MAT^2

MATerials MATemàtics
Volum 2016, treball no. 4, 75 pp. ISSN: 1887-1097
Publicació electrònica de divulgació del Departament de Matemàtiques
de la Universitat Autònoma de Barcelona
www.mat.uab.cat/matmat

La «Mémoire» d'Évariste Galois, anotada i comentada

Josep Pla i Carrera

Nitens lux,
horrenda procella,
tenebris æternis involuta.
[Esclat brillant,
en el terror de la tempesta,
embolcallat per sempre més de tenebres.]

Il ne leur a fallu qu'un moment pour faire tomber cette tête
et cent années, peut-être,
ne suffiront pas pour en reproduire une semblable
[N'hi ha hagut prou amb un instant per decapitar-lo,
però, molt probablement, cent anys
no seran suficients per aconseguir-ne un altre com ell.]

En aquest treball pretenc fer una lectura comentada de la famosa *Mémoire*[1] del jove matemàtic francès Évariste Galois. Vol ser un homenatge en el bicentenari del seu naixement i alhora una contribució a l'«Any Galois» de la Facultat de Matemàtiques i Estadística de la UPC de la que en sóc «magister honoris causa».

La lectura meditada d'una matèria —fins i tot quan no se n'és especialista— és una eina metodològica i didàctica excel·lent tant pels que ens dediquem a la recerca com a la docència o a la història de la matemàtica.

Ningú —cap mestre— ens pot ensenyar millor la matemàtica més autèntica que el creador d'una idea, d'una tècnica, d'una teoria —perquè la matemàtica, no ho dubteu gens, és una creació de la ment humana.

I això és precisament el que he pretès fer en aquesta anàlisi de la «Mémoire» d'aquest jove gegant.

[1] NTC: Vegeu (Galois, 1831).

1 La Memòria de Galois

[417]

MEMÒRIA

Sobre les condicions de resolubilitat de les equacions per radicals. [2]

1.1 Introducció

Aquesta memòria[3] l'he treta d'una obra que vaig tenir l'honor de presentar, ara fa un any, a l'*Académie*. No havent estat compresa, i havent-se dubtat de la veracitat de les proposicions que s'hi proposaven, m'he hagut d'acontentar amb donar, de forma sintètica, els principis generals, i una *única* aplicació de la meva teoria. Suplico als meus jutges que almenys llegeixin amb atenció aquestes poques pàgines.

Hom hi trobarà una *condició* general que *ha de satisfer tota equació resoluble per radicals*, i que recíprocament n'assegura la resolubilitat. S'aplica només a les equacions de grau primer. [4] Heus ací el teorema que donem en la nostra anàlisi:

[2] Émile Picard: Aquesta memòria, *Mémoire sur les conditions de résolubilité des équations par radicaux* (Galois, 1897, p 33-50), i *Des équations primitives qui sont solubles par radicaux* (Galois, 1897, p 51-61) es van trobar entre els papers de Galois i Joseph Liouville les va publicar, per primera vegada, l'any 1846, precedides de la nota següent:

«Inserint la carta que heu llegit [vegeu la nota 3], els editors de la *Revue encyclopédique* anunciaren que pròximament publicarien els manuscrits que havia deixat Galois. La promesa no s'acomplí. Tanmateix *monsieur* Auguste Chevalier havia preparat el treball. Ens els va enviar i hom els trobarà en els fulls que segueixen:

1º Una memòria sencera dedicada a les condicions de resolubilitat per radicals de les equacions, amb aplicació a les equacions de grau primer.

2º Un fragment d'una segona memòria on Galois tracta de la teoria general de les equacions que anomena *primitives*.

He conservat la major part de les notes que Auguste Chevalley va adjuntar a les memòries que hem esmentat. Totes elles van marcades amb les inicials A. Ch. Les notes que van signades són del propi Galois.

Completarem aquesta publicació amb d'altres fragments trets dels papers de Galois, i que, malgrat que no tenen massa importància, tanmateix els geòmetres els podran llegir amb interès.»

Els fragments dels que parla Liouville en la darrera frase mai no van ser publicats.

[3] A. Ch.: «M'ha semblat convenient encetar la *Memòria* amb aquest prefaci —que ara llegiu—, encara que, segons he trobat, en el manuscrit se li havia passat ratlla».

Ntc: A. Ch. abreuja, com ja s'ha dit, el nom d'Auguste Chevalier l'amic a qui Galois adreçà la carta testament (Galois, 1897, p 25-32), datada el 29 de maig de 1832, la nit abans del duel, a la qual adjunta tres memòries: dues fan referència a la Teoria d'Equacions i la tercera, a les Integrals.

[4] Ntc: El grau de la qual és un nombre primer.

> Per tal que una equació de grau primer, sense divisors commensurables, sigui resoluble per radicals, és *necessari* i *suficient* que totes les arrels siguin funcions racionals de dues qualssevol.

Les altres aplicacions de la teoria són, en elles mateixes, d'altres teories particulars. Requereixen, a més, de la teoria de nombres, i d'un algorisme particular: les reservem per a una altra ocasió. En part fan referència a les equacions modulars de la teoria de les funcions el·líptiques que, com demostrarem, no poden ser resoltes per radicals

16 de gener de 1831.

E. GALOIS.

1.2 Principis

[418]

PRINCIPIS

Començaré establint algunes definicions i una sèrie de lemes tots ells prou coneguts.

1.2.1 Definicions

Definicions. Diem que una equació és reductible[5] quan admet divisors racionals; i irreductible, en cas contrari.

Ara cal explicar què entenem amb la paraula *racional* ja que intervé sovint.

Quan una equació té *tots* els coeficients numèrics i racionals, això significa solament que l'equació es pot descompondre en factors que tenen els coeficients numèrics i racionals.

Comentari 1. Aquí Galois, en llenguatge d'avui, suposa que $f(X) \in \mathbb{Q}[X]$ i que *factoritza* en $\mathbb{Q}[X]$; és a dir, $f(X) = f_1(x) \cdot \cdots \cdot f_r(X)$ on, per a tot $i = 1, \ldots, r$, $f_i(X) \in \mathbb{Q}[X]$.

Recordem que $f(X) \in \mathbb{Q}[X]$ signfica que existeixen $a_0, a_1, \ldots, a_n \in \mathbb{Q}$ i que $f(X) := a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0$.

[5] Al llarg de la traducció trobareu dos tipus d'èmfasi: els que utilitzen *lletra cursiva* corresponen al text original, els subratllats són afegits pel traductor i comentarista.

Comentari 2. Un polinomi és *mònic* quan $a_m = 1$.

És clar que, quan els coeficients pertanyen a un cos K —és a dir, si $f(X) \in K[X]$—, també $\mu\big(f(X)\big) = \frac{1}{a_n} f(X) \in K[X]$. En canvi, quan inicialment estem en un anell A —és a dir, si $f(X) \in A[X]$, com ara en el cas en què els coeficients són nombres enters—, aleshores $\mu\big(f(X)\big) = \frac{1}{a_n} f(X) \in K_A[X]$, on K_A designa el *cos de fraccions de l'anell* A; en concret, $K_A = \left\{\frac{a_1}{a_2} : a_1, a_2 \in A, \text{ amb } a_2 \neq 0\right\}$, tancat per suma i producte. És el mínim cos que conté l'anell A.

Ara bé, quan no *tots* els coeficients d'una equació són numèrics i racionals, per divisor racional hem d'entendre un divisor els coeficients del qual s'expressen com a funcions racionals dels coeficients de l'equació proposada.

Comentari 3. Aquí Galois encara no ha precisat el significat de l'expressió «quan no *tots* els coeficients d'una equació siguin numèrics i racionals». Per tant, l'equació «redueix» si admet un divisor els coeficients del qual són funcions racionals dels coeficients de l'equació inicial que són donats i, per tant, coneguts.

Així, en general, per quantitat racional s'entén una quantitat que s'expressa com a funció racional dels coeficients de l'equació proposada.

Comentari 4. Aquí, tot avançant-se, Galois diu que, si $K_0 \supseteq \mathbb{Q}$ és el cos més petit que conté els coeficients de l'equació inicial —no necessàriament $\mathbb{Q}$—, aleshores els factors han de ser de $K_0[X]$.

De fet, el nostre punt de partida és una equació polinòmica $f(X) = 0$ i volem treballar en el mínim cos K_0 dels coeficients $a_0, a_1, \ldots, a_{n-1}, a_n$ del polinomi $f(X)$. Dit altrament, $K_0 = \mathbb{Q}(a_0, a_1, \ldots, a_{n-1}, a_n)$.

Admetem, doncs, que el *cos base* —el cos dels coeficients— és K_0 que, en ocasions, és $\mathbb{Q}$.

Però hi ha més: podem convenir a considerar com a racional qualsevol funció d'un cert nombre de quantitats determinades, que suposem conegudes per endevant. Per exemple, podem elegir una certa arrel d'un nombre enter i considerar racional qualsevol funció racional d'aquest radical.

Comentari 5. Aquí Galois *estén* l'àmbit dels coeficients amb d'altres objectes numèrics ben determinats, com ara una arrel $\sqrt[k]{n}$, amb $k \in \mathbb{N}$ i $n \in \mathbb{Z}$.

Si bé, en el paràgraf anterior, deia que treballaríem dins del cos K_0, eventualment $\mathbb{Q}$, ara accepta «coeficients» més sofisticats —perquè, de fet, es tractarà d'usar-los com a coeficients. I tot seguit aclareix, amb un exemple

concret, quina mena de naturalesa poden tenir aquests objectes. Apareixen, doncs, els objectes $K_0(\alpha, \beta, \cdots, \nu)$ i $K_0(\sqrt[k]{n})$, amb $k \in \mathbb{N}$ i $n \in \mathbb{Z}$.

Quan convinguem a considerar doncs, com a conegudes, certes quantitats, diem que les *hem adjuntat a l'equació* que volem resoldre. Diem que aquestes quantitats són *adjuntades a l'equació*.

Comentari 6. Aquí, d'una manera molt informal, Galois considera una *extensió* del cos $\mathbb{Q}$ per un cert element prèviament conegut. Malgrat l'exemple concret que ofereix Galois, cal plantejar la qüestió de si necessàriament pensa que els objectes han de ser *algèbrics* o bé poden ser també *transcendents*. Edwards diu (Edwards, 2012, p 912–913): «Amb K designaré el cos que s'obté del cos $\mathbb{Q}$ dels nombres racionals en adjuntar-li un nombre finit de quantitats irracionals, algèbriques o transcendents.» I, en una nota de peu de pàgina, fa la consideració següent: «D'antuvi, el més simple és considerar que el cos base K és $\mathbb{Q}$. Aquest cas exhibeix tots els fets del cas general. La possible inclusió de quantitats transcendents la indica la referència de Galois en les observacions que precedeixen la demostració de la Proposició 1: "Equacions algèbriques" [vegeu la p 28]. Potser pensa en polinomis els coeficients dels quals són transcendents o, parlant més col·loquialment, coeficients que són lletres, i no pas nombres».

Així Galois obté, com a elements resultants de les adjuncions, els elements de $\mathbb{Q}(\alpha)$ i successivament, ja que parla de «certes quantitats» i no només d'una quantitat. És difícil, en aquest context, pensar si Galois es refereix a «adjuncions successives» o a una «adjunció múltiple» efectuada de cop —que caldria definir com es fa, si no és de la forma anterior. És a dir, es refereix a $\Big(\Big(\big(\mathbb{Q}(\alpha)\big)(\beta)\Big)\cdots\Big)(\nu)$ o a $\mathbb{Q}(\alpha, \beta, \ldots, \nu)$?

Tanmateix, hem de pensar que, per a Galois, $K_0(\alpha, \beta, \ldots, \nu)$ s'obté adjuntant $\alpha, \beta, \ldots, \nu$ d'un amb un. Vegeu, per exemple, la nota 20, p 36.

Un cop establert això, anomenarem *racional* tota equació que s'expressi com a funció racional dels coeficients de l'equació i d'un cert nombre de quantitats *adjuntades* a l'equació i prèviament conegudes.

Comentari 7. Ara Galois passa de considerar polinomis de $K_0[X]$ —o funcions racionals d'elements de $K_0[X]$— a considerar polinomis de l'anell $K_0(\alpha, \beta, \ldots, \nu)[X]$ —o les corresponents funcions racionals.

Quan fem ús d'equacions auxiliars totes elles són funcions racionals en el benentès que els seus coeficients ho siguin en el sentit que he exposat.

S'observa, a més, que les propietats i les dificultats d'una equació poden ser força diferents segons quines siguin les quantitats que se li hagin adjuntat. Per exemple, l'adjunció d'una quantitat pot fer que una equació irreductible sigui reductible.

Així doncs, quan a l'equació

[419]

$$\frac{X^n-1}{X-1}=0, \text{ amb } n \text{ primer,}$$

li adjuntem una de les arrels de les equacions auxiliars de Gauss, l'equació factoritza; és a dir, esdevé reductible.

Comentari 8. Això justifica que Galois parli d'adjuncions a l'equació. Resulten molt importants en relació amb l'equació.

Fixem-nos que, de forma ben explícita, Galois fa dependre el caràcter irreductible de l'equació $f(X)=0$ —i també les seves característiques— del cos K_0, eventualment $\mathbb{Q}$, o del cos $K=K_0(\alpha,\beta,\ldots,\nu)$ i no només de l'equació com si aquesta fos quelcom d'absolut. En concret, doncs, certs trets íntimament lligats a l'equació són, sense cap mena de dubte, *relatius* al cos dels coeficients.

Comentari 9. L'equació $X^2+1=0$ és irreductible a $\mathbb{Q}$ però, en canvi, redueix a $\mathbb{Q}(i)$.

L'equació $X^4-2=0$ —irreductible a $\mathbb{Q}[X]$— redueix a $\mathbb{Q}\big(\sqrt{2}\,\big)[X]$, on es pot escriure en la forma $\big(X^2+\sqrt{2}\,\big)\big(X^2-\sqrt{2}\,\big)$. Si ara considerem l'extensió $\mathbb{Q}\big(\sqrt{2},\sqrt[4]{2}\,\big)=\mathbb{Q}\big(\sqrt[4]{2}\,\big)$ —si un cos de nombres K conté un nombre, conté el seu quadrat—, tindrem òbviament $\big(X^2+\sqrt{2}\,\big)\big(X+\sqrt[4]{2}\,\big)\big(X-\sqrt[4]{2}\,\big)$. Ara bé, per tal que redueixi completament, cal adjuntar la unitat imaginària i. Així, el polinomi X^4-2, irreductible a $\mathbb{Q}[X]$, factoritza totalment a $\mathbb{Q}\big(\sqrt[4]{2},i\big)$,

$$X^4-2=\big(X+\sqrt[4]{2}\,\big)\big(X-\sqrt[4]{2}\,\big)\big(X+i\sqrt[4]{2}\,\big)\big(X-i\sqrt[4]{2}\,\big).$$

L'*obtenció* de les arrels de $f(X)=0$ depèn, doncs, no només de l'equació, sinó també de l'adjunció d'arrels. En particular, la *resolució per radicals* d'una equació $f(X)=0$ pot dependre —i, en la majoria dels casos, en depèn,— de l'adjunció, al cos de partida K_0, d'objectes de la forma $\sqrt[k]{n}$. Les arrels $\sqrt[k]{n}$ són, de fet, arrels de l'*equació auxiliar* $X^k-n=0$.

Les equacions auxiliars jugaran un paper clau a partir de la Proposició II d'aquesta memòria [vegeu la p. 36].[6]

[6] Ntc: Vegeu com justifica Julio Rey Pastor (Rey Pastor, 1915, edició de 1947, p 168) el nom «arrel» d'una equació polinòmica pel fet que les equacions de grau segon, tercer i quart admeten solament, com a equacions auxiliars, *equacions binòmiques*; és a dir, de la forma $X^k-n=0$.

No és, doncs, el mateix dir que $f(X) \in K_0[X]$ que dir que $f(X) \in K[X]$, on el cos K s'ha obtingut del cos K_0, eventualment $\mathbb{Q}$, adjuntant-li certes quantitats.[7]

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

Comentari 10. En aquesta definició hi vull veure una diferència substancial entre *permutació* i *substitució*: les permutacions són estàtiques i les substitucions, dinàmiques en el sentit que permeten passar d'una permutació a una altra.

Comentari 11. A la p. 5 hem vist que Galois diu que «les propietats i dificultats d'una equació poden ser força diferents...». Les substitucions serveixen per aclarir el que Galois entén amb aquests termes —a més de la reductibilitat/irreductibilitat.

Per veure com actuen les substitucions quan a l'equació li adjuntem objectes, considerem l'equació $X^4-5\,X^2+6=0$. A $\mathbb{Q}[X]$, el polinomi $f(X) := X^4-5\,X^2+6$ descompon en factors quadràtics:

$$X^4-5\,X^2+6=\big(X^2-2\big)\big(X^2-3\big). \tag{1}$$

Hi ha quatre substitucions de les arrels que deixen fixa l'expressió (1) —de fet són *transposicions* de dos elements, com ara $(a\ \ b)$ que substitueix a per b i b per a:

$$\mathcal{G}_1=\Big\{\mathrm{Id},(\sqrt{2}\ \ -\sqrt{2}\,),(\sqrt{3}\ \ -\sqrt{3}\,),(\sqrt{2}\ \ -\sqrt{2}\,)\circ(\sqrt{3}\ \ -\sqrt{3}\,)\Big\}. \tag{2}$$

Però tot canvia si mirem el polinomi com un polinomi de $K := \mathbb{Q}\big(\sqrt{3}\,\big)$ perquè, dins d'aquest nou cos K, hi ha expressions numèriques [vegeu la nota 18, p. 28] que **no** es mantenen quan apliquem les substitucions de (2). Si fem

$$\xi_1=\sqrt{2},\ \ \xi_2=-\sqrt{2},\ \ \xi_3=\sqrt{3},\ \ \xi_4=-\sqrt{3}, \tag{3}$$

resulta que

$$2\,\sqrt{3}\,\xi_3+\sqrt{3}\,\xi_4=3, \tag{4}$$

la relació numèrica —que prové de l'expressió polinomial $2\,\sqrt{3}\,X+\sqrt{3}\,Y\in K[X,Y]$ quan fem $X=\xi_3$ i $Y=\xi_4$— **no** admet cap de les substitucions $(\sqrt{3}\ \ -\sqrt{3})$, $(\sqrt{2}\ \ -\sqrt{2}\,)\circ(\sqrt{3}\ \ -\sqrt{3}\,)$. Vegeu el comentari 41, p. 33.

[7] NTC: Això, implícitament, ja ho sabien Joseph Louis Lagrange i Paolo Ruffini. Vegeu (Tignol, 2001, capítol 10 i, en particular, p 127-132, 145-147; 209-218), (Rosso, 2012) o (Marachia, 2002).

Un altre exemple. L'equació $X^3 + X^2 - 2\,X + 1 = 0$ té les arrels ξ_1^*, ξ_2^* i ξ_3^*. Quan a les variables x_1, x_2 i x_3 els hi assignem els valors de les arrels $\xi_1^*, \xi_2^*, \xi_3^*$, l'expressió $g(x_1, x_2, x_3) := x_1^2\,x_2 + x_2^2\,x_3 + x_3^2\,x_1$ valdrà 3 o 4, segons com hàgim ordenat les variables x_1, x_2, x_3.

Si agafem l'ordre de $\xi_1^*, \xi_2^*, \xi_3^*$ de manera que valgui 3 i li apliquem la substitució $(\xi_1^* \;\; \xi_2^*)$, valdrà 4. Així doncs $g(\xi_1^*, \xi_2^*, \xi_3^*)$ no admet la substitució $(\xi_1^* \;\; \xi_2^*)$. Vegeu (Edwards, 2012, p 917).

Quan es tracta de funcions, la permutació de partença que serveix per indicar les substitucions és totalment arbitrària; això és degut al fet que, en una funció de vàries lletres, **no** hi ha cap raó perquè una lletra ocupi un lloc o un altre.

Comentari 12. Així doncs, es fixa *una* determinació de les lletres i aleshores *tot en depèn*; és a dir, la determinació que s'ha fixat *no determina* res.

A l'exemple segon del comentari anterior, hem considerat la funció $g(\xi_1^*, \xi_2^*, \xi_3^*)$, però res no ens impedeix de considerar $g(\xi_2^*, \xi_1^*, \xi_3^*)$.

A la memòria és molt important la *resolvent [de Galois]* v_1: permet d'expressar cada arrel ξ_i de $f(X) = 0$ en la forma $\xi_i := \ell_i(v_1)$, on cada funció ℓ_i és una funció racional dels coeficients de $f(X) = 0$ —vegeu el LEMA III, p. 14. De fet, v_1 és un element primitiu; vegeu el comentari 52, p. 43.

A la p. 35 veurem que el grup de Galois no depèn de la funció v_1 que Galois defineix en el LEMA II, p. 12.

Ara bé, com que no és possible fer-se la idea d'una substitució sense haver-se fet la d'una permutació, en l'ús lingüístic, usarem amb freqüència les permutacions i solament considerarem les substitucions com a pas d'una permutació a una altra.

Comentari 13. Heus ací el caràcter dinàmic de les substitucions que he esmentat al comentari 10, p. 7.

De fet, quan tenim dues permutacions π_1, π_i —on π_1 és la permutació fixa—, la substitució σ_i fa que passem de la permutació π_1 a la permutació π_i. Ho podem escriure $\sigma_i : \pi_1 \to \pi_i$ o bé en la forma $\sigma_i := \binom{\pi_1}{\pi_i}$. És el caràcter *dinàmic* de les substitucions damunt les permutacions.

Quan vulguem agrupar substitucions les farem provenir totes de la mateixa permutació.

Comentari 14. És a dir, per a Galois hi ha una permutació inicial —convinguda i bàsica— que podem considerar que és $1 \;\; 2 \;\; 3 \;\cdots\; n$. Aleshores

$$\sigma_1 := \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 1 & 2 & 3 & \cdots & n \end{pmatrix} \text{ i, en canvi, } \sigma_i := \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \pi_1^i & \pi_2^i & \pi_3^i & \cdots & \pi_n^i \end{pmatrix},$$

on, per a cada $k = 1, \ldots, n$, $\pi_k^i \in \{1, 2, \ldots, n\}$, amb $\pi_k^i \neq \pi_\ell^i$, si $k \neq \ell$.

La notació $(\pi_1 \ \ \pi_2 \ \ \cdots \ \ \pi_n)$ indica el *cicle* que envia π_1 a $\pi_2, \ldots, \pi_i$ a π_{i+1}, per a $i < n$, i π_n a π_1.

Com que, en tots els casos, tractem qüestions en les quals la disposició primitiva de les lletres no importa per a res, en els grups que considerem, hi haurà d'haver les mateixes substitucions sigui quina sigui la permutació de la qual s'hagi partit. Així doncs, si en aquest grup hi ha les substitucions S i T, també hi haurà d'haver la substitució ST.

Comentari 15. En aquest paràgraf Galois introdueix el terme *grup* que, malgrat les imprecisions que conté, serà un terme que es consolidarà en la literatura matemàtica.

Ens recorda, a més, que les substitucions actuen sobre lletres —en realitat, sobre les arrels de l'equació polinòmica $f(X) = 0$. L'ordre amb que prenguem aquestes lletres no és essencial. Si inicialment tenim les lletres $a, b, c, \ldots, m$ —que nosaltres indicarem $\xi_1, \xi_2, \ldots, \xi_n$—, el que importa és conèixer com es mouen les lletres quan se'ls hi aplica una substitució i això no depèn de l'enumeració inicial.

A més, diu ben clarament, «Si $S, T \in \mathcal{G}$, aleshores $S \circ T \in \mathcal{G}$».[8]

Òbviament cal suposar que aquesta propietat val també quan $S = T$. Considerem els dos exemples següents (Rey Pastor, 1915, edició de 1947, p 191):

$$\mathcal{G}_1 = \big\{(1\ \ 2), (3\ \ 4), (1\ \ 2)(3\ \ 4)\big\}, \tag{5}$$

$$\mathcal{G}_2 = \big\{\mathrm{Id}, (1\ \ 2\ \ 3\ \ 4), (1\ \ 4\ \ 3\ \ 2)\big\}. \tag{6}$$

És clar que $\mathcal{G}_1$ és tancat pel producte dels elements que conté, però no és un grup: li manca la permutació Id; ara bé, si imposem que la propietat anterior val també quan $S = T$, aleshores $\mathcal{G}_1$ conté $\mathrm{Id} = (1\ \ 2)^2 = (3\ \ 4)^2 = (1\ \ 2)^2 \circ (3\ \ 4)^2$.

En el segon cas, òbviament, $\mathrm{Id} = (1\ \ 2\ \ 3\ \ 4) \circ (1\ \ 4\ \ 3\ \ 2) = (1\ \ 4\ \ 3\ \ 2) \circ (1\ \ 2\ \ 3\ \ 4)$. Però $(1\ \ 2\ \ 3\ \ 4)^2 = (1\ \ 3) \circ (2\ \ 4)$ no hi és, si no acceptem que $\mathcal{G}_2$ és tancat pel producte també quan $S = T$.

Com veurem més endavant, al comentari 51 de la p. 43, això, al meu entendre, posa clarament de manifest que Galois distingia a la perfecció entre el quadre del grup, tal com l'ofereix —que és un quadre de permutacions—, i el grup de les substitucions que hi ha amagat a sota.

[8] NTC: Entendrem que, en primer lloc, actua la substitució T i després la S.

És difícil esbrinar si Galois aplica les susbstitucions per l'esquerra —com he triat jo de fer-ho— o bé per la dreta, però això no és essencial i no ens ha de preocupar; de fet es tracta de canviar $\sigma \circ \tau$ per $\tau \circ \sigma$. L'efecte és el mateix.

Aquestes són les definicions que m'ha semblat que calia recordar.

Comentari 16. Si consultem el *Comentari* de Jordan (Jordan, 1869), ens adonarem que, en les seves definicions, fa més èmfasi a la part de les substitucions —creu que cal aclarir-les millor— que no pas a la part de les adjuncions —que considera prou precises en el text de Galois.

