Evariste Galois (1811-1832)

ELS INICIS DE LA TEORIA DE GRUPS

per

Pere Menal i Brufal

El concepte de grup que tenim actualment és segurament una de les primeres estructures abstractes que fou introduïda el segle XIX. En primera aproximació podríem dir que hi ha una sèrie de descobriments que s'inicien al final del segle XVIII i que condueixen a la teoria dels grups de substitucions fins a arribar a la primera definició de grup abstracte, que anà evolucionant donant lloc a la definició de grup que avui emprem. A partir d'aquest moment s'inicia la teoria de grups pròpiament dita.

Un dels problemes d'àlgebra més interessants durant la primera meitat del segle XIX era el de la resolució algèbrica de les equacions polinòmiques. De fet l'interès per aquesta qüestió és més antic però ara nosaltres passarem directament, i molt breument, a considerar alguns aspectes del treball de Lagrange (1736-1813) relacionat amb aquest problema. Lagrange considera l'equació general de grau n

$$a_0 + a_1 x + \ldots + a_n x^n = 0 \qquad (*)$$

volent dir que els coeficients a_0, a_1, ... són independents o "completament arbitraris"; aleshores ell tracta de resoldre l'equació (*) mitjançant una "fórmula", és a dir, vol expressar les arrels de l'equació en funció dels coeficients de manera que els únics irracionals que hi intervinguin siguin els radicals. Hom veu que aquest plantejament és, des del punt de vista actual, una mica imprecís, però no per això podem dir que no és rigorós, car el rigor depèn de l'època; així, pot succeir que plantejaments que actualment són rigorosos no ho siguin al proper segle.

La idea o mètode de Lagrange [16] per a resoldre l'equació general de grau n és la següent: escollir una funció f_0 racional de les arrels de l'equació (*) invariant per a totes les permutacions de les arrels (en total n!); aquesta funció f_0 convé que relacioni arrels amb coeficients; per exemple si x_1, ..., x_n són les arrels de l'equació (*) aleshores les funcions f_0 que Lagrange empra són $x_1 + x_2$, $x_1 + x_2 + x_3$, $x_1 x_2 + x_3 x_4$ quan $n = 2, 3$ i 4 respectivament. Ara es tracta de considerar una funció f_1 que no sigui fixa per a totes les permutacions de les arrels, diguem que f_1 pren m valors diferents. Aleshores una tal funció f_1 satisfà una equació de grau m on els coeficients d'aquesta eqüació són funcions racionals de f_0 i els coeficients

de l'equació (*). Si dóna la casualitat que l'equació de grau m que hom obté és resoluble per radicals, podríem expressar f_1 com a funció de f_0 i els coeficients de l'equació. En els casos n = 2, 3, 4, hom veu que f_1 s'expressa com a funció dels coeficients de l'equació general. Ara escollim una funció f_2 que no és fixa per a totes les permutacions que fixen f_1 ; aleshores, com abans, f_2 satisfà una equació de grau m_1 on els coeficients d'aquesta equació són funcions racionals de f_1 i els coeficients de l'equació (*); si aquesta equació és resoluble per radicals, podem expressar f_2 com a funció de f_1 i els coeficients de l'equació (*) i per tant obtenim f_2 com a funció només dels coeficients de l'equació (*). Continuant aquest procediment s'obtindrien funcions f_0, f_1, f_2, ... de manera que si l'última fos, per exemple, x_1, el problema seria resolt.

Aquest mètode portà Lagrange a la resolució de les equacions de grau 2, 3, 4. En el cas de $n \geqslant 5$ no tingué èxit i, cap als anys 1824-1826, Abel [1] demostrà que l'equació general de grau $n \geqslant 5$ no és resoluble per radicals. Malgrat que el mètode de Lagrange no donà els fruits esperats, hom pot dir que motivà el primer resultat de la teoria de grups de permutacions. Concretament, el mètode de Lagrange fa ús del següent resultat:

"Si $f(x_1, ..., x_n)$, $g(x_1, ..., x_n)$ són funcions racionals de les arrels de l'equació (*) tals que, per al conjunt de permutacions, τ, de $x_1, ..., x_n$ que deixen fixa la funció f, τg pren m valors distints, aleshores g és arrel d'una equació de grau m els coeficients de la qual són funcions racionals de f i dels coeficients de l'equació (*)."

Endemés, Lagrange demostrà que aquest nombre m és un divisor de n. Aquesta sembla que és la forma original de l'avui conegut Teorema de Lagrange; l'enunciat que actualment hom dóna del Teorema de Lagrange és: l'ordre d'un subgrup és un divisor de l'ordre del grup. Per a demostrar el resultat de Lagrange emprant el teorema en la forma últimament esmentada ho podem fer així: considerem les permutacions τ de S_n (el grup simètric de grau n) tals que $\tau g = g$; llavors és clar com aquestes permutacions constitueixen un subgrup, diguem H, de S_n. Ara bé, el nombre de valors distints, diguem m, que pren la funció g coincideix amb el nombre de classes de G mòdul H. Per tant $n = |H| m$. En temps de Lagrange hom encara no parlava de grups i per tant no es posà de manifest que H fos un subgrup del grup de permutacions S_n, però ben aviat, l'any 1799, quan Ruffini publicà el seu tractat (vegeu [20]) diu explícitament que H és un subgrup de S_n. Hem de dir també que Ruffini en el seu tractat introdueix nous conceptes dins la teoria de grups de substitucions: transitivitat, primitivitat, etc. Ruffini nota que si hom té un grup d'ordre n no sempre hi ha subgrups d'ordre m, per a un cert $m < n$; l'any 1803 és quan es donà a conèixer definitivament el teorema de Lagrange.

