

LA GÈNESI DE LA TEORIA DE GRUPS
EN L'OBRA DE GALOIS

Antoni Malet

1. Introducció

Segons la tradició, la teoria de grups neix en un breu treball que Evariste Galois (1811-1832) va presentar a la Acadèmia de Ciències de Paris i que aquesta il·lustre institució li va retornar declarant, més o menys, que resultava intel·ligible. Uns quants anys més tard, el mateix treball i el mateix autor eren recuperats de l'oblit per la mateixa institució.

Recordarem ràpidament algunes dates i dades d'aquest afer. A començaments del 1831, Galois va presentar a l'Acadèmia una Memòria titulada *Sobre les condicions de resolubilitat de les equacions per radicals*. En el mes de juliol del mateix any, l'Acadèmia feia seu l'informe de Denis Poisson (1781-1840) sobre el treball de Galois i li negava la seva aprovació. Exactament dotze anys més tard, el 4 de juliol de 1843, la *Memòria sobre les condicions...* obtenia públicament el reconeixement acadèmic avalada per l'informe favorable de Joseph Liouville (1820-1882). Liouville va publicar aquesta Memòria i un parell més de treballs de Galois (tan curts com la Memòria) a l'any 1846. En un treball del 1852, Enrico Betti (1823-1892) republicava la famosa Memoria afegint

demostracions que Galois havia omès i retocant-ne d'altres. La Teoria de Galois apareix per primera vegada com un capítul d'un llibre de text en el 1866, en la 3^a edició del *Cours d'algèbre supérieure* de Joseph-Alfred Serret (1819-1885). La contribució de Serret és semblant a la de Betti.

El primer que va desenvolupar creadorament les idees contingudes en estat embrionari en l'obra de Galois fou Camille Jordan (1838-1921). En una sèrie molt nombrosa de treballs publicats entre 1861 i 1869, Jordan reelaborava els conceptes clau introduïts per Galois (grup, subgrup i grup quocient de permutacions), n'introduïa de nous (homomorfisme i factors de composició) i donava a la Teoria de Galois una nova consistència i un nou abast. Aquests treballs constitueixen la base del *Tractat de les substitucions i de les equacions algebriques* (1870), un volum de 700 pàgines que, com ha dit Dieudonné, fou la "Biblia" dels algebristes durant 50 anys.

Per comprendre que Jordan pecava de falsa modèstia quan deia, en el Prefaci del seu *Tractat*, que tot allò no era sinó un comentari de l'obra de Galois, n'hi ha prou de saber que el manuscrit original de la *Memòria sobre les condicions...*, avui conservat a París a la Biblioteca de l'Institut de França, no ocupava sinó sis folis. Aquest fulls acompanyaren a Galois des que li foren retornats per l'Acadèmia fins que morí, onze mesos més tard. En aquest interval, Galois hi va introduir algunes esmenes i afegits que després comentaré.

Els resultats més importants continguts en aquesta memòria són dos: l'associació d'un grup a cada equació polinòmica i

la caracterització de les equacions resolubles per radicals mitjançant aquest grup. Galois utilitza, certament, les paraules grup i subgrup: malgrat que enlloc no és definit allò que el lector ha d'entendre en aquest concepte. Tampoc no trobem cap definició d'altres conceptes que juguen un paper important en la formulació (almenys en termes moderns) dels seus resultats més notables, com ara subgrup normal, grup quocient, etc. Es tracta d'un tret sorprenent pel lector modern i especialment interessant si es té en compte que aquesta era la primera aparició dels grups de permutacions.

El que aquí pretenc és descriure els antecedents de l'obra de Galois i la manera concreta com ell va introduir els grups dins de la teoria d'equacions. A la llum de les característiques d'aquesta obra analitzaré, finalment, l'informe de Poisson que va impedir que obtingués l'aprovació de l'Acadèmia.

2. Els antecedents

2.1. Sobre permutacions

Cal mencionar, en primer lloc, una memòria molt llarga de Joseph-Louis Lagrange (1736-1813) on eren analitzats minuciosament els mètodes de resolució de les equacions de 3^r i 4^t grau i estudiada la possibilitat de generalitzar-los a les de graus superiors (1). En el transcurs d'aquesta anàlisi, Lagrange es veia enfrontat amb funcions racionals $F(x_1, x_2, \dots, x_n)$ de les arrels d'una equació sobre les que actuaven permutacions de

les arrels. Això el va portar a un resultat que encara avui coneixem com a teorema de Lagrange: si existeixen m permutacions que deixen formalment invariant F , el nombre de valors formalment diferents que pren F és $n!/m$. Aquest fou l'enunciat que va tenir durant molts anys el teorema que afirma que l'ordre d'un subgrup és un divisor de l'ordre del grup. Lagrange acabava la memòria conjecturant, sense gaire convicció, la impossibilitat de resoldre per radicals les equacions de grau superior al 4^t.

En aquests primers contactes entre les equacions i les permutacions, aquestes jugaven un paper merament auxiliar. D'aquesta manera eren tractades per Augustin-Louis Cauchy (1789-1857) en un treball no molt extens publicat en el 1815 (2). Cauchy no feia sinó demostrar el teorema de Lagrange i, com a continuació, que si $n \geq 5$ i el nombre de valors que pren $F(x_1, \dots, x_n)$ és > 2 , ha de ser per força ≥ 5 . El treball de Cauchy era directament inspirat en els intents de demostració de la impossibilitat de resoldre per radicals l'equació general de 5^è grau fets per Paolo Ruffini (1765-1822) al voltant del 1800. Cap de les sis demostracions que Ruffini arribà a publicar d'aquest resultat fou plenament acceptada. El seu treball, però, ha de ser mencionat perquè avençava pel camí indicat per Lagrange. Va calcular explícitament els elements de S_5 , va introduir alguna cosa que, salvant moltes distàncies, avui anomenariem grups primitius i transitius, i va demostrar, d'una forma bastant calculística, el teorema que Cauchy simplificaria notablement i incloiria, amb el de Lagrange, en la memòria ja

esmentada del 1815.

En aquesta memòria trobem el primer intent sistemàtic per a fixar unes notacions i una nomenclatura adients per a les permutacions. Cauchy introdueix la simbologia

$$A = \begin{pmatrix} a & b & c & \dots \\ b & c & a & \dots \end{pmatrix},$$

la notació exponencial A^n i el concepte d'ordre d'una substitució. També introdueix una distinció inconvenient que es mantindrà durant uns quants anys: una cosa són les *permutacions*, files de lletres, i una altra les *substitucions*, allò que permet passar d'una permutació a una altra. La distinció, adoptada per Galois, havia de ser dificultat a vèncer per poder arribar al concepte de grup.

