stone i Tutte, també coneguts com “els quatre de Trinity”

(Cambridge, Anglaterra, 1935)

Vladimir Iosifovich **Petviashvili**

(Rússia, 12 de setembre de 1936; Rússia, 21 de juliol de 1993)

Dmitrii Viktorovich **Anosov**

(Moscou, Rússia, 30 de novembre de 1936)

Yuri Ivanovitch **Manin**

(Simferopol, Crimea, Rússia, 16 de febrer de 1937)

David Bryant **Mumford**

(Worth, Sussex, Anglaterra, 11 de juny de 1937)

Vladimir Igorevich **Arnold**

(Odessa, Ucraïna, Rússia, 12 de juny de 1937; París, França, 3 de juny de 2010)

Barry Charles **Mazur**

(Nova York, Estats Units, 19 de desembre de 1937)

Phillip Augustus **Griffiths**

(Raleigh, Carolina del Nord, Estats Units, 18 d'octubre de 1938)

Alan **Baker**

(Londres, Anglaterra, 19 d'agost de 1939)

Hervé **Jacquet**

(França, 1939)

Stephen William **Hawking**

(Oxford, Anglaterra, 8 de gener de 1942)

Audrey **Terras**

(Washington, D.C., Estats Units, 10 de setembre de 1942)

Nicholas Michael **Katz**

(Baltimore, Maryland, Estats Units, 7 de desembre de 1943)

Pierre **Berthelot**

(França, 1943)

Pierre René **Deligne**

(Etterbeek, Brusselles, Bèlgica, 3 d'octubre de 1944)

Gerhard **Frey**

(Erlangen, Baviera, Alemanya, 1944)

Hiroshi **Umemura**

(Japó, 1944)

Richard Peirce **Brent**

(Melbourne, Austràlia, 20 d'abril de 1946)

George **Lusztig**

(Timisoara, Romania, 20 de maig de 1946)

Ina **Kersten**

(Hamburg, Alemanya, 1946)

Hermanus Johannes Joseph **te Riele**
(L'Haia, Holanda, 5 de gener de 1947)

Yuri Vladimirovich **Matijasevich**
(Leningrad, Rússia, 2 de març de 1947)

Alain **Connes**
(Draguignan, Var, França, 1 d'abril de 1947)

Suren Yurievich **Arakelov**
(Kharkiv, Rússia, 16 d'octubre de 1947)

Kenneth Alan **Ribet**
(Estats Units, 28 de juny de 1948)

Hendrik Willem **Lenstra Jr.**
(Zaandam, Holanda, 16 d'abril de 1949)

Andrew Michael **Odlyzko**
(Tarnów, Polònia, 23 de juliol de 1949)

Andrei Andreevich **Bolibrukh**
(Moscou, Rússia, 30 de gener de 1950; Moscou, Rússia, 11 de novembre de 2003)

Benedict **Gross**
(South Orange, New Jersey, Estats Units, 22 de juny de 1950)

Andrei Alexandrov **Suslin**
(Sant Petersburg, Rússia, 27 de desembre de 1950)

Don Bernard **Zagier**
(Heidelberg, Baden Württemberg, Alemanya, 29 de juny de 1951)

Alexander Borissowitsch **Zamolodchikov**
(Dubna, Moscou, Rússia, 18 de setembre de 1952)

Andrew John **Wiles**
(Cambridge, Anglaterra, 11 d'abril de 1953)

Gerd **Faltings**

(Gelsenkirchen Buer, Rin del Nord Westfàlia, Alemanya, 28 de juliol de 1954)

Alexander Sergejevitsch **Merkurjev**

(Rússia, 25 de setembre de 1955)

Thomas Callister **Hales**

(San Antonio, Texas, Estats Units, 4 de juny de 1958)

Christopher **Deninger**

(Alemanya, 1958)

Jeremy Thau **Teitelbaum**

(Setembre de 1959, Nova York, Estats Units)

Vadim Genrikhovich **Knizhnik**

(Kiev, Ucraïna, Rússia, 20 de febrer de 1962; Moscou, Rússia, 25 de desembre de 1987)

Franz Josef **Lemmermeyer**

(Alemanya, 20 de febrer de 1962)

Richard Lawrence **Taylor**

(Regne Unit, 19 de maig de 1962)

Fred **Diamond**

(19 de novembre de 1964)

Marcus Peter Francis du **Sautoy**

(Londres, Anglaterra, 26 d'agost de 1965)

Christophe **Breuil**

(França, 1969)

Brian **Conrad**

(Nova York, Estats Units, 20 de novembre de 1970)

Perfil biogràfic dels autors

Pilar **Bayer Isant**

(Barcelona, 13 de febrer de 1946)

És Catedràtica d'Àlgebra de la Universitat de Barcelona des de 1982 i especialista en teoria de nombres. Llicenciada i Doctora en Matemàtiques per la Universitat de Barcelona, ha estat professora contractada a la Universitat de Barcelona (1968–1975), a la Universitat Autònoma de Barcelona (1969–1977), i a la Universitat de Regensburg (Alemanya) (1977–1980); professora numerària a la Universitat de Santander (1980–1981) i a la Universitat Autònoma de Barcelona (1981–1982); i professora Emmy–Noether a la Universitat Georg August de Göttingen, Alemanya (2004). Les seves publicacions versen sobre problemes diofantins, funcions zeta, teoria de Galois, corbes modulars, corbes de Shimura i història de la matemàtica. Ha dirigit 10 tesis doctorals en teoria de nombres i nombrosos projectes de recerca. La seva activitat investigadora s'emmarca en el Seminari de Teoria de Nombres de Barcelona, del qual en fou fundadora l'any 1985 i que compta en l'actualitat amb destacats investigadors. Ha impartit conferències en universitats d'Alemanya, Àustria, Espanya, França, Grècia, Polònia, Portugal, el Regne Unit i Rússia, així com també

nombroses conferències de divulgació en centres del nostre país. És Acadèmica de la *Real Academia de Ciencias Exactas, Físicas y Naturales* (2010); de la Reial Acadèmia de Ciències i Arts (2001); de la Reial Acadèmia de Doctors (1994); i de l'Institut d'Estudis Catalans (2001). És en possessió de la Medalla Narcís Monturiol al Mèrit Científic i Tecnològic (1998), atorgada pel Govern de Catalunya.

Jordi Guàrdia Rúbies

(Balaguer, 5 de juny de 1967)

És Llicenciat i Doctor en Matemàtiques per la Universitat de Barcelona. Ha estat Professor Ajudant de la mateixa universitat, i Professor Consultor de la Universitat Oberta de Catalunya. Actualment treballa a l'Escola Politècnica Superior d'Enginyeria de Vilanova i la Geltrú, com a Professor Agregat de la Universitat Politècnica de Catalunya. La seva recerca se centra en el camp de la teoria de nombres, en la qual ha treballat en temes diversos, com ara teoria d'Arakelov, geometria aritmètica, varietats abelianes i funcions theta, i teoria de nombres computacional. A més de les seves publicacions en revistes científiques internacionals, és autor de diversos paquets de programari matemàtic, així com també de nombrosos materials docents.

Artur Travesa Grau

(Barcelona, 12 d'abril de 1956)

Professor Titular d'Universitat de l'àrea d'Àlgebra a la Universitat de Barcelona des de l'any 1992, exerceix les seves tasques docents i de recerca a la Facultat de Matemàtiques d'aquesta institució, especialment en teoria de nombres i àlgebra.

Llicenciat en Matemàtiques per la Universitat de Barcelona l'any 1980, la seva carrera s'ha desenvolupat en aquesta universitat, en la qual fou contractat com a professor el mateix any 1980. Amb la direcció de Pilar Bayer, hi defensà la tesi doctoral, *Nombres d'extensions abelianes i les seves funcions generatrius*, l'any 1988.

La seva tasca de recerca, i part de la seva tasca docent, ha transcorregut en el marc del Seminari de Teoria de Nombres de Barcelona. Des del començament, amb l'estudi d'extensions ciclotòmiques, fins a l'actualitat, amb l'estudi de funcions automorfes, s'ha deixat guiar per l'interès a entendre com es generen les extensions abelianes (*Jugendtraum*).

És autor de diverses publicacions de recerca, i també docents, en teoria de nombres i àlgebra. Per la seva relació amb l'obra que qui llegeix té entre les seves mans, cal destacar que va formar part de l'equip de persones que col·laborà amb Griselda Pascual en la seva traducció al català de les *Disquisitiones Arithmeticae* de C. F. Gauss, que publicà la Societat Catalana de Matemàtiques l'any 1996.

Bibliografia

- [1] Abel, N.H.: Recherches sur les fonctions elliptiques. *J. reine u. angew. Math.* **2** (1827), p. 101–181. *J. reine u. angew. Math.* **3** (1828), p. 160–190.
- [2] Albert, A.A.: On the construction of Riemann matrices. *Ann. of Math.* **35** (2) (1934), n. 1, p. 1–28.
- [3] Albert, A.A.: A solution of the principal problem in the theory of Riemann matrices. *Ann. of Math.* **35** (2) (1934), n. 3, p. 500–515.
- [4] Albert, A.A.: Cyclic fields of degree p^n over F of characteristic p . *Bull. Amer. Math. Soc.* **40** (1934), n. 8, p. 625–631.
- [5] Albert, A.A.: The principal matrices of a Riemann matrix. *Bull. Amer. Math. Soc.* **40** (1934), n. 12, p. 843–846.
- [6] Albert, A.A.; Hasse, H.: A determination of all normal division algebras over an algebraic number field. *Trans. Amer. Math. Soc.* **34** (1932), n. 3, p. 722–726.
- [7] Alsina, M.; Bayer, P.: *Quaternion orders, quadratic forms and Shimura curves*. CRM Monograph Series

- 22.** American Mathematical Society, Providence, RI, 2004, xvi+196 p. ISBN: 0-8218-3359-6.
- [8] Arenas, A.; Bayer, P.: Heegner points on modular curves. *Contributions to the algorithmic study of problems of arithmetic moduli. Rev. R. Acad. Cienc. Exactas Fís. Nat.* **94** (2000), n. 3, p. 323–332.
- [9] Arenas, A.; Bayer, P.: Complex multiplication points on modular curves. *Contributions to the algorithmic study of problems of arithmetic moduli. Rev. R. Acad. Cienc. Exactas Fís. Nat.* **94** (2000), n. 3, p. 333–338.
- [10] Artin, E.: Quadratische Körper im Gebiete der höheren Kongruenzen I, II. *Math. Z.* **19** (1924), p. 153–206.
- [11] Artin, E.: *Geometric Algebra*. Interscience Publishers, Inc., 1957.
- [12] Artin, E.: *Collected papers*. Lang, S.; Tate, J. T. eds. 1982, reimpressió de l'original de 1965. Springer Verlag, Nova York, Berlín, xvi+560 p. ISBN: 0-387-90686-X.
- [13] Artin, E.; Tate, J.: *Class field theory*. Benjamin, 1961.
- [14] Bachelier, L.: *Théorie de la spéculation (1900). Théorie mathématique du jeu (1901)*. Éditions Jacques Gabay, 1995.
- [15] Bayer, P.: *Poincaré i les funcions fuchsianes*. Memòria de recepció a la Reial Acadèmia de Ciències i Arts de Barcelona **LIX** (2001), n. 5, p. 193–228. ISSN: 0368-8283.

- [16] Bayer, P.: Uniformization of certain Shimura curves. *Differential Galois Theory*, Bedlewo, 2001, T. Crespo and Z. Hajto, eds. Banach Center Publications **58** (2002), p. 13–26. Polish Acad. Sci., Varsòvia, 2002.
- [17] Bayer, P.: La hipòtesi de Riemann. En el llibre *Els set problemes del mil·lenni*, J. Quer, ed. Fundació Caixa Sabadell 2007, p. 29–62. ISBN: 978–84–95166–67–8.
- [18] Bayer, P.: *Ensenyar matemàtiques, aprendre matemàtiques: variacions sobre un tema de Felix Klein*. Lliçó inaugural del curs acadèmic 2007–2008 de la Universitat de Barcelona. Publicacions i edicions de la Universitat de Barcelona, 2007, 27 p. DL: B–47.165–2007.
- [19] Bayer, P.: Emmy Noether: de l'àlgebra no commutativa a la teoria de nombres. En el llibre *Curs E. Noether*, S. Xambó, ed. Conferències FME, **6**, p. 169–203. Facultat de Matemàtiques i Estadística de la Universitat Politècnica de Catalunya, 2009. ISBN: 978–84–7653–391–8.
- [20] Bayer, P.: Jean-Pierre Serre: An Overview on his Work. *The Abel Prize 2003–2007. The first five years: 2003–2007*, p. 33–80. H. Holden and R. Piene (editors). Springer, 2010. ISBN: 978-3-642-01372-0.
- [21] Bayer, P.: *Antecedentes y evolución de la teoría de la multiplicación compleja*. Discurso de recepció en la Real Academia de Ciencias Exactas, Físicas y Naturales, Madrid, 2010, ix+198 p. ISBN: 978–84–87125–48–5.

- [22] Bayer, P.; Frey, G.: Galois representations of octahedral type and 2-coverings of elliptic curves. *Math. Z.* **207** (1991), n. 3, p. 395–408.
- [23] Bayer, P.; González-Rovira, J.: On Hasse-Witt invariants of modular curves. *Experiment. Math.* **6** (1997), p. 57–76.
- [24] Bayer, P.; Guàrdia, J.: A la recerca de pi. *But. Soc. Catalana Mat.* **17** (2002), n. 2, p. 7–19.
- [25] Bayer, P.; Guàrdia, J.: On equations defining fake elliptic curves. *J. Théor. Nombres Bordeaux* **17** (2005), n. 1, p. 57–67.
- [26] Bayer, P.; Guàrdia, J.: Uniformization of Fermat curves. *Ramanujan J.* **12** (2006), p. 207–223.
- [27] Bayer, P.; Lario, J.C.: On Galois representations defined by torsion points of modular elliptic curves. *Compositio Math.* **84** (1992), n. 1, p. 71–84.
- [28] Bayer, P.; Neukirch, J.: On values of zeta functions and l -adic Euler characteristics. *Invent. Math.* **50** (1978/79), p. 35–64.
- [29] Bayer, P.; Neukirch, J.: On automorphic forms and Hodge theory. *Math. Ann.* **257** (1981), p. 137–155.
- [30] Bayer, P.; Rio, A.: Dyadic exercises for octahedral extensions. *J. reine u. angew. Math.* **517** (1999), p. 1–17.
- [31] Bayer, P.; Travesa, A. (eds.): *Corbes modulars: Taules*. Notes del Seminari de Teoria de Nombres **1**, ISBN: 84-604-3577-6. Barcelona, 1992.

- [32] Bayer, P.; Travesa, A.: Órdenes matriciales generados por grupos de congruencia. *Contributions to the algorithmic study of problems of arithmetic moduli. Rev. R. Acad. Cienc. Exactas Fís. Nat.* **94** (2000), n. 3, p. 339–346.
- [33] Bayer, P.; Travesa, A.: Formas cuadráticas ternarias e inmersiones matriciales de órdenes cuadráticos. *Contributions to the algorithmic study of problems of arithmetic moduli. Rev. R. Acad. Cienc. Exactas Fís. Nat.* **94** (2000), n. 3, p. 347–355.
- [34] Bayer, P.; Travesa, A.: Inmersiones de órdenes cuadráticos en el orden generado por $\Gamma_0(N)$. *Contributions to the algorithmic study of problems of arithmetic moduli. Rev. R. Acad. Cienc. Exactas Fís. Nat.* **94** (2000), n. 3, p. 357–376.
- [35] Bayer, P.; Travesa, A.: Uniformization of triangle modular curves. *Publ. Mat.* (2007), extra vol., p. 43–106.
- [36] Bayer, P.; Travesa, A.: Uniformizing functions for certain Shimura curves, in the case $D = 6$. *Acta Arith.* **126** (2007), n. 4, p. 315–339.
- [37] Bayer, P.; Travesa, A.: On Local Constants Associated to Arithmetical Functions. *Pure Appl. Math. Q.* **4** (2008), n. 4, p. 1107–1132. [Special issue: in honor of Jean-Pierre Serre, Part 1 of 2].
- [38] Bershadski, M.; Radul, A.: Conformal field theories with additional $\mathbb{Z}_N$ symmetry. *International Journal of Modern Physics A* **2** (1987), n. 1, p. 165–171.