Si bé la teoria dels grups de substitucions és considerada com la preteoria de grups, no podem passar per alt el treball de Gauss sobre formes

quadràtiques. És clar que ara aquí no ens interessen directament els resultats que Gauss obté en formes quadràtiques, però sí que voldríem fer veure com aquest gran geòmetra és capaç de desenrotllar i intuir, en el cas que ell tracta, una gran quantitat de material que és situat actualment a la teoria de grups commutatius. L'any 1801 Gauss (1777-1855) publica un llibre titulat *Disquisitiones Arithmeticae*, amb tota una secció dedicada a l'estudi de "funcions de dues incògnites x, y de la forma $ax^2 + 2bxy + cy^2$" on a, b, c són nombres enters. Gauss anomena aquestes funcions formes quadràtiques o simplement formes. La forma és representada pel símbol (a,b,c). El mateix Gauss diu que el problema de trobar totes les solucions de les equacions de segon grau amb dues incògnites ha estat resolt per Lagrange, el qual endemés trobà d'altres resultats relatius a la naturalesa de les formes. Així, per exemple, Lagrange havia definit la composició de dues formes amb el mateix discriminant (recordem que el discriminant de la forma (a,b,c) és definit com $b^2 - ac$), i també dóna el concepte de formes equivalents, és a dir, existeix una substitució $x = \alpha x' + \beta y'$, $y = \gamma x' + \delta y'$, on α, β, γ, δ són nombres enters, i $(\alpha\gamma - \beta\delta)^2 = 1$ de manera que transforma una forma en l'altra. Aquesta relació és una relació d'equivalència en el conjunt de les formes del mateix discriminant (notem que mentre Lagrange empra el terme discriminant, Gauss parla de determinant).

Suposem que tenim dues formes (a,b,c), (a', b', c') amb el mateix discriminant; aleshores Gauss prova que existeix una substitució:

$$X = pxx' + p'xy' + p''yx' + p'''yy'$$
$$Y = qxx' + q'xy' + q''yx' + q'''yy',$$

amb la condició que els nombres pq'-p'q, pq''-p''q, pq'''-p'''q, p'q''-p''q', p'q'''-p'''q', p''q'''-p'''q'' són relativament primers i tal que

$$(ax^2 + 2bxy + cx^2)(a'(x')^2 + 2b'x'y' + c'(x')^2) = AX^2 + 2BXY + CY^2$$

on A, B, C són nombres enters.

La forma (A, B, C) és, per definició, la *composició* de les formes (a, b, c) i (a', b', c'). Gauss demostra que la composició de formes és compatible amb la relació d'equivalència definida anteriorment. Després en una sèrie de teoremes comprova que les classes de formes amb la composició tenen les propietats típiques d'un grup abelià; com que Gauss no disposa del llenguatge bàsic de la teoria de grups hom veu que alguns dels seus raonaments es repeteixen innecessàriament, la qual cosa fa que les comprovacions ocupin pàgines i pàgines; malgrat això és realment sorprenent veure la intuïció i subtilesa d'aquest gran matemàtic. Gauss observa com cada classe té una inversa [10] (p. 265) quan diu: si la classe K' es la oposada de la classe K (abans ell ha explicitat com hom pot construir l'oposada d'una classe),

K + K′ serà una classe principal amb el mateix determinant. A continuació demostra la unicitat de l'element neutre, en el seu cas particular, emprant el raonament habitual que hom fa en el cas general d'un grup qualsevol. Per exemple, la propietat associativa és enunciada en els següents termes: "si la forma F és la composta de les formes f, f′, la forma G, la de F i f″, la forma F′, la de f′, f″, i la forma G, la de F′ i f, aleshores les formes G i G′ són pròpiament equivalents".

Gauss associa a cada classe de formes uns "caràcters" i totes les formes amb un mateix caràcter defineixen un gènere; dit amb altres paraules, en aquest cas particular construeix un grup quocient.

Quan es tenen formes (a, b, c), (a′, b′, c′), (a″, b″, c″), ... on els primers termes a, a′, a″, ... són relativament primers, Gauss diu explícitament com se'n calcula la composició; recíprocament, si una forma (A, B, C) és tal que A es descompon com a producte de factors relativament primers, diguem $A = aa'a'' \ldots$, aleshores la forma (A, B, C) és la composició de formes del tipus (a, b, c), (a′, b′, c′), (a″, b″, c″) on b, b′, b″, ..., c, c′, c″, ... són calculats explícitament. Això fa pensar que Gauss tenia la idea del teorema d'estructura dels grups abelians finits, el qual teorema no fou demostrat per Kronecker [15] fins a l'any 1870.