Cauchy, com tampoc no ho havien fet Lagrange ni Ruffini, no parlava de grups ni de subgrups. L'única noció prefiguradora d'aquest concepte que hom troba en aquests primers treballs és el de *permutacions equivalents*. Ruffini havia anomenat *ordre d'equivalència* al nombre de valors igual que podia prendre una funció $F(x_1, \dots, x_n)$, i Cauchy va anomenar permutacions equivalents les que deixaven formalment invariant F .

2.2. Sobre resolubilitat per radicals

Niels-Henrik Abel (1802-1829) va publicar l'any 1829 una Memòria titulada *Sobre una classe particular d'equacions resolubles al-*

gebraicament (3). "Algebraicament" volia dir, a l'època, el mateix que avui "per radicals". Són dues les motivacions principals d'aquest treball, segons que el mateix Abel explica en un paràgraf introductori. D'una banda, és un intent de generalitzar una idea continguda en la demostració de la resolubilitat per radicals de les equacions de la forma $x^n - 1 = 0$. Aquesta és una aportació de Karl-Friedrich Gauss (1777-1855) publicada com una part de les *Disquisitiones Arithmeticae* l'any 1801 (4). Abel demostra que la resolubilitat per radicals és possible

"si totes les arrels d'una equació es poden expressar per

$$x, \theta x, \theta^2 x, \dots, \theta^{n-1} x$$

essent $\theta^n x = x$ i θx una funció racional de x ".

Aquí x representa una arrel qualsevol de l'equació; funció racional volia dir el mateix que avui. I continua:

"Aquest és el cas de l'equació $\frac{x^n - 1}{x - 1} = 0$, on n és un nombre primer, doncs, designant per α una arrel primitiva mòdul n , és possible expressar, com és sabut, les $n-1$ arrels per

$$x, x^\alpha, x^{\alpha^2}, \dots, x^{\alpha^{n-2}}$$

essent $x^{\alpha^{n-1}} = x$, ço és, posant $x^\alpha = x$, per

$$x, \theta x, \theta^2 x, \dots, \theta^{n-2} x, \quad \text{on } \theta^{n-1} x = x \quad (5).$$

Una arrel primitiva mòdul n és un número g tal que $g^{n-1} \equiv 1$, però $g \not\equiv 1 \pmod{n}$ si $0 < g < n - 1$.

D'una altra banda, Abel ha descobert en els seus treballs en un altre camp de les Matemàtiques que aquest enfocament donat a l'estudi de les equacions pot ser molt útil. Referint-se a l'expressió de totes les arrels d'una equació per $x, \theta x, \theta^2 x, \dots, \theta^{n-1} x$, diu:

"La mateixa propietat es dóna en una certa classe d'equacions a la que he arribat per la teoria de funcions el·liptiques"(5)

Abans de donar una idea de la demostració de la resolubilitat per radicals d'una equació les arrels de la qual són totes de la forma $\theta^m x$, cosa que cal fer perquè hi ha idees en aquesta demostració que juguen un paper en el treball de Galois, mencionaré els resultats generals assolits per Abel en aquesta memòria del 1829.

En primer lloc, Abel analitza la hipòtesi que dues arrels d'una equació es poden expressar racionalment una per mitjà de l'altra. Posant $x' = \theta x_1$, Abel demostra:

1) θ aplicada a qualsevol arrel de l'equació és una altra arrel.

n l'enter més petit tal que $\theta^n x_1 = x_1$. Les n arrels

$$x_1, \theta x_1, \dots, \theta^{n-1} x_1$$

són totes distintes.

3) Pot passar que aquestes siguin totes les arrels de l'equació o que n'hi hagi més. En l'últim cas, sigui x_2 una arrel diferent de les anteriors. Les n arrels $x_2, \theta x_2, \dots, \theta^{n-1} x_2$ són altres tantes arrels distintes de l'equació. Etc. Per tant, si μ és el grau de l'equació proposada, les μ arrels es poden dividir en m paquets

$$\begin{array}{ll} x_1, \theta x_1, \dots, \theta^{n-1} x_1 & \\ x_2, \theta x_2, \dots, \theta^{n-1} x_2 & \\ \cdot & \cdot \\ \cdot & \cdot \\ x_m, \theta x_m, \dots, \theta^{n-1} x_m & \end{array} \quad \mu = m.n$$

I diu Abel, referint-se a aquest resultat, que "les μ arrels d'aquesta equació es dividiran en diferents grups (sic) compostos de n termes" (6).

Respecte d'aquestes equacions, Abel es limita a demostrar que són resolubles per radicals si $\mu = n$.

Abel també analitza les conseqüències d'una altra hipòtesi: que *totes* les arrels d'una equació són funcions racionals d'una d'elles. En aquest cas, Abel demostra que una equació les arrels de la qual són $x_1, \theta x_1, \theta_2 x_1, \dots, \theta_{n-1} x_1$ és resoluble

per radicals si $\theta_i \theta_j x_1 = \theta_i \theta_i x_1$. Les equacions que compleixen aquesta condició s'anomenen *abelianes*. En termes moderns (Abel mai no va parlar del grup d'una equació), la commutativitat de les θ implica la commutativitat del grup de l'equació, i per això anomenem *abelians* els grups commutatius.

Per demostrar que una equació tal que totes les seves arrels són $x_1, \theta x_1, \dots, \theta^{n-1} x_1$ és resoluble per radicals, Abel agafa una arrel n -èsima de la unitat α , i construeix l'expressió

$$\Psi x_1 = (x_1 + \alpha \theta x_1 + \alpha^2 \theta^2 x_1 + \dots + \alpha^{n-1} \theta^{n-1} x_1)^n$$

Si substituïm la x per una altra arrel $\theta^m x_1$, aquesta quantitat no varia. Per tant tenim

$$\Psi x_1 = \Psi \theta x_1 = \Psi \theta^2 x_1 = \dots = \Psi \theta^{n-1} x_1$$

$$\Psi x_1 = \frac{1}{n} (\Psi x_1 + \Psi \theta x_1 + \dots + \Psi \theta^{n-1} x_1)$$

Això vol dir que Ψx_1 és una funció simètrica de les arrels de l'equació proposada, i Abel sabia que això vol dir que Ψx_1 , es pot expressar en funció racional dels coeficients d'aquesta equació, es a dir, que Ψx_1 és un nombre del cos dels coeficients, dit en el nostre llenguatge. Anomenem v aquest número i tindrem

$$\sqrt[n]{v} = x_1 + \alpha \theta x_1 + \dots + \alpha^{n-1} \theta^{n-1} x_1$$