1.2.2 Lemes

LEMA I. Una equació irreductible no pot tenir cap arrel comuna amb una altra equació racional sense dividir-la. [9]

Ja que el màxim comú divisor de l'equació irreductible i l'altra equació serà també racional, etc. □

Comentari 17. **Demostració** del LEMA I. Aquí Galois usa que, si $f(X)$, $g(X) \in K[X]$, aleshores

$$m(X) = \operatorname{mcd}\big(f(X), g(X)\big) \in K[X],$$

quelcom que garanteix l'*algorisme d'Euclides* que solament usa les quatre operacions elementals —suma, resta, producte i quocient— dels coeficients, totes elles vàlides al cos K.

Sigui ξ és una arrel comuna de $f(X)$ i $g(X)$, on $f(X)$ és irreductible a $K[X]$. Aleshores també ho és de $m(X)$, atès que, per l'*algorisme de divisió*, tenim

$$g(X) = f(X) \times q(X) + r(X), \text{ amb } \operatorname{grau}\big(r(X)\big) < \operatorname{grau}\big(f(X)\big).$$

Per tant, ξ és una arrel de $r(X) = 0$. Iterant en l'algorisme d'Euclides resulta que $m(\xi) = 0$. D'on: $\operatorname{grau}\big(m(X)\big) \geq 1$.

Ara bé, $m(X)\big|f(X)$ i $m(X)\big|g(X)$. De la primera relació en resulta que $m(X) = \lambda f(X)$, amb $\lambda \in K$, atès que, per hipòtesi, $f(X)$ és irreductible a $K[X]$ i, de la segona, en resulta, com volíem, que $f(X)\big|(X)$.

Comentari 18. **Realment important**. Fixem-nos que, encara que ξ sigui una arrel de $f(X) = 0$, si dividim $f(X)$ per $X - \xi$, el quocient cau fora de $K[X]$ perquè, com mostra la *regla de Ruffini*, en els coeficients de la divisió, apareixen potències de ξ i, si $\xi \notin K$, el quocient serà de $K(\xi)[X]$ [vegeu el lema 23.1 del comentari 23, p. 15].

En canvi, si dividim $f(X)$ per $m(X)$, no sortim de l'anell de polinomis $K[X]$.

[9] NTC: Vegeu (Jordan, 1869, p. 143-144).

Comentari 19. Aquest resultat el trobem ja a (Abel, 1829).

Comentari 20. Metodològic important. Aquest lema tan simple i el *teorema fonamental de les funcions simètriques* —que Galois no esmenta de forma explícita en cap moment però que usa de forma implícita en diverses ocasions de la «Memòria»— són les eines que precisa en moltes de les demostracions.

Recordem el *teorema fonamental de les funcions simètriques*. Tota funció racional simètrica de les arrels ξ_i de l'equació $f(X)=0$ es pot escriure com una funció racional —polinòmica, si la inicial és polinòmica— dels coeficients $a_0, a_1, \dots, a_{n-1}, a_n \in K$ del polinomi $f(X) \in K[X]$ i recíprocament.

Això és conseqüència immediata del

Lema 20.1. Tota funció racional simètrica es pot escriure com una funció racional de les *funcions simètriques elementals* $s_1 = \sum_i^n \xi_i, s_2 = \sum_{i,j,i<j}^n \xi_i\,\xi_j$, $\dots, s_n = \xi_1 \dots \xi_n$.

En efecte. Tota funció racional dels coeficients de l'equació polinòmica $f(X)=0$ és una funció simètrica de les arrels $\xi_1, \dots, \xi_n$ de l'equació polinòmica, ja que tenim les relacions

$$s_1 = -\frac{a_{n-1}}{a_n},\quad s_2 = \frac{a_{n-2}}{a_n}, \dots,\quad s_n = (-1)^n \frac{a_0}{a_n},$$

que s'obtenen trivialment de la identitat:

$$\begin{aligned} a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0 \\ &= a_n\big(X-\xi_1\big)\big(X-\xi_2\big)\cdots\big(X-\xi_n\big) \\ &= a_n\big(X^n - s_1 X^{n-1} + s_2 X^{n-2} + \dots + (-1)^n s_n\big) \end{aligned}$$

L'altre implicació és més delicada. Sigui

$$F(X_1, \dots, X_n) = \sum a_{i_1 \dots i_n} X_1^{i_1} \cdots X_n^{i_n}$$

una funció simètrica respecte de les variables $X_1, \dots, X_n$. Si conté el monomi $a_{i_1 \dots i_n} X_1^{i_1} \cdots X_n^{i_n}$, també conté el monomi $a_{i_1 \dots i_n} X_{\sigma(1)}^{i_1} \cdots X_{\sigma(n)}^{i_n}$ ja que, per hipòtesi, $F(X_1, \dots, X_n)$ és simètrica.

Ara, en cada un dels grups de monomis que es transformen entre si per les substitucions $\sigma \in \mathfrak{S}_n$, distingim el *monomi principal* —el monomi de *potència total* $i := i_1 + \dots + i_n$, $a_{i_1 \dots i_n} X_1^{i_1} \cdots X_n^{i_n}$, amb $i_1 \geq i_2 \geq \dots \geq i_n$.

Ordenem *tots* els monomis d'aquesta mena de la forma següent: si els monomis $a_{i_1 \dots i_n} X_1^{i_1} \cdots X_n^{i_n}$, amb $i_1 \geq i_2 \geq \dots \geq i_n$, i $a_{j_1 \dots j_n} X_1^{j_1} \cdots X_n^{j_n}$, amb $j_1 \geq j_2 \geq \dots \geq j_n$, són dos representants, diem que $a_{i_1 \dots i_n} X_1^{i_1} \cdots X_n^{i_n}$ *és més*

potent que $a_{j_1\cdots j_n}\, X_1^{j_1}\cdots X_n^{j_n}$, si $(i_1, i_2, \ldots, i_n) \triangleright (j_1, j_2, \ldots, j_n)$, on $\triangleright$ és l'*ordre lexicogràfic*; és a dir, el primer índex k per al qual $i_k \neq j_k$, satisfà $i_k > j_k$.

Agafem el terme de *màxima potència*: $a_{i_1\cdots i_n}\, X_1^{i_1}\cdots X_n^{i_n}$ i considerem l'expressió $s_1^{r_1}\, s_2^{r_2}\, \cdots\, s_{n-1}^{r_{n-1}}\, s_n^{r_n}$ en la qual $X_1^{r_1+r_2+\cdots+r_n}\, X_2^{r_2+\cdots+r_n}\, \cdots\, X_{n-1}^{r_{n-1}+r_n}\, X_n^{r_n}$ és el terme més potent. Cal, doncs, que $r_n = i_n$, $r_n + r_{n-1} = i_{n-1}, \ldots,$ $r_n + \cdots + r_2 = i_2, r_n + r_{n-1} + \cdots + r_2 + r_1 = i_1$. Això permet determinar els exponents r_1, r_2, $\ldots$, r_{n-1}, r_n.

Ara considerem

$$G(X_1, \ldots, X_n) = F(X_1, \ldots, X_n) - a_{i_1\cdots i_n}\, s_1^{i_1-i_2}\, s_2^{i_2-i_3}\, \cdots s_{n-1}^{i_{n-1}-i_n}\, s_n^{i_n}.$$

La potència total de la funció $G(X_1, \ldots, X_n)$ és inferior a la potència total de la funció $F(X_1, \ldots, X_n)$ i, iterant, s'arriba a la funció nul·la. Això prova el que volíem.[10]

LEMA II. Donada una equació arbitrària sense arrels múltiples, les arrels de la qual són $a, b, c, \ldots$, sempre podem considerar una funció V de les arrels de manera que els valors que s'obtinguin en permutar, en la funció V, les arrels de totes les maneres no siguin iguals.

Per exemple, podem prendre

$$V = A\,a + B\,b + C\,c \cdots,$$

on $A, B, C, \ldots$, són nombres enters elegits convenientment.[11] □

Comentari 21. Galois solament ho afirma. No ho demostra.

Cal fer algunes precisions:

Precisió 21.1. En aquest text Galois manté la mateixa postura conceptual que havia criticat Gauss als qui, abans d'ell, havien intentat de demostrar el *teorema fonamental de l'àlgebra*. Acceptaven, tàcitament, que les arrels de l'equació que es vol resoldre existeixen en algun indret. Per tal d'aconseguir la total correcció deductiva del text de Galois caldrà esperar la demostració

[10] Vegeu (TEIXIDOR and VAQUER, 1968, p 119-123).

NTC: Aquest resultat es coneix amb el nom de *teorema de Waring-Hilbert*. De fet, l'enuncià Edward Waring l'any 1770, i el demostrà Hilbert, l'any 1909. Vegeu (Waring, 1770) i (Hilbert, 1909).

[11] GALOIS: Hem transcrit textualment la demostració que donàrem d'aquest lema en una memòria presentada l'any 1830. Hi afegim, com a document històric, la nota següent que *monsieur* Poisson cregué que calia adjuntar-hi: «La demostració d'aquest lema no és suficient, però és veritat segons el núm. 100 de la memòria de Lagrange, Berlin, 1770». (Lagrange, 1771, §100, p. 374 i següents).

Hom jutjarà.

de Kronecker de 1884[12] encara que Cauchy, l'any 1842, ja havia definit el cos $\mathbb{C}$ dels nombres complexos com $\mathbb{R}[X]/(X^2+1)$.

Precisió 21.2. La restricció que totes les arrels siguin diferents —un fet essencial en els raonaments de Galois— no és restrictiva, atès que el polinomi $d(X) := \mathrm{mcd}\big(f(X), f'(X)\big)$ conté les arrels múltiples d'$f(X) = 0$, reduïdes, però, d'una unitat en l'ordre de multiplicitat.

Recordem que, si $f(X) = (X-\xi_1)^{m_1} \dots (X-\xi_n)^{m_n}$, amb almenys un índex $m_j > 1, 1 \leq j \leq n$, s'aconsegueix un polinomi $d(X)$ que té les mateixes arrels que el polinomi $f(X)$, però *simples*.

Ara només cal que ens preocupem de cercar les arrels de l'equació polinòmica $d(X) = 0$.

Precisió 21.3. Si $f(X)$ és irreductible en K, aleshores no té cap arrel múltiple.

En efecte. Si no, factoritzaria perquè $d(X)\big|f(X)$ i $\mathrm{grau}\big(d(X)\big) \geq 1$. □

Comentari 22. **Demostració** del LEMA II, que Galois omet. Siguin $\xi_1, \dots, \xi_n$, les n arrels de l'equació polinòmica $f(X) = 0$, amb $f(X) \in K[X]$, sense arrels dobles, on $K \supseteq K_0 \supseteq \mathbb{Q}$. Volem que *totes* les diferències de les $n!$expressions que s'obtenen de $v_1 = a_1\,\xi_1 + a_2\,\xi_2 + \dots + a_n\,\xi_n$ quan sotmetem les arrels $\xi_1, \dots, \xi_n$ a *totes* les permutacions del *grup simètric* $\mathfrak{S}_n$ siguin diferents de zero. En conseqüència, cal que el producte $\Delta = \Delta(a_1, a_2, \dots, a_n)$ de totes elles —consta de $n!(n!-1)$ factors— també sigui diferent de zero.

Ara bé, els coeficients de Δ —considerat com un polinomi en n variables— pertanyen a K ja que són funcions simètriques de les arrels $\xi_1, \dots, \xi_n$ de l'equació $f(X) = 0$.

Disposem, doncs, d'un polinomi $\Delta(Y_1, \dots, Y_n) \in K[Y_1, \dots, Y_n]$ i volem garantir l'existència d'enters que no l'anul·lin.

La qüestió és: Existeixen?

Resposta de Tignol (Tignol, 2001, p 245). En l'espai vectorial K^n considerem la unió d'una col·lecció finita de subespais vectorials de dimensió 1,que no aconsegueix en cap cas d'omplir l'espai. Hi ha punts de K^n que tenen la propietat que busquem. □

Resposta d'Edwards (Edwards, 2012, p 914). Una resposta positiva la podem fer per inducció sobre n.

Si $n = 1$, aleshores $\Delta(Y_1) \in K[Y_1]$. Per tant solament té un nombre *finit* d'arrels a $\mathbb{Z}$. Existeix, doncs, un element $a_1 \in \mathbb{Z}$ per al qual $\Delta(a_1) \neq 0$.

Sigui $n := m+1$ i suposem que el teorema és cert per a $n := m$. Tenim el polinomi $\Delta(Y_1, \dots, Y_m, Y_{m+1})$ i fem $Y_j = a_j, j = 1, \dots, m$. Obtenim un

[12] NTC: Vegeu (Kronecker, 1884).

polinomi $\Delta^*(Y_{m+1})$ els coeficients del qual són polinomis de $a_1, \ldots, a_m$. Ara, usant la hipòtesi d'inducció, agafem $a_1, \ldots, a_m \in \mathbb{Z}$ de manera que no anul·lin cap d'aquests polinomis coeficients —que, en nombre, són *finits*. Així obtenim un polinomi $\Delta^*(Y_{m+1}) \in K[Y_{m+1}]$ i li apliquem el cas anterior en què $n = 1$. □

Resposta de Rey Pastor (Rey Pastor, 1915, edició de 1947, p. 230), o també (Connes, 2005, p. 3). D'entrada es fixen els coeficients de manera adequada.

Per exemple, $a_i = q^i$, amb $q \in \mathbb{Z}$, o bé $a_i = i, i = 1, \ldots, n$. Quants valors de q fan $v_i = v_j, 1 \leq i < j \leq n$!? Solament un nombre *finit*, ja que, per a cada parella i, j, obtenim una equació polinòmica en q de grau $\leq n$. Solament admet un nombre finit de valors possibles de q; d'equacions també n'hi ha una quantitat finita. Agafem, doncs, un $q \in \mathbb{Z}$, diferent de tots aquests.

Nota. Lector, què passa si fas $a_i = i, i = 1, \ldots, n$? □

Resposta meva. Fixats $\xi_1, \ldots, \xi_n$, busquem $a_1, a_2, \ldots, a_n$, de manera que, en fer les diferències, s'obtinguin vectors de l'*hiperplà* ortogonal al vector $(\xi_1, \ldots, \xi_n)$. Hi ha vectors de K^n que no són d'aquest hiperplà. Agafem-ne un de fora de l'hiperplà. □

En la literatura actual, les funcions $v := v\big(\xi_1, \ldots, \xi_n\big)$ de les arrels ξ_1, …, ξ_n de l'equació $f(X) = 0$ que, en ser permutades, generen $n!$ valors diferents, es coneixen amb el nom de *resolvents de Galois*.

LEMA III. La funció V, elegida com s'ha indicat a l'article anterior, té
[420] aquesta propietat: totes les arrels de l'equació proposada s'expressen racionalment en funció de V.

En efecte, sigui

$$V = \varphi(a, b, c, d, \ldots),$$

o bé

$$V - \varphi(a, b, c, d, \ldots) = 0.$$

Multipliquem ara totes les equacions semblants a aquesta, que s'obtenen permutant en elles totes les lletres, deixant fixa solament la primera. S'obtindrà una expressió com la següent:

$$\big[V - \varphi(a, b, c, d, \ldots)\big]\,\big[V - \varphi(a, c, b, d, \ldots)\big]\big[V - \varphi(a, b, d, c, \ldots)\big]\ldots,$$

que és simètrica en $b, c, d, \ldots$. Per consegüent es podrà escriure en funció de a. Obtindrem, doncs, una equació de la forma:

$$F(V, a) = 0.$$

Afirmo que, d'aquí, se'n pot treure el valor d'a. Per aconseguir-ho cal buscar una solució comuna d'aquesta equació i de la proposada. Aquesta solució serà l'única comuna. No n'hi pot haver cap altra com ara

$$F(V, b) = 0,$$

que tingui una solució comuna amb l'equació semblant, sense que una de les funcions $\varphi(a, \dots)$ sigui igual a una de les funcions $\varphi(b, \dots)$ i això contradiu la hipòtesi.

Se'n segueix, doncs, que a s'expressa com una funció racional de V, i el mateix podem dir de les altres arrels. □

Aquesta proposició [13] és citada, sense demostració, per Abel en la memòria pòstuma sobre funcions el·líptiques.

Comentari 23. Per demostrar-la, cal un lema previ:

Lema 23.1. Siguin $\xi_1, \xi_2, \dots, \xi_n$ les arrels de l'equació polinòmica $f(X) = 0$. Aleshores els polinomis simètrics elementals de $\xi_2, \dots, \xi_n$ es poden expressar com a funcions polinòmiques de ξ_1.

En efecte. Sigui

$$\begin{aligned} f(X) &= (X - \xi_1)(X - \xi_2) \cdots (X - \xi_n) \\ &= X^n - s_1 X^{n-1} + \cdots + (-1)^{n-1} s_{n-1} X + (-1)^n s_n. \end{aligned} \tag{7}$$

Aleshores,

$$\begin{aligned} \frac{f(X)}{X - \xi_1} &= (X - \xi_2) \cdots (X - \xi_n) = \\ &= X^{n-1} - s_1^* X^{n-2} + \cdots + (-1)^{n-2} s_{n-2}^* X + (-1)^{n-1} s_{n-1}^*. \end{aligned} \tag{8}$$

Per la *regla de Ruffini*,

$$\begin{array}{cccccc} & 1 & -s_1 & +s_2 & \cdots & (-1)^{n-1} s_{n-1} & (-1)^n s_n \\ \xi_1 & & \xi_1 & -\xi_1 s_1^* & \cdots & (-1)^{n-2} \xi_1 s_{n-2}^* & (-1)^{n-1} \xi_1 s_{n-1}^* \\ \hline & 1 & -s_1^* & s_2^* & \cdots & (-1)^{n-1} s_{n-1}^* & 0 \\ & & \| & \| & & \| & \\ & & -s_1 + \xi_1 & s_2 - \xi_1 s_1^* & \cdots & (-1)^{n-1} s_{n-1} + (-1)^{n-2} \xi_1 s_{n-2}^* & \end{array}$$

[13] GALOIS. És remarcable que, d'aquesta proposició, se'n pugui concloure que tota equació depèn d'una equació auxiliar de manera que totes les arrels d'aquesta nova equació *són funcions racionals les unes de les altres*; l'equació auxiliar de V n'és un cas. [L'èmfasi és meu.]

Aquesta observació és una simple curiositat perquè una equació amb aquesta propietat no és, en general, més fàcil de resoldre que l'altra.

En resulta trivialment que les funcions simètriques elementals de $\xi_2, \ldots, \xi_n$, $s_1^*, \ldots, s_{n-1}^*$, són polinomis de l'arrel ξ_1. □

Aquestes relacions també s'aconsegueixen si multipliquem directament $X - \xi_1$ pel polinomi (8) i igualant els coeficients amb els de l'equació (7). S'obténen les igualtats (Tignol, 2001, p 244):

$$\begin{aligned}
s_1^* &= s_1 - \xi_1, \\
s_2^* &= s_2 - s_1\,\xi_1 + \xi_1^2, \\
s_3^* &= s_3 - s_2\,\xi_1 + s_1\xi_1^2 - \xi_1^3, \\
&\vdots \\
s_{n-1}^* &= s_{n-1} - s_{n-2}\,\xi_1 + s_{n-3}\,\xi_1^2 - \cdots + (-1)^{n-2}\,s_1\,\xi_1^{n-2} + (-1)^{n-1}\xi_1^{n-1}.
\end{aligned}$$

□

Corol·lari 23.2. Observem que els coeficients de les potències successives de ξ_1 en les expressions de les $s_j^*, j = 1, \ldots, n-1$, són independents de ξ_1; és a dir, s'obtenen els mateixos coeficients per a qualsevol arrel ξ_i.

Aquest fet és bàsic en la demostració del LEMA III del comentari 24. □

Comentari 24. Demostració del LEMA III. Considerem la funció polinòmica[14]

$$G(V) = (V - v_1)(V - v_2)\cdots(V - v_{n!}),$$

on els $v_i, i = 1, 2, \ldots, n!$, són els $n!$ valors diferents que pren la *resolvent de Galois* $v = a_1\,\xi_1 + a_2\,\xi_2 + a_3\,\xi_3 + \cdots + a_n\,\xi_n$ quan permutem les arrels $\xi_1, \ldots, \xi_n$, de totes les maneres possibles amb les permutacions $\sigma \in \mathfrak{S}_n$.

Ara agrupem en un producte $\overline{G}_1(V, \xi_1)$ els factors de la forma

$$\begin{aligned}
&V - (a_1\,\xi_1 + a_2\,\xi_2 + a_3\,\xi_3 + \cdots + a_{n-1}\,\xi_{n-1} + a_n\,\xi_n), \\
&V - (a_1\,\xi_1 + a_3\,\xi_3 + a_2\,\xi_2 + \cdots + a_{n-1}\,\xi_{n-1} + a_n\,\xi_n), \\
&\qquad\vdots \\
&V - (a_1\,\xi_1 + a_n\,\xi_n + a_{n-1}\,\xi_{n-1} + \cdots + a_3\,\xi_3 + a_2\,\xi_2).
\end{aligned}$$

És a dir, s'agrupen tots els v_i que s'obtenen permutant totes les arrels ξ_i, llevat de la primera ξ_1. De factors d'aquesta mena n'hi ha $(n-1)!$. Si ara fem el mateix amb les arrels $\xi_2, \ldots, \xi_n$, tindrem

$$G(V) = \overline{G}_1(V, \xi_1)\,\overline{G}_2(V, \xi_2)\,\cdots\,\overline{G}_n(V, \xi_n),$$

ja que, en virtut del lema 23.1, p. 15, cada $\overline{G}_i(V, \xi_i), i = 1, \ldots, n$, depèn de forma simètrica de les arrels $\xi_1, \ldots, \xi_{i-1}, \hat{\xi}_i, \xi_{i+1}, \ldots, \xi_n,\ i = 1, \ldots, n$.

[14] NTC: L'anomeno G en honor de Galois.

Pel corol·lari 23.2, totes les expressions $\overline{G}_i(V,\xi_i), i=1,\dots,n$, proporcionen el mateix polinomi de dues variables $\overline{G}(V,X)\in K[V,X]$. Així doncs,

$$G(V)=\overline{G}(V,\xi_1)\,\overline{G}(V,\xi_2)\cdots\overline{G}(V,\xi_n).$$

Lema 24.1. $\overline{G}(v_1,\xi_1)=0$, però, en canvi, $\overline{G}(v_1,\xi_i)\neq 0,\ i=2,\dots,n$.

En efecte. v_1 és una arrel simple de $G(V)$. Per tant, solament pot anul·lar un dels factors. □

Corol·lari 24.2. Tots els factors $\overline{G}(V,\xi_i),\ i=1,\dots,n$, són diferents. □

En efecte. Del 24.1 en resulta que el polinomi $\overline{G}(v_1,X)$ i l'equació polinòmica donada $f(X)=0$ solament tenen, en comú, l'arrel ξ_1. Per tant,

$$\operatorname{mcd}\big(\overline{G}(v_1,X),f(X)\big)$$

és un polinomi de primer grau en X amb coeficients en el cos $K(v_1)$.

O sigui, és de la forma

$$\alpha\big(v_1\big)\,X+\beta\big(v_1\big),\ \text{amb}\ \alpha(V),\beta(V)\in K(V).$$

A més, s'anul·la per a $X=\xi_1$. D'on: $\alpha\big(v_1\big)\,\xi_1+\beta\big(v_1\big)=0$ i en resulta que

$$\xi_1=-\frac{\beta\big(v_1\big)}{\alpha\big(v_1\big)}=\ell_1(v_1),$$

que és el que volíem provar.

Anàlogament, $\xi_2=\ell_2(v_1),\dots,\xi_n=\ell_n(v_1)$. □

Hom diu que v_1 és un *element primitiu*. Vegeu, en el comentari 32, p. 24, que, de fet, tenim que $K\big(v_1\big)=K\big(\xi_1,\xi_2,\dots,\xi_n\big)$.

Comentari 25. De fet és un cas particular d'un teorema que trobem a (Lagrange, 1771, §100) i que, actualment, es coneix com el *teorema de Lagrange*:

Teorema de Lagrange (Rey Pastor, 1915, edició de 1947, p 209-211) o (Tignol, 2001, p 142-144). Siguin $f\big(X_1,\dots,X_n\big)$, $g\big(X_1,\dots,X_n\big)$ dos elements de l'anell $K\big[X_1,\dots,X_n\big]$, on K és un cos que conté les funcions simètriques $s_1,\dots,s_n$ de les incògnites $x_1,\dots,x_n$. Aleshores

1. Si la funció $f(x_1,\dots,x_n)$ es pot expressar com a funció racional de $g(x_1,\dots,x_n)$, aleshores $f(x_1,\dots,x_n)$ *admet* les mateixes substitucions que $g(x_1,\dots,x_n)$.

2. Recíprocament, si una funció $f(x_1,\dots,x_n)$ *admet* totes les substitucions de la funció $g(x_1,\dots,x_n)$, aleshores $f(x_1,\dots,x_n)$ es pot expressar com a funció racional de $g(x_1,\dots,x_n)$.

En efecte. Teorema directe. Si

$$f(x_1,\dots,x_n)=\frac{b_h\,g^h+b_{h-1}\,g^{h-1}+\cdots+b_1\,g+b_0}{a_k\,g^k+a_{k-1}\,g^{k-1}+\cdots+a_1\,g+a_0}(x_1,\dots,x_n),$$

és evident que $f(x_1,\dots,x_n)$ admet *totes* les substitucions de $g(x_1,\dots,x_n)$.

Teorema recíproc. **Demostració de Lagrange** (Lagrange, 1771, §100, p 375) o (Tignol, 2001, p 142-143). En efecte. Siguin $g_1,g_2,\dots,g_\nu$ els valors diferents que pren g quan el sotmetem a *totes* les substituicions, amb $g_1:=g$, i $f_1:=f,f_2,\dots,f_\nu$ les que corresponen als $g_j,j=1,\dots,\nu$ en el sentit que f_j és el valor que pren f quan g pren el valor g_j [vegeu el lema 25.1, p 19].

