En el centenari de la mort de Leopold Kronecker (1823-1891)*

Griselda Pascual

El 23 de desembre de 1891 morí Leopold kronecker, figura molt rellevant en la recerca matemàtica del segle XIX. Aquest any es commemora, doncs, el centenari de la seva mort, i és per això que ens ha semblat escaient dedicar-li aquestes paraules, fent un breu recorregut per la seva vida i la seva obra.

Vida

Leopold Kronecker va néixer a Liegnitz (Prússia) el 7 de desembre de 1823. Fill d'una família jueva molt benestant, dedicada als negocis, rebé la primera educació del seu pare i d'un preceptor, Werner, que exerciren sobre ell una influència decisiva. En el «Gimnassium» va seguir sent deixeble de Werner, en les matèries de filosofia i teologia, i tingué la sort de trobar allà de professor de matemàtiques el gran Kummer, que va descobrir el seu talent per aquesta disciplina, li donà fins i tot lliçons particulars, injectant-li la droga de les matemàtiques que ja no abandonarà durant la resta de la seva vida. No es concentrà, però, Kronecker solament en aquesta ciència, sinó que estudià també filosofia, música i se l'escoltava com a crític d'art en pintura i escultura. Juntament a un gran talent, posseïa el do de l'amistat, que cultivava molt hàbilment.

A la primavera de 1841 va ingressar a la Universitat de Berlín on prengué contacte amb Dirichlet, Jacobi, Steiner i Eisenstein amb els quals va contraure amistat. Seguint el costum alemany, visità després altres universitats a Alemanya i restà molt temps a Bonn on de nou es trobà amb Kummer, que ocupava la càtedra de Matemàtiques, del qual no solament fou deixeble, sinó que n'esdevingué un gran amic. És aquí on decidí ja la seva dedicació a la teoria de nombres i, l'any 1845 a l'edat de vint-i-dos anys, escrigué la seva tesi doctoral *De unitatibus complexis*, referent a les unitats dels cossos ciclotòmics. Després d'això, una circumstància familiar fou la causa que durant vuit anys deixés, aparentment, la seva activitat matemàtica, i dic aparentment perquè encara que no publicà res, les seves aportacions deixen palès que ell no aban-

* Conferència pronunciada a l'acte inaugural del curs 1991-1992 de la Facultat de Matemàtiques de la Universitat de Barcelona.

donà mai el seu estudi. L'any 1845 morí un oncle seu, banquer ric, que el deixà encarregat d'administrar els seus béns, i Leopold hi dedicà tots els seus esforços. Dos anys més tard s'enamorà de la seva cosina, la filla del banquer, s'hi casà, tingueren sis fills, i casa seva es va convertir en un centre de reunió de científics, filòsofs, cultivadors de les belles arts, entre els quals se sap que hi era habitual el músic Meldelssohn. A més a més de viure feliç, tingué resolta per sempre la seva situació econòmica.

L'any 1883 sortí de nou a la llum la seva obra de recerca en matemàtiques. Com a membre de l'Acadèmia de Berlín, pogué accedir a donar, gratuïtament, conferències a la Universitat de Berlín i, des del 1861 fins al 1883, exposà en aquesta Universitat les seves investigacions matemàtiques, que es traduïren després en publicacions. No és fins l'any 1883, a causa de la jubilació del seu mestre Kummer, que pogué ocupar una càtedra a la Universitat de Berlín. A títol anecdòtic, direm que aquí va coincidir amb Weierstrass, i esdevingueren rivals de càtedra. El públic seduït per l'anàlisis i un xic espantat per la teoria de nombres, acudia a escoltar Weierstrass i deixava una mica buida l'aula de Kronecker, però ell feia com si no en fes cas i semblava feliç amb el seu auditori, poc nombrós però molt fidel, que fins i tot l'acompanyava a casa després d'acabada la classe. Aparentment Kronecker i Weierstrass eren amics, però és simptomàtic que a pesar del seu interès per les funcions el.líptiques no utilitzés mai la $\wp$ de Weierstrass en els seus treballs.

Tal com hem dit al principi, Leopold Kronecker morí a Berlín el 26 de desembre de 1981, víctima d'una pneumònia.

Es pot dir de Kronecker que la vida li va somriure. Fou un matemàtic d'ofici, si com a tal s'entén la definició que en dóna Dieudonne, és a dir, que és la persona que en la seva vida ha fet un teorema important, però va tenir la sort de no haver de viure de les matemàtiques.