- [39] Berthelot, P.; Ogus, A.: *Notes on crystalline cohomology*. Princeton University Press, Princeton, N.J.; University of Tokyo Press, Tòquio, 1978, vi+243 p. ISBN: 0-691-08218-9.
- [40] Birch, B. J.; Swinnerton-Dyer, H. P. F.: Notes on elliptic curves. I. *J. reine u. angew. Math.* **212** (1963), p. 7–25.
- [41] Birch, B. J.; Swinnerton-Dyer, H. P. F.: Notes on elliptic curves. II. *J. reine u. angew. Math.* **218** (1965), p. 79–108.
- [42] Borevich, A. I.; Shafarevich, I. R.: *Number theory*. Translated from the Russian by Newcomb Greenleaf. Pure and Applied Mathematics, **20**. Academic Press, Nova York, Londres, 1966, x+435 p.
- [43] Bost, J. B.; Mestre, J.-F.; Moret-Bailly, L.: Sur le calcul explicite des classes de Chern des surfaces arithmétiques de genre 2. *Astérisque* **183** (1990), p. 69–105.
- [44] Bourbaki, N.: *Éléments d'histoire des mathématiques*. París, Hermann, 1969.
- [45] Braden, H.; Enolski, V.: Remarks on the complex geometry of the 3-monopole. Pre-publicació (2006), disponible en <http://arxiv.org/abs/math-ph/0601040>.
- [46] Breuil, C.; Conrad, B.; Diamond, F.; Taylor, R.: On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises. *J. Amer. Math. Soc.* **14** (2001), n. 4, p. 843–939.

- [47] Brill, A.; Noether, M.: Über die algebraischen Functionen und ihre Anwendung in der Geometrie. *Math. Ann.* **7**, (2), (1874), p. 269–316.
- [48] Brill, A.; Noether, M.: Die Entwicklung der Theorie der algebraischen Functionen in älterer und neuer Zeit. *Jahresbericht der Deutschen Mathematiker-Vereinigung* **3** (1894), p. 107–566.
- [49] Brooks, R. L.; Smith, C. A. B.; Stone, A. H.; Tutte, W. T.: The Dissection of Rectangles into Squares. *Duke Mathematical Journal* **7** (1940), n. 1, p. 312–340.
- [50] Browder, F. E., ed.: *Mathematical developments arising from Hilbert problems*. Proceedings of the Symposium in Pure Mathematics of the American Mathematical Society held at Northern Illinois University, De Kalb, Ill., May, 1974. Proceedings of Symposia in Pure Mathematics **28**, American Mathematical Society, Providence, R. I., 1976, xii+628 p.
- [51] Brown Jr., J. L.: Generalization of Richert's theorem. *The American Mathematical Monthly* **83** (1976), p. 631–634.
- [52] Byers, N.: E. Noether's discovery of the deep connection between symmetries and conservation laws. The heritage of Emmy Noether. *Israel Math. Conf. Proc.*, **12** (1999), p. 67–81. (Ramat-Gan, 1996), Bar-Ilan Univ., Ramat Gan.
- [53] Cartan, E.: *Leçons sur les invariants intégraux*. Hermann, Paris, 1922.

- [54] Castelnuovo, G.: Alcuni risultati sui sistemi lineari di curve appartenenti ad una superficie algebrica. *Mem. Soc. It. Sci. XL* (3) **10** (1896), p. 82–102.
- [55] Castelnuovo, G.; Enriques, F.; Severi, F.: Max Noether / Mit Schriftenverzeichnis. *Math. Ann.* **93** (1925), p. 161–181.
- [56] Cayley, A.: A memoir on the theory of matrices. *Phil. Trans. R. Soc. London* **148** (1858), p. 17–37. Reproduced in *Papers* **2**, p. 475–496.
- [57] Cayley, A.: Desiderata and suggestions. *Amer. J. Math.* **1** (1878), p. 50–52.
- [58] Chebotarev, N.: Opredelenie plotnosti sovokupnosti prostykh chisel, primadlezhashchikh zadannomu klassu podstanovok. *Izv. Ross. Akad. Nauk* **17** (1923), p. 27–65.
- [59] Chebotarev, N.: Die Bestimmung der Dichtigkeit einer Menge von Primzahlen, welche zu einer gegebenen Substitutionsklasse gehören. *Math. Ann.* **95** (1925), p. 191–228.
- [60] Chudnovsky, D. V.; Chudnovsky, G. V.: *Transcendental Methods and Theta Functions*. Proc. Symp. Pure Mathematics **49** (1989), p. 167–232.
- [61] Conrad, K.: *History of Class Field Theory*.
<http://www.math.uconn.edu/~kconrad/blurbs/gradnumthy/cfthistory.pdf>.
- [62] Conrad, K.: The origin of representation theory. *L'enseignement Mathématique* **44** (1998), p. 361–392.

- [63] Conrad, B.; Diamond, F.; Taylor, R.: Modularity of certain potentially Barsotti–Tate Galois representations. *J. Amer. Math. Soc.* **12** (1999), n. 2, p. 521–567.
- [64] Cox, D.A.: *Primes of the form $x^2 + ny^2$: Fermat, class field theory and complex multiplication*. A Wiley Interscience Publication. John Wiley & Sons, Inc., Nova York, 1989, xiv+351 p. ISBN: 0–471–50654–0; 0–471–19079–9.
- [65] Crespo, T.; Hajto, Z.: *Algebraic groups and differential Galois theory*. Graduate Studies in Mathematics, **122**. American Mathematical Society, Providence, RI, 2011. xiv+225 p. ISBN: 978–0–8218–5318–4.
- [66] Curtis, C.W.: *Pioneers of Representation Theory: Frobenius, Burnside, Schur and Brauer*. History of Mathematics **15** (1999). American Mathematical Society. ISBN: 0–8218–9002–6.
- [67] Davenport, H.; Hasse, H.: Die Nullstellen der Kongruenz-zetafunktionen in gewissen zyklischen Fällen. *J. reine u. angew. Math.* **172** (1935), n. 1, p. 151–182. *Mathematische Abhandlungen* **3**. Walter de Gruyter, 1975.
- [68] Deahna, H.: Über die Bedingungen der Integrabilität linearer Differentialgleichungen erster Ordnung zwischen einer beliebigen Anzahl veränderlicher Grössen. *J. reine u. angew. Math.* **20** (1840), p. 340–349.
- [69] Dedekind, R.: Schreiben an Herrn Borchardt über die Theorie der elliptischen Modul-Functionen. *J. reine u. angew. Math.* **83** (1877), p. 265–292.

- [70] Dedekind, R.: *Gesammelte mathematische Werke*. Herausgegeben von R. Fricke, E. Noether, Ö. Ore. Erster Band. Friedr. Vieweg & Sohn, Brunsvic, 1930.
- [71] Dedekind, R.: *Gesammelte mathematische Werke*. Herausgegeben von R. Fricke, E. Noether, Ö. Ore. Zweiter Band. Friedr. Vieweg & Sohn, Brunsvic, 1931.
- [72] Dedekind, R.: *Gesammelte mathematische Werke*. Herausgegeben von R. Fricke, E. Noether, Ö. Ore. Dritter Band. Friedr. Vieweg & Sohn, Brunsvic, 1932.
- [73] Dehn, M.: Über Zerlegung von Rechtecken in Rechtecke. *Math. Ann.* **57** (1903), p. 314–332.
- [74] Deift, P. A.; Its, A. R.; Kapaev, A.; Zhou, X.: On the algebro-geometric integration of the Schlesinger equations. *Commun. Math. Phys.* **203** (1999), n. 3, p. 613–633.
- [75] Deligne, P.: Travaux de Shimura. *Séminaire Bourbaki*, 23ème année (1970/71), Exp. n. 389, p. 123–165. *Lecture Notes in Math.*, **244**, Springer, Berlín, 1971.
- [76] Deligne, P.: La conjecture de Weil. I. *Inst. Hautes Études Sci. Publ. Math.* **43** (1974), p. 273–307.
- [77] Deligne, P.: Variétés de Shimura: interprétation modulaire, et techniques de construction de modèles canoniques. *Automorphic forms, representations and L-functions*. (Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, Ore., 1977), Part 2, p. 247–289, *Proc. Sympos. Pure Math.*, **XXXIII**, Amer. Math. Soc., Providence, R.I., 1979.

- [78] Deuring, M.: Zur arithmetischen Theorie der algebraischen Funktionen. *Math. Ann.* **106** (1932), p. 77–102.
- [79] Deuring, M.: Zur Theorie der Idealklassen in algebraischen Funktionenkörpern. *Math. Ann.* **106** (1932), p. 103–106.
- [80] Deuring, M.: Galoische Theorie und Darstellungstheorie. *Math. Ann.* **107** (1932), p. 140–144.
- [81] Deuring, M.: *Algebren*. Zweite, korrigierte Auflage. Ergebnisse der Mathematik und ihrer Grenzgebiete **41**. Springer Verlag, Berlín, Nova York 1968, viii+143 p. (Primera edición: Ergebnisse der Mathematik und ihrer Grenzgebiete **4**, Springer, 1935.)
- [82] Deuring, M.: Anwendungen der Darstellungen von Gruppen durch lineare Substitutionen auf die galoissche Theorie. *Math. Ann.* **113** (1937), n. 1, p. 40–47.
- [83] Deuring, M.: Arithmetische Theorie der Korrespondenzen algebraischer Funktionenkörper, I. *J. reine u. angew. Math.* **177**, (1937), p. 161–191.
- [84] Deuring, M.: Invarianten und Normalformen elliptischer Funktionenkörper. *Math. Z.* **47** (1940), p. 47–56.
- [85] Deuring, M.: Arithmetische Theorie der Korrespondenzen algebraischer Funktionenkörper, II. *J. reine u. angew. Math.* **183**, (1941), p. 25–36.

- [86] Deuring, M.: Die Typen der Multiplikatorenringe elliptischer Functionenkörper. *Abh. Math. Sem. Han-sischen Univ.* (després, *Abh. Math. Sem. Hamburg*) **14** (1941), p. 197–272.
- [87] Deuring, M.: Reduktion algebraischer Funktio-nenkörper nach Primdivisoren des Konstantenkör-pers. *Math. Z.* **47** (1942), p. 643–654.
- [88] Deuring, M.: Die Anzahl der Typen von Maxima-lordnungen in einer Quaternionenalgebra von primer Grundzahl. *Nachr. Akad. Wiss. Göttingen. Math.-Phys. Kl. Math. Phys. Chem. Abt.* **1945** (1945), p. 48–50.
- [89] Deuring, M.: Teilbarkeitseigenschaften der singulä-ren Moduln der elliptischen Funktionen und die Disk-riminante der Klassengleichung. *Comment. Math. Helv.* **19** (1946), p. 74–82.
- [90] Deuring, M.: Zur Theorie der elliptischen Funk-tionenkörper. *Abh. Math. Sem. Univ. Hamburg* **15** (1947), p. 211–261.
- [91] Deuring, M.: Die Anzahl der Typen von Maxima-lordnungen einer definiten Quaternionenalgebra mit primer Grundzahl. *Jber. Deutsch. Math. Verein.* **54** (1950), p. 24–41.
- [92] Deuring, M.: Die Struktur der elliptischen Funkti-onenkörper und die Klassenkörper der imaginären quadratischen Zahlkörper. *Math. Ann.* **124** (1952), p. 393–426.

- [93] Deuring, M.: Die Zetafunktion einer algebraischen Kurve vom Geschlechte Eins. I, II, III, IV. *Nachr. Akad. Wiss. Göttingen. Math. Phys., Kl. Math. Phys. Chem. Abt.*, 1953 (1953), p. 85–94. *Nachr. Akad. Wiss. Göttingen. Math. Phys., Kl. IIa*, 1955 (1955), p. 13–42. *Nachr. Akad. Wiss. Göttingen. Math. Phys., Kl. IIa*, 1956 (1956), p. 37–76. *Nachr. Akad. Wiss. Göttingen. Math. Phys., Kl. IIa*, 1957 (1957), p. 55–80.
- [94] Deuring, M.: Zur Transformationstheorie der elliptischen Funktionen. *Akad. Wiss. Mainz. Abh. Math.-Nat. Kl.* 1954 (1954), p. 95–104.
- [95] Deuring, M.: On the zeta-function of an elliptic function field with complex multiplications. *Proceedings of the international symposium on algebraic number theory, Tokyo & Nikko, 1955*, p. 47–50. Science Council of Japan, Tôquio, 1956.
- [96] Deuring, M.: Die Klassenkörper der komplexen Multiplikation. *Enzyklopädie der mathematischen Wissenschaften: Mit Einschluss ihrer Anwendungen, Band I 2, Heft 10, Teil II (Article I 2, 23)* B. G. Teubner Verlagsgesellschaft, Stuttgart, 1958.
- [97] Deutsche Mathematiker-Vereinigung:
<https://www.dmv.mathematik.de/die-dmv/105-kurzbiographien/>
- [98] Diamond, F.: On deformation rings and Hecke rings. *Ann. Math.* **144** (1996), p. 137–166.
- [99] Dick, A.: *Emmy Noether: 1882–1935*. Elem. Math. Beiheft **13** (1970), Birkhäuser Verlag, Basilea, 72 p.

- [100] Dickson, E.: Linear Algebras and Abelian Extensions. *Trans. Amer. Math. Soc.* **15** (1914), p. 31–46.
- [101] Dickson, E.: New division algebras. *Trans. Amer. Math. Soc.* **28** (1926), p. 207–234.
- [102] Dieudonné, J., ed.: *Abrégé d'histoire des mathématiques 1700–1900*. Tome I. Algèbre, analyse classique, théorie des nombres. Hermann, Paris, 1978, x+392 p. ISBN: 2-7056-5870-X.
- [103] Dieudonné, J., ed.: *Abrégé d'histoire des mathématiques 1700–1900*. Tome II. Fonctions elliptiques, analyse fonctionnelle, topologie, géométrie différentielle, probabilités, logique mathématique. Hermann, Paris, 1978, vii+469 p. ISBN: 2-7056-5871-9.
- [104] Dieudonné, J., ed.: *Abrégé d'histoire des mathématiques 1700–1900*. Second edition. Hermann, Paris, 1986, viii+517 p. ISBN: 2-7056-6024-0.
- [105] Dieulefait, L.: The level 1 weight 2 case of Serre's conjecture. *Rev. Mat. Iberoam.* **23** (2007), n. 3, p. 1115–1124.
- [106] Dieulefait, L.; Vila, N.: On the images of modular and geometric three-dimensional Galois representations. *Amer. J. Math.* **126** (2004), n. 2, p. 335–361.
- [107] Dirichlet, P. G. L.: *Vorlesungen über Zahlentheorie*. 3a. ed., publicada i comentada per R. Dedekind, Braunschweig Vieweg (1893), Brunswick.
- [108] Ebin, D.; Farkas, H. M.: Thomae Formulae for Z_n Curves. *J. Anal. Math.* **111** (2010), p. 289–320.