Si bé el treball de Gauss pot ésser considerat com el primer on existeix la idea de grup abelià, el treball de Galois dóna un impuls considerable a la teoria de grups de permutacions introduint-hi nous conceptes i resultats. La major part de resultats obtinguts per Galois relatius a grups de permutacions (o substitucions) són motivats per la seva investigació sobre les equacions que són resolubles per radicals; el fet que l'equació general de grau $n \geqslant 5$ no és resoluble per radicals és ben conegut per Galois quan inicia aquesta investigació, és més, Galois [9] escriu: "és avui una veritat vulgar que les equacions generals de grau superior al 4^t no es poden resoldre per radicals..." Els resultats de les investigacions de Galois foren escrits per ell mateix en una sèrie de memòries, bé que aquest treball no fou conegut fins a l'any 1846, quan Liouville en publicà algunes parts. No és el nostre propòsit entrar ara a estudiar els resultats de Galois sobre equacions, més bé ens dedicarem a posar de manifest els conceptes i teoremes de grups que definitivament han quedat incorporats a la teoria.

Galois defineix el grup semblant com aquell "grup" generat quan s'opera sobre el grup G la substitució S; així doncs un grup semblant no és sinó la classe lateral GS. El teorema que dóna la descomposició d'un grup en classes laterals mòdul un subgrup és enunciat per Galois en els següents termes: si H és un subgrup contingut en el grup G, aleshores G és la suma d'un cert nombre de grups semblants a H, el qual hom diu que és un divisor de G. Notem, en particular, que es parla de suma i no d'unió: aquesta és una notació que encara es troba en llibres relativament moderns. Aquesta descomposició serveix a Galois per a resoldre equacions mitjançant

dues equacions sempre que la descomposició sigui pròpia, és a dir, dues descomposicions

$$G = H + HS + HS' + \ldots \qquad G = H + TH + T'H + \ldots$$

sempre coincideixen. Per tant, un subgrup dóna lloc a una descomposició pròpia si i només si és normal. En una lletra que Galois dirigeix al seu amic August Chevalier diu: si tenim una equació amb grup G el qual admet una descomposició pròpia, diguem amb m grups de n permutacions cadascun, aleshores l'equació corresponent es pot resoldre mitjançant dues equacions, una té un grup de m elements i l'altra un grup de n elements.

De la mateixa forma que el concepte d'isomorfisme de grups abelians es troba implícit en el treball de Gauss, també Galois té la idea d'isomorfisme de grups de permutacions. La composició o producte de grups és un altre dels conceptes que Galois introdueix; així (sense demostració) enuncia el següent teorema: sigui G un grup i suposem que les permutacions S_1, S_2, S_3, ... d'un altre grup H són tals que no fan sinó permutar entre si totes les permutacions del grup G; aleshores el conjunt de les permutacions $G + GS_1 + GS_2 + \ldots$ forma un grup que s'escriurà GH. Alguns d'aquests resultats que Galois enuncia sense prova foren demostrats posteriorment per altres matemàtics; així, per exemple, Cauchy (1789-1857) [4] demostra l'any 1844 que si un grup de permutacions té un ordre divisible per p^n, on p és primer, aleshores el grup té un subgrup d'ordre p, el qual resultat ja fou enunciat per Galois, i en aquest sentit hom pot dir que Galois "coneixia" els teoremes de Sylow. Un dels resultats més importants que Galois troba és la caracterització de les equacions resolubles per radicals com aquelles en què el grup corresponent es descompon (pròpiament) en un nombre primer de grups H semblants i idèntics, aquest H en un nombre primer de grups K semblants i idèntics i, així, fins a arribar a un cert grup M que no conté sinó un nombre primer de permutacions; un tal grup és actualment conegut sota la denominació de grup resoluble. Estudiant grups de permutacions de certes equacions particulars, Galois observa que llevat els grups d'ordre primer, el primer grup "indescomponible" (sense subgrups normals propis) té ordre 60, i aquesta sembla que és la primera vegada a la història que fan acte de presència els grups simples. L'estudi i la classificació dels grups simples ha constituït una de les àrees centrals de la teoria dels grups finits i ha estat objecte d'intenses investigacions; per bé que els resultats definitius no han estat publicats sembla que avui dia s'està a la recta final de la classificació.

Donada l'íntima relació entre la resolubilitat d'equacions i la teoria dels grups de permutacions hom pot fàcilment comprendre que la major part dels resultats de grups que foren descoberts la primera meitat del segle XIX eren enunciats amb termes de funcions racionals de les arrels de l'equació general de grau n. Ja hem vist que Lagrange enuncia el seu teorema en

aquest llenguatge, i podem també destacar el teorema de Cauchy que assegura que el nombre de distints valors d'una funció no-simètrica de n lletres no pot ésser inferior al primer més gran que divideix n! llevat del cas en què aquest sigui 2. Cauchy publica uns quants articles on sistematitza un cert nombre de conceptes i dóna nous resultats sobre primitivitat i transitivitat.

Després de la publicació duta a terme per Liouville sobre la teoria de Galois hi hagué un procés d'aclariment, car les memòries que Galois escriví, àdhuc la publicació de Liouville, no eren del tot intel·ligibles. En aquest procés d'aclariment és famós el curs que Serret donà a la Sorbona, que fou editat. Serret prova alguns resultats que milloren els obtinguts cinquanta anys abans per Cauchy. Un dels problemes que Serret planteja en una de les edicions del seu llibre, concretament l'any 1866, és el de trobar tots els grups que es poden formar amb n lletres; hom no té actualment la resolució completa d'aquesta qüestió, encara que hi ha resultats parcials. És interessant observar que la pregunta formulada per Serret ja surt fora de l'interès particular de la teoria d'equacions i així veiem com a poc a poc la teoria de grups comença a tenir sentit per ella mateixa i té interès independent.