$1, \alpha_1, \alpha_2, \dots, \alpha_{n-1}$ de l'equació $x^{n-1} = 0$, tenim

$$\begin{aligned} \sqrt[n]{v_1} &= x_1 + \theta x_1 + \dots + \theta^{n-1} x_1 \\ \sqrt[n]{v_2} &= x_1 + \alpha_1 \theta x_1 + \dots + \alpha_1^{n-1} \theta^{n-1} x_1 \\ &\vdots \\ \sqrt[n]{v_n} &= x_1 + \alpha_{n-1} \theta x_1 + \dots + \alpha_{n-1}^{n-1} \theta^{n-1} x_1 \end{aligned}$$

Per obtenir l'expressió de les arrels de l'equació en funció del radicals $\sqrt[n]{v_i}$ i de les arrels de la unitat, es pot agafar una arrel primitiva n-èsima de la unitat α , es a dir, una tal que les n arrels es poden escriure $1, \alpha, \alpha^2, \alpha^3, \dots, \alpha^{n-1}$. Aleshores tenim

$$\begin{aligned} \sqrt[n]{v_1} &= x_1 + \theta x_1 + \dots + \theta^{n-1} x_1 \\ \sqrt[n]{v_2} &= x_1 + \alpha\theta x_1 + \dots + \alpha^{n-1}\theta^{n-1} x_1 \\ &\vdots \\ \sqrt[n]{v_n} &= x_1 + \alpha^{n-1}\theta x_1 + \dots + \alpha^{(n-1)(n-1)}\theta^{n-1} x_1 \end{aligned}$$

Sumant aquestes expressions, tenim

$$\Sigma \sqrt[n]{v_i} = nx_1 + \theta x_1 (1 + \alpha + \dots + \alpha^{n-1}) + \dots + \theta^{n-1} x_1 (1 + \alpha^{n-1} + \alpha^{2(n-1)} + \dots + \alpha^{(n-1)(n-1)})$$

on tots els parèntesis s'anul·len, d'on $x_2 = \frac{1}{n} \sum \sqrt[n]{v_i}$. Per
aïllar les altres arrels, n'hi ha prou de multiplicar cada una
de les equacions per una potència adequada de α .

En acabar la demostració, Abel insisteix sobre les seves fonts:

"El mètode que fins aquí hem seguit (...) és en el fons el mateix que el que ha fet servir el Sr. Gauss en les seves "Disquisitione arithmeticae", art. 359 i ss., per a resoldre una certa classe d'equacions a la que havia arribat en investigar l'equació $x^n - 1 = 0$. Aquestes equacions tenen la mateixa propietat que la nostra...
que totes les arrels es poden representar per $x, \theta x, \dots, \theta^{n-1}x$ " (7)

La petita història de les equacions $x^n - 1 = 0$ també es interessant de conèixer per a comprendre les petites i progressives generalitzacions que configuren el camí dels resultats espectaculars. Gauss va arribar a interessar-se per aquestes equacions a partir del problema de la construcció de polígons regulars. Com es sabut, un dels seus primers descobriments, quan encara era un adolescent, fou el de la construcció amb regla i compàs del polígon regular de 17 costats. Gauss comenta, en començar la part de les *Disquisitione* dedicada a les equacions $x^n - 1 = 0$, titulada "Sobre les equacions que determinen les divisions del cercle", que les seves solucions ($r = \cos \frac{k}{n}2\pi + i \sin \frac{k}{n}2\pi$) permeten determinar els valors del sinus i cosinus dels angles $\frac{2\pi}{n}, \frac{2\pi}{n}2, \dots, \frac{2\pi}{n}(n-1)$. Les relacions $\sin \frac{k}{n}2\pi = \frac{1}{2i}(r - \frac{1}{r})$ etc., i el fet que les equacions $x^n - 1 = 0$ siguin més còmodes de manejar i estudiar que les que donen directament els sinus i cosinus de $\frac{2\pi}{n}k$ (les que donen els sinus, per exemple, són

$$x^n - \frac{1}{4} nx^{n-2} + \frac{1}{16} \frac{n(n-3)}{1 \cdot 2} x^{n-4} - \frac{1}{64} \frac{n(n-4)(n-5)}{1 \cdot 2 \cdot 3} x^{n-6} + \dots = 0,$$

són, explica Gauss, les raons per les que estudiarà aquelles equacions.

Gauss no va començar a partir de zero l'estudi de les equacions $x^n - 1 = 0$, sinó que va aprofitar uns resultats previs ja trobats sobre les equacions $x^5 - 1 = 0$, $x^7 - 1 = 0$ i $x^{11} - 1 = 0$, les quals havien estat considerades per Alexandre-Théophile Vandermonde (1735-1796). Vandermonde, en una memòria del 1771 (8), demostrava que aquestes equacions eren resolubles per radicals i concloïa que el mateix mètode utilitzat en aquests tres casos particulars era aplicable per a demostrar la mateixa cosa per a totes les equacions $x^p - 1 = 0$, p primer. Això és veritat i és mentida. És mentida perquè per a poder fer en general allò que Vandermonde feia en particular cal demostrar, i és el que va demostrar Gauss, que per a tot nombre primer p existeix una arrel primitiva mòdul p . Assegurat aquest punt, el mètode de Vandermonde funciona realment en general.

No vull acabar aquest apartat sense esmentar la valoració taxativa i un tant heterodoxa que va fer Lebesgue dels mèrits respectius de Vandermonde i Gauss:

"Certament, el treball de Gauss és una obra mestra; una obra mestra d'exposició elegant, rigorosa i completa, una obra mestra de comprensió i d'intel·ligència, però en la que la part d'invenció personal és en realitat molt petita. (...) (Gauss) segueix pas a pas Vandermonde, encara

que el perfecciona molt, evidentment"(9).

2.3. La impossibilitat de resoldre per radicals les equacions de grau superior a 4.

Ja he mencionat els intents de Ruffini de demostrar la impossibilitat de resoldre per radicals l'equació general de 5^è grau. Com és sabut, la primera demostració plenament acceptada d'aquest resultat és deguda a Abel i fou publicada l'any 1824. Millorada, fou publicada altra vegada el 1826. La idea que presideix totes les demostracions d'Abel és la mateixa: primer s'estableix la forma més general que poden adoptar les arrels d'una equació de 5^è grau expressades per radicals, i aleshores es demostra, de forma bastant calculística, que quan hom substitueix la incògnita de l'equació per aquestes expressions amb radicals, totes les substitucions condueixen a contradiccions (10).