Obra matemàtica

L'obra matemàtica de Kronecker, extensa, densa i de difícil lectura, va ser recollida i anotada per Hensel en una col.lecció de cinc volums. Voler comentar-la tota, seria d'una ambició inconcebible. És per això que hem escollit tres qüestions que considerem interessants, no solament pel fet d'haver estat tractades per primera vegada per Kronecker, sinó també perquè el seu estudi posterior ha estat de gran importància en la recerca en teoria de nombres, ja que ha donat lloc al plantejament de problemes alguns dels quals encara avui resten oberts. Aquestes són:

- el teorema de Kronecker-Weber
- el Somni de Joventud
- el grup de Galois de l'equació de divisió dels períodes de les funcions el.líptiques.

Per fer-nos una idea de com Kronecker va poder arribar a concebre aquestes

qüestions, ens ha semblat oportú recordar algunes de les grans aportacions a la recerca matemàtica dels segles XVIII i XIX relacionades amb elles i que Kronecker tenia davant seu. Citem:

- Les *Disquisitions Arithmaticae* de Gauss, on es troben, entre d'altres coses, demostracins de la llei de reciprocitat quadràtica, la teoria de les formes quadràtiques binàries enteres i la divisió de la circumferència en parts iguals.
- Els *treballs* d'Abel i de Galois sobre la resolució d'equacions algebraiques.
- Els *Fundamenta nova* de Jacobi, on, invertint la integral el·líptica de primera espècie de Legendre, s'introdueix la funció el·líptica *sin am*, i juntament amb ella *cos am* i Δam, creant la teoria de les funcions el·líptiques, de la qual destaquem les fórmules de multiplicació i divisió, i les fórmules de transformació.
- Els *treballs* de Kummer, principalment els referents a la descomposició en ideals primers en els cossos ciclotòmics dels ideals primer de $\mathbb{Q}$

1. Teorema de Kronecker-Weber

Tal com s'enuncia actualment diu:

Tota extensió abeliana de $\mathbb{Q}$ és ciclotòmica

és a dir, tota extensió abeliana de $\mathbb{Q}$ està continguda en un cos obtingut adjuntant a $\mathbb{Q}$ arrels de la unitat.

Generalment s'obté com una aplicació de la teoria global de cossos de classes. Cal notar, però, que si solament s'està en possessió de la teoria local de cossos de classes (que és més fàcil que la global), com a aplicació s'obté un teorema local de Kronecker-Weber, és a dir, que *tota extensió abeliana del cos $\mathbb{Q}_p$ dels nombres p-àdics és ciclotòmica*, i a partir d'aquest es passa al global utilitzant el comportament a $\mathbb{Q}(\mu_n)$ (on μ_n és el grup de les arrels n-èsimes de la unitat) dels ideals primer de $\mathbb{Q}$, i el teorema de Hermite-Minkowski que afirma que sobre $\mathbb{Q}$ tota extensió és ramificada.

Però a l'època de Kronecker no es coneixia la teoria de cossos de classes, ni tan sols Kronecker enuncià el teorema en el llenguatge de cossos.

La primera referència a aquest teorema es troba a [**Kr 1853**] amb l'enunciat següent:

Les arrels d'una equació abeliana amb coeficients racionals es poden expressar com a funcions racionals d'arrels de la unitat.

Una segona referència es troba a [**Kr 1877**] on diu:

Totes les arrels d'una equació abeliana amb coeficients enters són funcions racionals d'arrels de la unitat, i totes les funcions racionals de la unitat són arrels d'una equació abeliana entera.

La lectura dels dos enunciats fa pensar, a primera vista, que el que aporta de nou el segon respecte del primer és el fet que tota extensió de $\mathbb{Q}$ per arrels de la unitat és abeliana, i això mancaria d'interès perquè la seva demostració és fàcil; però no és així, ja que l'estudi d'ambdós articles posa de manifest que en el primer, quan Kronecker parla d'equació abeliana, es refereix a la que avui considerem una equació cíclica, mentre que en el segon el concepte d'equació abeliana es correspon amb l'actual. Per tant, el segon enunciat és més general que el primer.

1.1 Demostracions

Una demostració completa d'aquest teorema, Kronecker no la donà mai, però a [**Kr 1853**] en fa un intent en el cas cíclic de grau primer imparell, i la idea genial consisteix a utilitzar quocients adequats de les resolvents de Lagrange. La primera demostració, la donà Weber a [**We 1886**] aprofitant la idea de Kronecker, i és la que es troba també en el seu tractat d' Àlgebra [**We**] on el teorema està enunciat ja tal com es fa actualment. Aquesta demostració és llarga i laboriosa; a continuació n'indicarem, solament a grans trets, la línea seguida. Procedeix així:

En primer lloc, redueix el cas abelià al cas cíclic de grau una potència d'un primer p.