Considerem les expressions $a_0,\dots,a_{\nu-1}$ següents:

$$\begin{aligned}
d_0&=f_1+f_2+\cdots+f_\nu\\
d_1&=g_1\,f_1+g_2\,f_2+\cdots+g_\nu\,f_\nu\\
d_2&=g_1^2\,f_1+g_2^2\,f_2+\cdots+g_\nu^2\,f_\nu\\
&\vdots\\
d_{\nu-1}&=g_1^{\nu-1}\,f_1+g_2^{\nu-1}\,f_2+\cdots+g_\nu^{\nu-1}f_\nu
\end{aligned}\tag{9}$$

Per la manera com hem definit els $f_j,g_j,j=1,\dots,\nu$, resulta que els termes $d_0,\dots,d_{\nu-1}\in K$.

La regla de Cramer permet de resoldre aquest sistema i això acaba la demostració. □

Mètode de resolució de Lagrange (Lagrange, 1771, p 375). Sigui

$$\alpha(Z)=\big(Z-g_1\big)\big(Z-g_2\big)\cdots\big(Z-g_\nu\big)=Z^\nu+a_{\nu-1}\,Z^{\nu-1}+\cdots+a_1\,Y+a_0.$$

Dividim el polinomi $\alpha(Z)$ per $Z-g_1$. Obtenim:

$$\varphi(Z)=\frac{\alpha(Z)}{Z-g_1}=\big(Z-g_2\big)\cdots\big(Z-g_\nu\big)=Z^{\nu-1}+c_{\nu-2}\,Z^{\nu-2}+\cdots+c_1\,Z+c_0.$$

Pel lema 23.1, p. 15, els coeficients $c_0,c_1,\dots,c_{\nu-1}$ són fraccions racionals dels coeficients $b_0,b_1,\dots,b_{\nu-1},b_\nu$, i de g_1 i atès que aquests darrers són funcions simètriques de $g_1,\dots,g_\nu$, ho són de $x_1,\dots,x_n$ i, per tant, es poden determinar en funció de $s_1,\dots,s_n$; és a dir, $c_0,c_1,\dots,c_{\nu-1}\in K$, com volíem.

Si ara multipliquem la primera equació de (9) per c_0, la segona per c_1, la tercera per c_2, etc., i la última per 1 i sumem, obtenim una equació en la qual el coeficient de f_i és el valor que pren la funció $\varphi(Z)$ quan fem $Z=g_i,i=1,\dots,\nu$. O sigui

$$a_0\,d_0+a_1\,d_1+\cdots+a_{\nu-1}\,d_{\nu-1}=f_1\,\varphi\big(g_1\big)+f_2\,\varphi\big(g_2\big)+\cdots+f_\nu\,\varphi\big(g_\nu\big)$$

I ara, com que $\varphi\big(g_2\big) = \cdots = \varphi\big(g_\nu\big) = 0$, resulta que

$$f_1(x_1, \ldots, x_n) = \big(a_0\, d_0 + a_1\, d_1 + \cdots + a_{\nu-1}\, d_{\nu-1}\big) \times \varphi\big(g_1\big)^{-1}$$

com volíem atès que és una funció racional de g_1 i de $s_1, \ldots, s_n$. □

Lema 25.1. Hi ha una correspondència unívoca entre els valors de f_j i els de $g_j, j = 1, \ldots, \nu$.

En efecte. Si apliquem τ_ℓ a $f_h = \tau_h(f)$, el producte $\tau_\ell \circ \tau_h$ és necessàriament de la forma $\sigma_i \circ \tau_k$, on σ_i és una permutació que deixa invariant $f(x_1, \ldots, x_n)$ —de les que $f(x_1, \ldots, x_n)$ admet. És a dir,

$$\tau_\ell\big(f_h\big) = \tau_\ell\big(\tau_h(f)\big) = \big(f\big)\big(\tau_\ell \circ \tau_h\big) = \big(\tau_k \circ \sigma_i\big)(f) = \tau_k\big(\sigma_i(f)\big) = f_k.$$

Obtindrem un resultat anàleg amb la funció g atès que, per hipòtesi, g també admet σ_i. □

Demostració de Rey-Pastor (Rey Pastor, 1915, edició de 1947, p 210-211). Siguin $g_1, \ldots, g_\nu$ el valors *diferents* que pren la funció $g(x_1, \ldots, x_n)$ quan permutem les $x_i, i = 1, \ldots, n$. Pel lema 20.1, p. 11, els valors $g_j, j = 1, \ldots, \nu$, satisfan l'equació, amb coeficients en K,

$$\alpha(Z) = Z^\nu + a_{\nu-1}\, Z^{\nu-1} + \cdots + a_1\, Z + a_0 = \big(Z - g_1\big)\big(Z - g_2\big) \cdots \big(Z - g_\nu\big) \quad (10)$$

Atès que hi ha una correspondència unívoca entre els valors de f_j i els de $g_j, j = 1, \ldots, \nu$, [pel lema 25.1, p. 19] podem formar la funció

$$F(Z) = \frac{\alpha(Z)}{Z - g_1}\, f_1 + \frac{\alpha(Z)}{Z - g_2}\, f_2 + \cdots + \frac{\alpha(Z)}{Z - g_\nu}\, f_\nu. \quad (11)$$

Els coeficients del numerador pertanyen al cos K; el terme en el qual f i g tenen índex i es transforma en un altre que té índex j. En definitiva, doncs, $F\big(Z\big)$ és simètrica. Per tant,

$$F\big(Z\big) = b_{\nu-1}\, Z^{\nu-1} + b_{\nu-2}\, Z^{\nu-2} + \cdots + b_1\, Z + b_0. \quad (12)$$

Per a $Z := g_1$ s'anul·len tots el termes del membre de l'esquerra de l'equació (11) llevat del primer. Per tant,

$$\big(g_1 - g_2\big)\big(g_1 - g_3\big) \cdots \big(g_1 - g_\nu\big) = F\big(g_1\big) = b_{\nu-1}\, g_1^{\nu-1} + b_{\nu-2}\, g_1^{\nu-2} + \cdots + b_1\, g_1 + b_0. \quad (13)$$

Però aquest producte és exactament $\alpha'(Z)$ quan $Z = g_1$. De tot això en resulta (10) que

$$f(x_1, \ldots, x_n) = \frac{F\big(g_1\big)}{\alpha'\big(g_1\big)} = \frac{b_{\nu-1}\, g_1^{\nu-1} + b_{\nu-2}\, g_1^{\nu-2} + \cdots + b_1\, g_1 + b_0}{\nu\, Z^{\nu-1} + (\nu - 1)\, a_{\nu-1}\, Z^{\nu-2} + \cdots + a_1}, \quad (14)$$

que té tots els coeficients en el cos K.

Corol·lari del teorema de Lagrange. Cada una de les arrels $\xi_i, i = 1, \ldots, n$, es pot expressar com a funció racional de v_1.

En efecte. Les variables $\xi_i, i = 1, \ldots, n$, i la resolvent $v_1(\xi_1, \ldots, \xi_n) = a_1\,\xi_1 + \cdots + a_n\,\xi_n$ **no** admeten cap substitució de $\mathfrak{S}_n$.

Corol·lari 25.2. Generalització del teorema de Lagrange. Si la funció $f(x_1, \ldots, x_n)$ pren $m > 1$ valors $f_1, \ldots, f_m$ per les substitucions que deixen invariant la funció g, aleshores f és una arrel de

$$(Y - f_1) \cdots (Y - f_m) = 0.$$

Ara bé aquesta equació satisfà les condicions requerides en el teorema de Lagrange atès que és invariant per les substitucions que deixen invariant g. Per tant, $f(x_1, \ldots, x_n)$ és funció racional de $g(x_1, \ldots, x_n)$ al cos K. □

Comentari 26. Un exemple del teorema de Lagrange, manllevat del llibre (Rey Pastor, 1915, edició de 1947, p. 211).

Siguin ξ_1, ξ_2 les arrels de l'equació quadràtica $X^2 + p\,X + q = 0$. Volem expressar ξ_1 en funció de $\varphi_1 := \xi_1 + 2\,\xi_2$ o de $\varphi_2 := 2\,\xi_1 + \xi_2$.

En aquest cas tan senzill podem observar, a primer cop d'ull, que $\xi_1 = 2\,(\xi_1 + \xi_2) - \varphi_1 = -2\,p - \varphi_1$, quelcom que garanteix el teorema de Lagrange.

Si apliquem la metodologia descrita per Rey Pastor, tenim:

$$\alpha(Z) = (Z - \varphi_1)\,(Z - \varphi_2) = Z^2 - (\varphi_1 + \varphi_2)\,Z + \varphi_1\,\varphi_2 = Z^2 + 3\,p\,Z + (2\,p^2 + q).$$

En l'expressió (14, p. 19) de ξ_1 en funci|ó de φ_1, el numerador és

$$F(Z) = \xi_1\,(Z - \varphi_2) + \xi_2\,(Z - \varphi_1) = -p\,Z - 2\,(\xi_1^2 + \xi_1\,\xi_2 + \xi_2^2) = -p\,Z - 2\,(p^2 - q),$$

i el denominador

$$\alpha'(Z) = 2\,Z + 3\,p.$$

En resulta,

$$\xi_1 = \frac{-p\,\varphi_1 - 2\,(p^2 - q)}{2\,\varphi_1 + 3\,p}.$$

Aquesta expressió es pot racionalitzar, com s'indica al comentari 28, p. 21. Cal multiplicar el numerador i el denominador per $2\,\varphi_2 + 3\,p$ i usar el fet que $\varphi_1 + \varphi_2 = -3\,p$ i $\varphi_1\,\varphi_2 = 2\,p^2 + q$. □

Comentari 27. Del comentari anterior en resulta que, per trobar les arrels de $f(X) = 0$, n'hi ha ben bé prou a trobar les arrels v de $G(V) = 0$.

Ara bé, de fet, no hi hem guanyat res, perquè el grau de $G(V) \in K[V]$ és $n!$, enormement més gran que $n = \text{grau}\big(f(X)\big)$.

Caldrà, doncs, treballar amb els factors irreductibles $G_1(V), G_2(V), \ldots, G_r(V)$ de $G(V)$.

S'inicia el camí cap el *grup de Galois*.

LEMA IV. Suposem formada l'equació en V, i que hem pres un dels seus factors irreductibles de manera que V en sigui una arrel. [421]

Siguin $V, V', V'', \ldots,$ les arrels d'aquesta equació irreductible. Si $a = f(V)$ és una de les arrels de la proposada, $f(V')$ també en serà una.

En efecte. Si multipliquem tots els factors de la forma $V - \varphi(a, b, c, \ldots, d)$ que s'obtenen quan s'apliquen totes les permutacions possibles de les lletres, tindrem una funció racional en V.

Aquest producte serà divisible per l'equació en qüestió. Per tant, V' s'haurà obtingut per algun dels canvis de lletres en la funció V. Sigui $F(V; a) = 0$ l'équació que s'obté permutant en V totes les lletres, llevat de la primera. Tindrem, doncs, que $F(V'; b) = 0$, on b pot ser igual a a, essent però una de les arrels de l'equació proposada. Per consegüent, de la mateixa manera que de la proposada i de $F(V; a) = 0$ en resulta $a = f(V)$, de la proposada i de $F(V'; b) = 0$ combinades, la següent serà $b = f(V')$.□

Comentari 28. El resultat següent és ben conegut —però, per si de cas, recordem-lo:

Lema 28.1. Els elements del cos $K(v_1)$ es poden expressar, de forma única, com a polinomis de $K[v_1]$ de grau $\leq m$, on $m = \text{grau}\big(G_1(V)\big)$.

En efecte. Tot consisteix a *racionalitzar* i a *reduir mòdul* $G_1(v_1)$, on $G_1(V)$ és un factor irreductible de $G(V)$ en K de grau m que té com arrel v_1 —vegeu el comentari 27, p. 20.

Atès que

$$K(v_1) = \left\{ \frac{g_1(v_1)}{g_2(v_1)}, \text{ amb } g_2(v_1) \neq 0 \text{ i } g_1(V), g_2(V) \in K[V] \right\}$$

multipliquem els polinomis en $v_1, g_1(v_1), g_2(v_1) \neq 0$, del numerador i denominador pels polinomis que es dedueixen de $g_2(V)$ quan substituïm V pels *elements conjugats* de v_1; és a dir, pels valors que pren $g_2(V)$ en les altres arrels $v_i, i = 2, \ldots, m$, de $G_1(V) = 0$. Aleshores —atès que el producte dels termes del denominador és una funció simètrica de les arrels $v_1, v_2, \ldots, v_m$, de $G_1(V) = 0$— el denominador és un element de K i, segons el lema 23.1 aplicat a $G_1(V)$, el numerador és un polinomi de $K[v_1]$.

Al seu torn, els elements de l'anell $K[v_1]$ es poden escriure com a polinomis en v_1 de grau $< m = \text{grau}\big(G_1(V)\big)$ reduint-los mòdul $G_1(v_1)$: el fet que

$G(v_1) = g_m\, v_1^m + g_{m-1}\, v_1^{m-1} + \cdots + g_1\, v_1 + g_0 = 0$ permet d'expressar v_1^m com un polinomi de grau $< m$ amb coeficients en K; i, d'aquí, podem reduir també els termes $v_1^{m+1}, \ldots, v_1^{m+j}$.

— Pel que fa a la suma i la resta, tot rau a fer les operacions usuals i com que són polinomis en v_1 de grau $< m$, s'obtenen polinomis en v_1 de grau $< m$.

— Pel que fa al producte, s'obtindrà en principi un polinomi en v_1 de grau $\geq m$; el reduïm tal com hem indicat abans, mòdul $G(v_1)$.

— Pel que fa al quocient, només cal fixar-se en l'invers de $g(v_1) \in K[v_1]$, en el benentès que $g(v_1) \neq 0$. Ho resol la *identitat de Bezout* que, com és ben conegut, diu:

$$\operatorname{mcd}\big(g(V), G_1(V)\big) = q_1(V)\, g(V) + q_2(V)\, G_1(V) = k \in K, \text{ amb } k \neq 0,$$

atès que $\operatorname{grau}\big(q_1(V)\big) < m = \operatorname{grau}\big(G_1(V)\big)$ i $G_1(V)$ és irreductible.[15]

Per tant,

$$k = q_1(v_1)\, g(v_1) + q_2(v_1)\, G_1(v_1) = q_1(v_1)\, g(v_1).$$

En resulta, doncs, que $g^{-1}(v_1) = \frac{1}{k} q_1(v_1)$. □

Malgrat que aquest resultat no és al text de Galois ni explícita ni implícitament, en el cas d'una extensió simple $K(\eta)$ per una arrel d'un polinomi irreductible $g(Y) \in K[Y]$, és molt important i cal tenir-lo present a l'hora de fer demostracions correctes d'alguns dels seus enunciats, com podem veure, per exemple, en el comentari 50.

Corol·lari 28.2. Tota funció polinòmica de les arrels de $f(X) = 0$ es pot escriure, de forma única, com una funció polinòmica $p(v_1)$ de grau $< m$.

Comentari 29. Fem

$$G(V) = G_1(V)\, G_2(V) \cdots G_r(V), \tag{15}$$

[15] NTC: Si imposem que $\operatorname{grau}\big(q_1(V)\big) < \operatorname{grau}\big(G_1(V)\big) = m$ i $\operatorname{grau}\big(q_2(V)\big) < \operatorname{grau}\big(g(V)\big)$ —sempre és possible [vegeu (Dehn, 1960, p 4-6)]—, els polinomis $q_1(V)$ i $q_2(V)$ són únics.

Hem de recórrer al *lema de Gauss* per a polinomis: Siguin $p(X), q(X), r(X) \in K[X]$. Si $p(X)$ és irreductible i $p(X) \big| \big(q(X) \times r(X)\big)$, aleshores $p(X) | q(X)$ o $p(X) | r(X)$.

Suposem que hi hagués dues parelles de polinomis $q_1(V), q_1'(V)$; $q_2(V), q_2(V)$, amb $\operatorname{grau}\big(q_1(V), q_1'(V)\big) < m = \operatorname{grau}\big(G_1(V)\big)$ i $\operatorname{grau}\big(q_2(V), q_2'(V)\big) < \operatorname{grau}\big(g(V)\big)$, aleshores $G_1(V)$ hauria de dividir $q_1(V) - q_1'(V)$ o $g(V)$, ambdós de grau més petit que el grau de $G_1(V)$. Per tant, $q_1(V) - q_1'(V) = 0$.

on cada factor $G_i(V), i = 1, \ldots, r$, és irreductible a $K[V]$.

Pel LEMA III i el corol·lari 28.2, cada arrel de $G(V) = 0$ es pot escriure en la forma $p(v_1)$, on $\text{grau}\big(p(v_1)\big) < \text{grau}\big(G_1(V)\big) = m$, atès que cada una de les arrels v_i, $i = 1, 2, \ldots, n!$, és una funció polinòmica de les arrels $\xi_1, \ldots, \xi_n$, de $f(X) = 0$.

N'hi ha exactament m que són arrels de $G_1(V) = 0$ que pertanyen a $K(v_1)$; són $v_1, v_2, \ldots, v_m$, que Galois anomena $V, V', \ldots, V^{(n-1)}$.

El polinomi irreductible $G_1(V) = 0$ proporciona el *grup de Galois* de $f(X) = 0$: són les substitucions de $\xi_1, \ldots, \xi_n$ en les seves arrels $v_1, v_2, \ldots, v_m$.

L'aplicació que envia $p(v_1) \in K(v_1)$ a $p(v_i) \in K(v_1)$ és un *automorfisme* de $K(v_1)$ en $K(v_1)$, ja que v_1 i v_i satisfan la mateixa relació definitòria: ésser arrels del factor irreductible a K, $G_1(V) = 0$ [vegeu la PROPOSICIÓ A, p. 35.]

Aquests m automorfismes constitueixen el que hom anomena el *grup de Galois* de $K(V)$ sobre K —o millor, de $f(X) = 0$ sobre K.

Però m'estic avançant!

Comentari 30. Considerem la taula següent:

$$
\begin{array}{cc|cccccccc}
 & \leftarrow & v_1 & \ell_1(v_1) & \ell_2(v_1) & \ell_3(v_1) & \cdots & \ell_i(v_1) & \cdots & \ell_n(v_1) \\
\downarrow & & v_2 & \ell_1(v_2) & \ell_2(v_2) & \ell_3(v_2) & \cdots & \ell_i(v_2) & \cdots & \ell_n(v_2) \\
\sigma_j & & v_3 & \ell_1(v_3) & \ell_2(v_3) & \ell_3(v_3) & \cdots & \ell_i(v_3) & \cdots & \ell_n(v_3) \\
\downarrow & & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\
 & \rightarrow & v_j & \ell_1(v_j) & \ell_2(v_j) & \ell_3(v_j) & \cdots & \ell_i(v_j) & \cdots & \ell_n(v_j) \\
 & & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & & \\
 & & v_m & \ell_1(v_m) & \ell_2(v_m) & \ell_3(v_m) & \cdots & \ell_i(v_m) & \cdots & \ell_n(v_m)
\end{array}
$$

on $\xi_i = \ell_i(v_1)$, $i = 1, \ldots, n$; és a dir, la primera fila —la que correspon a v_1— és $\xi_1 \quad \xi_2 \quad \xi_3 \quad \ldots \quad \xi_n$. Aquest és l'ordre bàsic damunt del qual cal considerar les substitucions en el sentit que Galois usa en les definicions de permutació i substitució de la p. 8.

Galois la introdueix —aquesta taula— a la PROPOSICIÓ I, p. 28. El LEMA IV diu que els termes de cada fila són arrels de $f(X) = 0$. Però no sabem si són diferents o si n'hi ha de repetides.

Lema 30.1. Per a cada $i = 1, \ldots, m$, si $\ell_j(v_i) = \ell_k(v_i), j, k = 1, \ldots, n$, aleshores $j = k$.

En efecte. Suposem que $\ell_j(v_i) = \ell_k(v_i)$. Aleshores $(\ell_j - \ell_i)(v_i) = 0$. Pel LEMA I, $G_1(V)$ divideix $(\ell_j - \ell_i)(V)$. En resulta, doncs, que $(\ell_j - \ell_i)(v_1) = 0$. O sigui, $\xi_j = \ell_j(v_1)$ seria igual a $\xi_k = \ell_k(v_1)$. Però, ξ_j i ξ_k són diferents, quan $j \neq k$. □

Corol·lari 30.2. Les files de la taula anterior són permutacions de les arrels de $f(X) = 0$ que suposem inicialment en l'ordre de la primera fila. □

En definitiva, podem considerar les «substitucions» σ_j, $i = 1, \ldots, m$, que passen de la primera permutació a la j-èsima; o sigui, per a cada $j = 1, \ldots, m$:

$$\sigma_j(\xi_i) = \sigma_j\big(\ell_i(v_1)\big) = \ell_i\big(v_j\big) \quad i = 1, \ldots, n.$$

Dit més clarament,

$$\sigma_j := \begin{pmatrix} \ell_1(v_1) = \xi_1 & \ell_2(v_1) = \xi_2 & \ell_3(v_1) = \xi_3 & \cdots \ell_n(v_1) = \xi_n \\ \ell_1(v_j) = \xi_{\sigma_j(1)} & \ell_2(v_j) = \xi_{\sigma_j(2)} & \ell_3(v_j) = \xi_{\sigma_j(3)} & \cdots \ell_n(v_j) = \xi_{\sigma_j(n)} \end{pmatrix},$$

com veiem sintetitzat a la columna de l'esquerra de la taula anterior.

Comentari 31. Volem demostrar el LEMA IV. Per fer-ho, necessitem un lema previ.

Lema 31.1. Sigui ara $Q(V) = \frac{N(V)}{D(V)} \in K(V)$, amb $D(v_1) \neq 0$. Si $Q(v_1) = 0$, aleshores $Q(v_j) = 0$ per a tota arrel $v_j, j = 1, \ldots, m$, de $G_1(V) = 0$.

En efecte. Si $Q(v_1) = 0$, aleshores $N(v_1) = 0$. Pel LEMA I, $G_1(V)$ divideix $N(V)$ i, per tant, $N(v_j) = 0$ per a tota arrel v_j de $G_1(V) = 0$.

I, a més, $D(v_j) \neq 0$ per a tota arrel v_j de $G_1(V) = 0$ ja que, si $D(v_j) = 0$ per a una arrel v_j de $G_1(V) = 0$, aleshores, pel LEMA I, $D(v_1) = 0$ i això no és possible per com l'hem triat. □

Demostració del LEMA IV. Per a cada arrel $\xi_1, \xi_2, \ldots, \xi_n$, de $f(X) = 0$ tenim que $f(\xi_i) = f\big(\ell_i(v_1)\big) = 0$. En resulta que la funció racional de $K(V)$, $\big(f \circ \ell_i\big)(V)$ s'anul·la per a $V := v_1$ que és una arrel del polinomi irreductible a $K, G_1(V) \in K[V]$. Pel lema 31.1, s'anul·la per a tota arrel v_j de $G_1(V) = 0$. En resulta doncs que, per a cada $i = 1, \ldots, n$, i cada $j = 1, \ldots, m$, $f\big(\ell_i(v_j)\big) = 0$, com volíem. □

Comentari 32. Podem sintetitzar els LEMES III i IV, seguint (Tignol, 2001, p. 236-237).

LEMA III. Existeix un element $v_1 \in K(\xi_1, \ldots, \xi_n)$ per al qual $\xi_i \in K(v_1)$ per a $i = 1, 2, \ldots, n$. Els elements v_1 que tenen aquesta propietat són, com ja hem dit abans, les *resolvents de Galois* de l'equació $f(X) = 0$.

Tot rau, doncs, a trobar aquest objecte v_1 perquè aleshores coneixerem les arrels de $f(X) = 0$. De fet, $K(v_1) = K(\xi_1, \ldots, \xi_n)$.

A més, per a cada $u \in K(\xi_1, \ldots, \xi_n)$, existeix un polinomi irreductible $H(V) \in K[V]$ per al qual $H(u) = 0$ factoritza en factors lineals a $K(\xi_1, \ldots, \xi_n)$.

De retruc, si $u_1, u_2, \ldots, u_m$, en són les arrels, aleshores $K(\xi_1, \ldots, \xi_n) = K(v_1) = K(u_1, \ldots, u_m)$.

Corol·lari 32.1. Cada resolvent v_i de $f(X)=0$ es pot expressar com una funció racional de qualsevol altra resolvent v_j de $f(X)=0$.

En efecte. Atès que les arrels $\xi_k, k=1,\dots,n$, s'obtenen com a funcions racionals de qualsevol resolvent $v_i, i=1,\dots,n!$, en resulta que $K(v_i)=K(\xi_1,\dots,\xi_n)$. □

De fet, com ja hem indicat al comentari 25, p. 17, és una conseqüència immediata del teorema de Lagrange.

LEMA IV. Els automorfismes $\sigma_j, j=1,\dots,m$, descrits al comentari 29, p. 22, formen un grup $\{\sigma_1,\dots,\sigma_m\}$ que és el *grup de Galois* de $f(X)=0$ en K. Hom el designa $\mathrm{Gal}\big(f(X)/K\big)$.

De fet, és un subgrup del grup $\mathfrak{S}_n$ i no depèn de l'elecció de la resolvent v. Però aquests dos fets no es troben a la memòria de Galois.

Factoritza a $\mathbb{Z}[X]$:[16]

$$\begin{aligned} f(X) &= \big(X-1\big)\big(X^2-2\big)\big(X^2-3\big) \\ &= \big(X-1\big)\big(X-\sqrt{2}\big)\big(X+\sqrt{2}\big)\big(X-\sqrt{3}\big)\big(X+\sqrt{3}\big). \end{aligned}$$

Comentari 33. Un bon exemple pot ajudar a entendre aquests quatre lemes. El manllevem de (Tignol, 2001, p. 238-240):

Considerem el polinomi

$$f(X) := X^5 - X^4 - 5\,X^3 + 5\,X^2 + 6\,X - 6 \in \mathbb{Z}[X].$$

Les arrels d'aquest polinomi són, doncs,

$$\xi_1 = 1,\ \ \xi_2 = \sqrt{2},\ \ \xi_3 = -\sqrt{2},\ \ \xi_4 = \sqrt{3},\ \ \xi_5 = -\sqrt{3}.$$

Per trobar el grup de Galois cal determinar, abans, una resolvent. Serveix, per exemple,

$$v_1 = \xi_2 + \xi_4,$$

perquè, com veiem tot seguit, permet deduir racionalment les arrels $\xi_i, i=1,2,3,4,5$.