Durant la primera meitat del segle XIX la teoria de grups que hom anava desenvolupant era un estudi dels grups de permutacions; sol succeir en Matemàtiques que quan una determinada teoria adquireix cos i els resultats són nombrosos, aleshores hi ha canvis de llenguatge i generalitzacions que ens ajuden (a vegades) a comprendre-la millor o simplement a simplificar les proves dels resultats. En el cas que ens ocupa és Cayley (1821-1895) qui, en una sèrie de treballs [5] durant els anys 1849-1854, observa com el concepte de grup de permutacions pot ésser generalitzat i introdueix la primera definició de grup finit abstracte. La definició que Cayley proposa encara no coincideix amb l'actual, car hem de tenir en compte que en aquells temps eren pocs els exemples de grups, llevat dels de permutacions, que hom coneixia i, en conseqüència, l'esperit dels grups de permutacions es continua manifestant a la definició de Cayley. És a dir, els elements del grup, a la definició de Cayley, són operadors sobre un conjunt (hem de dir que de la manera que Cayley ho escriu hom interpreta que els operadors són injectius) de manera que la composició de dos operadors del grup és del grup i a més l'operador identitat és del grup. És clar que si el conjunt sobre el qual actuen els elements del grup és finit, aleshores hom dedueix immediatament que cada element del grup té un invers, però si el conjunt és infinit això no pot ésser deduit en general, i per tant la definició de Cayley no correspon, en el cas infinit, amb el concepte actual de grup, en el qual exigim que cada element tingui un invers. La definició de Cayley no atragué l'atenció dels de l'època per bé que Cayley dóna exemples de grups que no són estrictament de permutacions; així, comprova que els quaternions (amb la suma) formen un grup; diguem que els quaternions foren descoberts per Hamilton l'any 1843 però tot i amb això sembla que no eren del domini

públic. Així doncs els treballs de Cayley d'aquesta època quedaren aïllats i per tant hom no pot considerar que aquest sigui el moment en què neix la teoria de grups abstractes. Diguem de passada que en el treball de Cayley de l'any 1854 hom troba el resultat avui conegut com teorema de Cayley: tot grup finit es representa com un grup de permutacions. Des d'un punt de vista formal hom podria pensar que el teorema de Cayley és el punt de partida de la teoria de representació de grups, però això sembla que no és cert, car l'origen de la representació de grups és motivat per un problema de Física. Concretament, un físic, Bravais (1811-1863), investiga certs grups de transformacions lineals a fi de determinar les possibles estructures dels cristalls; el treball de Bravais motiva en part les investigacions que Jordan (1838-1922) publicà en un article, l'any 1868, titulat *Memòria sobre els grups de moviments* (vegeu [13]). En aquest article hom tracta de classificar els moviments en el sentit que explicitem a continuació.

Hom sap que un moviment d'un cos sòlid a l'espai és un moviment helicoïdal i per tant per a conèixer el moviment n'hi ha prou amb tenir (i) la situació a l'espai de l'eix A de rotació i lliscament, (ii) l'angle de rotació del sòlid α al voltant de l'eix A i (iii) el desplaçament longitudinal t en el sentit de l'eix. Representem doncs el moviment mitjançant $A_{\alpha,t}$. Suposem que a un mateix cos sòlid li apliquem successivament dos moviments qualssevol $A_{\alpha,t}$, $A'_{\alpha',t'}$; aleshores el desplaçament resultant, representat per $A_{\alpha,t}A'_{\alpha',t'}$, és un moviment helicoïdal. Jordan apunta que la determinació de la "composició" de dos moviments helicoïdals és un problema ben conegut i diu que hom acostuma a resoldre'l en els cursos de Mecànica (almenys en el cas de moviments infinitament petits). El problema que Jordan es planteja és el següent: suposem que partim de certs moviments $A_{\alpha,t}$, $A'_{\alpha',t'}$, $A''_{\alpha'',t''}$, ... i hom tracta de trobar tots els moviments que resulten de la combinació d'aquests components-los successivament en nombre qualsevol i en qualsevol ordre. Jordan observa que el "grup" format per tots els moviments gaudeix de la propietat que, donats dos moviments qualssevol d'aquest grup, M', M'', el moviment M'M'' forma part del grup. Aquesta observació ens indueix a pensar que el concepte rigorós de grup encara no hi és, car el terme de grup és emprat a vegades en un sentit poc clar; així veiem clarament que Jordan aquí empra el terme de grup quan en realitat parla de monoides car no exigeix que l'invers d'un moviment del grup sigui del grup; naturalment, els grups de moviments que Jordan obté i que són finits sí que són grups en el nostre sentit.

Després d'aquest plantejament del problema, Jordan de manera equivalent presenta el problema d'una forma que ell considera més geomètrica: suposem que tenim una molècula situada en un punt qualsevol de l'espai, diguem-ne m, i arbitràriament orientada. Siguin m', m'', ... les diverses posicions de la molècula quan se li apliquen tots els moviments que formen part d'un grup donat, aleshores diem que aquest sistema de molècules és "superposat". El problema consisteix a trobar tots aquests sistemes super-

posats. És sota aquesta forma que Bravais estudia el problema i obté resultats en casos particulars que, tal com afirma Jordan, tenen les aplicacions més importants en la cristal·lografia.