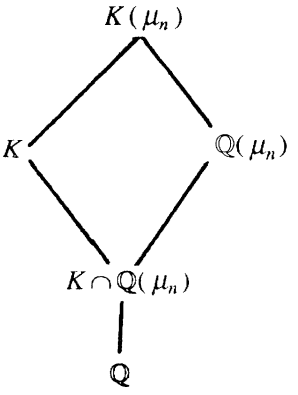
Ja en aquest cas, siguin: $f(x) \in \mathbb{Q}[x]$ un polinomi de grau $n = p^r$, $r \geq 1$ de grup de Galois G cíclic d'ordre n sobre $\mathbb{Q}$, i σ un generador de G; $z_0, z_1, \ldots, z_{n-1}$ les arrels de l'equació $f(x) = 0$ ordenades de manera que $z_{i+1} = \sigma(z_i)$; K el cos de descomposició de $f(x)$, és a dir, $G(K/\mathbb{Q}) = G$. Aleshores, seguint la idea de Kronecker, considera les resolvents de Lagrange

$$(\zeta_n^s, z_i) = z_i + z_{i+1}\zeta_n^s + \cdots + z_{i+n-1}\zeta_n^{(n-1)s} \qquad i = 0,1,\ldots,n-1,$$

on ζ_n és una arrel primitiva n-èsima de la unitat, els subíndexs de z estan calculats mòdul n, i s és un enter qualsevol. Sumant respecte a s s'obte:

$$nz_i = \sum_{s=0}^{n-1} (\zeta_n^s, z_i) \qquad i = 0,1,\ldots,n-1,$$

per tant, si es demostra que cada (ζ_n^s, z_i) $i = 0,1,\ldots,n-1$ pertany a un cos ciclotòmic es té demostrat el teorema. Per això Weber utilitza les extensions de cossos reflectides en el diagrama següent:



on μ_n és el grup de les arrels n-èsimes de la unitat. Les resolvents de Lagrange pertanyen al cos $K(\mu_n)$, i Weber construeix potències i quocients adequats d'aquestes resolvents de manera que els elements així obtinguts siguin del cos $\mathbb{Q}(\mu_n)$. Però en el seu raonament hi ha una llacuna, ja que el que fa és vàlid si $K \cap \mathbb{Q}(\mu_n) = \mathbb{Q}$, que és cert si $n = p$ és primer, però generalment no ho és si $n = p^r$ amb $r \geq 2$. Deixant a part aquesta llacuna, la resta del raonament és correcte. Ja situat a $\mathbb{Q}(\mu_n)$, utilitzant els resultats de Kummer sobre el comportament a $\mathbb{Q}(\mu_n)$ dels primers de $\mathbb{Q}$ i sobre les unitats dels cossos ciclotòmics, en el cas en què p és imparell aconsegueix provar, treballant molt, que les resolvents de Lagrange introduïdes pertanyen a un cos ciclotòmic que conté $\mathbb{Q}(\mu_n)$. El cas en què $p = 2$ requereix un tractament especial; necessita a més a més utilitzar que el nombre de classes d'ideals de $\mathbb{Q}(\mu_{2^r})$ és imparell, i això ho demostra a partir de la fórmula que dóna el nombre de classes d'ideals en els cossos ciclotòmics que s'obté aplicant els mètodes analítics de Dirichlet.

A Hilbert, aquesta demostració, encara que la dóna per correcta, no acaba d'agradar-li perquè no considera elegant fer servir resultats que s'obtenen per mètodes analítics per demostrar un teorema de caràcter purament algebraic. Hilbert a [**Hi 1896**], situant-se ja en el cas cíclic d'ordre una potència d'un primer p, en dóna una demostració per inducció sobre l'exponent de p, també llarga i laboriosa, totalment correcta, basada principalment en el comportament dels grups de ramificació, fent notar al principi que no utilitzarà ni els mètodes analítics de Dirichlet ni els teoremes de Kummer sobre els cossos ciclotòmics. En llegir-la, però, observem que fa servir el teorema de Minkowski sobre el discriminant dels cossos de nombres, és a dir, el teorema que afirma que sobre $\mathbb{Q}$ tota extensió algebraica és ramificada.

Weber replica a Hilbert amb una segona demostració [**We 1907**], que encara presenta la mateixa llacuna que la primera, en la qual aprofita la idea de la inducció, però sense utilitzar el teorema de Minkowski, ja que opina que aquest teorema tampoc té caràcter algebraic perquè la seva demostració es basa en els mètodes geomètrics.

Weber a [**We 1909**] en dóna encara una tercera demostració, i aquesta és ja totalment correcta.