Des del punt de vista de la gènesi de la noció de grup, el treball d'Abel es poc significatiu. Com ha dit Kiernan, és un treball que cal considerar essencialment de *vella escola* (11). Abel utilitza els resultats de Lagrange i de Cauchy mencionats a 2.1. (no els de Ruffini que, segons sembla, encara no coneixia), però només els teoremes allí mencionats. En particular, Abel mai no féu servir els grups de permutacions en les seves recerques sobre equacions.

3. La Memòria de Galois (12)

Unes observacions prèvies. Galois sempre utilitzarà equacions que tenen totes les arrels distintes. És una condició que juga un paper important en el desenvolupament de les seves idees i que no és restrictiva. A l'època ja existien mètodes de càlcul ben coneguts per a determinar si una equació té o no arrels múltiples i, en cas afirmatiu, per a trobar-ne una altra que no tingui sinó les arrels distintes de l'equació original.

Segona observació: no existien encara ni definicions precises ni notacions específiques pels diferents conjunts numèrics. A aquesta absència cal referir les primeres definicions que Galois inclou en la seva Memòria:

"DEFINICIONS. Direm que una equació és reduïble quan admet divisors racionals; irreduïble en cas contrari.

Cal explicar aquí el que s'ha d'entendre amb el mot racional, doncs es presentarà sovint.

Quan l'equació té tots els seus coeficients numèrics i racionals, vol dir simplement que l'equació es pot descompondre en factors que tenen llurs coeficients numèrics i racionals.

Però quan els coeficients d'una equació no siguin pas tots numèrics i racionals, aleshores caldrà entendre per divisor racional un divisor tal que els seus coeficients s'expressen en funció racional dels coeficients de la proposada; en general, per quantitat racional una

quantitat que s'expressa en funció racional dels coeficients de la proposada.

Es més: es pot convenir de considerar racional tota funció racional d'un cert nombre de quantitats determinades que es suposin conegudes a priori. Per exemple, es pot escollir una certa arrel d'un nombre enter i considerar racional tota funció racional d'aquest radical.(...)

Això establert, anomenarem RACIONAL qualsevol quantitat que s'expressi en funció racional dels coeficients de l'equació i d'un cert nombre de quantitats ADJUNTES a l'equació i convingudes arbitràriament. (...)

Es veu, a més a més, que les propietats i les dificultats d'una equació poden ser completament diferents segons les quantitats que li són adjuntades. Per exemple, l'adjunció d'una quantitat pot tornar reduïble una equació irreduïble". (p.45)

Es tracta d'una manera arcaica i feixuga de poder parlar d'altres cossos que no siguin el dels racionals i d'altres anells de polinomis que no siguin $\mathbb{Q}[X]$. Galois anomena *racionals* les quantitats que pertanyen a un cos K que es suposa conegut, i que pot ser $\mathbb{Q}$ o una extensió de $\mathbb{Q}$ generada per l'adjunció de certs irracionals. I anomena reduïbles els polinomis que es descomponen a $K[X]$.

En relació amb els conjunts numèrics emprats per Galois, també cal subratllar que no existia encara la distinció entre irracional algebraic i irracional transcendent. Fins l'any 1844,

Liouville no demostrà per primera vegada que existien irracionals que mai no podien ser arrels d'una equació polinòmica (13). Galois presuposa més d'un cop que una certa quantitat és algebraica sobre el camp de racionalitat on treballa. La hipòtesi, en tots els casos, podria ser demostrada fàcilment, però possiblement ell mai no es va plantejar aquesta qüestió.

Una tercera i última observació: Galois no utilitza el mot *permutació* amb el seu significat actual, sinó segons el que li va donar Cauchy l'any 1815. Per *permutació* cal entendre, doncs, una renglera ordenada de lletres o nombres.

La Proposició I de la *Memòria sobre les condicions de resolubilitat de les equacions per radicals* diu així:

"Proposició I

Siguin $a, b, c, \dots$ les m arrels d'una equació donada. Existirà sempre un grup de permutacions de les lletres $a, b, c, \dots$ que gaudirà de la propietat següent:

1^r Que tota funció de les arrels invariable per les substitucions d'aquest grup és racionalment coneguda [Es a dir, si K és el domini de racionalitat dels coeficients, i $K' = K(a, b, c, \dots)$, tot element de K' invariable formalment per les substitucions del grup és de K].

2ⁿ Recíprocament, tota funció de les arrels determinable racionalment és invariable per aquestes substituicions. [Si un element de K es pot expressar com a funció racional de $a, b, c, \dots$, aquesta expressió serà invariable per

les substitucions del grup]" (p. 51).

Per veure com Galois construeix aquest grup, hem d'esmen-
tar els lemes previs que ell utilitza. Es tracta, malgrat que
ens poden semblar rebuscats i estranys, de resultats ben cone-
guts a l'època i no originals de Galois:

1) Si V_0 és una quantitat obtinguda racionalment a par-
tir de les m arrels (podem posar $V_0 = V_0(a, b, c, \dots)$) tal
que quan permutem les m arrels de totes les maneres possibles
resulten $m!$ quantitats diferents, aleshores cadascuna de les
arrels es pot expressar racionalment utilitzant només la quanti-
tat V_0 . Posem

$$a = \varphi_0 V_0, \quad b = \varphi_1 V_0, \quad \dots$$

2) Sigui $G(x) = 0$ una equació racional irreduïble que
admet V_0 com arrel. G tindrà altres arrels $V_1, V_2, \dots, V_{n-1}$.
Aleshores es demostra que cadascuna d'elles ha de ser un dels
 $m!$ valors que hom obté permutant les arrels dins de V_0 .