- [109] Eichler, M.: Über die Idealklassenzahl total definiter Quaternionenalgebren. *Math. Z.* **43** (1938), p. 102–109.
- [110] Eichler, M.: Quaternäre quadratische Formen und die Riemannsche Vermutung für die Kongruenzzetafunktion. *Arch. Math.* **5** (1954), p. 355–366.
- [111] Eichler, M.: Zur Zahlentheorie der Quaternionenalgebren. *J. reine u. angew. Math.* **195** (1955), p. 127–151.
- [112] Eichler, M.: The basis problem for modular forms and the traces of the Hecke operators. *Modular functions of one variable, I (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*. Lecture Notes in Math., **320**, Springer, Berlin, 1973, p. 75–151.
- [113] Eichler, M.: Correction to: [112]. *Modular functions of one variable, IV (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*. Lecture Notes in Math., **476**, Springer, Berlin, 1975, p. 145–147.
- [114] Eichler, M.: Das wissenschaftliche Werk von Max Deuring. *Acta Arith.* **47** (1986), n. 3, p. 187–192.
- [115] Eilbeck, J. C.; Enolskii, V. Z.; Previato, E.: On a generalized Frobenius-Stickelberger addition formula. *Lett. Math. Phys.* **63** (2003), p. 5–17.
- [116] Eisenmann, A.; Farkas, H. M.: An Elementary Proof of Thomae's Formulae. *Online Journal of Analytic Combinatorics* **3** (2008).

- [117] Eisenstein, G.: Beiträge zur Theorie der elliptischen Funktionen I: Ableitung des biquadratischen Fundamentaltheorems aus der Theorie der Lemniskatenfunctionen, nebst Bemerkungen zu den Multiplications und Transformationsformeln. *J. reine u. angew. Math.* **30** (1846), p. 185–210.
- [118] Enolski, V.; Grava, T.: Thomae formulae for singular $\mathbb{Z}_n$ curves. *Letters in Math. Physics* **76** (2006), p. 187–214.
- [119] Enolski, V.; Richter, P.: Periods of hyperelliptic integrals expressed in terms of theta-constants by means of Thomae formulae. *Philos. Transact. A Math. Phys. Eng. Sci.* **366** (2008), p. 1005–1024.
- [120] Enriques, F.: Ricerche di geometria sulle superficie algebriche. *Mem. Acc. Torino* (2) **44** (1893) p. 171–232. Reproduit a *Memorie scelte* **1**, p. 31–106.
- [121] ERAM (Electronic Research Archive for Mathematics): *Jahrbuch database*.
<http://www.emis.de/cgi-bin/jfmen/MATH/JFM>
- [122] Euler, L.: De comparatione arcuum curvarum irrectificabilium (Sobre la comparació dels arcs de corba no rectificables). *Novi commentarii academiae scientiarum Petropolitanae* **6** (1756/57), p. 58–84. *Opera Postuma* 1, 1862, p. 452–486. *Opera Omnia*: Series 1, **21**, p. 296–357.
- [123] Faltings, G.: Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Invent. Math.* **73** (1983), n. 3, p. 349–366.

- [124] Farkas, H. M.; Zemel, S.: *Generalization of Thomae's formula for $\mathbb{Z}_n$ curves*. Developments in Math. **21**, Springer (2010).
- [125] Fay, J. D.: *Theta Functions on Riemann Surfaces*. Lecture Notes in Mathematics **352**, Springer, 1973.
- [126] Fay, J. D.: On the Riemann Jacobi formula. *Göttingen Nachrichten* (1979), p. 61–73.
- [127] Formanek, E.; Sibley, D.: The Group Determinant Determines the Group. *Proc. Amer. Math. Soc.* **112** (1991), p. 649–656.
- [128] Fourier, J-B. J.: *Théorie analytique de la chaleur*. Paris, 1822. Firmin Didot. Edició anglesa a Cambridge University Press, 2009; ISBN: 978–1–108–00180–9.
- [129] Frey, G.: Links between stable elliptic curves and certain diophantine equations. *Ann. Univ. Saraviensis, Math. Ser.* **1** (1986), p. 1–40.
- [130] Fricke, R.; Klein, F.: *Vorlesungen über die Theorie der automorphen Funktionen. Band 1: Die gruppentheoretischen Grundlagen. Band II: Die funktionentheoretischen Ausführungen und die Anwendungen*. Bibliotheca Mathematica Teubneriana, **3**, **4**. Johnson Reprint Corp., Nova York; B. G. Teubner Verlagsgesellschaft, Stuttgart 1965, Band I: xiv+634 p., Band II: xiv+668 p.
- [131] Frobenius, G. F.: Über die Entwicklung analytischer Functionen in Reihen, die nach gegebenen Functionen fortschreiten. *J. reine u. angew. Math.* **73** (1871),

- p. 1–30. Reproduit a *Gesammelte Abhandlungen I*, p. 35–64.
- [132] Frobenius, G. F.: Über die Integration der linearen Differentialgleichungen durch Reihen. *J. reine u. angew. Math.* **76** (1873), p. 254–272. Reproduit a *Gesammelte Abhandlungen I*, p. 84–105.
- [133] Frobenius, G. F.: Über das Pfaffsche Problem. *J. reine u. angew. Math.* **82** (1873), p. 230–315. Reproduit a *Gesammelte Abhandlungen I*, p. 249–334.
- [134] Frobenius, G. F.: Über lineare Substitutionen und bilineare Formen. *J. reine u. angew. Math.* **84** (1877), p. 1–63. Reproduit a *Gesammelte Abhandlungen I*, p. 343–405.
- [135] Frobenius, G. F.: Über homogene totale Differentialgleichungen. *J. reine u. angew. Math.* **86** (1879), p. 1–19. Reproduit a *Gesammelte Abhandlungen I*, p. 435–453.
- [136] Frobenius, G. F.: Zur Theorie der Transformation der Thetafunctionen. *J. reine u. angew. Math.* **89** (1880), p. 40–46. Reproduit a *Gesammelte Abhandlungen II*, p. 1–7.
- [137] Frobenius, G. F.: Über das Additionstheorem der Thetafunctionen mehrerer Variablen. *J. reine u. angew. Math.* **89** (1880), p. 185–220. Reproduit a *Gesammelte Abhandlungen II*, p. 11–46.
- [138] Frobenius, G. F.: Über die principale Transformation der Thetafunctionen mehrerer Variablen. *J. reine*

- u. angew. Math.* **95** (1883), p. 264–296. Reproduit a *Gesammelte Abhandlungen II*, p. 97–129.
- [139] Frobenius, G. F.: Über Gruppen von Thetacharakteristiken. *J. reine u. angew. Math.* **96** (1884), p. 81–99. Reproduit a *Gesammelte Abhandlungen II*, p. 130–148.
- [140] Frobenius, G. F.: Über Thetafunctionen mehrerer Variablen. *J. reine u. angew. Math.* **96** (1884), p. 100–122. Reproduit a *Gesammelte Abhandlungen II*, p. 149–171.
- [141] Frobenius, G. F.: Über die Grundlagen der Theorie der Jacobischen Functionen. *J. reine u. angew. Math.* **97** (1884), p. 16–48. Reproduit a *Gesammelte Abhandlungen II*, p. 172–204.
- [142] Frobenius, G. F.: Über die Grundlagen der Theorie der Jacobischen Functionen. *J. reine u. angew. Math.* **97** (1884), p. 188–223. Reproduit a *Gesammelte Abhandlungen II*, p. 205–240.
- [143] Frobenius, G. F.: Über die constanten Factoren der Thetareihen. *J. reine u. angew. Math.* **98** (1885), p. 244–263. Reproduit a *Gesammelte Abhandlungen II*, p. 241–260.
- [144] Frobenius, G. F.: Neuer Beweis des Sylowschen Satzes. *J. reine u. angew. Math.* **100** (1887), p. 179–181. Reproduit a *Gesammelte Abhandlungen II*, p. 301–303.
- [145] Frobenius, G. F.: Über die Congruenz nach einem aus zwei endlichen Gruppen gebildeten Doppelmodul. *J.*

- reine u. angew. Math.* **101** (1887), p. 273–299. Reproduit a *Gesammelte Abhandlungen II*, p. 304–330.
- [146] Frobenius, G. F.: Über vertauschbare Matrizen. *Söber. Akad. der Wiss. Berlin* (1896), p. 601–614. Reproduit a *Gesammelte Abhandlungen II*, p. 705–718.
- [147] Frobenius, G. F.: Über Beziehungen zwischen den Primidealen eines algebraischen Körpers und den Substitutionen seiner Gruppe. *Söber. Akad. der Wiss. Berlin* (1896), p. 689–703. Reproduit a *Gesammelte Abhandlungen II*, p. 719–733.
- [148] Frobenius, G. F.: Über Gruppencharaktere. *Söber. Akad. der Wiss. Berlin* (1896), p. 985–1021. Reproduit a *Gesammelte Abhandlungen III*, p. 1–37.
- [149] Frobenius, G. F.: Über die Primfactoren der Gruppendeterminante. *Söber. Akad. der Wiss. Berlin* (1896), p. 1343–1382. Reproduit a *Gesammelte Abhandlungen III*, p. 38–77.
- [150] Frobenius, G. F.: Zur Theorie der linearen Gleichungen. *J. reine u. angew. Math.* **129** (1905), p. 175–180. Reproduit a *Gesammelte Abhandlungen III*, p. 349–354.
- [151] Frobenius, G. F.: Über Matrizen aus positiven Elementen. *Söber. Akad. der Wiss. Berlin* (1908), p. 471–476. Reproduit a *Gesammelte Abhandlungen III*, p. 404–409.
- [152] Frobenius, G. F.: Über Matrizen aus nicht negativen Elementen. *Söber. Akad. der Wiss. Berlin* (1912),

- p. 456–477. Reproduit a *Gesammelte Abhandlungen III*, p. 546–567.
- [153] Frobenius, G.F.: *Gesammelte Abhandlungen*, **I**, **II**, **III**. Edició a cura de J.-P. Serre. Springer Verlag, Berlín, Nova York, 1968, Vol. I: vii+650 p., Vol. II: ii+733 p., Vol. III: iv+740 p.
- [154] Frobenius, G.F.; Stickelberger, L.: Über Gruppen von vertauschbaren Elementen. *J. reine u. angew. Math.* **86** (1879), p. 217–262. Reproduit a *Gesammelte Abhandlungen I*, p. 545–590.
- [155] Frobenius, G.F.; Stickelberger, L.: Über die Addition und Multiplication der elliptischen Functionen. *J. reine u. angew. Math.* **88** (1880), p. 146–184. Reproduit a *Gesammelte Abhandlungen I*, p. 612–659.
- [156] Fuchs, L.: Zur Theorie der linearen Differentialgleichungen mit veränderlichen Coefficienten. *J. reine u. angew. Math.* **66** (1866), p. 121–160.
- [157] Fuchs, L.: Über eine Klasse von Functionen mehrerer Variabeln, welche durch Umkehrung der Integrale von Lösungen der linearen Differentialgleichungen mit rationalen Coefficienten entstehen. *J. reine u. angew. Math.* **89** (1880), p. 151–169.
- [158] Fuchs, L.: *Gesammelte mathematische Werke I*. Herausgegeben von Richard Fuchs und Ludwig Schlesinger. Erster Band. Abhandlungen (1858–1875). Redigirt von L. Schlesinger. Mayer & Müller. Berlín, 1904.
- [159] Fuchs, L.: *Gesammelte mathematische Werke II*. Herausgegeben von Richard Fuchs und Ludwig Schlesinger.

- ger. Zweiter Band. Abhandlungen (1875–1887). Redigiert von L. Schlesinger. Mayer & Müller. Berlín, 1906.
- [160] Fuchs, L.: *Gesammelte mathematische Werke III*. Herausgegeben von Richard Fuchs und Ludwig Schlesinger. Zweiter Band. Abhandlungen (1888–1902) und Reden. Redigiert von R. Fuchs. Mayer & Müller. Berlín, 1909.
- [161] Gauss, C.F.: *Disquisitiones arithmeticae*. Lipsiae, 1801. Traducció catalana: *Disquisicions aritmètiques*. Traducció i pròleg de Griselda Pascual Xufré. Societat Catalana de Matemàtiques, 1996. ISBN 84–7283–313–5.
- [162] Gauss, C.F.: Gauss'wissenschaftliches Tagebuch 1796–1814. Mit Anmerkungen herausgegeben von Felix Klein. *Math. Ann.* **57** (1903), p. 1–34.
- [163] Gimbert, J.: Les Matemàtiques de GOOGLE: l'algorisme PageRank. *But. Soc. Cat. Mat.* **26** (2011), n. 1, p. 29–55.
- [164] Girstmair, K.: Kroneckers Lösung der Pellischen Gleichung auf dem Computer. *Math. Semesterbericht* **53** (2006), p. 45–64.
- [165] González-Rovira, J.; González Jiménez, E.; Guàrdia, J.: Computations on modular jacobian surfaces. *Algorithmic Number Theory*, Lecture Notes in Computer Science, **2369** (2002), p. 189–197.
- [166] Göpel, A.: Theoria transcendentium Abelianorum primi ordinis adumbratio levis, *J. für Math.*, **35** (1847).

- [167] Göttinger Digitalisierungszenter:
<http://gdz.sub.uni-goettingen.de/>
- [168] Gray, J. J.: Fuchs and the theory of differential equations. *Bull. Amer. Math. Soc.* **10** (1984), n. 1, p. 1–26.
- [169] Gray, J. J.: The Riemann-Roch theorem and geometry, 1854–1914. *Proceedings of the International Congress of Mathematicians, Vol. III (Berlin, 1998)*. Doc. Math. 1998, extra Vol. III, p. 811–822.
- [170] Gray, J. J.: *Linear differential equations and group theory from Riemann to Poincaré*. 2a. ed., Birkhäuser, 2008. ISBN: 978–0–81764–772–8.
- [171] Gross, B. H.; Zagier, D. B.: On singular moduli. *J. reine u. angew. Math.* **355** (1985), p. 191–220.
- [172] Gross, B. H.; Zagier, D. B.: Heegner points and derivatives of L -series. *Invent. Math.* **84** (1986), n. 2, p. 225–320.
- [173] Grothendieck, A.: Un théorème sur les homomorphismes de schémas abéliens. *Invent. Math.* **2** (1966), p. 59–78.
- [174] Grothendieck, A.: *Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas IV*. Inst. Hautes Études Sci. Publ. Math. **32** (1967), 361 p.
- [175] Grothendieck, A.: Le groupe de Brauer. III. Exemples et compléments. *Dix Exposés sur la Cohomologie des Schémas*. North-Holland, Amsterdam; Masson, Paris, 1968, p. 88–188.

- [176] Grothendieck, A.; et al.: *Théorie des Intersections et Théorème de Riemann-Roch* (SGA 6), 1966/67. LNM **225**, Springer Verlag, 1971.
- [177] Guàrdia, J.: Jacobian nullwerte and algebraic equations. *J. Algebra* **253** (2002), n. 1, p. 112–132.
- [178] Halberstam, H.; Richert, H-E.: *Sieve methods*. Academic Press, Londres, 1974, xiii+364 p.
- [179] Hamburger, M.: Bemerkungen über die Form der Integrale der linearen Differentialgleichungen mit veränderlichen Coefficienten. *J. reine u. angew. Math.* **76** (1873), p. 113–125.
- [180] Hasse, H.: Zum Hauptidealsatz der komplexen Multiplikation. *Monatsh. Math. Phys.* **38** (1931), n. 1, p. 315–322. *Mathematische Abhandlungen* **3**. Walter de Gruyter, 1975.
- [181] Hasse, H.: Ein Satz über die Ringklassenkörper der komplexen Multiplikation. *Monatsh. Math. Phys.* **38** (1931), n. 1, p. 323–330. *Mathematische Abhandlungen* **3**. Walter de Gruyter, 1975.
- [182] Hasse, H.: Das Zerlegungsgesetz für die Teiler des Moduls in den Ringklassenkörpern der komplexen Multiplikation. *Monatsh. Math. Phys.* **38** (1931), n. 1, p. 331–344. *Mathematische Abhandlungen* **3**. Walter de Gruyter, 1975.
- [183] Hasse, H.: Existenz separabler zyklischer unverzweigter Erweiterungskörper vom Primzahlgrade p über elliptischen Funktionenkörpern der Charakteristik p . *J. reine u. angew. Math.* **172** (1934), p. 77–85. *Math. Abhandlungen* **2**, p. 161–169.