El teorema enunciat per Kronecker, que avui es coneix amb el nom de «teorema de Kronecker-Weber» quedà finalmente demostrat, i alguns opinen que s'hauria d'anomenar «teorema de Kronecker-Hilbert-Weber», ja que a causa de la llacuna que presenten les dues primeres demostracions de Weber, fou Hilbert qui en donà la primera demostració correcta. Posteriorment, se n'han donat altres demostracions en què en general es fa ús del teorema de Minkowski abans citat.

1.2 Generalitzacions

L'intent de generalitzar el teorema de Kronecker-Weber a altres cossos ha donat lloc a un ampli i fructuós camp de recerca dins la teoria de nombres. En el breu recorregut que aquí farem de les generalitzacions obtingudes, per raons que es veuran posteriorment, no seguirem però un rigorós ordre cronològic. Començarem per les generalitzacions locals.

Ja hem dit anteriorment que el teorema de Kronecker-Weber és cert sobre el cos $\mathbb{Q}_p$ dels nombres p-àdics, i el podem enunciar de la manera següent:

L'extensió abeliana maximal de $\mathbb{Q}_p$ s'obté adjuntant a $\mathbb{Q}_p$ totes les arrels de la unitat.

El cos $\mathbb{Q}_p$ dels nombres p-àdics és un exemple de cos local. Un cos local és un cos complet per una valoració discreta, de cos residual finit. Els cossos locals de característica zero són les extensions finites de $\mathbb{Q}_p$. Per a aquests cossos locals, Lubin i Tate a [**Lu-Ta 1965**] donen un teorema que generalitza el de Kronecker-Weber, substituint les arrels de la unitat per uns nous elements que defineixen i que en el cas que el cos sigui $\mathbb{Q}_p$ coincideixen amb les arrels de la unitat. En línies generals procedeixen de la manera següent:

Sigui K un cos local de característica zero, $\mathcal{O}_K$ l'anell dels enters de K, π un uniformitzant de $\mathcal{O}_K$; seguint la definició de grups formals sobre O_K de Lubin [**Lu 1964**] defineixen els O_K-mòduls de Lubin-Tate i els grups $F(n)$ dels punts de π^n-divisió (que són els que corresponen amb els grups μ_n de les arres n-èsimes de unitat) i demostren el teorema següent:

L'extensió abeliana maximal K^{ab} d'un cos local K de característica zero és la composta de l'extensió no ramificada maximal K^{nr} de K i del cos $L_\pi = \bigcup_{n=1}^{\infty} L_n$ unió dels cossos $L_n = K(F(n))$ obtinguts adjuntant a K els grups $F(n)$ de punts de π^n-divisió.

Cercant de generalitzar el teorema de Kronecker-Weber sobre $\mathbb{Q}$ a altres cossos de nombres, o sigui tornant al cas global, el més natural és pensar en els cossos de nombres més senzills, és a dir, en els cossos quadràtics imaginaris, i això ens condueix novament a Kronecker i, precisament, a la segona qüestió que hem dit que tractaríem.

2. El somni de Joventut

Kronecker, al final de l'article ja citat [**Kr 1953**], on diu «les arrels de tota equació abeliana amb coeficients enters es poden expressar com a funcions racionals d'arrels de la unitat», afegeix:

També existeix la mateixa relació entre les arrels de les equacions abelianes els coeficients de les quals només contenen nombres complexos enters de la forma $a + b\sqrt{-1}$ *i les arrels de les equacions que apareixen en la divisió de la lemniscata; i el resultat anterior es pot generalitzar encara més enllà per a totes les equacions abelianes els coeficients de les quals contenen determinats nombres algebraics irracionals.*

És a dir, el que ens diu en primer lloc és que les arrels de les equacions abelianes els coeficients de les quals solament contenen enters de Gauss es poden expressar com a funcions racionals sobre $\mathbb{Q}(i)$ de les arrels de l'equació de la lemniscata, i després insinua que aquest resultat és generalitzable d'alguna manera a altres casos. A [**Kr 1877**] torna a referir-se a aquesta qüestió especificant ja que aquests altres casos als quals es pot generalitzar són les equacions abelianes els coeficiens de les quals solament contenen arrels quadrades de nombres enters negatius.

Finalment trobem *Der Brief* (La carta) que escriu Kronecker a Dedekind el 15 de març de 1880, desbordant d'alegria, en la qual li comunica que creu haver resolt l'última de les moltes dificultats de la investigació que l'ha tingut ocupat els darrers nou mesos. Diu:

...Es tracta del meu somni de joventut més estimat, és a dir, que les equacions abelianes amb coeficients arrels quadrades de nombres racionals poden exhaurir-se a través de les equacions de transformació de les funcions el.líptiques amb mòdul singular, de la mateixa manera que les equacions abelianes enteres amb les equacions ciclotòmiques.