3) Resulta, finalment, que $\varphi_0 V_1, \varphi_0 V_2$, etc. són
arrels de l'equació proposada. És a dir, que $\varphi_0 V_1, \varphi_0 V_2, \dots$
 $\varphi_0 V_{n-1}$, són algunes de (o totes) les m quantitats $a, b, c, \dots$

El grup de permutacions de l'equació, diu Galois, és el
següent. Associada al valor V_0 , tenim la permutació

$$(V_0) \quad \varphi_0 V_0 \quad \varphi_1 V_0 \quad \varphi_2 V_0 \quad \dots \quad \varphi_{m-1} V_0$$

Associada al valor V_1 , tenim

$$(V_1) \quad \varphi_0 V_1 \quad \varphi_1 V_1 \quad \varphi_2 V_1 \quad \dots \quad \varphi_{m-1} V_1$$

I, anàlogament, tenim

$$(V_2) \quad \varphi_0 V_2 \quad \varphi_1 V_2 \quad \varphi_2 V_2 \quad \dots \quad \varphi_{m-1} V_2$$

$$\dots \quad \dots \quad \dots \quad \dots \quad \dots$$

$$(V_{n-1}) \quad \varphi_0 V_{n-1} \quad \varphi_1 V_{n-1} \quad \cdot \quad \dots \quad \cdot \quad \varphi_{m-1} V_{n-1}$$

Anem a veure que aquest grup compleix les condicions del teorema. Per a donar una idea del que era l'estil extraordinàriament concís i sintètic de Galois, transcriuré textualment la seva demostració de la primera part: si una quantitat funció racional de les arrels és invariable per aquestes permutacions, aleshores és una quantitat racional. Diu Galois:

"Qualsevol funció F de les arrels invariable per les substitucions d'aquest grup es podrà escriure així
 $F = \Psi V_0$, i hom tindrà

$$\Psi V_0 = \Psi V_1 = \dots = \Psi V_{n-1}$$

El valor de F podrà, per tant, ser determinat racionalment".

Tot el que Galois no diu i pretén que el lector pensi és

el següent:

Si $F = F(a, b, c, \dots)$ és una funció racional de les arrels, serà $F = F(\varphi_0 V_0, \varphi_1 V_0, \varphi_2 V_0, \dots)$ i això es pot escriure $F = \Psi V_0$, essent Ψ una funció racional ja que les φ 's i la F ho són. Les permutacions del grup, per la seva definició, ens donem

$$(V_1) \quad F(\varphi_0 V_1, \varphi_1 V_1, \varphi_2 V_1, \dots) \text{ que és } \Psi V_1$$

$$(V_2) \quad F(\varphi_0 V_2, \varphi_1 V_2, \varphi_2 V_2, \dots) \text{ que és } \Psi V_2, \text{ etc.}$$

Si F és invariable per aquestes substitucions, tindrem

$$\Psi V_0 = \Psi V_1 = \dots = \Psi V_{n-1}$$

Per tant

$$F = \frac{1}{n}(\Psi V_0 + \Psi V_1 + \dots + \Psi V_{n-1})$$

I això significa que F és una funció simètrica de les V 's, és a dir, de les arrels de l'equació $G(x) = 0$. Per tant F es pot expressar racionalment en funció dels coeficients de G , que són racionals.

La segona part del teorema es demostra així: Posem, com abans, $F = F(a, b, c, \dots) = \Psi V_0$. Considerem l'equació racional

$$F - \Psi(X) = 0$$

que admet l'arrel V_0 . Com que $G(x) = 0$ és una equació racional irreducible, totes les arrels de G ho són de $F - \Psi(x) = 0$, per tant

$$F = \Psi V_0 = \Psi V_1 = \dots = \Psi V_{n-1}$$

I com que aquests són els valors que pren F quan hi actuen les permutacions del grup, queda demostrat que F és invariable per aquestes permutacions.

Hi ha algunes coses que cal comentar sobre aquesta primera aparició dels grups de permutacions en el pensament algebraic.

La primera és la *definició* galoisiana del grup d'una equació. Es tracta d'una definició constructiva, o feta per extensió: els elements del grup són aquest, aquest i aquest. No és una definició per comprensió: sigui G el grup format per les permutacions tals que... Per força havia de ser així tota vegada que Galois mai no va arribar a donar cap definició que identifiqués els grups com a certs conjunts privilegiats de permutacions.

La segona és la relació entre permutacions i substitucions. Galois mai no va arribar a resoldre satisfactòriament el problema de la identificació dels dos conceptes, malgrat que era conscient que allí hi havia un problema a resoldre. Sempre va mantenir la distinció entre unes i altres, seguint les definicions introduïdes per Cauchy en el treball de 1815, però en el manuscrit hom troba una sèrie de correccions que fan veure que Galois era conscient que allò no acabava de funcionar.

Els mots *permutació* i *substitució* apareixen superposats

un a l'altre com a fruit de successives correccions, de vegades múltiples en un mateix lloc. Fin i tot trobem en una marge l'advertència "En lloc de la paraula permutació, posar a tot arreu la paraula substitució", la advertència que el mateix Galois esborrà posteriorment!.

En el mateix marge trobem, però, una sèrie de notes sobre aquest problema amb la indicació clara "A incloure amb les *definicions*", i així han estat sempre publicades aquestes notes, incloses dins del text ordinari de la Memòria. Recordo aquí que aquestes correccions van ser fetes versemblantment, a la presó. La datació precisa d'aquestes correccions és molt difícil, així com la de les que van ser fetes exactament la nit abans del duel en el que va morir, però Bourgne i Azra, que han estudiat minuciosament els manuscrits, han pogut establir algunes conclusions prou sòlides basant-se en la pluma utilitzada, la tinta, fins i tot el tipus de lletra, etc.

Aquesta sèrie de notes sobre permutacions i substitucions diu:

"Les substitucions són el pas d'una permutació a l'altra.

La permutació de la que es parteix per indicar les substitucions és del tot arbitrària quan es tracta de funcions. Doncs no hi ha cap raó per a que dins d'una funció de diferents lletres una lletra ocupi un lloc i no un altre.

Tanmateix, com que no és gaire possible formar-se

la idea d'una substitució sense la d'una permutació, no saltres en parlar utilitzarem freqüentment les permutacions, i no considerarem les substitucions sinó com el pas d'una permutació a una altra.

Quan voldrem agrupar [textualment, *grouper*] substitucions, les farem provenir totes d'una mateixa permutació".

Apareix, a continuació, el vestigi més interessant de la gran idea que Galois només va arribar a entreveure en estat embrionari. És la frase inacabada "*El grup és un conjunt de permutacions tal que si es passa...*", que després Galois va barrar.

I acaba aquestes notes amb un altre comentari interessant:

"Com que es tracta sempre de qüestions on la disposició primitiva de les lletres no influeix per a res, en els grups que considerarem hom haurà de tenir les mateixes substitucions qualsevol que sigui la permutació de la que hom haurà partit. Per tant, si dins d'un d'aquests grups hom té les substitucions S i T , és segur que hom tindrà la substitució ST " (p.47).

Segons la meua interpretació, Galois està explicitant i cridant l'atenció sobre una propietat que tenen els seus grups. Sobre una propietat no imposada a priori, per a poder definir els grups, sinó sobre una propietat que hom pot constatar a posteriori, conseqüència de la manera com han estat construïts.