- [184] Hasse, H.: Abstrakte Begründung der komplexen Multiplikation und Riemannsche Vermutung in Funktionenkörpern. *Abh. Math. Sem. Hamburg* **10** (1934), p. 325–348. *Mathematische Abhandlungen* **3**. Walter de Gruyter, 1975.
- [185] Hasse, H.: Zur Theorie der abstrakten elliptischen Funktionenkörper I. Die Struktur der Gruppe der Divisorenklassen endlicher Ordnung. *J. reine u. angew. Math.* **175** (1935), n. 1, p. 55–62. *Mathematische Abhandlungen* **3**. Walter de Gruyter, 1975.
- [186] Hasse, H.: Zur Theorie der abstrakten elliptischen Funktionenkörper II. Automorphismen und Meromorphismen. Das Additionsth. *J. reine u. angew. Math.* **175** (1935), n. 1, p. 151–182. *Mathematische Abhandlungen* **3**. Walter de Gruyter, 1975.
- [187] Hasse, H.: Zur Theorie der abstrakten elliptischen Funktionenkörper III. Die struktur des Meromorphismenrings. Die Riemannsche Vermutung. *J. reine u. angew. Math.* **175** (1935), n. 1, p. 151–182. *Mathematische Abhandlungen* **3**. Walter de Gruyter, 1975.
- [188] Hasse, H.: Der n -Teilungskörper eines abstrakten elliptischen Funktionenkörpers als Klassenkörper, nebst Anwendung auf den Mordell-Weilschen Endlichkeitssatz. *Math. Z.* **48** (1942), p. 48–66. *Mathematische Abhandlungen* **3**. Walter de Gruyter, 1975.
- [189] Hasse, H.: Zetafunktion und L -Funktionen zu einem arithmetischen Funktionenkörper vom Fermatschen Typus. *Abh. Deutsch. Akad. Wiss. Berlin., Kl. Math. Nat.* 1954, n. 4, 70 p. (1955). *Mathematische Abhandlungen* **3**. Walter de Gruyter, 1975.

- [190] Hasse, H.: *Mathematische Abhandlungen*. Band 1. Herausgegeben von Heinrich Wolfgang Leopoldt und Peter Roquette. Walter de Gruyter, Berlin, Nova York, 1975, xv+535 p.
- [191] Hasse, H.: *Mathematische Abhandlungen*. Band 2. Herausgegeben von Heinrich Wolfgang Leopoldt und Peter Roquette. Walter de Gruyter, Berlin, Nova York, 1975, xv+525 p.
- [192] Hasse, H.: *Mathematische Abhandlungen*. Band 3. Herausgegeben von Heinrich Wolfgang Leopoldt und Peter Roquette. Walter de Gruyter, Berlin, Nova York, 1975, x+532 p.
- [193] Haubrich, R.: Frobenius, Schur, and the Berlin algebraic tradition. *Mathematics in Berlin*. H.G.W. Begehr, ed. Springer Verlag, 1998, p. 83–96. ISBN: 978–3–76435–943–0.
- [194] Hawkins, T.: The origins of the theory of group characters. *Arch. Hist. Exact. Sci.* **7** (1971), p. 142–170.
- [195] Hawkins, T.: New light on Frobenius' creation of the theory of group characters. *Arch. Hist. Exact Sci.* **12** (1974), p. 217–243.
- [196] Hawkins, T.: Frobenius, Cartan, and the problem of Pfaff. *Arch. Hist. Exact Sci.* **59** (2005), p. 381–436.
- [197] Hawkins, T.: Frobenius and the symbolical algebra of matrices. *Arch. Hist. Exact Sci.* **62** (2008), p. 23–57.

- [198] Hawkins, T.: Continued fractions and the origins of the Perron Frobenius theorem. *Arch. Hist. Exact Sci.* **62** (2008), p. 655–717.
- [199] Hecke, H.: Über die Bestimmung Dirichletscher Reihen durch ihre Funktionalgleichung. *Math. Ann.* **112** (1936), n. 1, p. 664–699.
- [200] Hecke, H.: *Lectures on the theory of algebraic numbers*. Translated from the German by George U. Brauer, Jay R. Goldman and R. Kotzen. Graduate Texts in Mathematics, **77**. Springer Verlag, Nova York, Berlin, 1981, xii+239 p. ISBN: 0–387–90595–2.
- [201] Hecke, H.: *Lectures on Dirichlet series, modular functions and quadratic forms*. Edited by Bruno Schoeneberg. With the collaboration of Wilhelm Maak. Vandenhoeck & Ruprecht, Göttingen, 1983, 98 p. ISBN: 3–525–40727–0.
- [202] Hecke, H.: *Mathematische Werke*. With introductory material by B. Schoeneberg, C. L. Siegel and J. Nielsen. Third edition. Vandenhoeck & Ruprecht, Göttingen, 1983, 960 p. ISBN: 3–525–40729–7.
- [203] Herglotz, G.: Über das quadratische Reziprozitätsgesetz in imaginären quadratischen Zahlkörpern. *Ges. Werke*, p. 396–410. *FdM* **48** (1921/22).
- [204] Hermite, Ch.: *Œuvres complètes*. 4 volumes. Émile Picard, ed. Académie des sciences de France. Gauthier-Villars, 1905–1917.
- [205] Hilbert, D.: Einer neuer Beweis des Kronecker-schen Fundamentalsatzes über Abelsche Zahlkörper.

Nachr. K. Ges. Wiss. Göttingen (1896), p. 29–39.
Ges. Abh. I p. 53–62.

- [206] Hilbert, D.: *The theory of algebraic number fields*. Translated from the German and with a preface by Iain T. Adamson. With an introduction by Franz Lemmermeyer and Norbert Schappacher. Springer Verlag, Berlín, 1998, xxxvi+350 p. ISBN: 3-540-62779-0. Traducció del *Zahlbericht*, la primera edició del qual aparegué l'any 1897.
- [207] Hilbert, D.: *Gesammelte Abhandlungen*. Erster Band. Zahlentheorie. Julius Springer, Berlín, 1932, xiv+539 p.
- [208] Hilbert, D.: *Gesammelte Abhandlungen*. Zweiter Band. Algebra, Invariantentheorie, Geometrie. Julius Springer, Berlín, 1933, viii+453 p.
- [209] Hilbert, D.: *Gesammelte Abhandlungen*. Dritte Band. Analysis, Grundlagen der Mathematik, Physik, Verschiedenes. Nebst einer Lebensgeschichte. Julius Springer, Berlín, 1935, 435 p.
- [210] Hilbert, D.: *Gesammelte Abhandlungen*. Herausgegeben von J-P. Serre in 3 Bänden. Springer Verlag, Berlín, Heidelberg, Nova York, 1968, Band I: vii+650 p., Band II: iii+733 p., Band III: iv+740 p.
- [211] Hirzebruch, F.: *Neue topologische Methoden in der algebraischen Geometrie*. Zweite ergänzte Auflage. Ergebnisse der Mathematik und ihrer Grenzgebiete, N.F., **9**, Springer Verlag, Berlín, Göttingen, Heidelberg, 1962, vii+181 p.

- [212] Howard, R. A., ed.: *Dynamic Probabilistic Systems. Vol I: Markov Models*. Wiley, Nova York, 1971.
- [213] Igusa, J. I.: On the nullwerte of Jacobians of odd theta functions. *Symposia Mathematica XXIV. (Sympos., INDAM, Rome, 1979)*, p. 83–95. Academic Press, Londres, 1981.
- [214] Igusa, J. I.: On Jacobi's derivative formula and its generalizations. *Amer. J. Math.* **102** (1980), n. 2, p. 409–446.
- [215] Igusa, J. I.: Problems on abelian functions at the time of Poincaré and some at present. *Bull. Amer. Math. Soc. (N.S.)* **6** (1982), n. 2, p. 161–174.
- [216] Ihara, Y.: Schwarzian equations. *J. Fac. Sci. University of Tokyo* **21** (1974), p. 97–118.
- [217] Jacobi, C. G. J.: *Fundamenta nova theoria functionum ellipticarum*. Regiomonti, sumtibus fratrum Bornträger, Königsberg, 1829. Reproduït a *Gesammelte Werke* **I**. Berlín, 1881, p. 49–239. Chelsea, reimpressió, 1969.
- [218] Jacobi, C. G. J.: Allgemeine Theorie der kettenbruchähnlichen Algorithmen, in welchen jede Zahl aus drei vorhergehenden gebildet wird. *J. reine u. angew. Math.* **63** (1868), p. 29–64. Publicat pòstumament per E. Heine. Reproduït a *Werke* **6**, p. 385–426.
- [219] Jacobi, C. G. J.: *Gesammelte Werke*. 8 volums. Chelsea, 1969.

- [220] Jacquet, H.; Langlands, R. P.: *Automorphic forms on GL(2)*. Lecture Notes in Mathematics, **114**. Springer Verlag, Berlin, Nova York, 1970, vii+548 p.
- [221] Jaremkewycz; Mahrenholz; and Sprague, R. P.: Answer to problem 1242. *Z. Math. Naturwiss. Unterricht Schulgattungen* **68** (1937), p. 43; Proposed in **66** (1935), p. 251.
- [222] de Jong, R.: Explicit Mumford isomorphism for hyperelliptic curves. *J. Pure Appl. Algebra* **208** (2007), n. 1, p. 1–14.
- [223] Kaneko, M.; Zagier, D.: Supersingular j -invariants, hypergeometric series, and Atkin's orthogonal polynomials. *Computational perspectives on Number Theory*, p. 97–126. AMS/IP Stud. Adv. Math. **7**. Amer. Math. Soc., Providence, RI, 1998.
- [224] Katz, N. M.; Mazur, B.: *Arithmetic moduli of elliptic curves*. Annals of Mathematics Studies **108**. Princeton University Press. Princeton, NJ, 1985, xiv+514 p. ISBN: 0-691-08349-5; 0-691-08352-5.
- [225] Kersten, I.: *Brauergruppen von Körpern*. Aspects of Mathematics, D6. Friedr. Vieweg & Sohn, Brunsvic, 1990, viii+176 p. ISBN: 3-528-06380-7.
- [226] Kitaev, A.; Korotkin, D.: On solutions of Schlesinger equations in terms of thetafunctions. *Int. Math. Res. Notices* **17** (1998), p. 877–905.
- [227] Klein, F.: Über die Transformation der elliptischen Functionen und die Auflösung der Gleichungen fünften Grades. *Math. Ann.* **14** (1879), p. 111–145.

- [228] Klein, F.: *Vorlesungen über das Ikosaeder und die Auflösung der Gleichungen vom fünften Grade*. Reprogr. Nachdr. der Ausg. Leipzig, Teubner 1884. Hrsg. mit einer Einf. und mit Kommentaren von Peter Slodowy. Birkhäuser, 1993. ISBN: 3-7643-2454-6.
- [229] Klein, F.: *Gesammelte mathematische Abhandlungen. Erster Band: Liniengeometrie, Grundlegung der Geometrie, zum Erlanger Programm*. Herausgegeben von R. Fricke und A. Ostrowski (von F. Klein mit ergänzenden Zusätzen versehen). Reprint der Erst Auflagen [Verlag von Julius Springer, Berlin, 1921]. Springer Verlag, Berlín, Nova York, 1973, ii+xii+612 p.
- [230] Klein, F.: *Gesammelte mathematische Abhandlungen. Zweiter Band: Anschauliche Geometrie, Substitutionsgruppen und Gleichungstheorie, zur mathematischen Physik*. Herausgegeben von R. Fricke und H. Vermeil (von F. Klein mit ergänzenden Zusätzen versehen). Reprint der Erstauflagen [Verlag von Julius Springer, Berlin, 1922]. Springer Verlag, Berlín, Nova York, 1973, ii+vii+713 p.
- [231] Klein, F.: *Gesammelte mathematische Abhandlungen. Dritter Band: Elliptische Funktionen, insbesondere Modulfunktionen, hyperelliptische und Abelsche Funktionen, Riemannsche Funktionentheorie und automorphe Funktionen, Anhang verschiedene Verzeichnisse*. Herausgegeben von R. Fricke, H. Vermeil und E. Bessel-Hagen (von F. Klein mit ergänzenden Zusätzen versehen). Reprint der Erstauflagen [Verlag

von Julius Springer, Berlin, 1923]. Springer Verlag, Berlín, Nova York, 1973, ii+ix+774+36 p.

- [232] Klein, F.: *Vorlesungen über die Entwicklung der Mathematik im 19 Jahrhundert*. GMW **24–25**. Springer, Berlín, 1926–1927. Reimpressió, Springer, 1979.
- [233] Klein, F.: *Vorlesungen über nicht-euklidische Geometrie. Neu bearbeitet von W. Rosemann*. GMW, **26**. Springer, Berlín, 1928.
- [234] Klein, F.: *Vorlesungen über die hypergeometrische Funktion gehalten an der Universität Göttingen im Wintersemester 1893/1894*. GMW **39**. Springer, Berlín, 1933.
- [235] Klein, F.: *Vorlesungen über die Theorie der elliptischen Modulfunktionen. Band I: Grundlegung der Theorie*. Ausgearbeitet und vervollständigt von Robert Fricke. Nachdruck der ersten Auflage. Bibliotheca Mathematica Teubneriana, **10**, Johnson Reprint Corp., Nova York; B. G. Teubner Verlagsgesellschaft, Stuttgart 1966, vol. I: xix+764 p.
- [236] Klein, F.: *Vorlesungen über die Theorie der elliptischen Modulfunktionen. Band II: Fortbildung und Anwendung der Theorie*. Ausgearbeitet und vervollständigt von Robert Fricke. Nachdruck der ersten Auflage. Bibliotheca Mathematica Teubneriana, **11**, Johnson Reprint Corp., Nova York; B. G. Teubner Verlagsgesellschaft, Stuttgart 1966, vol. II: xix+712 p.

- [237] Klein, F.; Fricke, R.: *Vorlesungen Über die Theorie der elliptischen modulfunktionen I und II*. Teubner Stuttgart, 1966. Reimpressió de 1890–1892.
- [238] Krazer, A.: *Lehrbuch der Thetafunktionen*. Chelsea, 1970. Primera edició: Leipzig, 1903.
- [239] Krazer, A.; Wirtinger, W.: Abelsche Funktionen und allgemeine Thetafunktionen. *Enzykl. Math. Wiss.* **II B.7** (1921), p. 604–873.
- [240] Kričever, I.M.: Elliptic solutions of the Kadomcev Petviavili equations, and integrable systems of particles. *Funktsional. Anal. i Prilozhen.* **14** (1980), n. 4, p. 45–54, p. 95.
- [241] Kronecker, L.: Über die algebraisch auflösbaren Gleichungen. *Monatsber. Akad. Berlin* (1853), p. 365–374; Werke **IV**, p. 3–11.
- [242] Kronecker, L.: Über die auflösung der Pellschen Gleichung mittels elliptischer Functionen. *Monatsberichte der Königlich Preussischen Akademie der Wissenschaften zu Berlin* (1863), p. 44–50.
- [243] Kronecker, L.: Über Abelsche Gleichungen. *Monatsber. Akad. Berlin* (1877), p. 845–851; Werke **IV**, p. 63–71.
- [244] Kronecker, L.: Carta a Dedekind del 15 de març de 1880. Werke **V**, p. 453–457.
- [245] Kronecker, L.: Zur Theorie der elliptischen Functionen. Recollit en *Leopoldt Kronecker's Werke*. Herausgegeben auf Veranlassung der preussischen Akade-

mie der Wissenschaften von K. Hensel. Vierter Band. Chelsea reprint, 1968, p. 345–495.