És per això que aquest problema plantejat per Kronecker es coneix amb el nomb de Somni de Joventut. No es té però cap notícia de la demostració que Kronecker semblà tenir.

El comentari a *Der Brief* que apareix a les obres completes de Kronecker és fet per Hasse, i diu que la certesa o no d'aquesta afirmació feta per Kronecker depèn del que vulgui dir quan parla de mòduls singulars de funcions el.líptiques i de les mateixes funcions el.líptiques singulars.

Es pot pensar en què es basava Kronecker per fer aquesta conjectura; però donada la genialitat de Kronecker, i tenint en compte que a la vegada es preocupava de l'estudi de la multiplicació complexa de les funcions el.líptiques, introduïda ja per Jacobi, no resulta gens estrany, perquè el que sí és clar és que en referir-se Kronecker a funcions el.líptiques singulars pensava en les funcions el.líptiques amb multiplicació

complexa. Ens ha semblat, per tant, oportú fer a continuació una petita referència a la multiplicació complexa i a la seva relació amb els cossos quadràtics imaginaris.

2.1 Multiplicació complexa

Per fer més comprensible el concepte de multiplicació complexa ens hi referirem en primer lloc autilitzant el llenguatge actual, és a dir, parlarem de la multiplicació complexa en les corbes el·líptiques sobre el cos $\mathbb{C}$ dels nombres complexos.

Sigui $E = \mathbb{C}/\Lambda$ una corba el·líptica definida sobre $\mathbb{C}$ i $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ la seva xarxa de períodes. L'anell R d'endomorfismes de E és isomorf a un anell que conté $\mathbb{Z}$ i genèricament és isomorf a $\mathbb{Z}$; si R és isomorf a un anell més gran que $\mathbb{Z}$ es diu que E té multiplicació complexa. Aquest anell R està íntimament lligat a una extensió quadràtica imaginària de $\mathbb{Q}$, ja que si $\tau = \omega_1 / \omega_2$ és el quocient dels períodes que té part imaginària positiva, el cos $K = \mathbb{Q}(\tau)$ és una extensió quadràtica imaginària de $\mathbb{Q}$, i R és isomorf a un ordre del cos K que en particular pot ser l'anell dels enters de K. De la mateixa manera que en l'anell dels enters, es defineixen en un ordre les classes d'ideals que són també en nombre finit. Una corba el·líptica es diu que pertany a un ordre si el seu anell d'endomorfismes és isomorf a aquest ordre; dues corbes el·líptiques pertanyents a un mateix ordre són isomorfes si els ideals generats pels períodes respectius són de la mateixa classe. Cada classe d'ideals en l'ordre defineix una classe de cobres el·líptiques isomorfes i a cada classe se li associa l'invariant modular j.

En el llenguatge de Jacobi i de Kronecker en lloc de parlar de corbes el·líptiques es parla de funcions el·líptiques; en particular consideren la funció el·lípica *sin am* que depèn d'un mòdul κ i demostren que per a tot $n \in \mathbb{Z}$, *sin am nu* es pot expressar com a funció racional de *sin am u*. Però per a certs valors del mòdul κ els enters no són els únics nombres pels quals això es verifica, sinó que existeixen altres nombres complexos $\alpha \in \mathbb{C} / \mathbb{Z}$ pels quals també *sin am* αu es pot expressar com a funció racional de *sin am u*. Aquests mòduls es denominen mòduls singulars i les funcions el·líptiques corresponents, funcions el·líptiques singulars.

2.2 Després d'enunciar-se el Somni de Joventut

Des que Kronecker conjeturà el Somni de Joventut fins que se'n donà un enunciat correcte i una demostració, passa molt temps, però mentrestant es produí un esdeveniment matemàtic molt notable que va incentivar els matemàtics del segle XX a ocuparse'n. Fou la presentació per Hilbert en el Congrès International des Mathématiciens de París, de l'any 1900, de la seva "Col·lecció de Problemes", el 12 dels quals fa referència a la conjetura de Kronecker però proposada encara de forma més general. L'enunciat resumit d'aquest probleme és el següent:

Sigui k un cos de nombres, K una extensió abeliana finita de k. Es poden trobar "bones" funcions analítiques $\phi_1(z), \ldots, \phi_r(z)$ *dependent de k, tals que per a valors convenients* $z_i (i = 1, \ldots, r)$ *de z el cos K sigui isomorf a un subcos de* $k(\phi_1(z_1), \ldots, \phi_r(z_r))$.