Jordan obté 174 tipus de grups de moviments, dels quals n'hi ha 23 que s'anomenen principals de tal manera que els altres es relacionen amb els principals i són de dues espècies, la primera espècie està formada per aquells grups que es dedueixen d'un de principal fent els paràmetres infinitesimals, per exemple, un dels grups principals és el format (millor dit generat) per tres translacions amb direccions independents, i el grup que conté totes les translacions s'obté d'aquest suposant les tres translacions infinitament petites. La segona espècie la formen aquells grups que contenen una fracció determinada dels moviments que constitueixen un dels grups principals. Els grups de la segona espècie s'anomenen merièdrics; els grups merièdrics són doncs subgrups dels principals.

Els resultats de Jordan sobre els grups de moviments són l'inici dels estudis de transformacions geomètriques desenrotllats per exemple per Klein: la idea de Klein és que cada geometria és caracteritzada per un grup de transformacions i la geometria té relació amb els invariants sota el grup de transformacions. D'altra banda el treball de Jordan és la primera investigació feta en grups infinits.

La contribució de Jordan a la teoria de grups no es limita al treball esmentat sobre grups de moviments sinó que la part més important de la seva investigació és la relativa als grups de substitucions, els resultats de la qual foren inclosos en el seu tractat titulat *Tractat de les substitucions i les equacions algèbriques* (1870). En aquest llibre es fa un estudi profund sobre les idees donades per Galois. Així Jordan introdueix el concepte de grup quocient demostrant que cada grup finit té una sèrie de composició; aquests resultats li permeten resoldre un problema posat per Abel, el de trobar les equacions d'un grau donat que són resolubles per radicals i reconèixer si una equació pertany o no a aquesta classe. Les propietats de grup que usualment empra Jordan són: transitivitat o intransitivitat, primitivitat o imprimitivitat, grups simples i compostos.

Jordan es caracterizà per la seva capacitat d'abstracció i per la generalitat amb què planteja els problemes sabent que moltes vegades l'estudi restrictiu de casos parcials pot amagar les vertaderes raons de les coses. En aquest sentit, Jordan fou un gran algebrista. D'altra banda, Jordan està sempre disposat al càlcul efectiu si convé, cosa que es veu quan enumera els distints grups de moviments o els distints tipus de grups resolubles fins al grau 10^6.

Si bé els resultats de Jordan sobre grups primitius, transitius, etc., són importants, probablement el resultat més conegut de Jordan és el que es refereix a sèries de composició; bé que la invariància dels factors de comcomposició no fou observada per Jordan, fou Holder (1859-1937) qui,

l'any 1889, demostrà aquest fet. Aquests dos resultats són ara coneguts com a teorema de Jordan-Holder.

D'altres coses a destacar del tractat de Jordan són els conceptes d'homomorfisme i isomorfisme de grups que ell anomena "isomorfisme merièdric" i "isomorfisme holoèdric", com sempre sobre grups de permutacions, car les propietats de grup abstracte encara no són mencionades explícitament (som a l'any 1870), és a dir, quan hom parla de grup de permutacions hom vol dir que és una col·lecció de permutacions tals que el producte de dues permutacions de la col·lecció és de la col·lecció. Aleshores, tractant-se de permutacions (és a dir, aplicacions bijectives d'un conjunt finit) la propietat associativa és automàtica, i endemés l'invers d'una permutació coincideix amb una certa potència d'aquesta i, en conseqüència, pertany a la col·lecció. És a dir, l'existència d'un invers és també automàtica. Per tant, sembla natural que fos precisament l'axioma: "cada element té un invers" el que costà més d'abstreure per a donar lloc a la definició de grup abstracte.

Els grups de permutacions que corresponen a equacions resolubles per radicals estan constituïts a partir d'uns certs grups que Jordan anomena Abelians i que també són coneguts com els grups commutatius. Els grups commutatius també aparegueren a l'estudi de Dedekind de l'any 1878 sobre nombres algèbrics i el mateix Dedekind proposà una definició de grup commutatiu abstracte. Hem de notar que Dedekind [6] igual que Cayley donà l'any 1858 una definició de grup abstracte.

Un altre aspecte important del treball de Jordan és el relatiu a grups lineals. Motivat pels resultats sobre els grups de moviments i el treball de Bravais, Jordan investiga la representació de grups; en llenguatge modern això correspon a estudiar els morfismes d'un grup abstracte a un grup lineal (un grup de matrius sobre un cos). La representació de permutacions sobre grups lineals on el cos de coeficients és finit d'ordre primer fou considerada, per primera vegada, per Galois (és per això que Bourbaki diu que Galois descobrí els grups lineals sobre un cos finit). Malgrat això, podem dir que els primers teoremes sobre grups lineals són atribuïts a Jordan, que demostrà un primer teorema que és bàsic per a la teoria de representació: una matriu de període p (primer) és diagonalitzable.

Jordan investiga igualment els subgrups dels grups lineals sobre un cos primer finit, i en aquest sentit ell considera com a fonamental el seu estudi del grup ortogonal, la determinació dels factors de descomposició d'un grup lineal, etc... Aquests resultats són l'origen de l'estudi dels grups lineals clàssics que intervenen en moltes àrees de les matemàtiques. Els resultats de Jordan foren generalitzats per Dickson a un cos finit al començament del segle actual i no és fins molt més tard (l'any 1936) que la teoria de Jordan i Dickson s'establí per a un cos arbitrari.