Quan Jordan desenvoluparà a fons les idees de Galois, s'en adonarà, però no immediatament, que aquesta és una idea fonamental a explotar i farà el que podríem anomenar una mena de capgirament teòric de les nocions involucrades en la teoria. Ell serà el primer en veure que hom pot començar dient "un grup és tal cosa, i les permutacions que hom associa a una equació formen un grup, etc". Exactament, el que Jordan va dir fou: "*Un sistema de substitucions formen un grup si el producte de dues substitucions qualssevol del sistema pertany al sistema*". I després va veure que les substitucions que transformen V_0 en $V_1, V_2, \dots, V_{n-1}$ formen un grup (en el seu sentit) que és el grup de l'equació en el sentit de Galois. Si bé Jordan va començar a desenvolupar les idees de Galois en el 1861, no és fins el 1867 que trobem publicada l'anterior definició de grup (14). No cal dir que si hom compara el treball de Galois amb la reformulació que en féu Jordan, una de les coses que més sobressurten és la nova flexibilitat, la nova suavitat fins i tot podriem dir, que adquireixen els mateixos enunciats i les mateixes demostracions quan són tractades amb la perspectiva introduïda per Jordan.

Les Proposicions II i III de la Memòria de Galois apareixen barrades pel llapis de Poisson. Al marge de la II, Galois va escriure "*Hi ha alguna cosa a completar en aquesta demostració. No tinc temps de fer-ho. Nota de l'A*". La III la va suprimir completament, substituint-la per un enunciat acompanyat del comentari "*Hom trobarà la demostració*". Aquestes correccions, amb les reserves mencionades més amunt, poden ser atribuïdes versemblantment a la nit anterior al duel. Es tracta, com la Proposició IV, de resultats preparatoris per a la Proposició V, l'altre resultat fona-

mental d'aquesta Memòria. El seus enunciats són els següents:

"Proposició II

TEOREMA. Si s'adjunta a una equació donada l'arrel r d'una equació auxiliar irreduïble, li succeirà una de les dues coses següents: o bé el grup de l'equació no canviarà pas, o bé es dividirà en p grups corresponent cadascun d'ells, respectivament, a l'equació proposada quan li es adjunta cadascuna de les arrels de l'equació auxiliar; 2n d'aquests grups gaudiran de la propietat remarcable que es passarà de l'un a l'altre operant sobre totes les permutacions del primer una mateixa substitució de lletres" (p. 55).

A l'enunciat d'aquest teorema, després dels mots *l'arrel r d'una equació auxiliar irreduïble*, apareixen barrats aquests altres: *de grau primer p*. Aquesta condició és necessària per la demostració que dona Galois, tal com ja va veure Liouville.

"Proposició III

TEOREMA. Si s'adjunta a una equació TOTES les arrels d'una equació auxiliar, els grups considerats en el teorema II gaudiran a més d'aquesta propietat: les substitucions són les mateixes dins de cada grup" (p. 57)

"Proposició IV

TEOREMA. Si s'adjunta a una equació el valor NUMÈRIC d'una certa funció de les seves arrels, el grup de l'equa

ció es reduirà de manera que no contindrà d'altres permutacions que aquelles per les quals aquesta funció és invariable" (p. 57).

En el nostre llenguatge, la Proposició V estableix que una equació és resoluble per radicals si i només si el seu grup G conté una cadena de subgrups $1 \subset F \subset \dots \subset H \subset G$ tal que cada subgrup és normal en el següent i tal que cada quocient G/H és d'ordre un nombre primer.

En aquestes Proposicions és admirable el talent de Galois per arribar a demostrar aquest resultat per mitjà d'uns conceptes tan primitius i d'un llenguatge tan arcaic. Per exemple, l'existència d'un subgrup normal $H \subset G$ tal que l'ordre de G/H és un nombre primer p és enunciada així:

"... El grup de l'equació haurà de descompondre's en p grups gaudint, els uns respecte dels altres, d'aquesta doble propietat: 1^r que es passarà de l'un a l'altre per una única i mateixa substitució; 2^n que tots contindran les mateixes substitucions" (p.59).

El que ell enten per això és el següent, segons un exemple que facilita pel cas de l'equació general de 4^t grau. Segons Galois, el grup

a b c d	a c d b	a d b c
b a d c	c a b d	d a c b
c d a b	d b a c	b c a d
d c b a	b d c a	c b d a

es descompon en tres grups que tenen les propietats anteriors, cadascun d'ells format per les permutacions integrades en cada una de les tres columnes. Per a poder interpretar-ho en el nostre llenguatge, posem

$$t_1 = \begin{pmatrix} a & b & c & d \\ b & a & d & c \end{pmatrix} \quad t_2 = \begin{pmatrix} a & b & c & d \\ c & d & a & b \end{pmatrix} \quad t_3 = \begin{pmatrix} a & b & c & d \\ d & c & b & a \end{pmatrix} \quad s = \begin{pmatrix} a & b & c & d \\ a & c & d & b \end{pmatrix}$$

Només $H = \{1, t_1, t_2, t_3\}$, les substitucions de la primera columna, és un grup en el nostre sentit. Les permutacions de la segona i tercera columna són les classes laterals sH i s^2H . D'altra banda, les substitucions que apareixen en aquestes columnes, les que transformen la primera permutació de cadascuna d'elles en les tres permutacions restants, no són sinó sHs^{-1} i s^2Hs^{-2} .

Resultaria molt llarg explicar pas per pas tots els raonaments de Galois per arribar a establir aquesta condició necessària i suficient de resolubilitat, però n'hi ha un de pas que sí vull descriure perquè hem sembla significatiu per entendre la gènesi de les seves idees. Es tracta de la demostració de la suficiència d'aquesta condició.

Diu Galois (p. 61): sigui θ una funció de les arrels invariable per totes les substitucions d'un dels p grups en què G es descompon i variable per totes les altres permutacions. Aplica a θ una de les permutacions que la fa variar, i obté θ_1 . Aplica a θ_1 la mateixa permutació i obté θ_2 , etc. Galois sap que els únics valors diferents que pot obtenir són $\theta, \theta_1, \theta_2, \dots, \theta_{p-1}$, i que totes les permutacions del grup, o bé deixen inva-

riant les θ 's, o bé les permuten entre elles. Aleshores agafa la quantitat

$$A = (\theta + \alpha \theta_1 + \alpha^2 \theta_2 + \dots + \alpha^{p-1} \theta_{p-1})^p$$

on α és una arrel primitiva p -èsima de la unitat. Utilitzant el mateix raonament d'Abel que abans he descrit. Galois veu que podrà expressar la quantitat θ en funció del radical $\sqrt[p]{A}$.