Per exemple, en el cas que $k = \mathbb{Q}$ la solució del problema ens la dóna el teorema de Kronecker-Weber que hem exposat anteriorment amb la funció $\phi_1(z) = e^z$.

Una de les tasques dels matemàtics del segle XX és intentar resoldre els problemes proposats per Hilbert, entre ells el que acabem d'enunciar. Íntimament lligat amb aquest encara que en principi poden semblar distants, se'n troba un altre que fa referència a la generalització de la llei de reciprocitat quadràtica. Cercant de resodre aquest últim, Takagi construí la teoria global de cossos de classes, establint una correspondencia bijectiva entre els grups ideals d'un cos de nombres K i les extensions abelianes de K. A cada cos associat al grup corresponent n'hi digué cos de classes. L'any 1903 intentà comprovar la conjetura de Kronecker construint els cossos de classes del cos $K = \mathbb{Q}(i)$ i es trobà que si adjuntava a K solament arrels de la unitat i mòduls singulars de corbes el·líptiques tenia més grups que cossos, i per tant li calia fer altres adjuncions que eren precisament les coordenades dels punts d'ordre finit de les corbes el·líptiques. Posteriorment, a l'any 1920 provà el resultat corresponent per a un cos quadràtic imaginari qualsevol.

Aquest resultat, que és la forma correcta del Somni de Joventut, l'enunciarem en el llenguatge actual de la forma següent:

Sigui K un cos quadràtic imaginari, R l'anell dels enters de K, $\{\Lambda\}$ una classe d'ideals de R, $E = \mathbb{C}/\Lambda$ una corba el·líptica tal que End $E \simeq R$, $j(E)$ l'invariant modular. Aleshores:

a) $j(E)$ és algebraic sobre K

b) $K(j(E))$ és l'extensió no ramificada maximal de K

c) $K^{ab} = K(j(E);\ x_E(T),\ T \in E_{tor})$ on $x_E(z)$ es la funció de Weber

$$x_E(z) = \begin{cases} \dfrac{g_2 g_3}{\Delta}\,\wp(z,E) & si \quad \mathrm{j(E)} \neq 0, 1728 \\ \dfrac{g_2^2}{\Delta}\,\wp(z,E)^2 & si \quad \mathrm{j(E)} = 1728 \\ \dfrac{g_3}{\Delta}\,\wp(z,E)^3 & si \quad \mathrm{j(E)} = 0 \end{cases}$$

$$g_2(E) = 60 \sum_{\substack{\omega \in \Lambda \\ \omega \neq 0}} \omega^{-4} \qquad g_3(E) = 140 \sum_{\substack{\omega \in \Lambda \\ \omega \neq 0}} \omega^{-6}.$$

Amb les demostracions de Weber, en el cas en què el cos base és $\mathbb{Q}$, i de Takagi, en el cas en què és un cos quadràtic imaginari, tenim dos casos en què el problema 12 de Hilbert té resposta afirmativa.

Una nova aportació a la solució d'aquest problema ens la dóna Hecke que l'any 1913 construeix extensions abelianes no ramificades de cossos biquadràtics mitjançant valors singulars de funcions modulars de Hilbert de dues variables.

Altres progressos sobre aquesta qüestió no es troben fins l'any 1955 amb les aportacions de Shimura-Taniyama-Weil, recollides a [**Sh-Ta 1961**], i que no comentem perquè el seu contingut queda fora del que és el marc d'aquesta exposició.

3. Grup de Galois de l'equació de divisió dels períodes de les funcions el·líptiques

Ja hem fet notar en el paràgraf anterior que un dels temes de recerca de Kronecker era l'estudi de les funcions el·líptiques i de manera especial el de les equacions de multiplicació i divisió en aquestes funcions. Cal destacar dins d'aquest estudi la seva comunicació [**Kr 1875**] que comença de la manera següent:

L'afecte de les equacions de grau $\frac{1}{2}(n^2-1)$ *que tenen per arrels, en la notació de Jacobi, el quadrat de*

$$sin\,am\,\frac{(2mK+2m'K'i)}{n}$$

$$(0\le m\le n-1;\ 1\le m'\le\frac{n-1}{2}) \qquad (1\le m\le\frac{n-1}{2};\ m'=0)$$

encara, que jo sàpiga, no ha estat determinat, malgrat que aquesta determinació o, el que la terminologia de Galois es denominaria l'esbrinament del grup de l'equació, és manifest que té un significat molt fonamental per a la part algebraica de la teoria de les funcions el·líptiques. Naturalment, la investigació corresponent presentaria dificultats molt peculiars si no es disposés de cap punt de referència; però el resultat final es pot deduir quasi directament de dues comunicacions molt valuoses, que des de fa aproximadament mig segle es troben en una publicació d'Abel i en una de Jacobi, i el coneixement del contingut em va facilitar substancialment trobar el camí.