Uns anys després de la publicació del tractat de Jordan foren demostrats els ara clàssics teoremes de Sylow. Recordem que Galois ja havia

enunciat, sense demostració, que si la potència d'un primer, p^n, divideix l'ordre del grup, aleshores el grup té un subgrup d'ordre p^n. Aquest resultat fou provat més tard per Cauchy i finalment Sylow [22] demostrà que els p-subgrups maximals d'un grup finit formen un sistema de subgrups conjugats. La demostració de Sylow és restringida als grups de permutacions, però cinc anys després, Frobenius demostrà els teoremes de Sylow per a grups finits abstractes.

Ja hem mencionat anteriorment com Klein, influït pels treballs de Jordan, nota com els grups infinits de transformacions s'empren per a la classificació de geometries. Aquests grups de transformacions s'anomenen *continus*, és a dir, són grups que depenen d'un o alguns paràmetres que poden prendre tots els valors reals, per exemple el grup de transformacions del pla complex format per totes les translacions i representat per:

$$z' = z + b \qquad \text{on b és una constant.}$$

Un altre tipus de grups apareix en l'estudi de les funcions automorfes dut a terme per Klein i Poincaré. Les funcions automorfes es poden considerar com una generalització de les funcions circulars i les funcions el·líptiques. Recordarem a continuació molt ràpidament com sorgeixen les funcions el·líptiques.

Durant el segle XVII hom intenta rectificar l'el·lipse, una qüestió de gran importància en l'Astronomia. Quan hom agafa com a equació de l'el·lipse:

$$x^2 / a^2 + y^2 / b^2 = 1$$

hom es troba immediatament amb la integral

$$s = \int_0^t \frac{a(1 - k^2 t^2)}{\sqrt{(1 - t^2)(1 - k^2 t^2)}}\, dt$$

on $k = a^2 - b^2/a^2$, $t = x/a$. En el cas particular d'una circumferència de radi 1 hom té $a = b = 1$, i la integral és de la forma

$$s = \int_0^t \frac{dt}{\sqrt{1 - t^2}}$$

és a dir $s = \arcsin t$.

Integrals d'aquest tipus també apareixen quan hom intenta determinar el període d'un pèndol simple, etc. Totes aquestes integrals són exemples d'integrals el·líptiques, més precisament, una integral el·líptica és una integral de la forma

$$s = \int_0^x \frac{P(x)}{\sqrt{R(x)}}\,dx$$

on P(x) és una funció racional i R(x) és un polinomi de grau 4. Legendre demostra que una integral el·líptica es pot reduir a un dels tres tipus següents:

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

$$E(k, \varphi) = \int_0^{\varphi} \sqrt{1 - k^2 \sin^2 \varphi}\,d\varphi \qquad n \text{ és constant, } k \in [0, 1].$$

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

Durant el segle XVII no era conegut el fet que les integrals el·líptiques no es poden expressar mitjançant funcions algèbriques, exponencials, logarítmiques o circulars. Això fou conegut en temps d'Euler (1707-1783). Les investigacions dutes a terme per Legendre i d'altres sobre integrals el·líptiques anaven dirigides a trobar resultats sobre la funció s(x), encara que en aquest sentit són pocs els resultats que s'obtenen.

La idea d'Abel i Jacobi és estudiar x com a funció de s de la mateixa manera com es fa en el cas de la circumferència on s'obté la funció sinus. D'aquesta forma s'obtenen les funcions el·líptiques; aquestes funcions es defineixen de fet sobre tots els complexos. Per exemple, quan hom té una integral del tipus

$$F(z) = \int_0^z \frac{dz}{\sqrt{(1 - z^2)(1 - k^2 z^2)}} \qquad 0 < k < 1$$

(aquesta integral s'obté per transformacions d'una del tipus $F(k, \varphi)$), aleshores la imatge del semiplà superior per la funció F és un rectangle de vèrtexs $K/2$, $-K/2$, $K/2 + iK'$, $-K/2 + iK'$, on

$$K = \int_{-1}^{1} \frac{dt}{\sqrt{(1 - t^2)(1 - k^2 t^2)}}$$

$$K' = \int_1^{1/k} \frac{dt}{\sqrt{(t^2 - 1)(1 - k^2 t^2)}}$$

i en conseqüència hom pot definir, en aquest rectangle, una funció f(z) que

és inversa de F(z). De fet, la funció f s'estén, per periodicitat, a tot el pla. Dit amb d'altres paraules, es compleix $f(z + 2K) = f(z + 2iK') = f(z)$. Per tant f(z) és una funció doblement periòdica o sigui que la funció el·líptica f és invariant pel grup de transformacions representat per

$$z' = z + 2mK + 2nKi \qquad m, n \text{ enters.}$$

En particular, la funció sin z és invariant pel grup de transformacions

$$z' = z + 2m\pi.$$

Les funcions el·líptiques són en particular funcions meromorfes doblement periòdiques i, precisament, les funcions que gaudeixen d'aquesta propietat són les que avui s'anomenen el·líptiques.