Observem tanmateix que s'obté sense recórrer ni al LEMA II, ni tampoc al teorema de Lagrange; s'obté per intuïció i ofici. Al comentari 71, p. 53, veurem el cas de la cúbica seguint, fil per randa, tot el que Galois proposa.

En efecte, fem:

$$v_1^2 = \xi_2^2 + \xi_4^2 + 2\,\xi_2\,\xi_4 = 2 + 3 + 2\sqrt{6}$$

[16] Òbviament, és resoluble per radicals. Però ara el que volem caracteritzar és el grup de Galois que li correspon.

i

$$2\,\xi_2\,v_1 = 2\,\xi_2^2 + 2\,\xi_2\,\xi_4 = 4 + 2\sqrt{6}.$$

Per tant,

$$v_1^2 - 2\,\xi_2\,v_1 - 1 = 0.$$

En resulta:

$$\xi_2 = \frac{v_1^2 - 1}{2\,v_1} = \ell_1(v_1), \tag{16}$$

$$\xi_3 = -\xi_2 = \frac{1 - v_1^2}{2\,v_1} = \ell_3(v_1). \tag{17}$$

I, atès que, $\xi_4 = v_1 - \xi_2$, tenim també:

$$\xi_4 = \frac{v_1^2 + 1}{2\,v_1} = \ell_4(v_1), \tag{18}$$

$$\xi_5 = -\xi_4 = -\frac{v_1^2 + 1}{2\,v_1} = \ell_5(v_1). \tag{19}$$

Finalment, $\xi_1 = 1 \in \mathbb{Z}$ i $\ell_1(v_1) = 1$ també és funció racional de v_1 amb coeficients en $\mathbb{Z}$.

v_1 és, doncs, una *resolvent de Galois* de $f(X) = 0$ en $\mathbb{Q}$.

Ara necessitem un *polinomi minimal* de v_1 en $\mathbb{Q}$. De (16) en resulta:

$$4\,\xi_2^2\,v_1^2 = \left(v_1^2 - 1\right)^2 \quad \text{que és} \quad 8\,v_1^2 = v_1^4 - 2\,v_1^2 + 1 = 0.$$

S'obté, doncs, el polinomi —irreductible a $\mathbb{Q}[V]$:

$$G(V) := V^4 - 10\,V^2 + 1 = 0.^{17} \tag{20}$$

Així s'obtenen 4 *permutacions* de v:

$$\begin{aligned}
v = v_1 &= \sqrt{2} + \sqrt{3}, & \sigma_1 &:= \{\mathrm{Id}\},\\
v_2 &= \sqrt{2} - \sqrt{3}, & \sigma_2 &:= \begin{pmatrix}\sqrt{3} & -\sqrt{3}\end{pmatrix} = \begin{pmatrix}\xi_4 & \xi_5\end{pmatrix},\\
v_3 &= -\sqrt{2} + \sqrt{3}, & \sigma_3 &:= \begin{pmatrix}\sqrt{2} & -\sqrt{2}\end{pmatrix} = \begin{pmatrix}\xi_2 & \xi_3\end{pmatrix},\\
v_4 &= -\sqrt{2} - \sqrt{3}, & \sigma_4 &:= \begin{pmatrix}\sqrt{3} & -\sqrt{3}\end{pmatrix} \circ \begin{pmatrix}\sqrt{2} & -\sqrt{3}\end{pmatrix}\\
& & &= \begin{pmatrix}\xi_4 & \xi_5\end{pmatrix} \circ \begin{pmatrix}\xi_2 & \xi_3\end{pmatrix}.
\end{aligned}$$

[17] Factoritza en la forma següent: $\left(V - (\sqrt{2} + \sqrt{3})\right)\left(V + (\sqrt{2} + \sqrt{3})\right)\left(V + (\sqrt{2} - \sqrt{3})\right)\left(V - (\sqrt{2} - \sqrt{3})\right)$.

Recordem que teníem:

$$\xi_1 = \ell_1(v_1),\ \ \xi_2 = \ell_2(v_1),\ \ \xi_3 = \ell_3(v_1),\ \ \xi_4 = \ell_4(v_1) \quad \text{i} \quad \xi_5 = \ell_5(v_1).$$

Ara hem de fer càlculs per saber com és la taula:

	ξ_1	ξ_2	ξ_3	ξ_4	ξ_5
v_1	$\ell_1(v_1)$	$\ell_2(v_1)$	$\ell_3(v_1)$	$\ell_4(v_1)$	$\ell_5(v_1)$
v_2	$\ell_1(v_2)$	$\ell_2(v_2)$	$\boldsymbol{\ell_3(\mathbf{v_2})}$	$\ell_4(v_2)$	$\ell_5(v_2)$
v_3	$\ell_1(v_3)$	$\ell_2(v_3)$	$\ell_3(v_3)$	$\ell_4(v_3)$	$\ell_5(v_3)$
v_4	$\ell_1(v_4)$	$\ell_2(v_4)$	$\ell_3(v_4)$	$\ell_4(v_4)$	$\ell_5(v_4)$

Per exemple,

$$\frac{1}{2}(1 - v_2^2) = -2 + \sqrt{6} = -\sqrt{2}\left(\sqrt{2} - \sqrt{3}\right)$$

i, per tant,

$$\ell_3(v_2) = -\sqrt{2} = \xi_3.$$

Els altres es fan igualment. [Lector, fes els càlculs següents: $v_i^2 - 1, v_i^2 + 1$, $-(v_i^2 - 1), -(v_i^2 + 1),\ \ i = 1, 2, 3, 4.$]

En definitiva s'obté:

	ξ_1	ξ_2	ξ_3	ξ_4	ξ_5
$\sigma_1 := \{\mathrm{Id}\}$	ξ_1	ξ_2	ξ_3	ξ_4	ξ_5
$\sigma_2 := (\xi_4\ \ \xi_5)$	ξ_1	ξ_2	$\boldsymbol{\xi_3}$	ξ_5	ξ_4
$\sigma_3 := (\xi_2\ \ \xi_3)$	ξ_1	ξ_3	ξ_2	ξ_4	ξ_5
$\sigma_4 := (\xi_4\ \ \xi_5) \circ (\xi_2\ \ \xi_3)$	ξ_1	ξ_3	ξ_2	ξ_5	ξ_4

Fixem-nos que el que fan les substitucions $\sigma_1, \sigma_2, \sigma_3, \sigma_4$ és intercanviar les arrels dels factors $X^2 - 2 = 0, X^2 - 3 = 0$, que són irreductibles a $\mathbb{Q}[X]$. Vegeu el comentari 41, p. 33, en què es parla de la «visibilitat» de les arrels.

Comentari 34. Ara, un cop establertes les definicions i els lemes, Galois inicia el camí cap a la resolució per radicals.

1.3 Proposicions

PROPOSICIÓ I.

TEOREMA. Considerem una equació donada les m arrels de la qual són $a, b, c, \ldots$ Sempre existeix un grup de permutacions de les lletres $a, b, c, \ldots$ que té la propietat següent:

1. Tota funció de les arrels, invariant [18] per les substitucions del grup, és racionalment coneguda.

2. Recíprocament, tota funció de les arrels, determinable racionalment, és invariant per les substitucions [del grup].

Comentari 35. El grup permet d'expressar els elements de K atès que són invariants.

El grup *caracteritza* les funcions racionals que no varien numèricament per les substitucions del grup —que *pertanyen al grup*, com es diu actualment. Vegeu (Rey Pastor, 1915, edició de 1947, p. 216 i 223).

Comentari 36. Els dos exemples que Galois ofereix tot seguit, entre parèntesis, posen de manifest que distingia ben clarament les *funcions polinòmiques generals* en el sentit de Lagrange i Abel —en elles els coeficients són generals; és a dir, són paràmetres— d'aquelles altres que tenen d'altres lligams estructurals diferents dels que estableixen les fórmules de Cardano-Viète, com ara

$$X^{p-1} + X^{p-2} + \cdots + X + 1 = 0, \text{ amb } p \text{ primer},$$

on les arrels $\xi_1, \ldots, \xi_{p-1}$, estan lligades per $\xi_1^g = \xi_2, \xi_2^g = \xi_3, \ldots, \xi_{p-2}^g = \xi_{p-1}, \xi_{p-1}^g = \xi_1$, on g és una arrel primitiva de la unitat mòdul p.

[422] (En el cas de les equacions algèbriques, el grup no és altre que el conjunt de les $1 \cdot 2 \cdot 3 \cdot \ldots \cdot m$ permutacions possibles de les m lletres, ja que, en aquest cas, les funcions simètriques són les úniques determinables racionalment.)

[18] GALOIS. Aquí anomenem *invariant* no només una funció la forma de la qual és invariant per les substitucions de les arrels entre si, sinó també aquelles per a les quals el *valor numèric* no varia amb aquestes substitucions. Per exemple, si $Fx = 0$ és una equació, Fx és una funció de les arrels que no varia.

Quan diem que una *funció és racionalment coneguda*, volem dir que el seu valor numèric es pot expressar com una funció racional dels coeficients de l'equació i de les quantitats adjuntes.

Comentari 37. Veiem que l'afirmació galoisiana és vertadera (Tignol, 2001, p. 146 i 241).

Considerem el *conjunt d'invariància* de la funció racional amb coeficients en K, $I(g) = \Big\{\sigma \in \mathfrak{S}_n : \sigma\big(g(\xi_1, \dots, \xi_n)\big) = g(\xi_1, \dots, \xi_n)\Big\}$.

Usant ara la definició de *grup de Galois* que estableix la PROPOSICIÓ I, veurem que el grup $\mathcal{G} = \mathrm{Gal}\big(f(X)/K_0\big) \subseteq \mathfrak{S}_n$ de l'equació general de grau n

$$f(X) := X^n - s_1\, X^{n-1} + \cdots + (-1)^n\, s_n = (X - \xi_1) \cdots (X - \xi_n) = 0, \quad (21)$$

on K_0 és el cos de fraccions dels coeficients de $f(X)$, és el grup simètric $\mathfrak{S}_n$.

Necessitem un lema previ:

Lema 37.1. Per a cada subgrup $\mathcal{S}$ de $\mathfrak{S}_n$, existeix una funció racional d'n variables, $g(X_1, \dots, X_n)$, per a la qual $I\big(g(X_1, \dots, X_n)\big) = \mathcal{S}$.

En efecte. Considerem un monomi $m(X_1, \dots, X_n)$ que varií per a tota-substitució $\sigma \in \mathfrak{S}_n$ —per exemple $m(X_1, \dots, X_n) = X_1\, X_2^2 \cdots X_n^n$— i la funció racional $g(X_1, \dots, X_n) = \sum_{\sigma \in \mathcal{S}} \sigma\big(m(X_1, \dots, X_n)\big)$.

Per a tot $\tau \in \mathcal{S}$, $\{\sigma \circ \tau : \sigma \in \mathcal{S}\} = \mathcal{S}$. Per tant,

$$\sum_{\sigma \in \mathcal{S}} (\sigma \circ \sigma)\big(m(X_1, \dots, X_n)\big) = \sum_{\sigma \in \mathcal{S}} \sigma\big(m(X_1, \dots, X_n)\big).$$

En resulta que $\tau\big(g(X_1, \dots, X_n)\big) = g(X_1, \dots, X_n)$ per a tot $\tau \in \mathcal{S}$. I, en conseqüència, $\mathcal{S} \subseteq I(g)$.

Si $\rho \notin \mathcal{S}$, el monomi $\rho\big(m(X_1, \dots, X_n)\big)$ forma part de $\rho\big(g(X_1, \dots, X_n)\big)$ però no de $g(X_1, \dots, X_n)$. Per tant, $\rho \notin I(f)$.

D'això se'n dedueix que $I\big(g(X_1, \dots, X_n)\big) = \mathcal{S}$. □

Proposició 37.2. El grup de Galois $\mathcal{G} = \mathrm{Gal}\big(f(X)/K\big)$ de l'equació general de grau n (21) és $\mathfrak{S}_n$.

En efecte. En cas contrari, pel lema 37.1, hi hauria una funció racional $g(X_1, \dots, X_n) \in K_0[X_1, \dots, X_n]$, on $K_0 = \mathbb{Q}(a_0, a_1 \dots, a_n)$ és el cos dels coeficients de $f(X)$, per a la qual l'expressió $g(\xi_1, \dots, \xi_n)$ no seria simètrica i, per tant, $g(\xi_1, \dots, \xi_n) \notin K_0$. En canvi,

$$g\big(\sigma(\xi_1), \dots, \sigma(\xi_n)\big) = g(\xi_1, \dots, \xi_n), \text{ per a tota } \sigma \in \mathrm{Gal}\big(f(X)/K\big).$$

I, per la PROPOSICIÓ I, $g(\xi_1, \dots, \xi_n) \in K_0$. Contradicció! □

(En el cas de l'equació $\frac{x^n-1}{x-1} = 0$, si suposem que $a = r, b = r\,g, c = r\,g^2$, $\dots$, on g és una arrel primitiva, el grup de les permutacions serà simple-

ment:

$$\begin{array}{l} a\,b\,c\,d\,\ldots\ldots\ldots k\,; \\ b\,c\,d\,\ldots\ldots\ldots k\,a\,; \\ c\,d\,\ldots\ldots\ldots k\,a\,b\,; \\ \ldots\ldots\ldots\ldots\ldots \\ k\,a\,b\,c\,\ldots\ldots\ldots i\,. \end{array}$$

En aquest cas particular, el nombre de les permutacions és igual al grau de l'equació, i el mateix succeeix amb les equacions les arrels de les quals són funcions racionals les unes de les altres.)

Comentari 38. Per a la darrera frase, vegeu (Rey Pastor, 1915, edició de 1947, p. 255-257).

Comentari 39. Per provar-ho, cal un lema.

Lema 39. 1. El grup de Galois és el més gran dels subgrups de $\mathfrak{S}_n$ que deixa numèricament invariants totes les funcions racionals de les incògnites $\xi_i, i = 1, 2, \ldots, n$, que tenen un valor racional determinat (Dehn, 1960, p. 146-147).

En efecte. Sigui $\varphi_1(\xi_1, \ldots, \xi_n) = k \in K_0$, on, recorde-m'ho, K_0 és el més petit cos que conté $\mathbb{Q}$ i els coeficients de $f(X) = 0$. Podem expressar la funció anterior en termes de la resolvent v_1 atès que $\xi_i = \ell_i(v_1), i = 1, \ldots, n$.

Tenim, doncs,

$$\varphi_1(\xi_1, \ldots, \xi_n) = \varphi(v_1), \tag{22}$$

on, recorde-m'ho, $v_1 = a_1\,\xi_1 + a_2\,\xi_2 + \cdots + a_n\,\xi_n$.

Ara sotmetem la igualtat (22) a les substitucions del grup de Galois, i obtenim

$$\varphi_t(\xi_1, \ldots, \xi_n) = \varphi(v_t),\ t = 1, \ldots, \mu.$$

Sabem que $\varphi(V) = k$ —o bé $\varphi(V) - k = 0$— té l'arrel v_1 com $G_1(V) = 0$ i, pel LEMA I, $G_1(V)|\varphi(V)$. Per tant,

$$\varphi(v_1) = \varphi(v_2) = \cdots = \varphi(v_m) = k.$$

Finalment, $\varphi_1(\xi_1, \ldots, \xi_n) = \cdots = \varphi_\mu(\xi_1, \ldots, \xi_n) = k$.

A més, si una permutació $\sigma' \in \mathfrak{S}_n$ deixa invariant qualsevol funció racional de les arrels $\xi_i, i = 1, \ldots, n$, que tingui un valor racional determinat, aleshores, com que $G_1(v_1) = 0$, resulta que $G_1\big(\sigma'(v_1)\big) = 0$.

Per tant, $\sigma'(v_1) = v_s$ és una arrel de la resolvent de Galois; és a dir, $\sigma' \in \mathrm{Gal}\big(f(X)/K_0\big)$. □

Les arrels de l'equació

$$X^{p-1} + X^{p-2} + \cdots + X + 1 = 0 \tag{23}$$

s'obtenen d'una d'elles ξ_1 —per exemple la d'argument $\frac{2\pi}{p}$— i d'una arrel r [primitiva] de la unitat, mòdul p. En concret,

$$\xi_1 = \xi_1,\ \ \xi_2 = \xi_1^r,\ \ \xi_3 = \xi_1^{r^2},\ \ \ldots,\ \ \xi_{p-1} = \xi_1^{r^{p-1}}. \tag{24}$$

De (24) en resulta que

$$\xi_1^r = \xi_2,\ \ \xi_2^r = \xi_3,\ \ \ldots,\ \ \xi_{p-2}^r = \xi_{p-1}. \tag{25}$$

En aquest cas, d'acord amb el lema 39.1, cal que els lligams estructurals $\xi_i \mapsto \xi_{i+1}, \xi_{n-1} \mapsto \xi_1, i = 1, \ldots, n-2$, es respectin en tot moment.

Proposició 39.2. El grup de Galois $\mathrm{Gal}\big(f(X)/\mathbb{Q}\big)$ de l'equació ciclotòmica $X^{p-1} + X^{p-2} + \ldots + X + 1 = 0$, amb p primer, és el grup $\mathcal{S}$, generat per la substitució circular $(1\ 2\ \cdots\ p-1)$.

En efecte. Si apliquem la substitució *circular* $(1\ 2\ \cdots\ p-1)$, amb p primer —que és el cas que ens interessa— cada una de les relacions de (25) es transforma en la següent. *Admeten*, doncs, la substitució circular $(1\ 2\ \cdots\ p-1)$ i totes les seves potències —que formen un subgrup $\mathcal{S}$.

Sigui ara una equació racional $\varphi(\xi_1, \ldots, \xi_n) = 0$ entre les arrels de l'equació. Si substituïm $\xi_i, i = 2, \ldots, p-1$, en funció de ξ_1, obtindrem $\Psi(v_1) = 0$, on $\Psi(X) \in \mathbb{Q}[X]$. Del Lema I en resulta que l'equació ciclotòmica (23) divideix $\Psi(X)$. Per tant, per a tot $i = 1, \ldots, p-1, \Psi(\xi_i) = 0$. Però aquestes equacions $\Psi(\xi_i) = 0$ són les transformades —les unes de les altres—pel subgrup $\mathcal{S}$ generat per la substitució *circular* $(1\ \ 2\ \ \cdots\ \ p-1)$. Per tant, $\varphi(\xi_1, \ldots, \xi_n) = 0$ *admet* el subgrup $\mathcal{S}$.

Recíprocament, si $\tau \in \mathfrak{S}_n$ conserva les relacions (25) i substitueix ξ_1 per ξ_2, aleshores substituirà ξ_i per $\xi_{i+1},\ \ i = 1, \ldots, p-2$, i ξ_{p-1} en ξ_1. Per tant és la substitució circular $\tau := (1\ \ 2\ \ \cdots\ \ p-1)$. Però, si τ substitueix ξ_1 per ξ_i, aleshores òbviament $\tau := (1\ \ 2\ \ \cdots\ \ p-1)^i, i = 1, \ldots, p-1$. Per fi, si $\tau(\xi_1) = \xi_1$, aleshores τ deixa invariant $\xi_i, i = 2, \ldots, p-1$. O sigui, $\tau = \mathrm{Id}$. En definitiva, doncs, $\tau \in \mathcal{S}$, com volíem. □

Demostració. Sigui quina sigui la funció racional donada, sempre es pot trobar una funció racional V de les arrels de manera que totes les arrels siguin funcions racionals de V. Un cop establert això, considerem l'equació irreductible que té l'arrel V (Lema III i IV). Siguin $V, V', V'', \ldots, V^{(n-1)}$ les arrels d'aquesta equació i $\varphi V, \varphi_1 V, \varphi_2 V, \ldots, \varphi_{m-1} V$ les arrels de l'equació proposada.

Escrivim les n permutacions següents de les arrels:

$$\begin{array}{l|lllll}
(V) & \varphi V & \varphi_1 V & \varphi_2 V, \ldots, & \varphi_{m-1} V, \\
(V') & \varphi V' & \varphi_1 V' & \varphi_2 V', \ldots, & \varphi_{m-1} V', \\
(V'') & \varphi V'' & \varphi_1 V'' & \varphi_2 V'', \ldots, & \varphi_{m-1} V'', \\
\ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots \\
(V^{(n-1)}) & \varphi V^{(n-1)} & \varphi_1 V^{(n-1)} & \varphi_2 V^{(n-1)}, \ldots, & \varphi_{m-1} V^{(n-1)}.
\end{array}$$

Afirmo que aquest grup de permutacions té la propietat enunciada.

En efecte:

1. Tota funció F de les arrels, invariant per les substitucions d'aquest grup, podrà ser escrita així: $F = \psi V$, i tindrem que

$$\psi V = \psi V' = \psi V'' = \cdots = \psi V^{(n-1)}.$$

El valor d'F es podrà determinar racionalment.

2. *Recíprocament.* Si una funció F és determinable racionalment, i fem
[423] $F = \psi V$, tindrem

$$\psi V = \psi V' = \psi V'' = \cdots = \psi V^{(n-1)},$$

ja que l'equació en V no té cap divisor comensurable i l'equació $F = \psi V$ és satisfeta per V, essent F una quantitat racional. Així doncs, la funció F és necessàriament invariant per les substitucions del grup descrit abans.

Aquest grup satisfà la doble propietat que s'estableix en l'enunciat del teorema proposat. El teorema queda, doncs, demostrat. □

El grup en qüestió l'anomenarem el grup de l'equació.

Comentari 40. La demostració que ofereix Galois —convenientment entesa— és la que trobem en els textos actuals. Vegeu, per exemple, el text (Rey Pastor, 1915, edició de 1947, p. 216,223) o bé (Tignol, 2001, p. 250-251).

De fet, volem demostrar que, si $Q(\xi_1, \ldots, \xi_n)$ és una funció racional de les n arrels $\xi_1, \ldots, \xi_n$, de $f(X) = 0$, amb coeficients en K, aleshores

1. Per a tota substitució $\sigma \in \mathrm{Gal}\big(f(X)/K\big)$, l'element determinat per $Q\big(\sigma(\xi_1), \ldots, \sigma(\xi_n)\big) \in K(\xi_1, \ldots, \xi_n)$, està ben definit, si $Q(\xi_1, \ldots, \xi_n)$ ho està.

2. A més,

$$Q(\xi_1, \ldots, \xi_n) \in K \text{ si, i només si, per a tota } \sigma \in \mathrm{Gal}\big(f(X)/K\big),$$
$$Q(\xi_1, \ldots, \xi_n) = Q\big(\sigma(\xi_1), \ldots, \sigma(\xi_n)\big).$$

Demostració de la PROPOSICIÓ I.

1. Solament hem de veure que, si $Q(X_1,\dots,X_n) = \frac{N(X_1,\dots,X_n)}{D(X_1,\dots,X_n)}$, amb $N(X_1,\dots,X_n), D(X_1,\dots,X_n) \in K[X_1,\dots,X_n]$ i $D(\xi_1,\dots,\xi_n) \neq 0$, aleshores, per a tota $\sigma \in \mathrm{Gal}\big(f(X)/K\big)$, $D\big(\sigma(\xi_1),\dots,\sigma(\xi_n)\big) \neq 0$.

Això és una conseqüència immediata del fet que $K(X_1,\cdots,X_n) = K(V)$ i del corol·lari 32.1, p. 25.

2. Sigui ara $Q(\xi_1,\dots,\xi_n)$ i substituïm les arrels ξ_i per $\ell_i(v_1), i = 1,\dots,n$. Tindrem:

$$h(v_1) = Q(\xi_1,\dots,\xi_n) = Q\big(\ell_1(v_1),\dots,\ell_n(v_1)\big) = \big(Q\circ(\ell_1,\dots,\ell_n)\big)(v_1),$$

on $h(V) \in K(V)$.

(a) Si $Q(\xi_1,\dots,\xi_n) \in K$ [és a dir, és racionalment conegut], aleshores

$$h(V) - \big(Q\circ(\ell_1,\dots,\ell_n)\big)(V) \in K(V)$$

i s'anul·la per a $V := v_1$ i, de retruc, per a $v_2,\dots,v_m$. És a dir,

$$k = h(v_j) = Q\big(\ell_1(v_j),\dots,\ell_n(v_j)\big),\quad j = 1,\dots,m.$$

O sigui que, per a tot $\sigma \in \mathrm{Gal}\big(f(X)/K\big)$,

$$Q(\xi_1,\dots,\xi_n) = Q\big(\sigma(\xi_1),\dots,\sigma(\xi_n)\big).$$

(b) Si per a tot $j = 1,\dots,m$, i tot $\sigma \in \mathrm{Gal}\big(f(X)/K\big)$, val la igualtat:

$$h(v_j) = Q(\xi_1,\dots,\xi_n) = Q\big(\sigma(\xi_1),\dots,\sigma(\xi_n)\big),$$

aleshores

$$Q(\xi_1,\dots,\xi_n) = \frac{1}{m}\big(h(v_1)+\cdots+h(v_m)\big).$$

Ara bé, la funció $H(V_1,\dots,V_m) = h(V_1)+\cdots+h(V_m)$ és simètrica respecte de les variables $V_1,\dots,V_m$. Per tant es pot expressar com a funció racional de les funcions simètriques elementals de V_1, …, V_m. Si ara fem $V_1 := v_1,\dots,V_m := v_m$, pel *teorema de les funcions simètriques*, resulta que és una funció racional dels coeficients de $G_1(V) = 0$. O sigui, $Q(\xi_1,\dots,\xi_n) \in K$.