- [246] Kronecker, L.: *Leopold Kronecker's Werke*. Bände I–V. Herausgegeben auf Veranlassung der Königlich Preussischen Akademie der Wissenschaften von K. Hensel. Chelsea Publishing Co., Nova York, 1968, vol. I: ix+483 p., vol. II: viii+540 p., vol. III, Part I: vii+473 p., Part II: iii+215 p. (Parts I i II relligades com una de sola), vol. IV: x+508 p., vol. V: x+527 p.
- [247] Kronecker, L.: *Vorlesungen über Zahlentheorie*. Erster Band. Reprint. Springer Verlag, Berlín, Nova York, 1978, xvi+509 p. ISBN: 3-540-08277-8.
- [248] Kummer, E.: De generali quadam æquatione differentiali tertii ordinis. *Liegnitz Gymnasium* 1834. Publicat posteriorment a *J. reine u. angew. Math.* **100** (1887), p. 1–9. Collected papers, **II**, p. 33–39.
- [249] Kummer, E.: *Collected papers. Volume I: Contributions to number theory*. Edited and with an introduction by André Weil. Springer Verlag, Berlín, Nova York, 1975, viii+955 p.
- [250] Kummer, E.: *Collected papers. Volume II: Function theory, geometry and miscellaneous*. Edited and with a foreword by André Weil. Springer Verlag, Berlín, Nova York, 1975, xi+877 p.
- [251] Lagrange, J.L.: Sur la construction des cartes géographiques. *Nouveaux Mémoires de l'Academie de Berlin*, 1779.

- [252] Laguerre, E.: Sur le calcul des systemes linéaires. *Journal École Polytechnique* **62** (1867). Reproduit a *Ceuvres* **1**, p. 221–267.
- [253] Lang, S.: *On quasi algebraic closure*. *Ann. of Math.* **55** (1952), p. 373–390.
- [254] Lange, H.; Birkenhake, C.: *Complex Abelian Varieties*. Springer Verlag, *GMW* **302**, 1992.
- [255] Langlands, R. P.: Modular forms and ℓ -adic representations. *Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, p. 361–500. *Lecture Notes in Math.*, **349**, Springer, Berlín, 1973.
- [256] Langlands, R. P.: Some contemporary problems with origins in the Jugendtraum. *Mathematical developments arising from Hilbert problems*. F. E. Browder, ed. *Proc. Sympos. Pure Math.* **28**, Northern Illinois Univ., De Kalb, Ill., 1974, p. 401–418. *Amer. Math. Soc.*, Providence, R. I., 1976.
- [257] Langlands, R. P.: Automorphic representations, Shimura varieties, and motives. Ein Märchen. *Automorphic forms, representations and L-functions*. *Proc. Sympos. Pure Math.*, Oregon State Univ., Corvallis, Ore., 1977, Part 2, p. 205–246, *Proc. Sympos. Pure Math.*, **28**, *Amer. Math. Soc.*, Providence, R.I., 1979.
- [258] Langlands, R. P.: *Base change for $GL(2)$* . *Annals of Mathematics Studies*, **96**. Princeton University Press, Princeton, N.J.; University of Tokyo Press,

Tòquio, 1980, vii+237 p. ISBN: 0-691-08263-4; 0-691-08272-3.

- [259] Lefschetz, S.: On certain numerical invariants of algebraic varieties with application to abelian varieties. *Trans. Amer. Math. Soc.* **22** (1921), n. 3, p. 327–406; **22** (1921), n. 4, p. 407–482.
- [260] Lefschetz, S.: Book Review: Vorlesungen über algebraische Geometrie. Geometrie auf einer Kurve, Riemannsche Flächen, Abelsche Integrale. *Bull. Amer. Math. Soc.* **28** (1922), n. 7, p. 365–366.
- [261] Lefschetz, S.: The early development of algebraic geometry. *Amer. Math. Monthly* **76** (1969), p. 451–460.
- [262] Lefschetz, S.: Reminiscences of a Mathematical Immigrant in the United States. *Amer. Math. Monthly* **77** (1970), n. 4, p. 344–350.
- [263] Lefschetz, S.: *Selected papers*. Chelsea Publishing Co., Bronx, N.Y., 1971, 639 p.
- [264] Legendre, A. M.: Recherches d'analyse indéterminée. *Histoire de l'Académie Royale des Sciences de Paris* (1785), p. 465–559, Paris, 1788.
- [265] Lemmermeyer, F.: *Reciprocity Laws: from Euler to Eisenstein*. Springer, 2000. ISBN: 3-540-66967-4.
- [266] Lemmermeyer, F.; Roquette, P.: *Helmut Hasse und Emmy Noether: Die Korrespondenz 1925–1935*. Edited and with commentary, and an introduction in English, by Franz Lemmermeyer and Peter Roquette. Universitätsverlag Göttingen, Göttingen, 2006, 301 p. ISBN: 3-938616-35-0.

- [267] Lenstra, H.W.: Solving the Pell equation. *Notices Amer. Math. Soc.* **49** (2002), n. 2, p. 182–192.
- [268] Manin, Yu. I.: The Hasse-Witt matrix of an algebraic curve. *Izv. Akad. Nauk SSSR Ser. Mat.* **25** (1961), p. 153–172.
- [269] Manin, Yu. I.: *Selected papers of Yu. I. Manin*. World Scientific Series in 20th Century Mathematics, **3**. World Scientific Publishing Co., Inc., River Edge, NJ, 1996, xii+600 p. ISBN: 981-02-2498-2.
- [270] Markov, A. A.: Rasprostranenie predelnykh teorem ischisleniya veroyatnostei na summu velichin svyazannykh v tsep. *Zap. (Mem.) Imp. Akad. Nauk St. Peterb. Fiz. Mat. Ser.* **8**, n. 3 (1908). Traducció anglesa de G. Petelin a [212].
- [271] Matsumoto, K.; Terasoma, T.: Degenerations of Triple Coverings and Thomae's Formula. Prepublicació, <http://arxiv.org/abs/1001.4868v1> (2010).
- [272] Mazur, B.: Modular curves and the Eisenstein ideal. *Inst. Hautes Études Sci. Publ. Math.* **47** (1977), p. 33–186.
- [273] Mazur, B.; Serre, J-P.: Points rationnels des courbes modulaires $X_0(N)$ (d'après A. Ogg). *Séminaire Bourbaki (1974/1975)*, Exp. n. 469, p. 238–255. *Lecture Notes in Math.*, **514**, Springer, Berlín, 1976.
- [274] Mestre, J.-F.: Moyenne de Borchardt et integrales elliptiques. *C. R. Acad. Sci. Paris Sér. I Math.* **313** (1991), p. 273–276.

- [275] Monna, A. F.: *Dirichlet's principle. A mathematical comedy of errors and its influence on the development of analysis*. Oosthoek, Scheltema & Holkema, Utrecht, 1975.
- [276] Molien, Th.: Über Systeme höherer komplexer Zahlen. *Math. Ann.* **41** (1893), p. 83–156.
- [277] Moroń, Z.: O Rozkładach Prostokatow Na Kwadraty. *Przeglad Mat. Fiz* **3** (1925), p. 152–153.
- [278] Mumford, D.: *Abelian varieties. With appendices by C. P. Ramanujam and Yuri Manin. Corrected reprint of the second (1974) edition*. Tata Institute of Fundamental Research Studies in Mathematics, **5**. Tata Institute of Fundamental Research, Bombay; Hindustan Book Agency, Nova Delhi, 2008, xii+263 p. ISBN: 978-81-85931-86-9; 81-85931-86-0.
- [279] Mumford, D.: *Tata lectures on theta*. Vol. 2. Progress in Math. **43**. Boston, MA. Birkhäuser (1984).
- [280] Nakayashiki, A.: On the Thomae Formulae for Zn Curves. *Pub. Res. Inst. Math. Science* **33** (1997), n. 6, p. 987–1015.
- [281] Neukirch, J.: *Algebraische Zahlentheorie*. Springer, 1992. ISBN: 3-540-54237-6.
- [282] Noether, E.: Invarianten beliebiger Differentia-
lausdrücke. *Nachr. v. d. Ges. d. Wiss. zu Göttingen* (1918), p. 37–44. Reproduit a *Gesammelte Abhandlungen*, p. 240–247.

- [283] Noether, E.: Invariante Variationsprobleme. *Nachr. v. d. Ges. d. Wiss. zu Göttingen* (1918), p. 235–257. Reproduit a *Gesammelte Abhandlungen*, p. 248–270.
- [284] Noether, E.: *Gesammelte Abhandlungen*. [Collected papers]. Edited and with an introduction by Nathan Jacobson. With an introductory address by P. S. Alexandrov. Springer Verlag, Berlín, Nova York, 1983, viii+777 p.
- [285] North Dakota State University; American Mathematical Society: Mathematics genealogy project.
<http://genealogy.math.uni-bielefeld.de/genealogy/>
- [286] O'Connor, J. J.; Robertson, E. F.:
[http://www-history.mcs.st-andrews.ac.uk/](http://www-history.mcs.st-andrews.ac.uk/Biographies)
Biographies.
- [287] Ogg, A. P.: *Modular forms and Dirichlet series*. W. A. Benjamin, Inc., Nova York, Amsterdam, 1969., xvi+173 p.
- [288] Ogg, A. P.: Rational points on certain elliptic modular curves. *Analytic number theory (Proc. Sympos. Pure Math., Vol XXIV, St. Louis Univ., St. Louis, Mo., 1972)*, p. 221–231. Amer. Math. Soc., Providence, R.I., 1973.
- [289] Ogg, A. P.: Hyperelliptic modular curves. *Bull. Soc. Math. France* **102** (1974), p. 449–462.
- [290] Ogg, A. P.: Über die Automorphismengruppe von $X_0(N)$. *Math. Ann.* **228** (1977), n. 3, p. 279–292.
- [291] Ogg, A. P.: On the Weierstrass points of $X_0(N)$. *Illinois J. Math.* **22** (1978), n. 1, p. 31–35.

- [292] Ônishi, Y.: Determinant expressions for abelian functions in genus two. *Glasg. Math. J.* **44** (2002), n. 3, p. 353–364.
- [293] Ônishi, Y.: Determinant expressions for hyperelliptic functions. With an appendix by Shigeki Matsutani. *Proc. Edinb. Math. Soc.* (2) **48** (2005), n. 3, p. 705–742.
- [294] Osgood, W.F.: *Lehrbuch der funktionentheorie*. Leipzig, Berlín, Teubner, 1912–1932.
- [295] Oyono, R.: Non-hyperelliptic modular Jacobians of dimension 3. *Math. Comp.* **78** (2009), n. 266, p. 1173–1191.
- [296] Peirce, B.: Linear Associative Algebras. *Amer. J. Math.* **4** (1881), p. 97–215.
- [297] Perron, O.: Zur Theorie der Matrizen. *Math. Ann.* **64** (1907), p. 248–263.
- [298] Plans, B.: On Noether’s problem for central extensions of symmetric and alternating groups. *J. Algebra* **321** (2009), n. 12, p. 3704–3713.
- [299] Poincaré, H.: Mémoire sur les fonctions fuchsiennes. *Acta Math.* **1** (1882), n. 1, p. 193–294. Reproduit a *Œuvres d’Henri Poincaré*, vol. II, p. 169–257.
- [300] Poincaré, H.: Sur la réduction des intégrales abéliennes. *Bull. Soc. Math. France* **12** (1884), p. 124–143. Reproduit a *Œuvres d’Henri Poincaré*, vol. III, p. 333–354.

- [301] Poincaré, H.: Mémoire sur les fonctions zétafuchsien-
nes. *Acta Math.* **5** (1884), n. 1, p. 209–278. Reproduït
a *Œuvres d'Henri Poincaré*, vol. II, p. 402–462.
- [302] Poincaré, H.: Sur les fonctions abéliennes. *Acta
Math.* **26** (1902), n. 1, p. 43–98. Reproduït a *Œuv-
res d'Henri Poincaré*, vol. IV, p. 473–526.
- [303] Poincaré, H.: *Science et méthode*. Flammarion, 1908.
Traducció al castellà de M. García Miranda: *Cien-
cia y método*. Colección Austral **409**. Espasa Calpe,
1963.
- [304] Poincaré, H.: Fonctions modulaires et fonctions fuch-
siennes. *Ann. Fac. Sci. Toulouse Sci. Math. Sci.
Phys. (3)* **3** (1911), p. 125–149. Reproduït a *Œuvres
d'Henri Poincaré*, vol. II, p. 592–618.
- [305] Poincaré, H.: *Œuvres d'Henri Poincaré*. Gauthier-
Villars, onze volums publicats i reimpressos entre
1916 i 1965: vol. I, 1951; vol. II, 1952; vol. III, 1965;
vol. IV, 1950; vol. V, 1950; vol. VI, 1953; vol. VII,
1952; vol. VIII, 1952; vol. IX, 1954; vol. X, 1954;
vol. XI, 1956.
- [306] Poincaré, H.: *Œuvres. Tome II. Fonctions fuchsien-
nes*. With a preface and a biographical sketch of Poin-
caré by G. Darboux. Reprint of the 1916 original. Les
Grands Classiques, Gauthier-Villars. Éditions Jac-
ques Gabay, Sceaux, 1995, lxxiv+632 p. ISBN: 2-
87647-172-8.
- [307] Poincaré, H.; Picard, E.: Sur un théorème de Rie-
mann relatif aux fonctions de n variables indépen-
dentes admettant $2n$ systèmes de périodes. *Comptes ren-*

- des de l'Académie des Sciences* **97** (1883), p. 1284–1287. Reproduit a *Œuvres d'Henri Poincaré*, vol. IV, p. 307–310.
- [308] Ramírez Alfonsín, J. L.: *The Diophantine Frobenius Problem*. Oxford Univ. P., 2005.
- [309] Reid, C.: *Hilbert. With an appreciation of Hilbert's mathematical work by Hermann Weyl*. Springer Verlag, Nova York, Berlín 1970, xi+290 p.
- [310] Ribet, K. A.: Endomorphisms of semi-stable abelian varieties over number fields. *Ann. Math. (2)* **101** (1975), p. 555–562.
- [311] Ribet, K. A.: On ℓ -adic representations attached to modular forms. *Invent. Math.* **28** (1975), p. 245–275.
- [312] Ribet, K. A.: A modular construction of unramified p -extensions of $\mathbb{Q}(\mu_p)$. *Invent. Math.* **34** (1976), n. 3, p. 151–162.
- [313] Ribet, K. A.: Endomorphism algebras of abelian varieties attached to newforms of weight 2. *Seminar on Number Theory, Paris 1979–80*, p. 263–276. Progr. Math., **12**, Birkhäuser, Boston, Mass., 1981.
- [314] Ribet, K. A.: On modular representations of $\text{Gal}(\overline{\mathbb{Q}}|\mathbb{Q})$ arising from modular forms. *Invent. Math.* **100** (1990), n. 2, p. 431–476.
- [315] Richert, H.: Über Zerfällungen in ungleiche Primzahlen. *Math. Z.* **52** (1949), p. 342–343.
- [316] Riemann, B.: *Grundlagen für eine allgemeine Theorie der Functionen einer veränderlichen*