La lectura d'aquest treball de Kronecker presenta moltes dificultats que es poden, fins a cert punt, superar consultant d'una banda Jacobi i de l'altra Weber. Per això, abans d'intentar comentar-lo, donarem primer una breu idea del que ens diu Weber a [**We**] sobre aquesta qüestió.

Weber considera la funció el·líptica *sin am u* multiplicació complexa de mòdul κ i períodes $4K$, $4K'i$ i calcula la fórmula que determina *sin am nu*, $n\in\mathbb{Z}$ en funció de *sin am u*, fórmula qie ja havia estat calculada anteriorment per Jacobi.

Si n és un enter senar i es posa $x = sin\ am\ u$ aquestà fórmula té l'expressió següent:

$$sin\,am\,nu=\frac{xA(x^2)}{D(x^2)}$$

on $A(x^2)$ i D(x2) són polinomis sobre $\mathbb{Q}(\kappa^2)$ de graus $\frac{n^2-1}{2}$ i $\frac{n^2-2}{2}$ en x^2, respectivament. Si en aquesta expressió se substitueix *nu* per v s'obté l'equació de grau n en x.

$$D(x^2)\,sin\,am\,v=xA(x^2)$$

que s'anomena l'equació de divisió de la funció el·líptica *sin am v* i que té per arrels

$$x_{m,m'} = sin\ am\left(\frac{\upsilon}{n} + \frac{4Km + 4K'im'}{n}\right),$$

on m i m' recorren un sistema complet de classes de restes mòdul n. Si υ és un període $sin\ am\ \upsilon = 0$ i s'obté l'equació de divisió dels períodes

$$xA(x^2) = 0$$

que té per arrels

$$x_{m,m'} = sin\ am\ \frac{4Km + 4K'im'}{n},$$

on m i m' recorren un sistema complet de classes de restes mòdul n.

El problema que tracta Kronecker a [**Kr 1875**] és el de la determinació del grup de Galois del polinomi $A(x^2)$ com a polinomi en x^2 sobre el cos $\mathbb{Q}(\kappa^2)$. Del paràgraf que hem transcrit de l'article de Kronecker, se'n podria concloure que ell fou el primer matemàtic que s'ocupà d'aquestà qüestió, però en una nota al final d'aquest article el mateix Kronecker fa esment de resultats anteriors obtinguts per Sylow referents a aquest probleme. L'article consta de dues parts. En la primera retroba les anomenades relacions d'Abel (ja que fou Abel el primer a obtenir-les):

$$\sum_{m=0}^{n-1} e^{\frac{8mm'\pi i}{n}} x_{m,m'} = 0$$

$$\sum_{m'=0}^{n-1} e^{\frac{8mm'\pi i}{n}} x_{m,m'} = 0$$

que li són fonamentals per determinar el grup de Galois que cerca i demostra el resultat següent enunciat per Jacobi en una carta dirigida a Legendre i també en una comunicació al *Journal de Crelle* (1829):

...Suposant coneguts tots els mòduls en els quals es pot transformar un mòdul donat k mitjançant una transformació corresponent al nombre n, totes les quantitats de la forma $sin^2\ am\ \frac{2mK + 2m'iK'}{n}$ *, on m i m' son nombres qualssevol, es poden expressar per aquests mòduls sense que sigui necessari resoldre cap equació algebraica.*

En la segona part calcula l'ordre del grup de Galois del factor irreductible de l'equació $A(x^2)$ sobre $\mathbb{Q}(\kappa^2)$ quan n és un nombre senar qualsevol (el cas en què n és un nombre primer ja havia estat calculat per Galois) i relaciona el grup de Galois d'aquest factor amb el de l'equació de transformació d' ordre n.