Comentari 41. Explicitem aquest lligam a través de l'equació: $f(X) := X^5 - X^4 - 5\,X^3 + 5\,X^2 + 6\,X - 6 \in \mathbb{Q}[X]$ del comentari 33, p. 25 d'arrels $1, \pm\sqrt{2}$ i $\pm\sqrt{3}$ i cos de partida —aquell al qual pertanyen els coeficients— $\mathbb{Q}$. Mentre ens hi mantinguem, ignorarem el significat dels símbols $\xi_2 = \sqrt{2}, \xi_3 = -\sqrt{2}$ i $\xi_4 = \sqrt{3}, \xi_5 = -\sqrt{3}$; contràriament, l'arrel $\xi_1 = 1$ és dins del cos $\mathbb{Q}$. En aquest

cas, tenim una existència ben definida i unes propietats intrínseques que li assignen una individualitat. Però, en canvi, dins del cos $\mathbb{Q}$, som incapaços de distingir realment $\xi_2;\xi_3$ i $\xi_4;\xi_5$: no són «visibles». Només podem atribuir-los una existència «virtual» i solament les podem reconèixer si ens fixem en les relacions que les uneixen; aquesta és la raó per la qual els algebristes les anomenen *quantitats conjugades*. Sabem que la seva suma és igual a 1, les sumes dels productes de dues, tres, quatre i cinc arrels donen -5, -5, 6, 6 —quelcom que respecten les funcions simètriques. Aquesta és la raó per la qual les úniques substitucions que hem de considerar són les que deixen invariants les relacions que hi ha entre aquestes les quantitats indiscernibles, és a dir, la identitat i les substitucions $(\xi_2 \quad \xi_3), (\xi_4 \quad \xi_5), (\xi_2 \quad \xi_3) \circ (\xi_4 \quad \xi_5)$. Aquestes quatre substitucions formen un grup.

Hom veu també la importància de la relativitat entre l'equació i el cos en el qual està definida, com ja hem esmentat en el comentari 11: atès que, en $\mathbb{Q}$, $\xi_2;\xi_3$ i ξ_4,ξ_5 només tenen una existència relativa i, en canvi, els manca una individualitat comparable amb l'existència discernible intrínscament dels elements del cos de base i, en particular, de ξ_1. La transposició que intercanvia ξ_1 i ξ_2 no té cap mena d'efecte perquè, en $\mathbb{Q}$, la seva actuació no és visible. Però, en el cos $\mathbb{Q}(\sqrt{2}) \supset \mathbb{Q}$, les arrels $\xi_2;\xi_3$ són «visibles» —racionals—, però $\xi_4;\xi_5$ segueixen essent invisibles i hem de recórrer al grup que formen la identitat i $(\xi_4 \quad \xi_5)$, perquè les altres —que transformen $\sqrt{2}$ en $-\sqrt{2}$— alteren lligams entre les arrels i els coeficients acceptables, com ara $\sqrt{2}\,X - 2 = 0$, que és vàlida per a $X := \xi_2$ i falsa per a $X := \xi_3$.

Escoli I. És evident que, en el grup de permutacions que tractem aquí, no té cap mena d'interès considerar la disposició de les lletres. Solament s'han de considerar les substitucions de les lletres amb les que hom passa d'una permutació a una altre.

Comentari 42. Aquí, d'alguna manera, Galois estableix la independencia del grup de l'elecció inicial de v_1. Vegeu la PROPOSICIÓ B, comentari 43, p. 35.

N'hi ha prou, doncs, a donar de forma arbitrària la primera presentació atès que la resta es dedueix d'ella per les mateixes substitucions de les lletres. El grup així format tindrà les mateixes propietats que el primer atès que, en el teorema precedent, solament es consideren les substitucions que podem fer en les funcions.

Escoli II. Les substitucions no depenen tampoc del nombre d'arrels de l'equació donada.

Comentari 43. Ara, si volem respectar el rigor que s'exigeix actualment en els textos matemàtics, hem d'establir tres resultats de caire formal:

(1) Els automorfismes s'estenen de forma natural a $K(\xi_1,\dots,\xi_n)$.

(2) Aquest subgrup és independent de la resolvent v_1.

(3) El grup de Galois és un subgrup de $\mathfrak{S}_n$.

(1) Proposició A. Cada substitució σ del grup de Galois s'estén a un automorfisme de $K(\xi,\dots,\xi_n)=K(v_1)$ que deixa K invariant, fent

$$\sigma\big(Q(\xi_1,\dots,\xi_n)\big)=Q\big(\sigma(\xi_1),\dots,\sigma(\xi_n)\big),$$

per a cada funció racional $Q(X_1,\dots,X_n)$ per a la qual $Q(\xi_1,\dots,\xi_n)$ estigui definit.

En efecte. $Q(\xi_1,\dots,\xi_n)$ està ben definit, en el sentit següent: Si es compleix $Q_1(\xi_1,\dots,\xi_n)=Q_2(\xi_1,\dots,\xi_n)$, aleshores

$$Q_1\big(\sigma(\xi_1),\dots,\sigma(\xi_n)\big)=Q_2\big(\sigma(\xi_1),\dots,\sigma(\xi_n)\big).$$

És una conseqüència immediata de la Proposició I aplicada a l'equació $(Q_1-Q_2)(\xi_1,\dots,\xi_n)=0$.

L'aplicació és, doncs, injectiva.

L'exhaustivitat l'estableix l'existència, per a cada substitució σ, de la corresponent substitució σ^{-1}.

El caràcter mòrfic es defineix de forma natural:

$$\sigma\big(Q_(\xi_1,\dots,\xi_n)\star Q_2(\xi_1,\dots,\xi_n)\big)\\ =Q_1\big(\sigma(\xi_1),\dots,\sigma(\xi_n)\big)\star Q_2\big(\sigma(\xi_1),\dots,\sigma(\xi_n)\big),$$

on $\star$ representa les operacions $+$ i $\cdot$. □

(2) Proposició B. El grup $\mathrm{Gal}\big(f(x)/K\big)$ no depèn de v_1.

En efecte. Suposem que $v'\in K(\xi_1,\dots,\xi_n)$ és una altra resolvent de $f(X)=0$ en K, $G_1'(V)$ el seu polinomi minimal sobre K, i ℓ_i', les funcions racionals sobre K que fan

$$\xi_i=\ell_i'(v'),\ \ i=1,\dots,n.$$

Hem de veure que cada element de $\mathrm{Gal}\big(f(X)/K\big)$, definit usant v_1, també és un element de $\mathrm{Gal}\big(f(X)/K\big)$, usant v'. Aleshores, canviant els papers de v_1 i v', tindrem el recíproc.

Hem de provar que

$$\sigma:\xi_i=\ell_i(v_1)\to\ell_i'(v_j'),$$

on v'_j és una arrel de $G'_1(V) = 0$.

Això és una conseqüència immediata de la PROPOSICIÓ A atès que $\xi_i = \ell'_i(v')$ implica $\sigma(\xi_i) = \ell'_i\big(\sigma(v')\big)$. I del fet que $G'_1(v') = 0$ se'n segueix també que $G'_1\big(\sigma(v')\big) = 0$. Agafem, doncs, $v'_j = \sigma(v'_1)$. □

(3) PROPOSICIÓ C. $\mathrm{Gal}\big(f(X)/K\big)$ és un subgrup de $\mathfrak{S}_n$.

En efecte. $\sigma_1 = \mathrm{Id} \in \mathrm{Gal}\big(f(X)/K\big)$.

Si $\sigma, \tau \in \mathrm{Gal}\big(f(X)/K\big)$, aleshores, per a $i = 1, \ldots, n$,

$$\begin{array}{lcll} \sigma : \xi_i = \ell_i(v_1) & \to & \ell_i(v_j), & \text{per a un cert } j = 1, \ldots, m, \\ \tau : \ell_i(v_j) = \ell_s(v_1) & \to & \ell_s(v_k), & \text{per a un cert } k = 1, \ldots, m. \end{array}$$

Se'n segueix que

$$\tau \circ \sigma : \xi_1 \to \ell_s(v_k).$$

Vegeu el comentari 15.

Tanmateix, la PROPOSICIÓ B permet donar una descripció explícita de l'invers σ^{-1} de σ.[19] □

PROPOSICIÓ II

TEOREMA.[20] Suposem que, a una equació donada, se li adjunta l'arrel
[424] r d'una equació auxiliar irreductible.

1º. Tindrà lloc una d'aquestes dues situacions: o bé el grup de l'equació no canviarà, o bé el dividirà en p grups cada un d'ells pertanyent a l'equació proposada quan se li adjunta respectivament cada una de les arrels de l'equació auxiliar.

2º. Aquests grups tenen la propietat remarcable següent: es passa de l'un a l'altre operant totes les permutacions del primer una mateixa substitució de les lletres.

[19] Vegeu (Tignol, 2001, p 253).

[20] A. CH. En l'enunciat del teorema, després de les paraules: *l'arrel r d'una equació auxiliar irreductible*, Galois havia escrit primerament això: *de grau p primer*, quelcom que més tard esborrà. Anàlogament, en la demostració, en lloc de $r, r', r'', \ldots$, *són d'altres valors de* r, la redacció primitiva deia: $r, r', r'', \ldots$, *són els diversos valors de* r. Finalment, al marge del manuscrit hi trobem la nota següent de l'autor:

«Hi ha quelcom que cal completar en aquesta demostració. Em falta temps.»

Aquesta línia fou escrita molt ràpidament; una circumstància que, juntament amb les paraules «Em falta temps», em fan pensar que Galois va rellegir la Memòria per corregir-la abans d'anar al duel.

1º. Si, després d'adjuntar r, l'equació en V, de la qual hem parlat abans, segueix essent irreductible, és clar que el grup de l'equació no canvia. Si, en canvi, es redueix, aleshores l'equació en V es descompondrà en p factors, tots del mateix grau i de la forma

$$f(V;r) \times f(V;r') \times f(V;r'') \times \cdots ,$$

essent $r, r', r'', \ldots$, d'altres valors de r. Així, el grup de l'equació proposada descompondrà també en grups cada un del mateix nombre de permutacions, ja que a cada valor de V li correspon una permutació. Aquests grups seran respectivament els de l'equació proposada, quan hom li anirà adjuntant successivament $r, r', r'', \ldots$.

2º. Abans hem vist que tots els valors de V són funcions racionals els uns dels altres. D'acord amb això, suposem que V és una arrel de $f(V;r) = 0$ i $F(V)$ n'és una altra; és clar que, igualment, si V' és una arrel de $f(V;r') = 0$, $F(V')$ en serà una altra, ja que tindrem

$$f\big(F(V);r\big) = \text{una funció divisible per } f(V;r).$$

Per tant, (*lema* I)

$$f\big(F(V');r\big) = \text{una funció divisible per } f(V';r).$$

Un cop establert això, afirmo que el grup relatiu a r' s'obté operant arreu damunt el grup relatiu a r una mateixa substitució de les lletres. En efecte, si hom té, per exemple,

$$\varphi_\mu F(V) = \varphi_\nu(V),$$

tindrà també (*lema* I),

$$\varphi_\mu F(V') = \varphi_\nu(V'),$$

Per tant, per pasar de la permutació $\big[F(V)\big]$ a la permutació $\big[F(V')\big]$, caldrà aplicar la mateixa substitució que per passar de la permutació (V) a la permutació (V'). I així el teorema queda demostrat. □ [425]

Comentari 44. Ara podem retornar al comentari 33, p. 25, i veure com es trenca el grup de Galois inicial o grup de l'equació.

Hem vist, equació (20), p. 26, que

$$\begin{aligned} G(V) = \big(V - (\sqrt{2}+\sqrt{3})\big)\,\big(V + (\sqrt{2}+\sqrt{3})\big)\,\big(V - (\sqrt{2}-\sqrt{3})\big) \\ \big(V + (\sqrt{2}+\sqrt{3})\big) \\ = V^4 - 10\,V^2 + 1. \end{aligned}$$

El podem reagrupar així:

$$\left(V^2 - 2\sqrt{2} - 1\right)\left(V^2 + 2\sqrt{2} - 1\right).$$

És clar que, si adjuntem les arrels de l'equació auxiliar $Y^2 - 2 = 0$, obtenim el cos $K_1 = \mathbb{Q}(\sqrt{2})$ i aleshores ambdós factors pertanyen a $K_1[V]$. A més, en aquest cos, ambdós factors són irreductibles. Així, per exemple, el factor $G_1\left(V, \sqrt{2}\right) = V^2 - 2\sqrt{2} - 1$ proporciona el grup de Galois següent — que correspon al cos $\mathbb{Q}[\sqrt{2}]$. Hem d'agafar les substitucions σ_1 i σ_2 del segon quadre de la p. 26 —que són les que deixen invariants $\sqrt{2}$ i $-\sqrt{2}$.

Sabem que

$$G_1\left(V, \sqrt{2}\right) = V^2 - 2\sqrt{2} - 1 = \left(V - (\sqrt{2} + \sqrt{3})\right)\left(V + (\sqrt{2} + \sqrt{3})\right)$$

i ambdós factors són irreductibles a $K_2 = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. De les substiutcions anteriors cal agafar la que deixa invariant $V - (\sqrt{2} + \sqrt{3})$, o sigui $\sqrt{3}$. És σ_1.

Recordem que $\xi_1 = 1, \xi_2 = \sqrt{2}, \xi_3 = -\sqrt{2}, \xi_4 = \sqrt{3}$ i $\xi_5 = -\sqrt{3}$. Aleshores el grup de Galois i els subgrups en que es trenca per efecte de les successives adjuncions els podem representar ara així:

	ξ_1	ξ_2	ξ_3	ξ_4	ξ_5
$\sigma_1 := \{\mathrm{Id}\}$	ξ_1	ξ_2	ξ_3	ξ_4	ξ_5
$\sigma_2 := (\xi_4 \quad \xi_5)$	ξ_1	ξ_2	ξ_3	ξ_5	ξ_4
$\sigma_3 := (\xi_2 \quad \xi_3)$	ξ_1	ξ_3	ξ_2	ξ_4	ξ_5
$\sigma_4 := (\xi_4 \quad \xi_5) \circ (\xi_2 \quad \xi_3)$	ξ_1	ξ_3	ξ_2	ξ_5	ξ_4

Tornarem a tractar aquesta qüestió en el comentari 71, p. 53.

Comentari 45. Josep Liouville dóna una demostració de la proposició quan p és primer, una demostració que recull Paul Tannery a (Tannery, 1908, p. 9). Val a dir, però, com provà Jordan (Jordan, 1869, §22), que la restricció p primer, on p és el grau de l'equació auxiliar, es pot suprimir.

Comentari 46. Veiem quin és l'argument de Liouville (Tannery, 1908, p. 9). Vegeu també (Neumann, 2011, p. 159-161).

Sigui $\psi(V) = 0$ l'equació de la qual parla l'autor i siguin $f(V, r)$, $f_1(V, r)$, $\ldots$, $f_{i-1}(V, r)$ els factors irreductibles en els quals factoritza per l'adjunció d'r, de manera que

$$\psi(V) = f(V, r) \times f_1(V, r) \times \cdots \times f_{i-1}(V, r).$$

Atès que r és l'arrel d'una equació irreductible hom pot reemplaçar r per $r', r'', \ldots, r^{(p-1)}$ en el segon membre. Aleshores $\psi(V)^p$ és el producte de les i

quantitats

$$\begin{array}{llll} f(V,r) & f(V,r') & \cdots & f(V,r^{(p-1)}) \\ f_1(V,r) & f_1(V,r') & \cdots & f_1(V,r^{(p-1)}) \\ & & \cdots & \\ f_{i-1}(V,r) & f_{i-1}(V,r') & \cdots & f_{i-1}(V,r^{(p-1)}) \end{array}$$

Cada fila és simètrica en $r, r', r'', \ldots, r^{(p-1)}$ i, per tant, és expressable com a funció racional de V, independent de qualsevol adjunció. Hem de vidir, doncs, $\psi(V)^p$. Per tant, es redueix a una potència simple de $\psi(V)$ que no es resol en factors quan no s'adjunta $r, r', r'', \ldots, r^{(p-1)}$.

Afirmo que el grau de les potències és el mateix per a totes. En efecte, les equacions $f(V,r) = 0, f_1(V,r) = 0, \ldots, f_{i-1}(V,r) = 0$ que deriven de $\psi(V)$ i les arrels de les quals són funcions racionals les unes de les altres *no poden deixar de tenir el mateix grau.* De

$$\psi(V)^\mu = f(V,r) \times f(V,r') \times \cdots \times f(V,r^{(p-1)}),$$

s'en conclou que $p = i\,\mu$, amb $i > 1$ i p primer. Per tant, $i = p$ i $\mu = 1$.

Per fi, doncs,

$$\psi(V) = f(V,r) \times f(V,r') \times \cdots \times f(V,r^{(p-1)})$$

que és el que volíem demostrar. □

Comentari 47. L'afirmació de Liouville diu:

Proposició 47.1. Tots els polinomis $H_i(V,\eta_1), i = 1, \ldots, \mu$, —són les $f_j(V,r)$ de Galois i els $\eta_i, i = 1, \ldots, m$, les r i, si cal, renumerades— de la factorització de $G_1(V)$ a $K_1 := K(\eta_1)$

$$G_1(V) = H_1(V,\eta_1) \times H_2(V,\eta_1) \times \cdots \times H_\mu(V,\eta_1) \tag{26}$$

tenen el mateix grau. En efecte. Es basa en el fet que cada un d'ells és irreductible i en el corol·lari 32.1, p. 25.

Considerem, per exemple, $H_1(V,\eta_1)$ i $H_2(V,\eta_1)$. Suposem que $v_1, \ldots, v_r$ són les arrels de $H_1(V,\eta_1)$ —o sigui $\text{grau}\big(H_1(V,\eta_1)\big) = r$— i $w_1, \ldots, w_s$ les de $H_2(V,\eta_1)$ —o sigui, $\text{grau}\big(H_2(V,\eta_1)\big) = s$—, totes elles diferents entre si i les unes amb les altres, atès que les arrels $v_i, i = 1, \ldots, v_{n!}$ són totes diferents. Pel corol·lari 32.1, p. 25, sabem que $w_1 = p(v_1)$, on $p(Z) \in K_1[Z]$. Per tant, a $K_1, H_1(V,\eta_1)$ i $H_2\big(p(V),\eta_1\big)$ tenen l'arrel comuna v_1 i, pel lema I, $H_1(V,\eta_1)\big|H_2\big(p(V),\eta_1\big)$.

Ara, per a cada arrel v_j de $H_1(V,\eta_1)$, considerem les arrels $p(v_j), j = 1, \ldots, r$, de $H_2\big(V,\eta_1\big)$ —de fet, són algunes de les arrels $w_j, j = 1, \ldots, s$. En

conseqüència, totes són diferents. Per tant, l'equació $H_2(V, \eta_1)$ té, almenys, tantes arrels com $H_1(V, \eta_1)$.

En resulta, doncs, que $s \geq r$. I, mutatis mutandis, $r \geq s$, com volíem demostrar. □

Comentari 48. Una demostració general l'ofereix Jordan a (Jordan, 1869, §22); vegeu també (Malet, 1984, p. 52-53). Vegeu el comentari 50.

Comentari 49. L'enunciat d'aquest teorema planteja problemes diversos com posa de manifest (Edwards, 2012, p. 917-920).

En primer lloc, en esborrar el text de la redacció anterior, esborra també el significat de p que apareix més endevant però que no s'ha precisat abans.

En segon lloc, si s'estén K amb una arrel η d'una equació auxiliar $g(Y) = 0$, irreductible, en general $K(\eta)$ no conté les altres arrels de $g(Y) = 0$. Això obliga a precisar on es troba cada funció —de fet, quins coeficients té, en cada cas. Vegeu els exemples del comentari 9.

Comentari 50. Demostració detallada de la PROPOSICIÓ II, p. 36. La factorització en K de $G(V)$ en factors irreductibles

$$G(V) = G_1(V) \times G_2(V) \times \ldots \times G_r(V) \text{ [vegeu (15)]}$$

proporciona una *partició* de les arrels $v_i, i = 1, \ldots, n!$, de la resolvent $G(V)$.

Hem partit, doncs, la col·lecció dels v_i en r conjunts —que són *disjunts* atès que les arrels $v_i, i = 1, \ldots, n!$, de $G(V)$ són simples.

Recordem, si ho hem oblidat, que $G(V) = \prod_{i=1}^{n!}(V - v_i)$ i que els v_i, $i = 1, \ldots, n!$, són *tots diferents*. Així doncs, si $k \neq j$ i $G_j(v_i) = 0$, aleshores $G_k(v_i) \neq 0$, perquè $G(V)$ no té arrels dobles. Galois anomena cada un d'aquests conjunts d'arrels v_i de $G(V)$ *grup* de $f(X) = 0$. No depèn de l'elecció de la resolvent i, per tant, tots els conjunts proporcionen el mateix grup.

Ara considerem l'equació auxiliar $g(Y) = 0$ i sigui $K_1 = K(\eta_1)$ una extensió simple de K, on η_1 és una arrel de $g(Y) = 0$; o sigui, $g(\eta_1) = 0$. Aleshores el factor irreductible $G_1(V)$ de $G(V)$ a K pot factoritzar a K_1. Sigui $H_1(V)$ el factor irreductible de $G_1(V)$ a K_1 que té l'arrel v_1. Els seus coeficients, en tant que elements de K_1, s'expressen com a polinomis en η_1 de grau $< r = \text{grau}\big(g(Y)\big)$ amb coeficients en K [comentari 28, p. 21]. Per tant, $H_1(V)$ és un polinomi *mònic* $H(V, \eta_1)$ de V i η_1, amb coeficients en K, irreductible. Com dèiem, en resulta, doncs, que $\text{Gal}\big(f(X)/K_1\big)$ conté $\text{grau}_V H_1(V, \eta_1)$ permutacions; són precisament les permutacions dels v_j per als quals $H(v_j, \eta_1) = 0$.

De fet, cal treballar amb el polinomi

$$H(V, \eta_1) \times H(V, \eta_2) \times \ldots \times H(V, \eta_r), \tag{27}$$

on $\eta_1, \eta_2, \ldots, \eta_r$, són les arrels de l'equació polinòmica auxiliar $g(Y) = 0$.

En principi, aquest producte té els coeficients en el cos de factorització lineal de $g(Y) = 0$, $K(\eta_1, \eta_2, \ldots, \eta_r)$. Però, com que és simètric en $\eta_1, \eta_2, \ldots, \eta_r$, els seus coeficients pertanyen al cos K dels coeficients de $g(Y) = 0$.[21]

Anàlogament, en virtut del LEMA I, una altra arrel η_2 de $g(Y) = 0$ proporciona una extensió $K_2 := K(\eta_2)$ i un factor *mònic* $H(V, \eta_2)$ de $G_1(V)$, irreductible en K_2. En efecte,

$$G_1(V) = H(V, \eta_1)\, Q(V, \eta_1), \text{ on } Q(V, Y) \in K[V, Y]$$

permet d'escriure $G_1(V) - H(V, \eta_1)\, Q(V, \eta_1)$ en la forma:

$$\Phi_r(Y)\, V^r + \Phi_{r-1}(Y)\, V^{r-1} + \cdots + \Phi_1(Y)\, V + \Phi_0(Y),$$

el qual, per a $Y := \eta_1$, és idènticament nul com a polinomi en V. Això diu que, per a tot $s = 0, 1, \ldots, r$, $\Phi_s(\eta_1) = 0$, on $\Phi_s(Y) \in K[Y]$. Pel LEMA I, tots els $\phi_s(Y)$ són divisibles per $g(Y)$. De retruc, doncs, $\Phi_s(\eta_t) = 0$ per a tota arrel η_t de $g(Y) = 0$. És a dir,

$$G_1(V) = H(V, \eta_t)\, Q(V, \eta_t), \text{ per a tota arrel } \eta_t \text{ de } g(Y) = 0.$$

Però Galois va més lluny i s'adona d'una propietat molt important:

Lema 50.1. Siguin v i $\ell(v)$ dues arrels de $H(V, \eta_1)$ —recordem que tota arrel de $G(V)$ es pot expressar racionalement en funció de v_1 i, de retruc, racionalitzant en funció polinòmica de v_1. Aleshores, si v' és una arrel de $H(V, \eta_2)$, $\ell(v')$ en serà una altra.

En efecte. Atès que $H(V, \eta_1)$ és irreductible, pel LEMA I i per la hipòtesi, resulta que $H(V, \eta_1) | H\big(\ell(V), \eta_1\big)$. O sigui,

$$H\big(\ell(V), \eta_1\big) = H(V, \eta_1) \times Q(V, \eta_1).$$

De retruc,

$$H\big(\ell(V), \eta_1\big) - H(V, \eta_1) \times Q(V, \eta_1) = 0$$

per a tot V. Això, com abans, implica que els coeficients $P_j(\eta_1) = 0$ per a tot j i, per tant, $g(Y) | P_j(Y)$.En resulta, doncs, que tota arrel η de $g(Y) = 0$ és arrel de $P_j(Y)$.

O sigui,

$$H\big(\ell(V), \eta_2\big) - H(V, \eta_2) \times Q(V, \eta_2) = 0.$$

Aleshores, trivialment, si v' és un zero de $H(V, \eta_2)$, òbviament $\ell(v')$ en serà un altre. □

[21] Edwards (Edwards, 1984, p. 120) l'anomena la *norma* de $H_1(V)$ sobre K.

Corol·lari 50.2. Els conjunts d'arrels $H(V,\eta_s)$ i de $H(V,\eta_t)$ de (26), p. 39, amb $s \neq t$, —que designarem també $H(V,\eta_s), H(V,\eta_t)$— o coincideixen o són disjunts.

En efecte. Si els polinomis $H(V,\eta_s)$ i $H(V,\eta_t)$ tenen una arrel comuna $v = v'$, aleshores cada arrel del polinomi $H(V,\eta_s)$ ho és del polinomi $H(V,\eta_t)$ i recíprocament i, com que ambdòs són mònics, coincideixen. □

Corol·lari 50.3. Considerem el polinomi

$$L(V) := H(V,\eta_1) \times H(V,\eta_2) \times \cdots \times H(V,\eta_p),$$

on $\eta_t, t = 1,\ldots,p$, són les arrels de $g(Y) = 0$. Aleshores $L(V) \in K[V]$.

En efecte. Aquest producte és simètric respecte de les arrels $\eta_1, \eta_2, \ldots, \eta_p$. Per tant, $L(V) \in K[V]$.

Corol·lari 50.4. A més, $G_1(V)|L(V)$.

En efecte. Les arrels $v_i, i = 1,\ldots,\mu$, de cada $H(V,\eta_s), s = 1,\ldots,p$, són arrels de $G_1(V)$ ja que cada $H(V,\eta_s)|G_1(V)$ i, a més, totes són diferents. □

Però, atenció! Els conjunts d'arrels $H(V,\eta_s)$ **o són disjunts o coincideixen**.