Les funcions el·líptiques suggereixen l'estudi de funcions més generals: les funcions automorfes. Una funció f(z) meromorfa diem que és automorfa respecte a un grup de transformacions lineals si

$$f(z) = f(Tz) \qquad \text{per a tot T del grup.}$$

En aquest cas, transformacions lineals vol dir transformacions homogràfiques, o sigui del tipus

$$z' = \frac{az + b}{cz + d} \qquad ad - bc = 1.$$

Observem que els grups que porten associades les funcions automorfes són restringits. En efecte, suposem que f(z) és una funció automorfa amb grup G i sigui z_0 un punt arbitrari. Considerem els transformats del punt z_0 per totes les transformacions del grup, o sigui el conjunt

$$C = \left\{ Tz_0 : T \in G \right\}.$$

Si z_0 és un pol per a la funció f(z), donat que el conjunt de pols és un conjunt aïllat, la intersecció de C amb cada domini afitat del pla és un conjunt finit. Si z_0 no és un pol, aleshores existeix un entorn de z_0 de manera que la funció f(z) és analítica, si la funció f(z) no és constant, és a dir la funció $f(z) - f(z_0)$ és no nul·la, tenim que el conjunt de zeros d'aquesta funció és un conjunt discret i, per tant, com abans la intersecció de C amb un cert entorn dy z_0 és finit. Resumint, els grups associats a les funcions automorfes no constants gaudeixen de la propietat següent:

"El conjunt dels transformats d'un punt per totes les transformacions del grup és finit en cada part finita del pla".

Un grup de transformacions amb aquesta propietat fou anomenat per Poincaré *grup discontinu.*

També els grups discontinus apareixen en l'estudi d'una equació diferencial de segon ordre, inicialment a l'equació hipergeomètrica estudiada per Riemann. Aquests grups discontinus també són grups de transformacions associats a funcions automorfes.

La teoria dels grups continus fou sistematitzada per Lie (1842-1899); l'estudi que féu Lie dels grups continus [17] és motivat pel fet que moltes equacions diferencials són invariants per certs grups continus. Actualment, parlar de grup continu és, a vegades, sinònim de grup topològic però, inicialment, els grups continus eren grups de transformacions que depenien d'un cert nombre finit de paràmetres (per això Lie parla de grups continus finits), i cada element del grup és representat per $x_i = f_i(x_1, \ldots, x_n, \eta_1, \ldots, \eta_m)$ $i = 1, \ldots, n$ on els paràmetres són $\eta_1, \ldots, \eta_m$; endemés les funcions f_i són analítiques en x_i, η_i. La composició de dues transformacions x_i', x_i'' és una altra transformació on els paràmetres s'obtenen com a funció dels paràmetres de x_i' i x_i''. Un exemple de grup continu és el grup de les matrius 2 x 2

$$X = \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix}$$

amb $(x_1, x_2, x_3, x_4) \in C^4$ i $x_1 x_4 - x_2 x_3 \neq 0$. Aquest grup és un grup topològic interpretant-lo com l'espai $C^4 - el$ con $x_1 x_4 - x_2 x_3 = 0$.

És un estudiant de Klein, von Dyck (1856-1934), qui al començament dels anys 1880 [23] comença a tractar conjuntament els grups continus i discontinus sota una mateixa òptica, és a dir, mirats com a grups abstractes. La definició de grup abstracte donada per von Dyck és la que tenim actualment. Sembla que el moment en què von Dyck introdueix el concepte de grup és el moment oportú i en conseqüència tingué més èxit que Cayley.

Cal destacar també que Netto, l'any 1882, publica un llibre en què recull una gran quantitat del material que hom coneixia a l'època sobre grups de permutacions, però ja s'hi manifesta un tractament més general en el sentit que comença a reconèixer el caràcter abstracte dels conceptes. Això fa comprendre com hom ja era disposat, en aquesta època, a admetre el concepte de grup abstracte i més considerant la gran quantitat d'exemples de grups de la qual hom disposava.

Von Dyck introdueix el concepte de sistema de generadors d'un grup (recordem que Jordan quan treballa amb grups de transformacions descriu un determinat tipus de grup donant generadors dels quals el grup es deriva); al mateix temps Von Dyck introdueix la noció de grup lliure com aquell en què hi ha un sistema de generadors els quals no estan lligats per cap relació. El fet que tot grup és donat per generadors i relacions es troba també implícit en el treball de Von Dyck.

Com a conseqüència del treball de Von Dyck hom ja comença a plantejar problemes propis de la teoria de grups abstractes. Potser el més antic i famós d'aquests problemes ve motivat per l'observació que tot grup és definit per generadors i relacions. Aleshores hom pot pensar que la qüestió interessant és com decidir si dos grups donats per generadors i relacions són isomorfs o, més senzill, decidir quan un grup donat per generadors i relacions és el grup trivial. Aquest últim problema es coneix com el problema de les paraules i fou formulat per primera vegada per Dehn [7] l'any 1911. Actualment sabem que el problema de les paraules no és resoluble, però això no fou provat fins a l'any 1955 per Novikov [18]. Problemes que es deriven del de les paraules han estat estudiats per un gran nombre de teoristes de grups; així en el cas de grups definits per una única relació el problema de les paraules té solució, un fet provat per Magnus l'any 1932.

Hom pot consultar l'article de Rabin [19] on hi ha una discussió del problema de les paraules i d'altres de relacionats.