L'adjunció d'aquest radical, com ha demostrat a la Proposició IV, redueix el grup de l'equació al subgrup que deixa invariant θ . Galois acaba dient

"Adjunteu a l'equació el radical en qüestió; ara podrem raonar sobre el nou grup com sobre el precedent, i caldrà que es descompongui de la manera indicada; i així successivament fins a un cert grup que només contindrà una única permutació" (p. 61).

Jordan, a partir d'aquest resultat va assolir els conceptes de *successió* i de *factors de composició* d'un grup, i el va reenunciar dient que una equació és resoluble per radicals si i només si els seus factors de composició són tots primers.

Diguem, finalment, que la Memòria de Galois conté 3 Proposicions més dedicades al cas particular de les equacions de grau primer. El que Galois arriba a demostrar aplicant el seu criteri de resolubilitat és, primer, que una condició necessària i suficient per tal que aquestes equacions siguin resolubles per radi-

cals és que el seu grup no contingui sinó permutacions

$$s = \begin{pmatrix} 1 & 2 & 3 & \dots \\ s(1) & s(2) & s(3) & \dots \end{pmatrix}$$

de la forma $s(k) = ak + b$, a i b constants. Per mitjà d'això, demostra que es condició necessària i suficient que totes les arrels de l'equació es puguin expressar racionalment en funció de dues arrels qualssevol.

4. L'informe de Poisson

Es fífficil d'entendre que un home de la competència matemàtica de Poisson no advertís la importància de la Memòria de Galois, tanmateix aquesta fos extraordinàriament concisa i difícil de llegir. Això no obstant, les paraules de Poisson ens permeten reconstruir un context en el que es fa més comprensible el fracàs de Galois,

L'informe acaba amb aquestes frases (15):

"Sigui com sigui, nosaltres hem fet tots els esforços per comprendre la demostració del Sr. Galois. El seus raonaments ni són prou clars ni estan prou desenvolupats perquè haguem pogut jutjar llur exactitud, i no estem en disposició de donar-ne una idea en aquest Informe. L'autor anuncia que la proposició que és l'objecte especial de la seva Memòria és una part d'una teoria general sus-

ceptible de moltes altres aplicacions. Succeeix sovint que les diferents parts d'una teoria, aclarint-se mútuament, son més fàcils de copsar en llur conjunt que aïlladament. Hauríem d'esperar, doncs, que l'autor hagi publicat enterament el seu treball per formar-nos una opinió definitiva; però en l'estat que ara és la part que ha sotmès a l'Acadèmia, no podem proposar-vos que hi doneu la vostra aprovació".

La falta de desenvolupament de les idees de Galois que Poisson troba a faltar és molt més un efecte òptic de perspectiva que una insuficiència real. Em penso que un factor clau per valorar un resultat en Matemàtiques és moltes vegades la seva utilitat, la seva capacitat per a ser aplicat, entenent *aplicat* en un sentit molt ampli. La importància del criteri d'utilitat, almenys en el cas de Poisson, queda explicitat en el següent paràgraf del mateix informe on es qüestionen el sentit i la finalitat de les aportacions de Galois:

"En tot cas, cal remarcar que [*la Memòria*] no conté pas, com el títol de la Memòria ho prometia, la condició de resolubilitat de les equacions per radicals doncs, admetent com a certa la proposició del Sr. Galois, no hauríen avençat gaire per saber si una equació donada de grau primer és resoluble o no per radicals, ja que caldria, en primer lloc, assegurar que l'equació es reduïble, i, després, que una de les arrels es pot expressar en funció racional de dues altres. La condició de resolubilitat, si

existeix, hauria de tenir un caràcter exterior que es pot gués verificar per l'inspecció dels coeficients d'una equació donada, o com a molt resolent altres equacions de grau menys elevat que el de la proposada".

Sembla clar que Poisson continua pensant en la resolubilitat per radicals d'una forma antiga; es a dir, d'una forma molt lligada als radicals com a mètode efectiu de càlcul de les solucions. Si no com a mètode per a usar pràcticament, sí com a mètode en principi practicable i que arriba a donar, en concret, l'expressió de les arrels com a combinació explícita de radicals (tal com ho fan els mètodes de resolució de les equacions de 3^r i 4^t grau).

El que és interessant és que Galois ja ho sabia això, ja s'havia plantejat aquesta objecció i havia explicat el que hi havia de nou en el seu enfocament. Al respecte, Galois havia escrit:

"Donada una equació algebraica amb coeficients qualssevol, numèrics o literals, reconèixer si les arrels poden expressar-se per radicals és la qüestió de la que oferim una solució completa.

Ara bé, si em doneu una equació que haureu escollit lliurement i desitgeu saber si és o no resoluble per radicals, jo no podré fer-hi res més que indicar-vos el mitjà de respondre a la vostra qüestió sense voler encarregar ni a mi ni a ningú el fer-ho. En una paraula, els càlculs

son impracticables.

Semblarà després d'això que no es pot treure cap profit de la solució que proposem.

Seria així, en efecte, si el problema es presentés ordinàriament des d'aquest punt de vista. Però gairebé sempre, en les aplicacions de l'Anàlisi Algebraica, es ve a parar a equacions de les quals es coneixen per endavant totes les propietats: propietats per mitjà de les quals sempre serà fàcil respondre a la qüestió amb les regles que anem a exposar. (...)

Citaré com exemple les equacions que donen la divisió de les funcions el·líptiques i que el cèlebre Abel ha resolt. Certament, no es pas a partir de llur forma numèrica que ho ha conseguit". (16).

Sembla clar que per la pròpia dinàmica del desenvolupament de les Matemàtiques en d'altres branques que no eren l'Àlgebra, que eren, essencialment, l'estudi de les funcions el·líptiques mencionades per Galois, ell, com Abel i alguns pocs més, va arribar a veure que el problema de la resolubilitat per radicals no era interessant des del punt de vista estrictament numèric lligat a la resolució d'equacions concretes. Que podia ser interessant disposar d'un criteri teòric per a poder fer anar famílies d'equacions de les quals la informació que hom disposava ja no eren els coeficients, sinó, directament, relacions funcionals entre les arrels, etc. Aquests problemes matemàtics nous en els que les equacions jugaven un paper nou van aparèi-

xer de manera oficial amb Jacobi l'any 1830. Poc després, tot això va trobar un camp amplíssim d'aplicació en el desenvolupament de la Geometria Analítica, però ara ja parlem de coses que van passar a començaments del anys 1850.