En principi, no sabem si tots ells són diferents. L'única cosa que sabem és

$$\text{Totes les arrels de } L(V) \text{ són arrels de } G_1(V). \qquad (*)$$

Per tant $G_1(V)\big|L(V)$ i, en conseqüència $L(V) = G_1(V)^k$ per a un cert k.[22] En resulta que, en el membre de la dreta, tota arrel de $G_1(V)$ —que és irreductible a $K(\eta_1)$— té multiplicitat k. Per tant, també l'haurà de tenir en el membre de l'esquerra. Però, hem vist que els factors $H(V,\eta_s)$ *o són disjunts o coincideixen*. Cal, doncs, que els que siguin diferents —amb arrels diferents i simples— es repeteixin k vegades. De factors, en total, n'hi ha p. Això comporta que p sigui divisible per k [i, en el cas, en què p sigui primer, $k = 1$]. Si, en cada grup de factors $H(V,\eta_s)$ repetits n'agafem un, tindrem, en total, $\frac{p}{k}$ factors diferents que serveixen per a representar-los.

Per fi, sigui $P(V)$ el producte d'aquests $\frac{p}{k}$ representants. Tenim dos polinomis mònics de $K[V]$, amb arrels simples i totes elles són les de $G_1(V)$. Per tant, $P(V)|G_1(V)$ i, pel Lema I, $G_1(V)|P(V)$. En definitiva, doncs,

$$G_1(V) = P(V) = \prod_{\nu=\frac{p}{k}} H(V,\eta_s),$$

[22] És una conseqüència immediata del Lema I: $G_1(V)\big|L(V)$, d'on $L(V) = G_1(V) \times L_1(V)$. Totes les arrels de $L_1(V)$ són arrels de $L(V)$ i, per $(*)$, de $G_1(V)$. Si el $\text{grau}\big(L_1(V)\big) \geq 1$, $L_1(V)$ i $G_1(V)$ tenen una arrel en comú i $G_1(V)$ és irreductible en K. D'on $G_1(V)\big|L_1(V)$. Iterem i obtindrem que $L(V) = G_1(V)^k$ per un cert $k \geq 1$.

on els factors $H(V,\eta_s)$ són diferents dos a dos. El nombre de factors $\nu = \frac{p}{k}$ divideix a p.

En definitiva: $G_1(V)$ és el producte de ν polinomis $H(V,\eta_s)$ diferents, i òbviament $\nu|p$. □

Comentari 51. Cal observar dos fets.

El primer és que Galois és conscient que tant en un grup com en un altre —en la seva terminologia— el lligam de les files és el mateix. És el que diu el lema 50.1, p. 41.

El segon fa referència al concepte de grup que usa Galois quan, de fet, es tracta de *classes laterals*. Si el grup $\mathcal{G}$ de l'equació $f(X) = 0$ sobre K és $\{\sigma_1, \ldots, \sigma_m\}$ i τ pertany al grup següent, aquest és, de fet, $\mathcal{G}' := \tau \circ \mathcal{G}$ [τ actua sobre $\mathcal{G}$]. Les substitucions que fan passar d'un element de $\mathcal{G}'$ a un altre són les mateixes que fan passar els elements de $\mathcal{G}$ d'un a l'altre. Ho veurem més endevant en l'exemple que acompanya la PROPOSICIÓ V, p. 45.

Com és ben conegut, cal recórrer al conjunt $\tau \circ \mathcal{G} \circ \tau^{-1}$ per tenir un grup en el sentit actual. S'anomenen *grups transformats* del grup $\mathcal{G}$.

PROPOSICIÓ III

TEOREMA. Si a una equació li adjuntem *totes* les arrels d'una equació auxiliar, els grups dels que es parla en el teorema II tenen, a més, aquesta propietat: en cada un dels grups les substitucions són les mateixes.

Hom trobarà la demostració. [23] □

Comentari 52. L'adjunció de totes les arrels la podem substituir per l'adjunció d'una sola arrel que correspongui a una equació irreductible auxiliar. Suposem que tenim l'equació auxiliar $g(Y) = 0$ d'arrels $\eta_1, \ldots, \eta_p$. En considerem la seva resolvent w i, encara, l'equació irreductible $\overline{g}(W) = 0$ per a

[23] A. CH. En el manuscrit, l'enunciat del teorema que acabem de llegir es troba al marge i en substitueix un altre que Galois havia acompanyat de la demostració corresponent i que anomenà amb el mateix títol PROPOSICIÓ III. Heus ací el text primitiu: TEOREMA. *Si l'equació en r és de la forma $r^p = A$, i una de les arrels primitives de la unitat es troba entre els nombres prèviament adjuntats, els p grups dels que es parla en el teorema* II *tenen, a més, la propietat següent: en cada grup, les substitucions de lletres amb les que hom passa d'una permutació a una altra són les mateixes.*

En efecte. En aquest cas, tant li fa adjuntar a l'equació aquest o aquell valor de r. Per consegüent, les seves propietats han de ser les mateixes un cop feta l'adjunció d'aquest o d'aquell valor. Així el seu grup ha d'ésser el mateix pel que fa a les substitucions (Proposició I, escoli). Per tant, etc.

Tot això fou esborrat curosament; l'enunciat nou porta la data de 1832 i mostra, d'acord amb l'afirmació que he fet sobre la manera com està escrit, que l'autor tenia molta pressa, i confirma l'opinió que ja he expressat a la nota precedent.

la qual $\overline{g}(w) = 0$. Òbviament, $K(\eta_1, \ldots, \eta_p) = K(w)$. Galois ha establert el *teorema de l'element primitiu* (Stillwell, 1994, p 146-147).

Fixem-nos que ara Galois precisa una qüestió que havíem deixat en suspens a la consideració 6, p. 5.

Per a aquesta equació auxiliar, com hem vist al corol·lari del comentari 32, p. 24, tots els $K(w_j)$ són el mateix, atès que $K(\eta_1, \ldots, \eta_p) = K(w_j)$ per a cada w_j; de retruc, cada w_j és una funció racional amb coeficients a K de $w_{j'}$. És a dir, per a tot j, $K' = K(w_j) = K(\eta_1, \ldots, \eta_p) = K(w_{j'})$. En resulta que cada $\overline{H}(V, w_j)$ és un factor irreductible sobre el cos comú K'. Aleshores les arrels v_i^j de $G_1(V)$ —que són arrels de $\overline{H}(V, w_j)$— proporcionen una presentació del grup de Galois de $f(X) = 0$ sobre K'. Cada factor presenta el grup sobre el cos que correspon a la w_i amb el qual està associat, però tots aquests cossos són iguals. Per tant, els grups corresponents a les diferents w_i tenen les mateixes substitucions, com volíem. □

Vegeu la nota 5 de (Malet, 1984, p. 53) que correspon a la prova donada a (Jordan, 1869, §24).

Comentari 53. En el sentit de la segona observació del comentari anterior, aquí Galois diu que *totes* les classes laterals del grup $\mathcal{G}$ són iguals; de retruc, doncs, tots els grups transformats són iguals. Per tant, per a tota substitució τ del grup anterior al grup actual $\mathcal{G}$, $\tau \circ \mathcal{G} \circ \tau^{-1} = \mathcal{G}$. Heus ací doncs com apareix, sense referir-s'hi explícitament, el concepte de *subgrup normal* o *subgrup invariant*.

Comentari 54. La nota de peu de pàgina nº 23, p. 43, diu que la condició que imposa la PROPOSICIÓ III —tots els grups es redueixen a un mateix grup— és condició necessària quan adjuntem una arrel p-èsima i una arrel p-èsima de la unitat, amb p primer, ja que aleshores s'han adjuntat totes.

Així doncs, per tal que puguem resoldre l'equació proposada per radicals la condició anterior és una condició necessària.

Fixem-nos que, en l'enunciat nou de la PROPOSICIÓ III, Galois l'únic que fa és donar un teorema més general; en el text esborrat, en canvi, limitava l'enunciat al cas particular en què l'equació adjuntada era de la forma $X^p - a = 0$, amb $a \in K$.

Comentari 55. Hem de veure que la condició és suficient i interpretar-la en llenguatge actual.

Això Galois ho fa en la PROPOSICIÓ V, on arriba al resultat central del treball; la resta de la memòria —una aplicació concreta al cas en què el grau de l'equació a resoldre és un nombre primer— en depèn totalment.

PROPOSICIÓ IV

TEOREMA. Si hom adjunta a una equació el valor *numèric* d'una certa funció de les seves arrels, el grup de l'equació s'abaixarà de manera que no contingui d'altres permutacions que aquelles per a les quals aquesta funció és invariant.

En efecte. D'acord amb la proposició I, tota equació coneguda ha de ser invariant per les permutacions del grup de l'equació. □

Comentari 56. En concret, si $u \in K\big(\xi_1, \ldots, \xi_n\big)$ —és a dir, u és un polinomi en les arrels $\xi_1, \ldots, \xi_n$ de $f(X) = 0$—, aleshores, per a tot σ,

$$\sigma \in \mathrm{Gal}\big(f(X)/K(u)\big) \text{ si, i només si, } \sigma \in \mathrm{Gal}\big(f(X)/K\big) \text{ i } \sigma(u) = u.$$

En efecte. Si $\sigma \in \mathrm{Gal}\big(f(X)/K(u)\big)$, pel teorema I, $\sigma(u) = u$, atès que $u \in K(u)$. Òbviament, per la construcció de $\mathrm{Gal}\big(f(X)/K(u)\big)$, tenim que $\mathrm{Gal}\big(f(X)/K(u)\big) \subseteq \mathrm{Gal}\big(f(X)/K\big)$.

Recíprocament, sigui $\sigma \in \mathrm{Gal}\big(f(X)/K\big)$ i $\sigma(u) = u$. Atès que $u = g\big(\xi_1, \ldots, \xi_n\big) \in K$, u és invariant per a tota $\sigma \in \mathrm{Gal}\big(f(X)/K(u)\big)$. Sigui ara el polinomi $H\big(V, u\big)$, minimal en $K(u)$, que $H\big(v_1, u\big) = 0$. Per la hipòtesi, u depèn de $\xi_1, \ldots, \xi_n$. Per tant, $H^*\big(v_1\big) = H\big(v_1, u\big) = 0$, on $H^*(V) \in K[V]$. Pel teorema I, $H^*\big(\sigma(v_1)\big) = 0$. Però, ho podem reescriure, $H\big(\sigma(v_1), \sigma(u)\big) = H\big(\sigma(v_1), u\big) = 0$. Per tant, $\sigma \in \mathrm{Gal}\big(f(X)/K(u)\big)$. □

Podíem haver usat la PROPOSICIÓ A del comentari 43, p. 35, atès que $H\big(v_1, u\big) = \sum \Phi_k(u)\, v_1^k$.

PROPOSICIÓ V [426]

PROBLEMA. En quins casos una equació es resoluble per radicals simples?

Comentari 57. Aquí, usant la nomenclatura heretada de la matemàtica grega, Galois distingeix teoremes i problemes.

I aquest és el primer dels problemes que Galois planteja en la Memòria.

Observo, per endevant, que, per poder resoldre una equació, cal abaixar successivament el seu grup fins que només contingui una única permutació. Ja que, quan s'aconsegueix de resoldre una equació, se'n coneix qualsevol funció de les seves arrels àdhuc aquelles que no són invariants per cap permutació.

Comentari 58. Cal doncs una cadena d'extensions del cos inicial K_0 amb adjuncions adequades de manera que els grups associats en cada adjunció s'abaixi respecte de l'anterior fins arribar al grup $\mathcal{G}_0 := \{\mathrm{Id}\}$.

Un cop establert aquest fet, busquem quina és la condició que ha de satisfer el grup d'una equació, per tal que es pugui abaixar fins a aquest extrem adjuntant quantitats radicals.

Seguim el camí de les operacions possibles en aquesta solució, considerant com operacions diferents l'extracció de cada arrel de grau primer.

Afegim aleshores a l'equació el primer radical que hem realitzat en la resolució. Hom podrà trobar-se amb dues situacions: o bé, amb l'adjunció d'aquest radical, el grup de les permutacions de l'equació disminuirà; o bé, l'extracció d'aquesta arrel, no essent altra cosa que una preparació, deixarà que el grup sigui el mateix.

En qualsevol dels casos, serà sempre després d'un cert nombre *finit* d'extraccions d'arrels que s'haurà aconseguit de disminuir el grup ja que sinó l'equació no seria resoluble.

Si, assolit aquest punt, hi ha maneres diverses de disminuir el grup de l'equació proposada amb una sola extracció d'arrels, caldrà, d'acord amb allò que hem dit, considerar solament un radical del grau més petit possible d'entre tots els radicals simples, que siguin d'aquells que el seu coneixement permet disminuir el grup de l'equació.

Comentari 59. Aquesta minimalitat força que l'extracció de l'arrel sigui de grau primer.

Sigui doncs p el nombre primer que representa aquest grau mínim, de manera que amb l'extracció d'una arrel de grau p, s'aconsegueixi disminuir el grup de l'equació.

Podem suposar sempre, si més no pel que fa al grup de l'equació, que entre les quantitats adjuntades a l'equació per endevant s'hi troba una arrel p-èsima de la unitat. Atès que, com que aquesta expressió s'obté per
[427] extraccions d'arrels de grau inferior a p, conèixer-la no altera en res el grup de l'equació.

Comentari 60. De fet, $X^p - 1 = 0$ es reduiex a l'equació, irreductible en $\mathbb{Q}$, $X^{p-1} + X^{p-2} + \cdots + X + 1 = 0$ que és de grau menor que p.

En conseqüència, d'acord amb els teoremes II i III, el grup de l'equació s'haurà de descompondre en p grups que, els uns respecte dels altres, tinguin aquesta doble propietat: 1º. Que hom passi de l'un a l'altre per una

sola substitució, la mateixa en tots els casos; 2º. Que tots ells continguin les mateixes substitucions.

Afirmo, recíprocament, que si el grup de l'equació es por trencar en p grups amb aquesta doble propietat, hom podrà, amb una simple extracció d'arrels p-èsimes, i amb l'adjunció d'aquesta arrel p-èsima, reduir el grup de l'equació a un dels grups parcials.

Agafem, en efecte, una funció de les arrels que sigui invariant per totes les substitucions d'un d'aquests grups parcials, i que varií per a qualsevol altre substitució. (Per això només cal agafar una funció que sigui simètrica respecte dels valors diversos que pren sotmesa a les permutacions d'un dels grups parcials i que no ho sigui, d'invariant, per cap altre substitució). [24]

Sigui θ aquesta funció de les arrels.

Operem damunt la funció θ una de les substitucions del grup total que no sigui comuna amb les dels grups parcials. Sigui θ_1 el que en resulta. Operem ara damunt d'aquesta funció θ_1 la mateixa substitució. En resulta θ_2. I així successivament.

Atès que p és un nombre primer, aquesta successió s'aturarà en el terme θ_{p-1}; seguidament tindrem $\theta_p = \theta_1, \theta_{p+1} = \theta_2$, i així successivament.

Un cop això establert, és clar que la funció

$$\left(\theta + \alpha\,\theta_1 + \alpha^2\,\theta_2 + \cdots + \alpha^{p-1}\,\theta_{p-1}\right)^p$$

serà invariant per totes les permutacions del grup total i, per tant, serà actualment coneguda.

Si traiem l'arrel p-èsima d'aquesta funció, i l'adjuntem a l'equació, aleshores, per la proposició IV, el grup de l'equació no contindrà altres substitucions que les del grup parcial.

Així doncs, aquesta condició és necessària i suficient per tal que el grup d'una equació es pugui abaixar amb la simple extracció d'una arrel.

Comentari 61. Aquí Galois pren, com a inspiració, el camí que ja havia caminat —amb no tanta profunditat, però amb una gran lucidesa— Lagrange en la seva anàlisi de 1770. Vegeu (Tignol, 2001, p 145-147).

Comentari 62. Aquesta és la condició suficient de la que parlàvem a l'observació 52.

Sigui θ una funció de les arrels *invariant* —és bàsic— per un dels grups parcials $\mathcal{H} \subset \mathcal{G}$ i que varií per a qualsevol altra substitució $\tau \in \mathcal{G} - \mathcal{H}$. Tindrem $\theta_1 = \tau(\theta), \theta_2 = \tau(\theta_1), \ldots, \theta_{p-1} = \tau(\theta_{p-2})$ i, atès que p és primer, $\theta_p = \theta_1, \theta_{p+1} = \theta_2, \ldots$.

[24] Vegeu (Dehn, 1960, p 28, ítem 21).

Proposició 62.1. D'això en resulta que, per a tota substitució $\sigma \in \mathcal{G}$, la funció

$$\Delta_0(\xi_1, \dots, \xi_n) = \big(\theta + \epsilon\,\theta_1 + \epsilon^2\,\theta_2 + \cdots + \epsilon^{p-1}\,\theta_{p-1}\big)^p \tag{28}$$

és invariant.

En efecte.

(1) Les permutacions $\sigma \in \mathcal{H}$ deixen fixa l'expressió (28).[25]

$$\sigma\Big(\big(\theta + \epsilon\,\theta_1 + \epsilon^2\,\theta_2 + \cdots + \epsilon^{p-1}\,\theta_{p-1}\big)^p\Big) = \big(\theta + \epsilon\,\theta_1 + \epsilon^2\,\theta_2 + \cdots + \epsilon^{p-1}\,\theta_{p-1}\big)^p.$$

(2) D'altra banda, per a $i = 1, 2, \dots, p-1$,[26]

$$\begin{aligned}\tau^i\Big(\sigma\Big(\big(\theta + \epsilon\,\theta_1 + \epsilon^2\,\theta_2 + \cdots + \epsilon^{p-1}\,\theta_{p-1}\big)^p\Big)\Big)&\\ = \big(\theta_i + \epsilon\,\theta_{i+1} + \epsilon^2\,\theta_{i+2} + \cdots + \epsilon^{p-1}\,\theta_{i-1}\big)^p&\\ = \Big(\epsilon^{p-i}\big(\epsilon^i\theta_i + \epsilon^{i+1}\,\theta_{i+1} + \epsilon^{i+2}\,\theta_{i+2} + \cdots + \epsilon^{i-1}\,\theta_{i-1}\big)\Big)^p&\\ = \big(\theta + \epsilon\,\theta_1 + \epsilon^2\,\theta_2 + \cdots + \epsilon^{p-1}\,\theta_{p-1}\big)^p.&\end{aligned}$$

Per tant, (28) és invariant per a tota substitució $\sigma \in \mathcal{G}$ i, per la PROPOSICIÓ I, actualment coneguda. Tenim, doncs,

$$A_0 = \Delta_0(\xi_1, \dots, \xi_n) = \Delta_i(\xi_1, \dots, \xi_n)$$

i, de retruc,

$$A_0 = A_i = \tau^i\Big(\sigma\Big(\big(\theta + \epsilon\,\theta_1 + \epsilon^2\,\theta_2 + \cdots + \epsilon^{p-1}\,\theta_{p-1}\big)^p\Big)\Big),$$

per a $i = 0, 1, 2, \dots, p-1$. En resulta que

$$\begin{aligned}\Delta_0(\xi_1, \dots, \xi_n) = \frac{1}{p}\big(&\Delta_0(\xi_1, \dots, \xi_n) + \Delta_1(\xi_1, \dots, \xi_n) + \cdots\\ &+ \Delta_{p-1}(\xi_1, \dots, \xi_n)\big).\end{aligned}$$

I, d'altra banda,

$$\begin{aligned}
\sqrt[p]{A_0} &= \theta + \quad \theta_1 + \quad \theta_2 + \cdots + \quad \theta_{p-1}\\
\sqrt[p]{A_1} &= \theta + \epsilon\,\theta_1 + \epsilon^2\,\theta_2 + \cdots + \epsilon^{p-1}\,\theta_{p-1}\\
\sqrt[p]{A_2} &= \theta + \epsilon^2\,\theta_1 + \epsilon^4\,\theta_2 + \cdots + \epsilon^{2(p-1)}\,\theta_{p-1}\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
\sqrt[p]{A_{p-1}} &= \theta + \epsilon^{p-1}\,\theta_1 + \epsilon^{2(p-1)}\,\theta_2 + \cdots + \epsilon^{(p-1)(p-1)}\,\theta_{p-1}
\end{aligned}$$

[25] Aquí hem de recórrer al fet que $\mathcal{H}$ és normal dins de $\mathcal{G}$ [vegeu el comentari 53, p. 44]. És a dir, $\tau \circ \sigma = \sigma' \circ \tau$, amb $\sigma' \in \mathcal{H}$. Aleshores, $\sigma'(\theta) = \theta$ i, per tant, $\tau^i \circ \sigma = \tau^{i-1} \circ \sigma' \circ \tau = \tau^{i-2} \circ \sigma^{(2)} \circ \tau^2 = \cdots = \sigma^{(i)} \circ \tau^i$, on $\sigma^{(i)} \in \mathcal{H}$.

[26] Aquí fem servir que les diverses classes laterals s'obtenen fent $\sigma \circ \tau^i$, $i = 0, 1, 2, \dots, p-1$.

D'on:

$$\theta = \frac{1}{p}\Big(\sqrt[p]{A_0} + \sqrt[p]{A_0} + \cdots + \sqrt[p]{A_{n-1}}\Big).$$

Els altres valors $\theta_1, \theta_2, \ldots, \theta_{p-1}$ els podem aconseguir usant la regla de Cramer o bé el fet que $1 + \epsilon + \epsilon^2 + \cdots + \epsilon^{p-1} = 0$, atès que $\epsilon^p - 1 = 0$.

En particular, si $\theta_i = \xi_i, i = 1, 2, \ldots, p-1$, tindrem les arrels de l'equació inicial per radicals.

Excel·lent treball!

Adjuntem a l'equació el radical en qüestió; aleshores podrem raonar sobre el grup nou tal com ho havíem fet sobre el precedent, i caldrà que també aquest es descompongui de la manera indicada, i així successivament fins assolir un grup que només contingui una única permutació. □ [428]

Comentari 63. Arribem al teorema clàssic de la teoria de Galois tal com s'exposa en els textos usuals. Dues cadenes, l'una creixent de cossos, cada una extensió de l'anterior per una arrel de grau primer, i l'altra, de grups, cada un subgrup normal de l'anterior d'índex primer:

$$\begin{array}{ccccccc} \mathbb{Q} & \subset & \mathbb{Q}(\eta_1) & \subset & \cdots & \subset & K \\ \mathrm{Gal}\big(f(X)/\mathbb{Q}\big) = \mathcal{G}_r & \supset & \mathcal{G}_{r-1} & \supset & \cdots & \supset & \mathcal{G}_0 = \{\mathrm{Id}\}. \end{array}$$

Escoli. És fàcil d'observar aquest camí en la resolució coneguda de les equacions generals de quart grau.

Comentari 64. Segueix, de fet, el mateix camí que Lagrange a la seva ànalisi de 1770.

La quàrtica general és $f(X) := X^4 + A\,X^3 + B\,X^2 + C\,X + D$, on A, B, C i D són *lletres*. Aquí pren sentit el comentari 6, p. 5, sobre les extensions transcendents. Tot s'inicia en el cos $K_0 = \mathbb{Q}(A, B, C, D)$.

Al comentari 37 hem vist que el grup de Galois de l'equació polinòmica $X^4 + A\,X^3 + B\,X^2 + C\,X + D = 0$ és $\mathcal{G}_1 := \mathfrak{S}_4$, que té 24 elements. Si les arrels les designem $\xi_1, \xi_2, \xi_3, \xi_4$, són:

$\xi_1\,\xi_2\,\xi_3\,\xi_4$; $\xi_1\,\xi_3\,\xi_4\,\xi_2$; $\xi_1\,\xi_4\,\xi_2\,\xi_3$;	$\xi_2\,\xi_1\,\xi_3\,\xi_4$; $\xi_2\,\xi_3\,\xi_4\,\xi_1$; $\xi_2\,\xi_4\,\xi_1\,\xi_3$;
$\xi_2\,\xi_1\,\xi_4\,\xi_3$; $\xi_3\,\xi_1\,\xi_2\,\xi_4$; $\xi_4\,\xi_1\,\xi_3\,\xi_2$;	$\xi_1\,\xi_2\,\xi_4\,\xi_3$; $\xi_3\,\xi_2\,\xi_1\,\xi_4$; $\xi_4\,\xi_2\,\xi_3\,\xi_1$;
$\xi_3\,\xi_4\,\xi_1\,\xi_2$; $\xi_4\,\xi_2\,\xi_1\,\xi_3$; $\xi_2\,\xi_3\,\xi_1\,\xi_4$;	$\xi_3\,\xi_4\,\xi_2\,\xi_1$; $\xi_4\,\xi_1\,\xi_2\,\xi_3$; $\xi_1\,\xi_3\,\xi_2\,\xi_4$;
$\xi_4\,\xi_3\,\xi_2\,\xi_1$; $\xi_2\,\xi_4\,\xi_3\,\xi_1$; $\xi_3\,\xi_2\,\xi_4\,\xi_1$;	$\xi_4\,\xi_3\,\xi_1\,\xi_2$; $\xi_1\,\xi_4\,\xi_3\,\xi_2$; $\xi_3\,\xi_1\,\xi_4\,\xi_2$.