Weber a [**We**] determina, d'una manera molt comprensible, el grup de Galois G

del polinomi $A(x^2)$ considerat com a polinomi en x sobre el cos $\mathbb{Q}(\kappa^2)$, quan n és un enter senar i la funció *sin am* corresponent a κ no té multiplicació complexa. Partint de les fórmules d'addició i multiplicació de *sin am* per enter, prova que G és un subgrup del grup $GL_2(\mathbb{Z}/n\mathbb{Z})$; per obtenir aquest subgrup, també com a Kronecker, li són fonamentals les relacions d'Abel que ja hem escrit anteriorment i que li serveixen per demostrar que el subgrup $SL_2(\mathbb{Z}/n\mathbb{Z})$ de $GL_2(\mathbb{Z}/n\mathbb{Z})$ està contingut a G i que coincideix precisament amb el grup de Galois del polinomi $A(x^2)$ com a polinomi en x sobre cos $\mathbb{Q}(\kappa^2,\zeta_n)$ i que l'anomena el grup de monodromia de l'equació de divisió. Després, seguint de nou la idea de Kronecker, calcula els ordres dels grups $SL_2(\mathbb{Z}/n\mathbb{Z})$ i $GL_2(\mathbb{Z}/n\mathbb{Z})$ i d'aquest càlcul en dedueix que el grup de Galois G cercat coincideix amb $GL_2(\mathbb{Z}/n\mathbb{Z})$. Finalment, observa que quan n és compost el polinomi $A(x^2)$ no és irreductible sobre $\mathbb{Q}(\kappa^2)$ i que el grup de Galois del factor irreductible és el mateix G. També, citant els resultats de Kronecker, relaciona el grup de Galois G amb el grup de Galois de l'equació de transformació.

Si es designa per K_n el cos de descomposició del polinomi $A(x^2)$ els resultats de Weber es poden resumir en el diagrama següent:

$$\begin{array}{lcl} & K_n & \\ GL_2(\mathbb{Z}/n\mathbb{Z}) & \mathbb{Q}(\kappa^2,\zeta_n) & SL_2(\mathbb{Z}/n\mathbb{Z}) \\ & \mathbb{Q}(\kappa^2) & (\mathbb{Z}/n\mathbb{Z})^* \end{array}$$

Actualment, els resultats de Weber es donen utilitzant el llenguatge de les corbes el·líptiques en lloc del de les funcions el·líptiques, i així es diu per exemple, el cos que s'obté adjuntant a $\mathbb{Q}(t)$ els punts de n-torsió d'una corba el·líptica definida sobre $\mathbb{C}$, etc.

La generalització d'aquest problema a un cos de nombres K es troba en l'article de Serre [**Se 1972**] en el qual entre altres coses demostra el resultat següent:

Sigui E una corba el·líptica sobre un cos de nombres K, sense multiplicació complexa, i E_l el grup dels punts de l-torsió amb l primer, llavors el grup de Galois de $K(E_l)$ sobre K és $GL_2(\mathbb{Z}/l\mathbb{Z})$ per quasi tots els nombres primers l.

Bibliografia

[**Hi 1896**] Hilbert, D., *Ein neuer Beweis des Kroneckerschen Fundamentalsatzes über Abelsche Zahlkörper*, Nachrichten der Gesellschaft der Wissenschaften zu Göttingen (1896), 29-39.

[**Kr 1853**] Kronecker, L., *Über die algebraisch auflösbaren Geichungen (I.Abhand-*

lung), Monatsberichte der Königlich Preussischen Akademie der Wissenschaften zu Berlín (1853), 365-374.

[**Kr 1875**] Kronecker, L., *Über die algebraischen Gleichungen, von denen die Theilung der elliptischen Functionen abhängt*, Monatsberichte del Königlich Preussischen Akademie der Wissenschaften zu Berlín (1875), 489-507.

[**Kr 1877**] Kronecker, L., *Über Abelsche Gleichungen*, Monatsberichte der Königlich Preussischen Akademie der Wissenschaften zu Berlín (1877), 845-851.

[**Lu 1964**] Lubin, J., *One-Parameter Formal Lie Groups Over* $\mathfrak{p}$ *- Adic Integer Rings*, Ann. of Math. **80** (1964), 464-484.

[**Lu-Ta 1965**] Lubin, J.; Tate, J., *Formal Complex Multiplications in local Field*, Ann. of Match. **81** (1965), 380-387.

[**Se 1972**] Serre, J-P., *Propiétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), 259-331.

[**Sh-Ta 1961**] Shimura, G; Taniyama, Y., *Complex Multiplications of Abelian Varieties and its Applications to Number Theory*, Math. Soc. Japan (1961).

[**We**] Weber, H., *Lehrbuch der Algebra.*

[**We 1886**] Weber, H., *Theorie der Abel'schen Zahlkörper. I Abel'sche Körper und Kreiskörper; II Über die Anzahl der Idealklassen und die Einheiten in der Kreiskörpern, deren Ordnung eine Potenz von 2 ist; III Der Kronecker'sche Satz*, Acta Math. **8** (1886), 193-263.

[**We1907**] Weber, H., *Über zyklische Zahlkörper*, J. reine angew. Math. **132** (1907), 167-188.

[**We 1909**] Weber, H., *Zur Theorie der zyklischen Zahlkörper*, Math. Annalen **67** (1909), 32-60.