Em penso que es per això, per l'anacronisme dels seus criteris de valoració, que Poisson no va poder apreciar el treball de Galois. En qualsevol cas, que el problema mencionat havia de ser una dificultat real en el segle passat queda corroborat per unes paraules de Jordan, de l'any 1867, que insisteixen sobre el mateix:

"Cal reconèixer que aquest criteri, satisfactori des del punt de vista teòric, conduiria generalment a càlculs impracticables en la seva aplicació; però hi ha equacions força interessants (en la teoria de les funcions el·líptiques, per exemple) els coeficients de les quals no estan donats immediatament i es determinen amb molta menys facilitat que el propi grup. (...)

D'altra banda, el mètode citat té un avantatge bastant més considerable que una aplicació més o menys fàcil a tal o tal equació numèrica, és el de permetre *enumerar i classificar* immediatament, per cada grau donat, els diversos tipus generals d'equacions resolubles per radicals, i de determinar per cadascun d'ells el nombre i el grau de les extraccions d'arrels a efectuar per resoldre'l". (17).

Que Jordan trobés interessant d'incloure aquest comentari en una carta a Liouville permet entendre que per la mentalitat de l'època no havia de ser fàcil adonar-se'n de la revolució metodològica que es produïa dins de l'Àlgebra.

Em penso que podem concloure, doncs, que Galois es va veure perjudicat per ser doblement revolucionari: per ser-ho de vida i obra. Molts autors han subratllat la importància que podien tenir els factors polítics i ideològics en els fracassos acadèmics de Galois. Per dir-ho amb les paraules d'un il·lustre historiador de la ciència, R. Taton,

"Cauchy i Poisson, monàrquics convençuts, gent d'ordre, no havien d'estar pas predisposats en favor d'aquell jove que s'els apareixia com un agitador, com un esperit subversiu en tots els camps; i potser cregueren trobar-se amb un d'aquests individus utòpics que cada dia pretenen resoldre problemes difícils o impossibles". (18)

És evident que no cal contraposar una explicació sociològica a una altra d'intrinseca per entendre aquest afer, més aviat cal pensar que ambdues explicacions es complementen. Si Galois hagués estat ben considerat per l'*establishment* acadèmic, possiblement el seu treball hagués estat avaluat amb més benevolència. Però si Poisson l'hagués pogut ponderar amb un criteri no anacrònic, tampoc no hagués deixat de reconèixer les idees innovadores i fèrtils que contenia.

Cal dir, finalment, que el concepte de grup encara va

tardar molt en trobar la seva definició actual. Ja he mencionat quina fou la definició de Jordan de grup de permutacions. Arthur Cayley (1821-1895), abans, havia donat una definició més general de grup *finit* que va aplicar a matrius i a quaternions, però aquest fou un treball que va passar desapercbut fins a l'últim quart del segle 19 i que no va influir en el desenvolupament de la Teoria de Galois (19). Segons Dieudonné, la primera definició acceptable, des del punt de vista contemporani, de *grup abstracte infinit* és deguda a Heinrich Weber (1842-1913) i fou publicada l'any 1899. (20)

No vull acabar sense dir en veu alta una pregunta que jo em faig a la vista d'aquesta història. Fins a quin punt no es falseja la realitat quan es diu, com ho ha dit Bourbaki i com ho han repetit molts d'altres, que la funció essencial d'una estructura algebraica com la de grup es la d'expressar sintèticament, de forma conceptualment econòmica, les propietats comunes a molts conjunts dotats d'operacions internes?

NOTES

1. J.-L. Lagrange: "Reflexions sur la résolution algébrique des équations", *Oeuvres*, vol. III, p. 205-421, Paris, Gauthier Villars, 1867-1892.
2. A.-L. Cauchy: "Mémoire sur le nombre des valeurs qu'une fonction peut acquérir lorsqu'on y permute de toutes les manières possibles les quantités qu'elle renferme", *Oeuvres complètes*, 2e série, vol I, p. 64-90, Gauthier-Villars, Paris, 1882-1974.
3. N.-H. Abel: "Mémoire sur une classe particulière d'équations résolubles algébriquement", *Oeuvres*, vol I, p. 478-507, Christiania, 1881.
4. Existeix versió francesa facsímil de la de 1807: *Recherches Arithmétiques*, Paris, Albert Blanchard, 1979.
5. l.c. nota 3, 478-9
6. l.c. nota 3, p. 483
7. l.c. nota 3, p. 491
8. A.-T. Vandermonde: "Mémoire sur la résolution des équations". *Histoire de l'Académie royale des sciences, année 1771, 1774*, p. 365-416.
9. H. Lebesgue: "L'oeuvre mathématique de Vandermonde", *L'Enseignement Mathématique*, (2), vol. I, 1956, p. 203-23.
10. El treball de 1824 és la "Mémoire sur les équations algébriques, où l'on démontre l'impossibilité de la résolution de l'équation générale du cinquième degré", *Oeuvres*, vol I, p. 28-33. El de 1826 es titula "Demonstration de

l'impossibilité de la résolution algébrique des équations générales qui passent le quatrième degré", *Oeuvres*, vol I, p. 66-87.

11. B.M. Kiernan: "The Development of Galois Theory from Lagrange to Artin", *Archive for History of Exact Sciences*, vol. 8, 1-2, 1971, p. 40-154. L'opinió esmentada es troba a la p. 71.
12. He fet servir l'edició de R. Bourgne i J.P. Azra: *Écrits et Mémoires mathématiques d'Evariste Galois*, París, Gauthier-Villars, 1962. Les referències a pàgines que hom trobarà a continuació corresponen a aquesta edició.
13. cf. J. Dieudonné i altres: *Abrégé d'histoire des Mathématiques (1700-1900)*, París, Hermann, 1978, vol I, p. 283.
14. C. Jordan: "Mémoire sur la résolution algébrique des équations", *Oeuvres*, vol I, p. 109-57, París, Gauthier-Villars, 1961-1964. La definició es troba a la p. 109.
15. Hom pot trobar reproduït tot l'informe de Poisson a l'article de Taton citat a la nota 18, p. 120-2.
16. l.c. nota 12, p. 39-41. Aquest text fou publicat per primera vegada per J. Tannery l'any 1906.
17. "Lettre a M. Liouville sur la résolution algébrique des équations", *Oeuvres*, vol. I, p. 105-8. El fragment citat es troba a les p. 107-8. Els subratllats són de l'autor.
18. R. Taton: "Les relations d'Evariste Galois avec les mathématiciens de son temps", *Revue d'Histoire des Sciences*, vol I, num 2, 1947, p. 114-30. El fragment citat es troba a les p. 129-30.
19. cf. Kiernan, l.c. nota 11, p. 94, i Dieudonné, l.c. nota 13,

vol. I, p. 116.

20. l.c. nota 13, vol I, p. 116.