Escoli. En efecte, aquestes equacions es resolen per mitjà d'una equació de grau tres que, al seu torn, exigeix l'extracció d'una arrel quadrada. En la successió natural de les idees cal començar per aquesta arrel quadrada. Aleshores, un cop adjuntada a l'equació de grau quatre aquesta arrel quadrada, el grup de l'equació —que en total conté vint-i-quatre substitucions— es descomposa en dos, cada un dels quals en té dotze. Si les arrels les designem a, b, c, d, heus ací un d'aquests grups:

$$\begin{array}{lll} abcd; & acdb; & adbc; \\ badc; & cabd; & dacb; \\ cdab; & dbac; & bcad; \\ dcba; & bdca; & cbda. \end{array}$$

Comentari 65. Reduirem el grup $\mathfrak{S}_4$ per la meitat si aconseguim trobar una equació polinòmica de les arrels $\xi_1, \xi_2, \xi_3, \xi_4$ que prengui dos valors, cada un d'ells invariant per un subgrup de 12 elements [vegeu el quadre anterior]. Com és ben conegut, el *discriminant*

$$\theta_1(\xi_1, \xi_2, \xi_3, \xi_4) := \sqrt{\Delta} = (\xi_1 - \xi_2)(\xi_1 - \xi_3)(\xi_1 - \xi_4)(\xi_2 - \xi_3)(\xi_2 - \xi_4)(\xi_3 - \xi_4)$$

es manté invariant amb les substitucions de l'esquerra de la doble barra del quadre anterior —és el *grup alternat* $\mathfrak{A}_4$— i canvia de signe amb les de la dreta. Aleshores, segons hem vist a (28) de la PROPOSICIÓ V, $\left(\theta_{11} - \theta_{12}\right)^2 = \left(\sqrt{\Delta} - \sqrt{-\Delta}\right)^2 = 4\,\Delta$. Això equival a adjuntar $\sqrt{\Delta}$.

El *discriminant* Δ és una funció simètrica —un fet conegut pels algebristes que havien precedit Galois. En canvi, $\sqrt{\Delta} = \begin{vmatrix} 1 & 1 & 1 & 1 \\ \xi_1 & \xi_2 & \xi_3 & \xi_4 \\ \xi_1^2 & \xi_2^2 & \xi_3^2 & \xi_4^2 \\ \xi_1^3 & \xi_2^3 & \xi_3^3 & \xi_4^4 \end{vmatrix}$ classifica les permutacions en *parells* i *senars*.

És resoluble per radicals en el cos $\mathbb{Q}(A, B, C, D, \sqrt{\Delta}) = K_0(\sqrt{\Delta}) = K_1$.

Ara, d'acord amb el que s'indica als teoremes II i III, aquest grup es descomposa en tres grups. D'aquesta manera, amb l'extracció d'una sola arrel de grau tres, s'obté el grup:

$$\begin{array}{l} abcd; \\ badc; \\ cdab; \\ dcba. \end{array}$$

Comentari 66. Necessitem trencar el grup l'alternat —de les permutacions parelles— en tres subgrups de quatre elements cada un. Necessitem

una funció $\theta_2(\xi_1,\xi_2,\xi_3,\xi_4)$ que prengui tres valors quan la sotmetem a les substitucions del grup alternat.

Com va posar de manifest Lagrange —és una de les resolvents de la quàrtica que proporciona— les tres quantitats són:

$$\begin{aligned}\theta_{2,1}(\xi_1,\xi_2,\xi_3,\xi_4) &:= (\xi_1+\xi_2-\xi_3-\xi_4)^2,\\ \theta_{2,2}(\xi_1,\xi_2,\xi_3,\xi_4) &:= (\xi_1-\xi_2+\xi_3-\xi_4)^2,\\ \theta_{2,3}(\xi_1,\xi_2,\xi_3,\xi_4) &:= (\xi_1-\xi_2-\xi_3+\xi_4)^2.\end{aligned} \tag{29}$$

S'intercanvien per les substitucions del subgrup $\mathcal{G}_2 := \mathfrak{A}_4$ segons que els seus elements siguin de la primera —$\mathcal{G}_3$—, segona o tercera columna de

σ	$\tau\circ\sigma$	$\tau^2\circ\sigma$
$\xi_1\,\xi_2\,\xi_3\,\xi_4$	$\xi_1\,\xi_3\,\xi_4\,\xi_2$	$\xi_1\,\xi_4\,\xi_2\,\xi_3$
$\xi_2\,\xi_1\,\xi_4\,\xi_3$	$\xi_3\,\xi_1\,\xi_2\,\xi_4$	$\xi_4\,\xi_1\,\xi_3\,\xi_2$
$\xi_3\,\xi_4\,\xi_1\,\xi_2$	$\xi_4\,\xi_2\,\xi_1\,\xi_3$	$\xi_2\,\xi_3\,\xi_1\,\xi_4$
$\xi_4\,\xi_3\,\xi_2\,\xi_1$	$\xi_2\,\xi_4\,\xi_3\,\xi_1$	$\xi_3\,\xi_2\,\xi_4\,\xi_1$.

Ara hem de recórrer, novament per (28), a

$$\left(\theta_{2,1}+\epsilon\,\theta_{2,1}+\epsilon^2\,\theta_{2,3}\right)^3,$$

on $\epsilon = \frac{-1+\sqrt{-3}}{2}$ és una arrel cúbica de la unitat. El cos és, doncs, $K_2 = K_1(\sqrt{-3}) = K_1(\epsilon)$.

Aquest grup es descomposa, novament, en dos grups:

$$\begin{array}{ll} abcd; & cdab;\\ badc; & dcba.\end{array}$$

Comentari 67. El subgrup $\mathcal{S}_2$ el trenquem en dos

σ	$\tau\circ\sigma$
$\xi_1\,\xi_2\,\xi_3\,\xi_4$	$\xi_3\,\xi_4\,\xi_1\,\xi_2$
$\xi_2\,\xi_1\,\xi_4\,\xi_3$	$\xi_4\,\xi_3\,\xi_2\,\xi_1$

usant $\theta_3(\xi_1,\xi_2,\xi_3,\xi_4) := \xi_1+\xi_2-\xi_3-\xi_4$ ja que les substitucions de la columna de l'esquerra —que formen el subgrup $\mathcal{S}_3$— mantenen el valor i les de la dreta, el canvien. Cal, doncs, afegir $\xi_1+\xi_2-\xi_3-\xi_4$ que és una arrel quadrada de $(\xi_1+\xi_2-\xi_3-\xi_4)^2$ i obtenim com a nova extensió el cos K_3.

Així, per una simple extracció d'una arrel quadrada, quedarà

$$abcd;$$
$$badc;$$

i això es resoldrà finalment amb l'extracció d'una sola arrel quadrada. [429]

Comentari 68. Per fi $\mathcal{S}_4$ el trenquem en dos

σ	$\tau \circ \sigma$
$\xi_1\,\xi_2\,\xi_3\,\xi_4$	$\xi_2\,\xi_1\,\xi_4\,\xi_3$

usant $\theta_4(\xi_1, \xi_2, \xi_3, \xi_4) := \xi_1 - \xi_2 + \xi_3 - \xi_4$ que es manté amb la identitat i canvia amb l'altra substitució. Obtenim el cos K_4 on resoldre afegint a K_3 una arrel quadrada de $(\xi_1 - \xi_2 + \xi_3 - \xi_4)^2$; o sigui el grup s'ha reduït a la unitat.

Vegeu la resolució de Vandermonde (Tignol, 2001, p. 154-156).

D'aquesta manera s'obtè la solució de Descartes, o la d'Euler; ja que, encara que aquest darrer, un cop feta la resolució de l'equació auxiliar de grau tres extreu tres arrels quadrades, sabem que n'hi ha prou amb dues ja que la tercera se'n dedueix racionalment.

Comentari 69. Pel que fa a aquest comentari de Galois, podeu consultar (Edwards, 2012, p. 921-922).

Comentari 70. Ara considerem el que Galois anomena grups

$$\begin{array}{lll} \xi_1\,\xi_2\,\xi_3\,\xi_4; & \xi_1\,\xi_3\,\xi_4\,\xi_2; & \xi_1\,\xi_4\,\xi_2\,\xi_3; \\ \xi_2\,\xi_1\,\xi_4\,\xi_3; & \xi_3\,\xi_1\,\xi_2\,\xi_4; & \xi_4\,\xi_1\,\xi_3\,\xi_2; \\ \xi_3\,\xi_4\,\xi_1\,\xi_2; & \xi_4\,\xi_2\,\xi_1\,\xi_3; & \xi_2\,\xi_3\,\xi_1\,\xi_4; \\ \xi_4\,\xi_3\,\xi_2\,\xi_1; & \xi_2\,\xi_4\,\xi_3\,\xi_1; & \xi_3\,\xi_2\,\xi_4\,\xi_1. \end{array}$$

I mirem quines substitucions proporcionen cada columna i quines passen dels elements d'una columna a l'altra.

Comencem amb la primera columna. És una columna de «permutacions». Seguint ara la presentació de Galois —vegeu les definicions de permutació i de substitució, p. 7–9—, la «substitució» passa de la permutació bàsica 1 2 3 4 a la permutació de cada fila; o sigui tenim les substitucions

fila 1:	1	2	3	4
fila 2:	2	1	4	3
fila 3:	3	4	1	2
fila 4:	4	3	2	1

$$\sigma_1 = \begin{pmatrix} 1\,2\,3\,4 \\ 1\,2\,3\,4 \end{pmatrix},\ \sigma_2 = \begin{pmatrix} 1\,2\,3\,4 \\ 2\,1\,4\,3 \end{pmatrix},\ \sigma_3 = \begin{pmatrix} 1\,2\,3\,4 \\ 3\,4\,1\,2 \end{pmatrix},\ \sigma_4 = \begin{pmatrix} 1\,2\,3\,4 \\ 4\,3\,2\,1 \end{pmatrix}$$

És clar que el conjunt $\mathcal{H} := \{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}$ conté Id —és σ_1— i és tancat per la composició $\circ$. És un grup, tant en la nomenclatura galoisiana com en la nostra.

Ara bé, si apliquem el mateix criteri amb les altres dues columnes obtenim, respectivament, el conjunt $\mathcal{H}_1$ de les τ_i i el conjunt $\mathcal{H}_2$ de les $\upsilon_i, i = 1, 2, 3, 4$.

$$\tau_1 = \begin{pmatrix} 1&2&3&4\\1&3&4&2\end{pmatrix}, \quad \tau_2 = \begin{pmatrix} 1&2&3&4\\3&1&2&4\end{pmatrix}, \quad \tau_3 = \begin{pmatrix} 1&2&3&4\\4&2&1&3\end{pmatrix}, \quad \tau_4 = \begin{pmatrix} 1&2&3&4\\2&4&3&1\end{pmatrix},$$

$$\upsilon_1 = \begin{pmatrix} 1&2&3&4\\1&4&2&3\end{pmatrix}, \quad \upsilon_2 = \begin{pmatrix} 1&2&3&4\\4&1&3&2\end{pmatrix}, \quad \upsilon_3 = \begin{pmatrix} 1&2&3&4\\2&3&1&4\end{pmatrix}, \quad \upsilon_4 = \begin{pmatrix} 1&2&3&4\\3&2&4&1\end{pmatrix}.$$

És clar que els conjunts $\mathcal{H}_1$ i $\mathcal{H}_2$ ni tenen la unitat ni són tancats per $\circ$. Però, Galois, que els anomena grups, ens ha dit que els grups han d'estar tancats per $\circ$ [vegeu la p. 9].

Calen tres observacions:

Primera observació. «Tots» els elements de $\mathcal{H}_1$ s'obtenen dels del grup $\mathcal{H}$ multiplicant-los per una mateixa substitució; en concret, $\mathcal{H}_1 = \tau_1 \circ \mathcal{H}$ i $\mathcal{H}_2 = \upsilon_1 \circ \mathcal{H}$, on, a més, $\upsilon_1 = \tau_1^2$.

Segona observació. Per aconseguir que siguin grups en el sentit actual, cal recórrer a l'argúcia següent. Volem que $\tau_1 \mapsto \tau_1^* = \begin{pmatrix} 1&3&4&2\\1&3&4&2\end{pmatrix}$ que, reordenant-ho sobre la permutació bàsica, dóna $\mathrm{Id} = \begin{pmatrix} 1&2&3&4\\1&2&3&4\end{pmatrix}$.

Això ho aconseguim molt fàcilment fent

$$\tau_1 \circ \tau_1^{-1} = \begin{pmatrix} 1&2&3&4\\1&3&4&2\end{pmatrix} \circ \begin{pmatrix} 1&2&3&4\\1&4&2&3\end{pmatrix} = \begin{pmatrix} 1&2&3&4\\1&2&3&4\end{pmatrix} = \mathrm{Id}.$$

El que és interessant d'aquesta argúcia és que, si l'apliquem a les substitucions de $\mathcal{H}_1$, obtenim $\mathcal{H}_1^* = \mathcal{H}_1 \circ \tau_1^{-1}$. I anàlogament, $\mathcal{H}_2^* = \mathcal{H}_2 \circ \upsilon_1^{-1}$.

Tercera observació. Aquest exemple, els tres grups són iguals; o sigui $\mathcal{H}_1^* = \mathcal{H}_1 \circ \tau_1^{-1} = \mathcal{H}$ i $\mathcal{H}_2^* = \mathcal{H}_2 \circ \upsilon_1^{-1} = \mathcal{H}$. En definitiva, $\tau_1 \circ \mathcal{H} \circ \tau_1^{-1} = \mathcal{H}$ i $\upsilon_1 \circ \mathcal{H} \circ \upsilon_1^{-1} = \mathcal{H}$. És a dir, $\mathcal{H}$ és un *subgrup normal* de $\mathcal{G}$.

Heus ací els conceptes de Galois a partir d'aquest exemple.

Comentari 71. Un exemple sempre ajuda. Ens plantejarem el cas de la *resolució de la cúbica general*.

Considerem la cúbica general irreductible $f(X) := X^3 + pX + q = 0$, amb $p, q \in \mathbb{Q}$, i arrels ξ_1, ξ_2 i ξ_3. Per la precisió 21, p. 13, són diferents.

Primera etapa. Una possible resolvent és $v_1 = V\big(\xi_1, \xi_2, \xi_3\big) = \xi_1 - \xi_2$. Genera els sis valors diferents

$$v_2 = \xi_1 - \xi_3; v_3 = \xi_2 - \xi_1; v_4 = \xi_2 - \xi_3; v_5 = \xi_3 - \xi_1 \text{ i } v_6 = \xi_3 - \xi_2.^{27}$$

Tenim

$$\begin{aligned} G(V) &= \big(V - v_1\big)\,\big(V - v_2\big)\,\big(V - v_3\big)\,\big(V - v_4\big)\,\big(V - v_5\big)\,\big(V - v_6\big) \\ &= \big(V - (\xi_1 - \xi_2)^2\big)\,\big(V - (\xi_2 - \xi_3)^2\big)\,\big(V - (\xi_1 - \xi_3)^2\big) \\ &= V^6 + \big(2\,s_1^2 + 6\,s_2\big)\,V^4 + \big(s_1^4 - 6\,s_1^2\,s_2 + 9\,s_2^2\big)\,V^2 \\ &\qquad + 4\,s_1^3 - s_1^2 s_2^2 + 27\,s_3^3 - 18\,s_1\,s_2\,s_3 + 4\,s_1^3\,s_2 \\ &= V^6 + 6\,p\,V^4 + 9\,p^2\,V^2 + 4\,p^3 + 27q^2. \end{aligned} \tag{30}$$

on $s_1 = \xi_1 + \xi_2 + \xi_3 = 0; s_2 = \xi_1\,\xi_2 + \xi_2\,\xi_3 + \xi_1\,\xi_3 = p$ i $s_3 = \xi_1\,\xi_2\,\xi_3 = -q$. $(*)$

Segona etapa. Tenim que $v_1 = \xi_1 - \xi_2$. Per tant, $v_1^2 = \xi_1^2 + \xi_2^2 + 2\,\xi_1\,\xi_2 \underset{(*)}{=} \xi_1^2 + \xi_2^2 - 2\,\frac{q}{\xi_3}$. D'on: $\xi_1^2 + \xi_2^2 = v_1^2 + 2\,\frac{q}{\xi_3}$. D'altra banda,

$$0 \underset{(*)}{=} \big(\xi_1 + \xi_2 + \xi_3\big)^2 = \xi_1^2 + \xi_2^2 + \xi_3^2 + 2\,\xi_1\,\xi_2 + 2\,\xi_2\,\xi_3 + 2\,\xi_1\,\xi_3 \underset{(*)}{=} \xi_1^2 + \xi_2^2 + \xi_3^2 + 2\,p.$$

O sigui, $\xi_1^2 + \xi_2^2 = v_1^2 + 2\,\frac{q}{\xi_3} = -\xi_3^2 - 2\,p$. En resulta, atès que ξ_3 és una arrel de $f(X) = 0$, que

$$\xi_3^3 + 2\,p\,\xi_3 + 2\,q + \xi_3\,v_1^2 = p\,\xi_3 + q + \xi_3\,v_1^2 = 0.$$

Per tant,

$$\xi_3 = -\frac{-q}{p + v_1^2}.$$

Finalment, del fet que $\xi_1 - \xi_2 = v_1$ i $\xi_1 + \xi_2 = -\xi_3$ se'n dedueixen els valors de ξ_1 i ξ_2 en funció racional de v_1. Són

$$\xi_1 = \frac{v_1^3 + p\,v_1 - 3\,q}{2\,(v_1^2 + p)} \text{ i } \xi_1 = -\frac{v_1^3 + p\,v_1 + 3\,q}{2\,(v_1^2 + p)}.$$

Tercera etapa.

- Si $G(V)$ és irreductible, aleshores el grup de Galois és $\mathcal{G} = \mathfrak{S}_3$.

[27] Altrament, una arrels seria necessàriament, la semisuma de les altres dues. O sigui, $\xi_1 + \xi_2 + \xi_3 = 0$ i $2\,\xi_1 = \xi_2 + \xi_3$. Per tant, $\xi_1 = 0$ i $f(X)$ seria reductible.

- Si $G(V)$ factoritza a $\mathbb{Q}$ en la forma

$$\left(V^3+3p\,V+\sqrt{-27\,q^2-4\,p^3}\right)\left(V^3+3p\,V-\sqrt{-27\,q^2-4\,p^3}\right),$$

i aleshores $\sqrt{-27\,q^2-4\,p^3}\in\mathbb{Q}$,

Fixem-nos que una funció invariant pel grup simètric $\mathcal{A}_3$ és:

$$\Delta:=\Delta(\xi_1,\xi_2,\xi_3)=(\xi_1-\xi_2)\,(\xi_2-\xi_3)\,(\xi_1-\xi_3).$$

Aquesta funció pren encara un altre valor quan la sotmetem a una substitució $\sigma\in\mathfrak{S}_3-\mathfrak{A}_3$: el valor $-\Delta$. Ara usem una arrel quadrada de la unitat diferent de $+1$ i calculem, seguint el text de Galois,

$$\big(\Delta+(-1)\Delta\big)^2=\Big(2\,(\xi_1-\xi_2)\,(\xi_2-\xi_3)\,(\xi_1-\xi_3)\Big)^2=-4\,(27\,q^2+24\,p^3).$$

Quarta etapa. Si $\sqrt{-27\,q^2-4\,p^3}\notin\mathbb{Q}$, hem d'adjuntar les arrels de l'equació auxiliar $Y^2=\pm\big(27\,q^2+24\,p^3\big)$ i, potser, la unitat imaginària i, i automàticament el grup $\mathfrak{S}_3$ reduirà al grup $\mathfrak{A}_3$, si l'equació

$$G_1(V)=V^3+3p\,V+\sqrt{-27\,q^2-4\,p^3}$$

és irreductible a $\mathbb{Q}\big(\sqrt{-27\,q^2-4\,p^3}\,\big)[Y]$.

Resolt aquest primer pas, ara podem considerar (comentari 62, p. 47)

$$\omega=\big(\xi_1+\epsilon\,\xi_2+\epsilon^2\,\xi_3\big)^3=-\frac{27}{2}q-\frac{2\sqrt{3}\,i}{2}\sqrt{-27q^2-4p^3}$$

Si adjuntem, doncs, ϵ i $\sqrt[3]{\omega}$, el grup es redueix al $\mathcal{G}_0=\{\mathrm{Id}\}$.

Aplicació a les equacions irreductibles de grau primer

PROPOSICIÓ VI

LEMA. Una equació irreductible de grau primer no pot esdevenir reductible per l'adjunció d'un radical l'índex del qual sigui diferent del propi grau de l'equació.

Doncs, si $r,r',r'',\ldots$, són els diversos valors del radical, i $Fx=0$ l'equació proposada, caldria que Fx es partís en factors

$$f(x,r)\times f(x,r')\times\cdots,$$

tots del mateix grau. I això no és possible, llevat $f(x,r)$ sigui de primer grau.

Així, una equació irreductible de grau primer no pot esdevenir reductible, llevat en el cas que el seu grup es redueixi a una única permutació. □

Comentari 72. L'adjunció d'una arrel *només* pot reduir un polinomi irreductible de grau primer si fa que factoritzi totalment —és a dir, en factors tots de primer grau. D'acord amb les PROPOSICIONS II i III (i, en el benentès que s'hagin adjuntat les p arrels de la unitat, amb p primer), $G_1(V)$ factoritza en factors del mateix grau.

Però ara, de fet, Galois estableix el teorema següent:

Teorema 72.1. Si, en un cos extensió per un radical $X^q - k = 0$, amb q primer, que, a més, contingui les arrels q-èsimes de la unitat, tot polinomi irreductible $f(X)$ es manté irreductible o factoritza completament en factors tots ells del mateix grau.

Teorema de reciprocitat de Dedekind. Siguin $f(X), g(X) \in K[X]$ irreductibles. Factoritzem $f(X) = f_1(X,\eta_1)\dots f_r(X,\eta_1)$ a $K\big(\eta_1\big)$, on $g\big(\eta_1\big) = 0$ i $g(X) = g_1(X,\xi_1)\dots g_s(X,\xi_1)$ a $K\big(\xi_1\big)$, on $f\big(\xi_1\big) = 0$. Aleshores $r = s$ i podem reordenar els factors de manera que, per a tot $k = 1,\dots,r$, $\dfrac{\text{grau}\big(f_k\big)}{\text{grau}\big(g_k\big)} =$ constant.[28]

Corol·lari 72.2. Siguin $f(X), g(X) \in K[X]$ són irreductibles de graus primers p, q. Si $f(X) = \prod_{i=1}^{s} f_i\big(X,\eta_1,\dots,\big)$ a $K\big(\eta_1,\dots,\eta_q\big)$ on $\eta_k, k = 1,\dots,q$, són les arrels de $g(X) = 0$, aleshores $p = q$ i $\text{grau}\big(f_i(X,\eta_1,\dots,)\big) = 1$.

És evident, atès que, a $K\big(\eta_1,\dots,\eta_q\big)$, $g(X) = \big(X-\eta_1\big)\cdots\big(X-\eta_q\big)$. Apliquem el teorema de reciprocitat de Dedekind. En resulta que $p = q$ i aleshores $p = p \times \text{grau}\big(f_1\big)$. □

Demostració del teorema de Dedekind. Pel corol·lari 74, p. 64, es pot afirmar que $\text{Gal}\big(f(X)g(X)/K\big(\eta_1\big)\big)$ actua transitivament sobre els factors $f_i, i = 1,\dots,r$, en que factoritza f en aquest cos $K\big(\eta_1\big)$. Per la PROPOSICIÓ IV, comentari 56, p. 45, $\text{Gal}\big(f(X)g(X)/K\big(\eta_1\big)\big)$ conté les substitucions de $\text{Gal}\big(f(X)g(X)/K\big)$ que deixen fix η_1. Cada una d'aquestes substitucions transformen arrels de f_k en arrels de f_k.

Lema 72.3. Siguin σ_1, σ_2 dues substitucions donades. Aleshores, existeix τ_1 amb $\tau_1\big(\eta_1\big) = \eta_1$ i $\big(\tau_1 \circ \sigma_1\big)\big(\xi_1\big) = \sigma_2\big(\xi_1\big)$ si, i només si, existeix τ_2 amb $\tau_2\big(\xi_1\big) = \xi_1$ i $\big(\tau_2 \circ \sigma_1^{-1}\big)\big(\eta_1\big) = \sigma_2^{-1}\big(\eta_1\big)$.

[28] Vegeu (Scharlau, 1982).

N'hi ha prou en agafar $\tau_2 = \sigma_2^{-1} \circ \tau_1 \circ \sigma_1$. $\square$

Les σ actuen transitivament sobre les $\xi_i, i = 1, \ldots, n$. Per tant, el nombre de σ que transformen ξ_1 en ξ_j és el mateix per a tot índex j. Anomenem-lo ν. Aleshores $\nu \times \mathrm{grau}\big(f(X)\big) =$ número de σ i $\nu \times \mathrm{grau}\big(f_k(X, \eta_1)\big) =$ número de σ que transformen ξ_1 en una arrel de f_k. Però, pel lema 72.3, es compleix que $\sigma\big(\xi_1\big)$ és una arrel de f_k si, i només si, $\sigma^{-1}\big(\eta_1\big)$ és una arrel de g_k. Per tant,

$$\begin{aligned}\frac{\mathrm{grau}\big(f_k\big)}{\mathrm{grau}\big(f\big)} &= \text{proporció de } \sigma \text{ que porten } \xi_1 \text{ a una arrel de } f_k \\ &= \text{proporció de } \sigma \text{ per a les quals } \sigma^{-1}\big(\eta_1\big) \text{ és una arrel de } g_k \\ &= \frac{\mathrm{grau}\big(g_k\big)}{\mathrm{grau}\big(g\big)}. \qquad \square\end{aligned}$$

PROPOSICIÓ VII

PROBLEMA. Quin és el grup d'una equació irreductible d'un grau primer n, resoluble per radicals?

D'acord amb la proposició precedent [i amb la PROPOSICIÓ II], el grup més petit possible, abans del que solament té una única permutació, en contindrà n, de permutacions. Ara bé, un grup de permutacions d'un nombre primer n de lletres no es pot reduir a n permutacions, llevat que una d'aquestes permutacions s'obtingui d'una altra per una substitució circular d'ordre n. (Vegeu la «Mémoire de M. Cauchy», *Journal de l'École Polytechnique*, XVIIe cahier. [29]) Així, el penúltim grup serà [430]

$$(G) \qquad \begin{cases} x_0, & x_1, & x_2, & x_3, & \cdots & x_{n-3}, & x_{n-2}, & x_{n-1}, \\ x_1, & x_2, & x_3, & \cdots, & x_{n-3}, & x_{n-2}, & x_{n-1}, & x_0, \\ x_2, & x_3, & \ldots\ldots & & x_{n-2}, & x_{n-1}, & x_0, & x_1, \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ x_{n-2}, & x_{n-1}, & \ldots\ldots & & \ldots & x_{n-5}, & x_{n-4}, & x_{n-3}, \\ x_{n-1}, & \ldots\ldots & & & \ldots & x_{n-4}, & x_{n-3}, & x_{n-2}, \end{cases}$$

on $x_0,\ x_1,\ x_2, \ldots,\ x_{n-1}$ són les arrels.