- complexen Grösse*. [Inauguraldissertation, Göttingen, 1851; zweiter unveränderter Abdruck, Göttingen 1867.] Reproduit a *Gesammelte mathematische Werke und wissenschaftlicher Nachlass*, I. Transcribed by D. R. Wilkins, preliminary version: december 1998, corrected: april 2000. <http://www.maths.tcd.ie/pub/HistMath/People/Riemann/Grund/Grund.pdf>
- [317] Riemann, B.: Allgemeine Voraussetzungen und Hilfsmittel für die Untersuchung von Functionen unbeschränkt veränderlicher Grössen. *J. reine u. angew. Math.* **54** (1857), p.101–104. Reproduit a *Gesammelte mathematische Werke und wissenschaftlicher Nachlass*, VI, 1.
- [318] Riemann, B.: Lehrsätze aus der analysis situs für die Theorie der Integrale von zweigliedrigen vollständigen Differentialen. *J. reine u. angew. Math.* **54** (1857), p.105–110. Reproduit a *Gesammelte mathematische Werke und wissenschaftlicher Nachlass*, VI, 2.
- [319] Riemann, B.: Bestimmung einer Function einer veränderlichen complexen Grösse durch Grenz- und Unstetigkeitsbedingungen. *J. reine u. angew. Math.* **54** (1857), p.111–114. Reproduit a *Gesammelte mathematische Werke und wissenschaftlicher Nachlass*, VI, 3.
- [320] Riemann, B.: Theorie der *Abel*'schen Functionen. *J. reine u. angew. Math.* **54** (1857), p.115–155. Reeditat a *Gesammelte mathematische Werke*. Teu-

- ber, 1892. Reproduit a *Gesammelte mathematische Werke und wissenschaftlicher Nachlass*, VI, 4.
- [321] Riemann, B.: Über die Anzahl der Primzahlen unter einer gegebenen Grösse. *Monatsberichte der Berliner Akademie* (Novembre, 1859), p. 145–153. Reproduit a *Gesammelte mathematische Werke*, editat per H. Weber. Teubner, Leipzig, 1892, p. 671–680. Reproduit a *Gesammelte mathematische Werke und wissenschaftlicher Nachlass*, VII.
- [322] Riemann, B.: *Gesammelte mathematische Werke*. H. Weber, ed. Teubner, Leipzig, 1892.
- [323] Riemann, B.: *Gesam. math. Werke; Nachtrage von M. Noether und W. Wirtinger*. Teubner, 1902. Reeditat per Dover, 1953.
- [324] Riemann, B.: *Gesammelte mathematische Werke und wissenschaftlicher Nachlass*. Dover Publications, Inc., Nova York, 1953, xix+558+viii+116 p.
- [325] Riemann, B.: *Riemanniana selecta*. Editada i amb un estudi introductori de José Ferreirós. Clásicos del Pensamiento. Consejo Superior de Investigaciones Científicas, Madrid, 2000, clvii+138 p. ISBN: 84-00-07910-8.
- [326] Ritter, E.: Die multiplicativen Formen auf algebraischem Gebilde beliebigen Geschlechtes mit Anwendung auf die Theorie der automorphen Formen. *Math. Ann* **44** (1894), p. 261–374.
- [327] Roch, G.: Über die Anzahl der willkürlichen Constanten in algebraischen Functionen. *J. reine u. angew. Math.* **64** (1865), p. 372–376.

- [328] Roquette, P.: *The Brauer-Hasse-Noether theorem in historical perspective*. Schriften der Mathematisch-Naturwissenschaftlichen Klasse der Heidelberger Akademie der Wissenschaften. Publications of the Mathematics and Natural Sciences Section of Heidelberg Academy of Sciences **15**. Springer Verlag, Berlin, 2005. vi+92 pp. ISBN: 3-540-23005-X.
- [329] Rosenhain, J. G.: Sur les fonctions de deux variables et à quatre périodes, qui sont les inverses des intégrales ultra-elliptiques de la première classe. *Mémoires couronnées et mémoires des savants étrangers, publiées par l'Académie royale des sciences, des lettres et des beaux-arts de Belgique* **XI** (1851), p. 362–468.
- [330] Rotger, V.: *Abelian varieties with quaternionic multiplication and their moduli*. Tesi. Dir. Pilar Bayer. Universitat de Barcelona, 2002.
- [331] Rotger, V.: On the group of automorphisms of Shimura curves and applications. *Compositio Math.* **132** (2002), n. 2, p. 229–241.
- [332] Rotger, V.: Quaternions, polarization and class numbers. *J. reine u. angew. Math.* **561** (2003), p. 177–197.
- [333] Rotger, V.: Modular Shimura varieties and forgetful maps. *Trans. Amer. Math. Soc* **356** (2004), n. 4, p. 1535–1550.
- [334] Sansone, G.; Gerretsen, J.: *Lectures on the Theory of Functions of a Complex Variable. II Geometric Theory*. Wolters-Noordhoff Publishing Groningen, 1969.

- [335] Santcliment, F.: *Summa de l'art d'Aritmètica*. Introducció, transcripció i notes a cura d'Antoni Malet, de l'original català *Suma de la art de Arismetica*, Barcelona, Pere Posa, 1482. Eumo Editorial, 1998. ISBN: 84-7602-350-2.
- [336] Schmidt, F.K.: Zur arithmetischen Theorie der algebraischen Funktionen I. *Math. Z.* **41** (1936), n. 1, p. 415–438.
- [337] Schmidt, F.K.: Zur arithmetischen Theorie der algebraischen Funktionen II. Allgemeine Theorie der Weierstraßpunkte. *Math. Z.* **45** (1939), n. 1, p. 75–96.
- [338] Schwarz, H.A.: Über diejenigen Fälle, in welchen die *Gaussische* hypergeometrische Reihe eine *algebraische* Function ihres vierten Elementes darstellt. *J. reine u. angew. Math.* **75** (1873), p. 292–335.
- [339] Selberg, A.; Chowla, S.: On Epstein's zeta-function. *J. reine u. angew. Math.* **227** (1967), p. 86–110.
- [340] Serre, J-P.: Local class field theory. *1967 Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965)*, p. 128–161. Thompson, Washington, D.C., 1967.
- [341] Serre, J-P.: *Corps locaux*. Hermann, 1968.
- [342] Serre, J-P.: *Abelian ℓ -adic representations and elliptic curves*. Benjamin, Nova York, Amsterdam, edited in collaboration with W. Kuyk and J. Labute; 2nd. ed. AK Peters, 1998, xvi+177 p. Primera edició, 1968.

- [343] Serre, J-P.: Facteurs locaux des fonctions zeta des variétés algébriques (définitions et conjectures). 1969/70 *Séminaire Delange-Pisot-Poitou: Théorie des Nombres*, Exp. 19. Secrétariat mathématique, Paris. *Œuvres. Collected Papers* **2**. Springer, 1986.
- [344] Serre, J-P.: Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.* **15** (1972), n. 4, p. 259–331.
- [345] Serre, J-P.: Représentations ℓ -adiques. *Algebraic number theory (Kyoto Internat. Sympos., Res. Inst. Math. Sci., Univ. Kyoto, Kyoto, 1976)*, p. 177–193. Japan Soc. Promotion Sci., Tôquio, 1977.
- [346] Serre, J-P.: Sur les représentations modulaires de degré 2 de $\text{Gal}(\overline{\mathbb{Q}}|\mathbb{Q})$. *Duke Math. J.* **54** (1987), n. 1, p. 179–230. *Œuvres. Collected Papers* **4**. Springer, 2000.
- [347] Serre, J-P.: *Œuvres. Vol. I, 1949–1959*. Springer Verlag, Berlín, 1986, xviii+596 p. ISBN: 3–540–15621–6.
- [348] Serre, J-P.: *Œuvres. Vol. II, 1960–1971*. Springer Verlag, Berlín, 1986, iv+740 p. ISBN: 3–540–15621–6.
- [349] Serre, J-P.: *Œuvres. Vol. III, 1972–1984*. Springer Verlag, Berlín, 1986, iv+728 p. ISBN: 3–540–15621–6.
- [350] Serre, J-P.: *Œuvres. Vol. IV, 1985–1998*. Springer Verlag, Berlín, 2000, viii+657 p. ISBN: 3–540–65683–9.

- [351] Serre, J-P.; Tate, J.: Good reduction of abelian varieties. *Ann. of Math.* (2) **88** (1968), p. 492–517.
- [352] Shafarevich, I. R.: *Basic Algebraic Geometry 2*. 2a. ed., Springer Verlag, 1994.
- [353] Shimura, G.: Correspondances modulaires et les fonctions ζ de courbes algébriques. *J. Math. Soc. Japan* **10** (1958), p. 1–28. Collected Papers, I. Springer, 2002–2003.
- [354] Shimura, G.: Construction of class fields and zeta functions of algebraic curves. *Annals of Math.* **85** (1967), p. 58–159. Collected Papers, II. Springer, 2002–2003.
- [355] Shimura, G.: *Introduction to the Arithmetic Theory of Automorphic Functions*. Iwanami Shoten and Princeton University Press, 1971.
- [356] Shimura, G.: *Abelian Varieties with Complex Multiplication and Modular Functions*. Princeton Mathematical Series **46**. Princeton University Press, 1998.
- [357] Shimura, G.: *Collected papers*. Vol. I, 1954–1966; Vol. II, 1967–1977; Vol. III, 1978–1988; Vol. IV, 1989–2001. Springer, 2002.
- [358] Shimura, G.; Taniyama, Y.: *Complex multiplication of abelian varieties and its applications to number theory*. Publications of the Mathematical Society of Japan, **6**. The Mathematical Society of Japan, Tôquio, 1961, xi+159 p.

- [359] Silverman, J.H.: *The arithmetic of elliptic curves*. GTM **106**, Springer Verlag. Berlín, Nova York, 1986. Segona edició ampliada, 2009.
- [360] Silverman, J.H.: *Advanced topics in the arithmetic of elliptic curves*. GTM **151**, Springer Verlag. Berlín, Nova York, 1995.
- [361] Smirnov, F.: Form factors, Deformed Knizhnik-Zamolodchikov equations and finite-gap integration. *Comm. Math. Phys.* **155** (1993), p. 459–487.
- [362] Sprague, R.P.: Über mathematische Kampfspiele. *Tôhoku Mathematical Journal* **41** (1935–36), p. 438–444.
- [363] Sprague, R.P.: Über ein elementares Variationsproblem. *Mat. Tidsskr. B, København* (1936), p. 96–98.
- [364] Sprague, R.P.: Bemerkung über ungerade vollkommene Zahlen. *Bol. Mat. Buenos Aires* **9** (1936).
- [365] Sprague, R.P.: Über zwei Abarten von Nim. *Tôhoku math. J.* **43** (1937), p. 351–354.
- [366] Sprague, R.P.: Ein Satz über Teilfolgen der Reihe der natürlichen Zahlen. *Math. Ann.* **115** (1937), p. 153–156.
- [367] Sprague, R.P.: Bemerkungen über gewisse Zahlfolgen. *Math. Z.* **44** (1938), p. 20–22.
- [368] Sprague, R.P.: Aufgabe 240. (Gestellt in Jber. Deutsche Math.-Verein. 47 (1937)) Lösungen von A. Stöhr, G. Lochs. *Jber. Deutsche Math. Verein.* **48** (1938), p. 53–55.

- [369] Sprague, R. P.: Beispiel einer Zerlegung des Quadrats in lauter verschiedene Quadrate. *Math. Z.* **45** (1939), p. 607–608.
- [370] Sprague, R. P.: Über die Zerlegung von Rechtecken in lauter verschiedene Quadrate. *J. reine u. angew. Math.* **182** (1940), p. 60–64.
- [371] Sprague, R. P.: Zur Abschätzung der Mindestzahl inkongruenter Quadrate, die ein gegebenes Rechteck ausfüllen. *Math. Z.* **46** (1940), p. 460–471.
- [372] Sprague, R. P.: Zur Theorie der Umfüll-Aufgaben. *Jber. Deutsche Math. Verein.* **49** (1940), p. 65–73.
- [373] Sprague, R. P.: Über Zerlegungen in ungleiche Quadratzahlen. *Math. Z.* **51** (1948), p. 289–290.
- [374] Sprague, R. P.: Über Zerlegungen in n -te Potenzen mit lauter verschiedenen Grundzahlen. *Math. Z.* **51** (1948), p. 466–468.
- [375] Stöhr, A.: Über Zerlegungen von Rechtecken in inkongruente Quadrate. *Schr. Math. Inst. Angew. Math. Univ. Berlin* **4** (1939), Part 5, p. 118–140.
- [376] Swinnerton-Dyer, H. P. F.: *Analytic theory of abelian varieties*. London Mathematical Society Lecture Note Series, **14**, Cambridge University Press, Londres, Nova York, 1974, viii+90 p.
- [377] Takagi, T.: *Collected papers*. With a preface by S. Iyanaga. Segona edició. Editat i amb un prefaci d'Iyanaga, K. Iwasawa, K. Kodaira and K. Yosida. Amb apèndixs d'Iyanaga, Iwasawa i Yosida. Springer Verlag, Tòquio, 1990, xvi+376 p. ISBN: 4-431-70057-9.

- [378] Takase, K.: A generalization of Rosenhain's normal form for hyperelliptic curves with application. *Proc. Japan. Acad.* **72** (1996), p. 162–165.
- [379] Taniyama, Y.: L -functions of number fields and zeta functions of abelian varieties. *J. Math. Soc. Japan* **9** (1957) p. 330–366.
- [380] Taylor, R; Wiles, A.: Ring-theoretic properties of certain Hecke algebras. *Ann. of Math.* **141** (1995), p. 553–572.
- [381] Teicher, M.: *On Emmy Noether. The heritage of Emmy Noether.* (Ramat-Gan, 1996), Israel Math. Conf. Proc. **12**. Bar-Ilan Univ., Ramat Gan, 1999, p. 1–3.
- [382] Thomae, C. J.: Beitrag zur Bestimmung von $\vartheta(0, 0, \dots, 0)$ durch die Klassenmoduln algebraischer Functionen. *J. reine u. angew. Math.* **71** (1870), p. 201–222.
- [383] Tsen, C.: Zur Stufentheorie der Quasi algebraisch Abgeschlossenheit kommutativer Körper. *J. Chinese Math. Soc.* **171** (1936), p. 81–92.
- [384] Umemura, H.: Solution of algebraic equations by theta constants. Apèndix a [279].
- [385] Vladut, S. G.: *Kronecker's Jugendtraum and modular functions.* Traduït del rus per M. Tsfasman. Studies in the Development of Modern Mathematics, **2**. Gordon and Breach Science Publishers, Nova York, 1991, x+411 p. ISBN: 2-88124-754-7.

- [386] Waerden, B.L. van der: *A History of Algebra. From al-Khwārizmī to Emmy Noether*. Springer Verlag, Berlín, 1985, xi+271 p. ISBN: 3-540-13610-X.
- [387] Waerden, B.L. van der: *Algebra*. Vol. I. Based in part on lectures by E. Artin and E. Noether. Traduït de la setena edició alemanya per Fred Blum i John R. Schulenberger. Springer Verlag, Nova York, 1991, xiv+265 p.
- [388] Waerden, B.L. van der: *Algebra*. Vol. II. Based in part on lectures by E. Artin and E. Noether. Traduït de la setena edició alemanya per John R. Schulenberger. Springer Verlag, Nova York, 1991, xii+284 p.
- [389] Waerden, B.L. van der: *Meine Göttinger Lehrjahre*. Amb un epíleg de Peter Roquette. Mitt. Dtsch. Math. Ver. 1997, **2**, p. 20–27.
- [390] Weber, H.: *Lehrbuch der Algebra*, Bde.I–II–III. Chelsea, 1895, 1896, 1908.
- [391] Weber, H.: Zur Theorie der zyklischen Zahlkörper, II. *Math. Ann.* **70** (1911), p. 459–470.
- [392] Wedderburn, J.H.M.: On hypercomplex numbers. *Proc. London Math. Soc.* **6** (1908), p. 77–118.
- [393] Weierstrass, K.: *Beitrag zur Theorie der Abel'schen Integrale*. 1849. Reeditat a *Math. Werke* **1**. Berlín, 1894.
- [394] Weil, A.: *Sur les courbes algébriques et les variétés qui s'en déduisent*. Actualités Sci. Ind., **1041** = Publ. Inst. Math. Univ. Strasbourg **7** (1945). Hermann et Cie., París, 1948, iv+85 p.