Un problema no menys famós és el conegut com a Problema de Burnside. L'any 1902 Burnside [3] escriu: "encara és una qüestió sense decidir a la teoria dels grups discontinus la de si l'ordre d'un grup pot ésser no finit quan l'ordre de tota operació que conté és finit". Hem d'interpretar que Burnside es refereix a grups finitament generats i, aleshores, la pregunta es pot formular:

I. Si els elements d'un grup finitament generat són tots d'ordre finit, és el grup finit?

Amb aquesta generalitat el problema no fou atacat al començament, de fet els resultats que s'obtenen són en relació amb el següent problema:

II. Sigui G un grup finitament generat i de torsió afitada. És G un grup finit?

El problema I es coneix com el problema de Burnside generalitzat. No és fins l'any 1964 que Golod [11] contestà negativament aquesta pregunta. Les tècniques emprades per Golod són molt enginyoses i al mateix temps elementals, i a més donen una aplicació de la teoria abstracta de les àlgebres lliures a la teoria de grups. També el problema II, conegut com el problema de Burnside, té una resposta negativa per grups d'exponent senar $\geqslant 4381$; això fou demostrat per Novikov i Adjan l'any 1968. Encara hi ha una altra pregunta derivada del problema de Burnside:

III. Si G és un grup finit d'exponent n i generat per m elements, ¿podem dir que l'ordre de G és afitat per una funció de n i m que no depèn del grup?

El problema III és el problema restringit de Burnside. Fou demostrat per Kostrikin l'any 1959 i la resposta és afirmativa per a grups d'exponent primer.

En néixer la teoria de grups abstractes hi hagué una gran profusió d'articles, una part dels quals amb la finalitat de resoldre antics problemes plante-

jats a la teoria dels grups de substitucions, com per exemple el de determinar els grups d'un ordre donat. Una altra part de treballs foren dedicats al problema de trobar els grups simples i resolubles. En aquesta època, Hölder [12] demostra que el grup alternat A_n és simple quan $n \geqslant 5$. Miller estudia els grups amb tots els subgrups normals, els avui coneguts com a grups Hamiltonians; ell és també qui introdueix el concepte de commutador, que també fou introduït per Dedekind.

Els primers resultats sobre grups resolubles abstractes es deuen a Frobenius (1849-1917), que demostrà que els grups d'ordre no divisible pel quadrat d'un número primer són resolubles. Un altre resultat important de Frobenius és: si G és un grup de permutacions de grau n que és transitiu i tal que tots els seus elements, llevat del neutre, deixen com a màxim una lletra invariant, aleshores el conjunt dels elements que no deixen fixa cap lletra, junt amb l'element neutre, és un subgrup normal de G. Aquest és un resultat que necessita la teoria de representacions de grups per a ésser demostrat, i no és un cas aïllat, és a dir que de nou, per a demostrar resultats de grups abstractes, hom torna a la representació. La teoria de representació de grups finits abstractes fou impulsada per diversos matemàtics com ara Frobenius, Schur (1875-1941), però l'època daurada ja en correspon a la primera meitat del nostre segle.*

* Em plau reconèixer que les converses sobre el tema d'aquesta conferència mantingudes amb en Julià Cufí i Pascual Llorente han estat per a mi molt profitoses.

REFERÈNCIES

[1] Abel, N. H.: "Obres", **1**, 66-94 (1881) Johnson R.C., 1964.
[2] Bourbaki, N.: "Eléments d'histoire des mathématiques", Hermann, Paris, 1969.
[3] Burnside, W.: *Quart J. of Math.*, **33**, 230-38 (1902).
[4] Cauchy, A.-L.: "Obres", **(2), 13**, 171-282.
[5] Cayley, A., *Phil. Mag.*, **(3), 34**, 527-529 (1849) - **7**, 40-47 (1854) - **7**, 408-409 (1854).
--- The collected mathematical paper, 2, Cambridge, 1889.
[6] Dedekind, R., Werke, **3**, 439-46 (1858).
[7] Dehn, M., *Math. Ann.*, **71**, 116-44 (1911).
[8] Frobenius, *J. für Math.*, **100**, 179-81 (1887).
[9] Galois, E.: "Oeuvres mathematiques", Gauthier-Villans, 1897.
[10] Gauss, C.F.: "Disquisitiones Arithmeticae", 1801.
[11] Golod, E.S., *Izr. Akad. Nauk. SSSR*, **28**, 273-76 (1964).
[12] Hölder, L.O., *Math. Ann.* **34**, 26-56 (1889) - **40**, 55-88 (1892) - **43**, 301-412 (1983) - **46**, 321-422 (1895).
[13] Jordan, C.: "Obres", Gauthier-Villars, 1961-1964.
[14] Kline, M.: "Mathematical thought from Ancient to Modern Times", Oxford University Press, 1972.
[15] Kronecker, L., Monatsber. Berliner Akad., 881-889 (1870).
[16] Lagrange, J.L.: "Réflexions sur la résolution algébrique des équations", Obres, 3, 205-241.
[17] Lie, S.: "Nachrichten König", *Ges. des Wiss. zu Gött.*, 529-42 (1874).
[18] Novikov, P.S., *Iz. Akad. Nauk. SSR* (1955) (Am. Math. Sor. Trans. **(2), 9**, 1-122 (1958)).
[19] Rabin, M.O., *Ann. of Math.* **(2), 67**, 172-194 (1958).
[20] Ruffini, P.: "Teoria generalle delle equazioni", 1799.
[21] Schur, I., *Crelle J.*, **127**, 20-50 (1904).
[22] Sylow, L., *Math. Ann.*, **5**, 581-94 (1872).
[23] Von Dyck, W., *Math. Ann.*, **20**, 1-44 (1882) - **22**, 70-118 (1883).