- [395] Weil, A.: *Foundations of Algebraic Geometry*. American Mathematical Society Colloquium Publications, **29**. American Mathematical Society, Nova York, 1946, xix+289 p.
- [396] Weil, A.: *Foundations of algebraic geometry*. American Mathematical Society, Providence, R.I. 1962, xx+363 p.
- [397] Weil, A.: *Variétés abéliennes et courbes algébriques*. Actualités Sci. Ind., **1064** = Publ. Inst. Math. Univ. Strasbourg **8** (1946). Hermann, Paris, 1948, 165 p.
- [398] Weil, A.: Numbers of solutions of equations in finite fields. *Bull. Amer. Math. Soc.* **55** (1949), p. 497–508. *Scientific works. Collected papers I*. Springer, 1979.
- [399] Weil, A.: Jacobi sums as “Größencharaktere”. *Trans. Amer. Math. Soc.* **73** (1952), p. 487–495. *Scientific works. Collected papers II*. Springer, 1979.
- [400] Weil, A.: Über die Bestimmung Dirichletscher Reihen durch Funktionalgleichungen. *Math. Ann.* **168** (1967), p. 149–156. *Scientific works. Collected papers III*. Springer, 1979.
- [401] Weil, A.: *Number theory. An approach through history. From Hammurapi to Legendre*. Birkhäuser Boston, Inc., Boston, MA, 1984, xxi+375 p. ISBN: 0-8176-3141-0.
- [402] Weil, A.: *Scientific works. Collected papers. Vol. I (1926–1951)*. Springer Verlag, Nova York, Heidelberg, 1979, xviii+574 p. ISBN: 0-387-90330-5.

- [403] Weil, A.: *Scientific works. Collected papers. Vol. II (1951–1964)*. Springer Verlag, Nova York, Heidelberg, 1979, xii+561 p. ISBN: 0–387–90330–5.
- [404] Weil, A.: *Scientific works. Collected papers. Vol. III (1964–1978)*. Springer Verlag, Nova York, Heidelberg, 1979, xii+465 p. ISBN: 0–387–90330–5.
- [405] Weil, A.: Prehistory of the zeta-function. *Number theory, trace formulas and discrete groups (Oslo, 1987)*, p 1–9. Academic Press, Boston, MA, 1989.
- [406] Weil, A.: On Eisenstein's copy of the Disquisitiones. *Algebraic number theory*. Adv. Stud. Pure Math. **17**, Academic Press, Boston, MA, 1989, p. 463–469.
- [407] Weil, A.: *Basic number theory*. Reimpressió de la segona edició (1973). Classics in Mathematics. Springer Verlag, Berlín, 1995, xviii+315 p. ISBN: 3–540–58655–5.
- [408] Weil, A.: *Elliptic functions according to Eisenstein and Kronecker*. Reimpressió de l'original de 1976. Classics in Mathematics. Springer Verlag, Berlín, 1999, viii+93 p. ISBN: 3–540–65036–9.
- [409] Weyl, H.: David Hilbert and his mathematical work. *Bull. Amer. Math. Soc.* **50** (1944), n. 9, p. 612–654.
- [410] Weyl, H.: *Raum, Zeit, Materie. Vorlesungen über allgemeine Relativitätstheorie*. Sechste, unveränderte Auflage, Springer Verlag, Berlín, Nova York, 1970, viii+338 p.
- [411] Weyl, H.: *Die Idee der Riemannschen Fläche*. Reimpressió de l'original alemany de 1913. Amb assajos de

- Reinhold Remmert, Michael Schneider, Stefan Hildebrandt, Klaus Hulek i Samuel Patterson. Editat i amb un prefaci i una biografia de Weyl de Remmert. Teubner-Archiv zur Mathematik. Supplement 5. B. G. Teubner Verlagsgesellschaft, Stuttgart, 1997, xxii+240 p. ISBN: 3-8154-2096-2.
- [412] Weyl, H.: *Algebraic theory of numbers*. Reimpressió de l'original de 1940. Princeton Landmarks in Mathematics. Princeton Paperbacks. Princeton University Press, Princeton, NJ, 1998, x+223 p. ISBN: 0-691-05917-9.
- [413] Weyl, H.: *Gesammelte Abhandlungen. Bände I, II, III, IV*. Herausgegeben von K. Chandrasekharan. Springer Verlag, Berlín, Nova York, 1968., Band I: vi+698 p., Band II: iv+647 p., Band III: iv+791 p., Band IV: ix+694 p.
- [414] Wiles, A.: Modular elliptic curves and Fermat's Last Theorem. *Ann. of Math.* **141** (1995), p. 443–551.
- [415] Yandell, B.H.: *The honors class. Hilbert's problems and their solvers*. A K Peters, Ltd., Natick, MA, 2002, x+486 p. ISBN: 1-56881-141-1
- [416] Yoshida, M.: *Fuchsian Differential Equations*. Max Planck Institut für Mathematik. Vieweg & Sohn, 1987.
- [417] Yui, N.; Zagier, D.B.: On the singular values of Weber modular functions. *Math. Comp.* **66** (1997), n. 220, p. 1645–1662.

- [418] Zagier, D.B.: *Zetafunktionen und quadratische Körper. Eine Einführung in die höhere Zahlentheorie*. Hochschultext, Springer Verlag, Berlin, Nova York, 1981, viii+144 p. ISBN: 3-540-10603-0.
- [419] Zagier, D.B.: Newman's short proof of the prime number theorem. *Amer. Math. Monthly* **104** (1997), n. 8, p. 705–708.
- [420] Zagier, D.B.: Traces of singular moduli. *Motives, polylogarithms and Hodge theory, Part I (Irvine, CA, 1998)*, p. 211–244. Int. Press Lect. Ser., **3**, I, Int. Press, Somerville, MA, 2002.

Part IV

Índexs

Índex de figures

Fig. 1: Superfícies simplement connexes	117
Fig. 2: Superfícies 2-múltiplement connexes . . .	117
Fig. 3: Superfícies 3-múltiplement connexes . . .	118
Fig. 4: Talls a la superfície	267
Fig. 5: Rectangle 32×33	623
Fig. 6: Rectangle 47×65	624
Fig. 7: Quadrat de costat 4205	625

Índex de taules

Taula 1: Els precursors	14
Taula 2: Orígens de les escoles de Göttingen i de Berlín	25
Taula 3: Arbre genealògic (1666–1845)	26
Taula 4: Arbres genealògics (1713–1950)	27
Taula 5: Una selecció de funcions zeta i funcions L	221
Taula 6: Una selecció de funcions zeta i funcions L (cont.)	222
Taula 7: Primers zeros de la funció zeta de Riemann	224
Taula 8: Altres zeros de la funció zeta de Riemann	224
Taula 9: Nombre de zeros de la funció zeta de Riemann	225

Índex antroponímic

- Abel, 21, 31, 34, 36, 41–44,
49, 61, 64, 65, 68–
70, 72, 76, 79, 81,
87, 89, 101, 102, 104–
106, 113, 123, 127,
140, 152, 161, 177,
180, 258, 273, 302,
357, 359, 368, 398,
407, 409, 481–483,
485, 487, 497, 502,
650
- Ackermann, 141, 673
- Ahlfors, 153, 677
- Albert, 188, 484, 677
- Albert de Prússia, 34, 638
- Alexandre V, 11, 638
- Anosov, 153, 685
- Arakelov, 260, 399, 687, 690
- Aristòtil, vi, 637
- Arnauld, 13, 639
- Arnold, 149, 685
- Arquimedes, 144, 243, 637
- Artin, 99, 147, 151, 157, 161,
164–166, 168–171, 177,
184, 186, 187, 191,
192, 220, 221, 484,
486, 505, 674
- Atkin, 503, 504, 682
- Bäcklund, 225, 658
- Babbage, 13, 649
- Bachelier, 45, 666
- Baker, 146, 686
- Baltzer, 296, 653
- Bauer, 608, 667
- Bayer, Pilar, ix, 689, 691
- Beethoven, 21, 647
- Beltrami, 145, 220, 657
- Bernays, 141, 202, 672
- Bernoulli, Jakob, 26, 55, 641
- Bernoulli, Johann, 26, 641
- Bernstein, 202, 668
- Berstein, 152, 669
- Berthelot, 503, 686
- Bessel, 24, 25, 35, 36, 47,
648
- Betti, 113, 483, 655
- Bianchi, 441, 661
- Bieberbach, 137, 151, 202,
671
- Biot, 50, 647

- Bismarck, 4, 5, 78, 652
 Bolibrukh, 153, 687
 Bolyai, Farkas, 21, 647
 Bolyai, János, 21, 650
 Bolza, 137, 662
 Borchardt, viii, 37, 38, 48,
 66, 67, 114, 129, 301,
 302, 313, 653
 Born, 219, 670
 Bose, 226, 673
 Bouquet, 73, 368, 654
 Bourbaki, 176, 685
 Boyle, 15, 640
 Brauer, 87, 159, 160, 168,
 171, 172, 175, 178,
 179, 181–183, 185,
 484, 675
 Braun, 203, 680
 Brent, 225, 686
 Breuil, 197, 688
 Brill, 121, 122, 125, 126, 658
 Briot, 73, 368, 653
 Brooks, 625, 680, 685
 Brouncker, 242, 640
 Brouwer, 139, 669
 Brown, 626, 682
 Burnside, 101, 103, 660

 Calogero, 88, 685
 Cantor, Georg, 32, 54, 61,
 67, 78, 80, 81, 130,
 143, 151, 241, 659
 Cantor, Moritz, 25, 655
 Capelli, 97, 661
 Cardano, 562, 638

 Carles Guillem Ferran, 8, 9,
 21, 22, 645
 Carles VI, 9, 642
 Carlitz, 222, 678
 Cartan, Élie, 89, 91, 156, 171,
 666
 Cartan, Henri, 80, 676
 Castelnuovo, 126, 665
 Cauchy, 72, 73, 91, 101, 103,
 113, 115, 271, 648
 Cayley, 75, 92, 93, 101, 102,
 654
 Chevalley, 161, 165, 181, 678
 Christoffel, 54, 655
 Churchill, 204, 667
 Clebsch, 35, 38, 54, 90, 91,
 124, 407, 656
 Cohen, 143, 684
 Cohn Vossen, 141, 675
 Connes, 222, 687
 Conrad, 197, 688
 Courant, 110, 134, 141, 166,
 202, 205, 672
 Crelle, 43, 48, 52, 53, 61, 66,
 67, 72, 82, 178, 249,
 301, 648

 Davis, 148, 684
 Deahna, 91, 653
 Debye, 166, 670
 Dedekind, viii, 25, 32, 52,
 54–56, 59, 69, 72, 81,
 87, 98, 99, 104, 105,
 109, 113, 114, 127–
 132, 140, 143, 173,

- 196, 221, 246, 301–
311, 313, 360, 361,
486, 488, 494, 507,
613, 656
- Dehn, 144, 202, 623, 669
- Deligne, 189, 220, 503, 686
- Deninger, 222, 688
- Descartes, Blanche, 625, 685
- Descartes, René, 13, 15, 639
- Deuring, viii, 27, 71, 167–
169, 180, 182, 187–
192, 194, 195, 198,
481, 482, 485–492,
494–505, 508, 510,
517, 524, 527, 530,
538, 544, 605, 608,
678
- Diamond, 197, 688
- Dickson, 157, 178, 667
- Dinghas, 27, 108, 678
- Diofant, 28, 37, 637
- Dirac, 105, 171, 676
- Dirichlet, 21, 25, 26, 28, 37,
47, 50–53, 55, 57–
60, 66, 82, 104, 107,
109, 112, 114, 118,
119, 123, 128, 130,
132, 140, 151, 152,
161, 198, 221, 227,
245, 249, 252, 255,
324, 650
- Dirksen, 27, 36, 47, 648
- Dogson, 94, 656
- Drobisch, 125, 650
- Dudeney, 622, 662
- Dyck, 101, 662
- Eichler, 491, 510, 605, 606,
680
- Einstein, 202, 226, 440, 467,
669
- Eisenstein, 52, 55, 57, 63,
66, 82, 86, 112, 148,
191, 655
- Elisabet Cristina, 9, 642
- Elisabeth Cristina, 10, 645
- Elisabeth von Holwede, 10,
645
- Encke, 25, 649
- Engel, 470, 663
- Enriques, 126, 666
- Epstein, 202, 206, 222, 667
- Eratòstenes, 243, 637
- Erdős, 198, 680
- Euler, 16, 19–22, 26, 29, 35,
36, 38, 40, 41, 44,
50, 59, 60, 128, 131,
132, 194, 212, 213,
223, 227, 242, 243,
246, 441, 442, 643
- Fagnano, 38, 642
- Faltings, 500, 503, 688
- Fay, 259, 401
- Felip V, 10, 642
- Fermat, 29, 42, 50, 54, 55,
140, 149, 196, 197,
242, 639
- Fitting, 169, 677
- Fokker, 445, 672

- Fontené, 96, 97, 659
- Fourier, 26, 45, 50, 52, 61,
215, 233, 261, 311,
396, 647
- Fraenkel, 143, 673
- Frederic Guillem II, 10, 645
- Frederic I, 11, 638
- Frederic I de Prússia, 4, 641
- Frederic II, 9, 10, 643
- Frege, 79, 659
- Freud, 202, 661
- Frey, 196, 197, 310, 686
- Fricke, 126, 131, 137, 310,
507, 663
- Friedrich Wilhelm IV, 37, 649
- Frobenius, viii, 25, 54, 61,
71, 73, 81–100, 102–
107, 109, 141, 156,
159, 219, 220, 395,
396, 400–402, 405,
483, 495, 659
- Fuchs, Lazarus, viii, 25, 54,
61, 71–77, 83, 84, 152,
153, 198, 259, 301–
307, 313, 314, 343,
344, 357–361, 363,
656
- Fuchs, Richard, 77, 667
- Fueter, 70, 71, 161, 162, 669
- Furtwängler, 137, 161, 179,
666
- Gödel, 143, 144, 677
- Göpel, 396, 652
- Galois, 21, 68, 98–102, 104,
129, 136, 137, 140,
149, 161, 162, 173,
174, 181, 182, 185,
186, 188, 190, 221,
439, 495, 498, 499,
505, 513, 519, 521,
523, 525, 529, 532,
534, 536, 552, 554,
583, 596, 610, 652,
689
- Gauss, 11, 21–25, 27–32, 34,
36, 40, 42, 44, 47,
51, 53–56, 59, 70, 72,
102, 104, 109, 112–
114, 116, 119, 127,
128, 130, 146–148,
151–154, 161, 191,
192, 205, 227, 238,
244, 260, 302, 306,
328, 336, 342, 486,
506, 507, 559, 648,
691
- Gelfond, 146, 677
- Georg August, 19, 642
- Gerling, 25, 27, 648
- Giorgi, 152, 683
- Gleason, 145, 681
- Godement, 222, 681
- Goethe, 21, 645
- Goldbach, 35, 147, 642
- Gordan, 27, 37, 38, 78, 124,
139, 166, 173, 407,
657
- Gordon, 261, 673

- Gourdon, 225
Gram, 225, 660
Green, 151, 649
Griffiths, 153, 686
Gross, 503, 687
Grothendieck, 127, 189, 220,
221, 503, 683
Grundy, 108, 622, 681
Gruyter, 49, 664
Guàrdia, ix, 690
Gudermann, 25, 44, 60, 649
Guillem II el Ric, 11, 638
Guillem II, Kàiser, 5, 663
Gutzwiller, 222, 225, 682

Hölder, 102, 663
Hadamard, 216, 217, 665
Hahn, 207, 669
Halberstam, 199, 683
Hales, 151, 688
Hamel, 145, 445, 668
Hamilton, 92, 93, 154, 156,
651
Hardy, 217, 668
Harnack, 150, 660
Hasse, 68, 71, 109, 148, 160,
161, 164, 165, 167,
168, 170–172, 177–
182, 184, 188, 189,
191–197, 202, 206,
220, 221, 481, 484–
488, 491, 492, 495,
497, 503, 505–507,
510, 511, 514, 516,
518, 577, 587, 593,
674, 716
Haubrich, 84
Hausdorff, 202, 206, 666
Hausen, 14, 27, 643
Hawking, 222, 686
Hecke, 27, 132, 147, 170, 171,
195, 221, 486, 672
Hegel, 21, 647
Heilbronn, 87, 678
Heine, 37, 77, 78, 80, 654
Heisenberg, 142, 203, 207,
219, 675
Helmholtz, 83, 84, 654
Hensel, 68, 170, 178, 202,
664
Herbrand, 168, 169, 171, 184,
185, 678
Herglotz, 188, 206, 445, 505,
507, 514, 669
Hermite, 55, 93, 148, 302–
305, 314, 319, 340,
342, 361, 655
Hesse, 35, 37, 441, 652
Heun, 449, 663
Hey, Käte, 222, 676
Hilbert, 11, 27, 35, 68, 109,
129, 130, 134, 136,
138–153, 161, 162,
166, 169, 170, 179,
188, 192, 206, 218–
220, 241, 261, 439–
441, 452, 474, 476,
478, 482, 623, 664
Hirzebruch, 126, 683

- Hitler, 5, 672
 Hodge, 221, 676
 Hopf, 87, 675
 Humboldt, Alexander Georg
 von, 10, 644
 Humboldt, Alexander von, 10,
 11, 24, 34, 37, 47,
 50, 51, 647
 Humboldt, Wilhelm von, 10,
 11, 33, 34, 647
 Hurwitz, 35, 85, 121, 137,
 485, 499, 663
 Hutchinson, 225, 665
 Huygens, 12–15, 640

 Igusa, 402, 682
 Iwasawa, 221, 681

 Jacobi, 21, 25, 27, 35–38, 42–
 47, 49, 51, 53, 60,
 61, 66, 77, 80, 82,
 90, 91, 95, 112, 123,
 189, 196, 207, 230,
 246, 258, 264, 302,
 344, 357, 363, 395,
 396, 398–401, 403,
 405, 407, 409, 482,
 483, 485, 497, 650
 Jacobson, 187, 679
 Jacquet, 221, 686
 Joachimsthal, 38, 48, 53, 654
 Jordan, 72, 75, 101, 136, 657

 Kästner, 20–23, 27, 125, 644
 Köthe, 168, 169, 181, 677
 Kadomstev, 261, 684

 Kaluza, 206, 671
 Kant, 21, 35, 644
 Katz, 503, 686
 Kepler, 151, 639
 Kersten, Ina, 183, 686
 Killing, 61, 156, 659
 Klein, 27, 101, 109, 126, 133–
 139, 144, 153, 156,
 166, 169, 174, 196,
 206, 222, 307, 310,
 360, 361, 440, 445,
 446, 452, 467, 472,
 474, 479, 659
 Kneser, Adolf, 446, 664
 Kneser, Hellmuth, 202, 674
 Knizhnik, 261, 688
 Knoblauch, 62, 661
 Koříněk, 608, 674
 Kodaira, 194, 680
 Koebe, 153, 670
 Kolmogorov, 146, 149, 676
 Korteweg, 261, 659
 Kovalevskaya, Sofia, 61, 660
 Krazer, 81, 401, 662
 Kronecker, vii, 26, 31, 34,
 52, 53, 56, 57, 59,
 61, 65–70, 72, 82, 83,
 86, 87, 91, 97–102,
 125, 129, 140, 148,
 161, 196, 241–247,
 249, 301, 303, 305,
 306, 311, 314, 481,
 501, 504, 515, 609,
 613, 655
 Krull, 168, 169, 176, 675

- Kummer, 25, 34, 38, 48, 52–56, 61, 65–67, 71, 72, 82, 86, 87, 102, 107, 114, 129, 140, 161, 311, 498, 652
- Kunth, 10, 646
- Lady Isabel, 622, 675
- Lagrange, 22, 26, 29, 36, 77, 90, 243, 244, 440–442, 448–452, 455, 457, 467, 470, 475, 645
- Laguerre, 92, 657
- Landau, 87, 166, 202, 668
- Lang, Fritz, 202, 673
- Lang, Serge, 170, 184, 683
- Laplace, 50, 60, 119, 220, 645
- Lasker, Else, 202, 666
- Lasker, Emanuel, 622, 666
- Laurent, 246, 652
- Lefschetz, 220–222, 483, 503, 671
- Legendre, 21, 29, 36, 39, 40, 42–44, 50, 51, 58, 59, 76, 147, 344, 492, 496, 501, 508, 511, 577, 590, 646
- Lehman, 225
- Lehmer, 225, 676
- Leibniz, Friedrich, 12, 14, 639
- Leibniz, Gottfried, 11–18, 26, 641
- Lemmermeyer, 170, 688
- Lenstra, 244, 687
- Leopoldt, 221, 683
- Lerch, 61, 663
- Lessing, 51, 644
- Lie, 136, 137, 145, 146, 156, 174, 221, 222, 439, 440, 445, 447, 453–455, 459, 463, 464, 468, 478, 658
- Lindemann, 27, 35, 137, 138, 146, 660
- Linné, 32, 643
- Lipschitz, 52, 656
- Listing, 25, 112, 127, 651
- Littlewood, 217, 671
- Lluís XIV, 13, 640
- Llull, 15, 17, 638
- Lorentz, 445, 660
- Lovelace, Ada, 14, 653
- Lune, 225
- Lusztig, 222, 686
- Möbius, 125, 215, 649
- Münchhausen, 19, 642
- Maass, 27, 679
- Maclaurin, 223, 643
- Malebranche, 13, 26, 640
- Mangoldt, 61, 217, 661
- Manin, 503, 685
- Maria Antonieta, 9, 646
- Maria Teresa, 9, 644
- Markov, 95, 96, 661
- Mascheroni, 213, 246, 645
- Maschke, 176, 661
- Matijasevich, 148, 687

- Matsumoto, 260
 Mayer, Johann Tobias, 24,
 27, 646
 Mayer, Tobias, 24, 644
 Mazur, 221, 310, 503, 685
 Meller, 225
 Mellin, 196, 661
 Mencke, 11, 14, 641
 Mendelssohn, Abraham, 51,
 648
 Mendelssohn, Fanny, 51, 68,
 651
 Mendelssohn, Felix, 51, 68,
 107, 651
 Mendelssohn, Joseph, 51, 647
 Mendelssohn, Moses, 51, 644
 Mendelssohn, Ottilie Ernes-
 tine, 53, 107, 654
 Mendelssohn, Rebecka, 51,
 53, 107, 652
 Merkurjev, 183, 688
 Mersenne, 14, 639
 Mertens, 222, 657
 Mestre, 260
 Mills, 441, 683
 Minkowski, 35, 56, 134, 136,
 139, 142, 148, 150,
 170, 664
 Mises, 202, 670
 Molien, 106, 156, 159, 663
 Montgomery, 145, 679
 Monturiol, 654, 690
 Moroń, 623, 676
 Moser, 88, 684
 Mozart, 21, 646
 Mumford, 81, 257, 259, 503,
 685
 Néron, 503, 682
 Nagata, 149, 683
 Nakayashiki, 261
 Napoleó, 4, 10, 13, 33, 647
 Napoleó III, 4, 651
 Nash, 152, 684
 Nehr Korn, 527, 679
 Netto, 101, 659
 Neugebauer, 110, 111, 206,
 674
 Neumann, Carl Gottfried, 35,
 77, 277, 656
 Neumann, Franz Ernst, 35,
 36, 649
 Neumann, John von, 142, 146,
 219, 676
 Newman, 218, 684
 Newton, 7, 12, 15, 22, 640
 Nielsen, 222, 672
 Noether, Emmy, viii, 27, 109,
 130, 131, 134, 141,
 149, 157, 160, 164–
 176, 178–184, 186–
 188, 202, 205, 439–
 441, 443, 445, 484,
 670, 689
 Noether, Max, 121, 122, 125–
 127, 166, 401, 658
 Ocagne, 149, 664
 Odlyzko, 222, 223, 687
 Ogg, 310, 503, 684

- Olbers, 24, 646
Ore, 131, 675
Osgood, 126, 664
Ostrowski, 137, 673
- Pólya, 218, 672
Painlevé, 72, 664
Pascal, 13, 640
Pascual, Griselda, 29, 682, 691
Peano, 130, 143, 662
Peirce, Benjamin, 155, 651
Peirce, Charles, 155, 657
Pell, vii, 32, 57, 241–244, 249, 254, 255, 639
Pere I el Gran, 35, 641
Pere II, 35, 643
Perron, 94–96, 669
Petviashvili, 261, 685
Pfaff, 21, 23, 27, 90, 91, 93, 97, 646
Pfister, 151, 684
Picard, 72, 259, 662
Plücker, 27, 650
Plank, 207, 662
Poincaré, 16, 65, 72, 81, 150, 153, 310, 359–361, 661
Poisson, 21, 26, 50, 646
Posa, 7, 638
Prym, 54, 82, 401, 411, 658
Puiseux, 113, 654
Putnam, 148, 682
- Ragsdale, Virginia, 150, 666
- Ramanujan, 222, 672
Remón, ix
Reuter, 25, 653
Rey Pastor, 97, 672
Ribet, 185, 197, 310, 503, 687
Richelot, 37, 38, 651
Richert, viii, 27, 198, 199, 621, 622, 626, 631, 682
Riemann, vii, 25, 52, 65, 72–74, 78–80, 89, 109, 112–116, 118–133, 147, 152, 189, 192–195, 211–218, 220–227, 238, 261, 263, 264, 266, 267, 269, 273, 307, 326, 336, 344, 345, 360, 396, 401, 411, 432, 482–485, 487, 497, 505, 507, 516, 655
Riesz, 198, 671
Ritter, 126, 665
Robinson, Julia, 148, 681
Roch, 73, 125–127, 129, 193, 485, 497, 516, 657
Rockefeller, 169, 657
Roosevelt, 204, 670
Roquette, 170, 178, 196, 683
Rosati, 483, 484, 668
Rosenhain, 37, 259, 260, 292, 396, 399, 400, 409, 653
Rosser, 225, 678

- Rothe, 62, 667
 Rouché, 96, 97, 656
 Ruelle, 222, 685
 Runge, 61, 662

 Santcliment, 7, 638
 Sautoy, 226, 688
 Schönberg, 202, 667
 Schönlies, 54, 660
 Schönhage, 223, 685
 Schering, 27, 28, 78, 656
 Scherk, 25, 47, 53, 650
 Schiller, 21, 646
 Schilling, 169, 679
 Schlesinger, 77, 261, 665
 Schmidt, Erhard, 27, 627, 668
 Schmidt, Friedrich Karl, 126,
 191, 485, 505, 675
 Schmuck, Catherina, 12, 640
 Schneider, 146, 679
 Schooten, 14, 639
 Schottky, 61, 82, 153, 660
 Schrödinger, 142, 671
 Schröter, 38, 655
 Schubert, 150, 659
 Schumacher, 24, 648
 Schur, 86, 87, 175, 180, 202,
 668
 Schwarz, Elisabeth, 107, 658
 Schwarz, Hermann, 25, 54,
 61, 71, 76, 77, 82,
 107, 135, 337, 360,
 361, 658
 Schwarz, Ottilie, 664
 Scorza, 483, 485, 668

 Scott, Charlotte, 168, 662
 Segner, 20, 643
 Seidel, 37, 655
 Selberg, 220, 222, 225, 681
 Serre, 141, 161, 166, 190, 197,
 221, 310, 503, 682
 Severi, 150, 485, 669
 Shafarevich, 503, 682
 Shannon, 149, 680
 Shimura, 126, 190, 195–197,
 221, 310, 311, 503,
 684, 689
 Siegel, 86, 87, 148, 207, 223,
 397, 398, 673
 Skolem, 175, 671
 Smale, 222, 684
 Smirnov, 261
 Smith, 625, 681, 685
 Sobolev, 152, 678
 Speiser, 181, 185, 671
 Sprague, viii, 27, 107, 108,
 621, 622, 624–627,
 631, 633, 673
 Springer, 28, 141, 653
 Stöhr, 624, 627, 680
 Stark, 222, 678
 Stauffer, Ruth, 171, 679
 Steiner, 49, 66, 112, 649
 Steinitz, 176, 667
 Stern, 112, 651
 Stickelberger, 87, 88, 99, 102,
 660
 Stone, 625, 680, 685
 Suárez, 15, 639
 Sucarrats, Maria Teresa, ix

- Suslin, 183, 687
Swan, 174, 684
Swinnerton-Dyer, 503, 683
Sylow, 101–103, 656
Sylvester, 107, 652
- Takagi, 70, 71, 161–164, 668
Tamagawa, 222, 682
Taniyama, 190, 195–197, 503, 683
Tate, 161, 166, 184–186, 190, 221, 500, 503, 682
Taussky, Olga, 141, 165, 168–170, 677
Taylor, Brook, 401, 642
Taylor, Richard, 149, 197, 688
te Riele, 225, 687
Teichmüller, 202, 680
Teitelbaum, 221, 688
Terasoma, 260
Terras, 222, 686
Thomae, vii, 27, 77–81, 124, 257–261, 263, 400, 409, 657
Thomasius, Christian, 18, 641
Thomasius, Jakob, 14, 15, 18, 640
Titchmarsh, 225, 674
Toeplitz, 202, 670
Torelli, 260, 644
Travesa, ix, 690
Tschirnhaus, 13, 641
Tsen, 169, 674
Turing, 148, 203, 225, 680
- Tutte, 625, 681, 685
Txeboxev, 626, 631, 632, 654
Txeboxarev, 87, 101, 161, 190, 673
- Ulrich, 112, 649
Umemura, 259, 260, 686
- Vahlen, 202, 666
Vallée Poussin, 217, 218, 665
Voltaire, 19, 643
Vries, 261, 665
- Waerden, 150, 168, 169, 171, 188, 676
Walther, 203, 674
Weber, Heinrich, vii, 68–70, 101, 102, 114, 125, 129, 140, 161, 162, 196, 311, 336, 409, 501, 515, 516, 580, 583, 586, 609, 613, 614, 658
Weber, Werner, 169, 202, 536, 677
Weber, Wilhelm Eduard, 24, 112, 127, 650
Wedderburn, 156, 157, 159, 670
Wedeniowski, 225
Weierstrass, 34, 38, 44, 48, 53, 60–64, 66, 67, 71–73, 78, 79, 82–84, 86–88, 91, 114, 124, 125, 129, 155, 196, 302, 337, 396, 405, 407,

- 451, 482, 492, 511,
591, 653
Weil, 54, 81, 150, 168, 169,
171, 189–191, 194–
197, 220, 221, 225,
242, 396, 401, 402,
486, 503, 677
Weill, 202, 675
Weyl, 126, 150, 168, 170, 171,
205, 445, 671
Wichmannshausen, 14, 641
Wiles, 149, 190, 197, 687
Wirtinger, 401, 665
Witt, 156, 157, 168, 169, 171,
183, 492, 495, 503,
511, 679

Yang, 441, 681
Young, Grace, 134, 137, 665

Zagier, 503, 504, 687
Zamolodchikov, 261, 687
Zariski, 126, 149, 674
Zermelo, 77, 143, 667
Zippin, 145, 676
Zuse, 203, 679