[29] Vegeu (Cauchy, 1815, p. 78).

És clar. Si el grup $\mathcal{S} \neq \{\mathrm{Id}\}$, conté una permutació circular d'ordre > 1. Aquest ordre ha de ser p, perquè no pot ser d'ordre inferior a p. Si ho fos tindríem una contradicció: la permutació circular d'ordre k generaria un subgrup d'ordre k del grup d'ordre p. Però aleshores, $k|p$, però $k \neq 1, k \neq p$. Contradicció!

Aleshores, el grup que el precedirà immediatement en l'ordre de les descomposicions es compondrà d'un cert nombre de grups, tots ells amb les mateixes substitucions que aquest. Per tant, s'observa que aquestes substitucions es poden expressar així (fent, en general, $x_n = x_0$, $x_{n+1} = x_1, \ldots$, és clar que cada una de les substitucions del grup (G) s'obté collocant arreu en el lloc de x_k, x_{k+c}, on c és una constant).

Considerem un qualsevol dels grups semblants al grup (G). D'acord amb el teorema II, l'haurem d'obtenir operant arreu en aquest grup una mateixa substitució; per exemple, posant arreu en el grup (G), en lloc d'x_k, $x_{f(k)}$, essent f una certa funció.

Les substitucions d'aquests nous grups havent d'ésser les mateixes que les del grup (G), tindrem

$$f(k+c) = f(k) + C,$$

on C és independent de k.

D'on:

$$\begin{aligned} f(k+2c) &= f(k) + 2C, \\ &\cdots\cdots\cdots\cdots\cdots\cdots \\ f(k+mc) &= f(k) + mC. \end{aligned}$$

Si $c = 1$, $k = 0$, tindrem

$$f(m) = am + b,$$

o bé

$$f(k) = ak + b,$$

on a i b són constants.

D'on, el grup que precedeix immediatement el grup (G) només haurà
[431] de contenir substitucions com ara

$$x_k, \quad x_{ak+b},$$

i no contindrà, per consegüent, cap altre substitució circular que la del grup (G).

Hom raonarà sobre aquest grup com sobre el precedent, i s'obtindrà que el primer grup en l'ordre de les descomposicions, és a dir el grup actual de l'equació, només pot contenir substitucions de la forma

$$x_k, \quad x_{ak+b}.$$

D'on, «si una equació irreductible de grau primer és resoluble per radicals, el seu grup solament contindrà substitucions de la forma

$$x_k, \quad x_{ak+b},$$

on a i b són constants».

Recíprocament, si té lloc aquesta condició, afirmo que l'equació serà resoluble per radicals. Considerem, en efecte, les funcions

$$\begin{aligned}(x_0 + \alpha\, x_1 + \alpha^2\, x_2 + \cdots + \alpha^{n-1}\, x_{n-1})^n &= X_1,\\ (x_0 + \alpha\, x_a + \alpha^2\, x_{2\,a} + \cdots + \alpha^{n-1}\, x_{(n-1)\,a})^n &= X_a,\\ (x_0 + \alpha\, x_{a^2} + \alpha^2\, x_{2\,a^2} + \cdots + \alpha^{n-1}\, x_{(n-1)\,a^2})^n &= X_{a^2},\\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\end{aligned}$$

on α és una arrel n-èsima de la unitat i a una arrel primitiva de n.

És clar que tota funció invariant per les substitucions circulars de les quantitats $X_1, X_a, X_{a^2}, \ldots$, serà, en aquest cas, immediatament conegut. D'on, hom podrà trobar $X_1, X_a, X_{a^2}, \ldots$, pel mètode de *monsieur* Gauss per a les equacions binòmiques. D'on, etc.

Així, per tal que una equació irreductible de grau primer sigui resoluble per radicals, és *necessari i suficient* que tota funció invariable per les substitucions

$$x_k, \quad x_{ak+b}$$

sigui racionalment coneguda.

Així, la funció [432]

$$(X_1 - X)(X_a - X)(X_{a^2} - X)\cdots$$

haurà de ser coneguda, sigui qui sigui X.

És, doncs, *necessari i suficient* que l'equació que dóna aquesta funció de les arrels admeti, qualsevol que sigui X, un valor racional.

Si l'equació proposada té tots els coeficients racionals, l'equació auxiliar que dóna aquesta funció també els hi tindrà, i n'hi haurà prou a reconèixer si aquesta equació auxiliar de grau $1 \times 2 \times 3 \times \cdots \times (n-2)$ té o no una arrel racional, quelcom que hom sap fer. □

És el mitjà que cladrà emprar a la pràctica. Però aquest mateix teorema el presentem d'una altra manera.

Comentari 73. Teorema de Galois. Si una equació irreductible té grau primer p i és resoluble per radicals, aleshores les arrels $\xi_1, \ldots, \xi_p$ poden ser reordenades de manera que les substitucions $\sigma \in \mathrm{Gal}\big(f(X), K_0\big)$ siguin de la forma $\sigma(\xi_i) = \xi_{a\,i+b}$, on ξ_i està definit per a tots els enters i per als quals $\xi_i = \xi_j$ quan $i \equiv j \pmod{p}$, on a i b són dos enters i $a \not\equiv 0 \pmod{p}$. I, recíprocament.

En efecte. El recíproc és evident en virtut de la Proposició v i usant alguns resultats elementals de l'aritmètica de $\mathbb{Z}_p$ —anell dels enters mòdul p.

Sigui a una arrel primitiva de la unitat mòdul p i considerem les substitucions de la forma $\begin{pmatrix} \xi_1 & \xi_2 & \xi_3 & \cdots & \xi_{p-1} \\ \xi_{a^k} & \xi_{2\,a^k} & \xi_{3\,a^k} & \cdots & \xi_{(p-1)\,a^k} \end{pmatrix}$, $k = 0, 1, \ldots, p-1$. Totes elles són substitucions de la forma $\xi_k \to \xi_{\lambda\,k}$.

Considerem ara les funcions

$$X_{a^k} = \big(\xi_0 + \epsilon\,\xi_{a^k} + \epsilon^2\,\xi_{2\,a^k} + \cdots + \epsilon^{p-1}\,\xi_{(p-1)\,a^k}\big)^p,\ \ k = 0, 1, \ldots, p-1.$$

L'equació $g(X) = (X - X_1)\big(X - X_a\big)\big(X - X_{a^2}\big)\cdots = 0$ té els coeficients racionals. Sigui $\varphi\big(X_1, X_a, X_{a^2}, \ldots\big)$ un quantitat racional. Per la definició de les $X_{a^k}, k = 0, 1, \ldots, p-1$, $\varphi\big(X_1, X_a, X_{a^2}, \ldots\big)$ és invariant per una substitució de les arrels $\xi_i, i = 1, \ldots, n$ si, i només si, és de la forma $\xi_k \mapsto \xi_{\lambda\,k+\mu}$, la qual indueix la substitució $X_k \mapsto X_{\lambda\,k}$. En resulta que el grup de l'equació $g(X) = 0$ està format pel grup de les substitucions generades per la substitució circular $\big(X_1 \quad X_a \quad X_{a^2} \ \cdots\big)$. El grup de $g(X) = 0$ és, doncs, el mateix que el de $\frac{X^p-1}{X-1} = 0$. Per tant, serà resoluble per radicals. I l'adjunció de $X_1,\ X_a,\ X_{a^2}, \ldots,$ permet d'expressar per radicals les arrels $\xi_1,\ \xi_2, \ldots,\ \xi_n$ amb el mètode explicitat en el comentari 62, p. 47.

Cal veure, doncs, l'afirmació directa. I Galois ho fa retrocedint del grup $\{\mathrm{Id}\}$ al grup $\mathrm{Gal}\big(f(X), K_0\big)$.

El grup anterior al darrer, $\mathcal{G}_0 = \{\mathrm{Id}\}$, és un grup cíclic d'ordre p i el podem posar en la forma

$$\begin{array}{ccccc} \xi_1 & \xi_2 & \cdots & \xi_{p-1} & \xi_p \\ \xi_2 & \xi_3 & \cdots & \xi_p & \xi_1 \\ \xi_3 & \xi_4 & \cdots & \xi_1 & \xi_2 \\ \multicolumn{5}{c}{\cdots\cdots\cdots\cdots\cdots\cdots} \\ \xi_p & \xi_1 & \cdots & \xi_{p-2} & \xi_{p-1}. \end{array}$$

Si σ és una substitució de les arrels que ocorren en el subgrup *precedent* i s representa una permutació dels enters mòd p donada per $\sigma\big(\xi_i\big) = \xi_{s(i)}$, l'aplicació de s dóna el grup

$$\begin{array}{ccccc} \xi_{s(1)} & \xi_{s(2)} & \cdots & \xi_{s(p-1)} & \xi_{s(p)} \\ \xi_{s(2)} & \xi_{s(2)} & \cdots & \xi_{s(p)} & \xi_{s(1)} \\ \xi_{s(3)} & \xi_{s(4)} & \cdots & \xi_{s(1)} & \xi_{s(2)} \\ \multicolumn{5}{c}{\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots} \\ \xi_{s(p)} & \xi_{s(1)} & \cdots & \xi_{s(p-2)} & \xi_{s(p-1)}, \end{array}$$

que és el mateix grup d'abans. En resulta que la substitució que canvia la primera fila per la segona ha de canviar la primera fila de la primera presentació del grup per una altre de les files d'aquesta mateixa presentació. Existeix,

doncs, un $a \not\equiv 0 \pmod p$ tal que $\xi_{s(2)} = \xi_{s(1)+a}$, $\xi_{s(3)} = \xi_{s(2)+a}, \ldots$, $\xi_{s(p)} = \xi_{s(p-1)+a}$, on els subíndexos s'han d'interpretar mòd p. Així:

$$\begin{aligned}
&s(2) \equiv s(1) + a, \\
&s(3) \equiv s(2) + a && \equiv s(1) + 2\,a, \\
&s(4) \equiv s(3) + a && \equiv s(1) + 3\,a, \\
&\quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
&s(j) \equiv s(1) + (j-1)\,a && \equiv r\,a + b, \\
&\quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots
\end{aligned}$$

on $b = s(1) - a$.

En resulta que el grup precedent solament conté substitucions de la forma prescrita.

Considerem ara el grup que el precedeix. Per la mateixa raó d'abans, si τ és una substitució d'aquest grup, aleshores la substitució que transforma la permutació $\xi_{t(1)}\xi_{t(2)}\cdots\xi_{t(p-1)}\xi_{t(p)}$ en $\xi_{t(2)}\xi_{t(3)}\cdots\xi_{t(p)}\xi_{t(1)}$ ha de ser de la forma anterior; han d'existir α, β de manera que

$$\begin{aligned}
&t(2) \equiv \alpha\,t(1) + \beta, \\
&t(3) \equiv \alpha\,t(2) + \beta \equiv \alpha^2\,t(1) + \alpha\,\beta + \beta, \\
&t(4) \equiv \alpha\,t(3) + \beta \equiv \alpha^3\,t(1) + \alpha^2\,\beta + \alpha\,\beta + \beta, \\
&\quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
&t(j) \equiv \alpha^{j-1}\,t(1) + \left(\alpha^{j-2} + \alpha^{j-3} + \cdots + \alpha + 1\right)\beta, \\
&\quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots
\end{aligned}$$

Per tant,

$$t(1) \equiv t(p+1) \equiv \alpha^p\,t(1) + \left(\alpha^{p-1} + \alpha^{p-2} + \cdots + \alpha + 1\right)\beta$$

i, pel teorema petit de Fermat, $\alpha^p \equiv \alpha$, en resulta que $(1-\alpha)\,t(1) \equiv \left(\alpha^{p-1} + \alpha^{p-2} + \cdots + \alpha + 1\right)\beta$. Si ara ho multipliquem per $1-\alpha$ obtenim $(1-\alpha)^2\,t(1) \equiv \left(1-\alpha^p\right)\beta \equiv (1-\alpha)\,\beta$. Si $\alpha \not\equiv 1$, $t(1) \equiv (1-\alpha)^{-1}\,\beta$. Si procedim de forma anàloga, tenim que, mòd p,

$$t(2) \equiv t(p+2) \equiv \alpha^p\,t(2) + \left(\alpha^{p-1} + \alpha^{p-2} + \cdots + \alpha + 1\right)\beta,$$

que porta a $t(2) \equiv (1-\alpha)^{-1}\,\beta \equiv t(1) \pmod p$. Però això és impossible. Per tant, $\alpha \equiv 1 \pmod p$. En resulta doncs que, mòd p,

$$t(2) \equiv t(1) + \beta, \quad t(3) \equiv t(2) + \beta, \quad t(4) \equiv t(3) + \beta, \quad \text{etc.}$$

I, com hem vist abans, implica l'existència d'$a', b', a' \not\equiv 1 \pmod p$ de manera que $t(j) = a'\, j + b'$.

De la mateixa manera, iterant enrere, arribem al grup Gal $\big(f(X)/K\big)$ i en resulta que les substitucions que conté són d'aquesta forma.

Corol·lari 73.1. La quíntica general no és resoluble per radicals.

En efecte. Si ho fos, el grup de Galois tindria solament les substitucions de la forma $\sigma(\xi_i) = a\, i + b$, on a només pot prendre quatre valors i b, cinc. Per tant, com a màxim, tindria 20 elements.

$\xi_1\,\xi_2\,\xi_3\,\xi_4\,\xi_5$	$\xi_1\,\xi_3\,\xi_5\,\xi_2\,\xi_4$	$\xi_1\,\xi_5\,\xi_4\,\xi_3\,\xi_2$	$\xi_1\,\xi_4\,\xi_2\,\xi_5\,\xi_3$
$\xi_2\,\xi_3\,\xi_4\,\xi_5\,\xi_1$	$\xi_3\,\xi_5\,\xi_2\,\xi_4\,\xi_1$	$\xi_5\,\xi_4\,\xi_3\,\xi_2\,\xi_1$	$\xi_4\,\xi_5\,\xi_1\,\xi_2\,\xi_3$
$\xi_3\,\xi_4\,\xi_5\,\xi_1\,\xi_2$	$\xi_5\,\xi_2\,\xi_4\,\xi_1\,\xi_3$	$\xi_4\,\xi_3\,\xi_2\,\xi_1\,\xi_5$	$\xi_2\,\xi_5\,\xi_3\,\xi_1\,\xi_4$
$\xi_4\,\xi_5\,\xi_1\,\xi_2\,\xi_3$	$\xi_2\,\xi_4\,\xi_1\,\xi_3\,\xi_5$	$\xi_3\,\xi_2\,\xi_1\,\xi_5\,\xi_4$	$\xi_5\,\xi_3\,\xi_1\,\xi_4\,\xi_2$
$\xi_5\,\xi_1\,\xi_2\,\xi_3\,\xi_4$	$\xi_4\,\xi_1\,\xi_3\,\xi_5\,\xi_2$	$\xi_2\,\xi_1\,\xi_5\,\xi_4\,\xi_3$	$\xi_3\,\xi_1\,\xi_4\,\xi_2\,\xi_5$

Però, com hem vist en el comentari 37, p. 29, n'ha de tenir 120. Per tant, no és resoluble per radicals.

I Galois és conscient de la importància del resultat i per això en la taula final, p. 64, dóna les vint substitucions possibles. Edwards diu (Edwards, 2012, p. 922): «No hem necessitat la simplicitat del grup alternat $\mathfrak{A}_5$, tan sovint invocada en les demostracions dels llibres de text».

PROPOSICIÓ VIII

TEOREMA. Per tal que una equació irreductible de grau primer sigui resoluble per radicals, *és necessari i suficient* que dos qualssevol de les arrels siguin conegudes, i les altres s'en dedueixin racionalment.

Primerament, cal perquè la substitució

$$x_k, \quad x_{a\,k+b}$$

no deixa mai dues lletres al mateix lloc i aleshores, per la proposició IV, és clar que adjuntant dues arrels a l'equació el seu grup s'haurà de reduir a una única permutació.

En segon lloc, és suficient perquè, en aquest cas, cap substitució del grup no deixa dues lletres als mateixos llocs. Per consegüent, el grup contindrà com a màxim $n(n-1)$ permutacions. D'on en resulta que només contindrà una única substitució circular (altrament en contindria almenys n^2, de permutacions). Així doncs, tota substitució del grup, $x_k, \;\; x_{fk}$, haurà de satisfer la condició

$$f(k+c) = f(k) + C.$$

D'on, etc.

El teorema queda així demostrat. □

Comentari 74. Malgrat la simplicitat de la demostració, el resultat és força original i Galois el posa de relleu a la introducció de la Memòria.

Demostració de la PROPOSICIÓ VIII. La condició és necessària. Si $f(X)=0$, de grau primer p, és resoluble per radicals a K amb més raó ho serà a $K' := K(\xi_1, \xi_2)$. Veiem ara que $\mathrm{Gal}\big(f(X)/K'\big) = \big\{\mathrm{Id}\big\}$. Per la PROPOSICIÓ I —Galois fa referència a la PROPOSICIÓ IV— $\mathrm{Gal}\big(f(X)/K'\big)$ conté solament substitucions que deixen fixes les arrels ξ_1 i ξ_2. Però, com hem vist a la proposició anterior, la substitució és de la forma $\xi_k \to \xi_{a\,k+b}$ que no deixa fix cap arrel. Per tant, $\mathrm{Gal}\big(f(X)/K'\big) = \big\{\mathrm{Id}\big\}$. En resulta aleshores que totes les arrels $\xi_i,\ i=1,2,\ldots,\ p$, resten fixes. Per tant, $\xi_i \in K\big(\xi_1,\xi_2\big), i=1,\ldots,p$. I la condició és necessària.

La condició és suficient. Necessitem un lema:

Lema 74.1. Tota equació irreductible $f(X)=0$ té un grup *transitiu* —és a dir, cada arrel pot ser duta a qualsevol lloc— i recíprocament.

En efecte. Suposem que el grup de Galois $\mathcal{G}$ de $f(X)=0$ no fos transitiu. Sigui ξ_1 una arrel arbitrària i suposem que es transformada solament en $\xi_1,\ldots,\xi_m$, amb $m<n$, quan la sotmetem a les substitucions $\tau \in \mathcal{G}$. Aleshores aquestes arrels es transformen les unes amb les altres per les substitucions de $\mathcal{G}$. En efecte. Si τ_1 mou ξ_1 a ξ_m i τ_2 mou ξ_m anviant-la a ξ_κ, aleshores $\tau_2 \circ \tau_1$ envia ξ_1 a ξ_κ. Per tant, ξ_κ és una de les arrels $\xi_j, j=1,\ldots,m$. En resulta que les substitucions $\tau \in \mathcal{G}$ no alteren les funcions simètriques de $\xi_1,\ldots,\xi_m$. Per tant, $g(X) := (X-\xi_1)\ldots(X-\xi_m) \in K[X]$ divideix $f(X) \in K[X]$. Impossible.

Recíprocament. Si $\mathcal{G}$ és transitiu, $f(X)$ no pot admetre cap divisor de la forma $g(X) := (X-\xi_1)\ldots(X-\xi_m)$. El grup $\mathcal{G}$ contindrà, doncs, una substitució τ per la qual ξ_1 en ξ_{m+1}, on $\xi_{m+1} \neq \xi_j, j=1,\ldots,m$. Per tant, $g(X)$ no és invariant per les substitucions de $\mathcal{G}$ i, en conseqüència, per la PROPOSICIÓ I, és irracional, o sigui $g(X) \notin K[X]$. □.

Suposem que totes les arrels són funció racional de les arrels $\xi_1,\ \xi_2$. Les substitucions han d'intercanviar els llocs de ξ_1 i ξ_2. En total, com a molt, n'hi haurà $p(p-1)$. D'altra banda, atès que $\mathcal{G}$ és transitiu, té ordre divisible per p —conté les substitucions que envien ξ_1 a la resta de les arrels $\xi_i, i=1,\ldots,p$. Conté, doncs, una substitució circular σ d'ordre p, però no més: si en tingués dues, l'ordre seria $\geq p^2$. Suposem ara que τ és una substitució de $\mathcal{G}$ d'ordre p. No pot ser que les substitucions $\sigma^r\,\tau^s$ siguin totes diferents. D'on: per a certs r,s,r',s', $\sigma^{r'}\,\tau^{s'} = \sigma^r\,\tau^s$. En definitiva, τ és una potència de σ —és a dir, pertany al subgrup $\mathcal{S}$ engendrat per σ. Si τ és la substitució que

$\tau\big(\xi_k\big) = \xi_{t(k)}$, aleshores $\tau \circ \sigma \circ \tau^{-1}$ ha de ser un potència de σ. És a dir, $\tau\big(\xi_k\big) = \xi_{k+a}$. Si $\sigma = \big(\xi_1 \quad \xi_2 \quad \cdots \quad \xi_n\big)$, tindrem que $\tau \circ \sigma \circ \tau^{-1}$ serà de la forma $\xi_{t(k)} \to \xi_{t(k+1)}$. En resulta, com hem vist en el comentari. 73, p. 59, que $t(k+1) = t(k) + a$. Se'n dedueix que $t(k) = a\,k + b$.

Corol·lari 74.2. $\mathrm{Gal}\big(f(X)/K\big)$ actua transitivament en un factor $f_1(X)$ de $f(X)$ si, i només si, $f_1(X)$ és irreductible.

Comentari 75. Aquest resultat, com recorda (Edwards, 2012, p 923), fou el que «induí Lacroix i Poisson a rebutjar la memòria. Desitjaven, com és natural, un criteri de resolubilitat que pogués ser aplicat a un polinomi donat arbitari». Tanmateix, aquest resultat evita haver de recórrer a les teories de cossos i de grups. Edwards opina que el que atreia Galois era que, de la resolubilitat, se'n conferís el lligam de les arrels que el resultat expressa.

Exemple del teorema VII

[433]

Sigui $n = 5$; el grup serà el següent :

$abcde$	$acebd$	$aedcb$	$adbec$
$bcdea$	$cebda$	$edcba$	$deabc$
$cdeab$	$ebdac$	$dcbae$	$becad$
$deabc$	$bdace$	$cbaed$	$ecadb$
$eabcd$	$daceb$	$baedc$	$cadbe$

Referències

Abel, N. H. (1829). Mémoire sur une classe particulière d'équations résolubles algèbriquement. *Journal de Crelle*, 26: p. 131–156.

Cauchy, A.-L. (1815). «Mémoire sur le nombre des valeurs qu'une fonction peut acquérir lorsqu'on y permute de toutes les manières possibles les quantités quelle renferme». *Journal de l'École Polytechnique*, 10, llibreta XVII:p. 1–28. Llegit l'any 1812, recopilat a (Cauchy, 1882, serie2, volum 1, p. 64-90).

Cauchy, A.-L. (1882). *Œuvres complètes* 1882-1974. Gauthier-Villars, París. Vegeu
https://archive.org/search.php?query=Cauchy AND collection:americana,
o
http://gallica.bnf.fr/Search?ArianeWireIndex= index &p=1 & lang=FR & q=Cauchy &x=0 &y=0.

Connes, A. (2005). «La penseé d'Évariste Galois et le formalisme moderne». Conferència d'Alain Connes, 8 juny a la «Banque Nationnel Français» dins del cicle de conferències *Un texte un mathÈmaticien* de l'associació «Animath».

Dehn, E. (1960). *Algebraic Equations. An Introduction to the Theories of Lagrange and Galois*. Dover Phoenix Editions, Nova York. Reditat l'any 2004. ISBN 0-486-43900-3.

Edwards, C. H. J. (1984). *Galois theory*. Springer-Verlag, Nova York.

Edwards, H. M. (2012). «Galois for 21st-Century Readers». *Notices of the American Mathematical Society*, 59:912–923.

Galois, E. (1831). «Mémoire sur les conditions de résolubilité des équations par radicaux». *Journal de Mathématiques Pures et Appliées*, •: p. 417–433. Vegeu (Malet, 1984, p. 21-38).

Galois, E. (1897). *Œuvres Mathématiques d'Évariste Galois publiées sous l'auspice de la Société mathématique de France*. Gauthier-Villars, París.

Hilbert, D. (1909). «Beweis für die Darstellbarkeit der ganzen Zahlen durch eine feste Anzahl n-ter Potenzen (Waringsches Problem)». *Matematische Annalen*, 67: p. 281–310.

Jordan, C. (1869). «Commentaire sur Galois». *Matematische Annalen*, 1: p. 141–160.

Kronecker, L. (1865). *Werke*. Teubner, Leipzig. Publicat en cinc volums. Reeditat per Chelsea Publishing Company. Nova York, 1968.

Kronecker, L. (1884). «Näherungsweise ganzzahlige Auflösung linearer Gleichungen». *Gelesen in der Akademie der Wissenschaften*, 11: p. 1179–1193, 1271–1299. Vegeu (Kronecker, 1865, p. 47-109).

Lagrange, J. L. (1770-1771). «Réflexions sur la résolution algébrique des équations». *Nouveaux Mémoire de l'Acadèmie des Sciences et des Belles-Lettres de Berlín*, 1 i 2: p. 134–215 (1770); 138–253 (1771). A (Lagrange, 1867, p. 205-421).

Lagrange, J. L. d. (1867). *Œuvres de Lagrange*. Gauthier-Villars, París. Publicat per M. J.-A. Serret i M. Gaston Darboux, entre els anys 1867 i 1892.

Malet, A. (1984). *L'obra d'Évariste Galois*. Publicacions de l'IEC, Barcelona.

Marachia, S. (2002). *Storia dell'algebra*. Liguori Editore, Napoli. ISBN 88-207-3603-9.

Neumann, P. M. (2011). *The Mathematicals Writings of Évariste Galois*. European Mathematical Society, Zürich.

Rey Pastor, J. ((1915)). *Resumen de las Lecciones de Análisis Matemático*. Universidad de Oviedo, Oviedo. Reeditat amb el títol *Lecciones de álgebra*. A. Medina, edicions segona i tercera, i C. Bermejo, edició quarta. Madrid, 1947.

Rosso, R. (2012). *Corso di Storia della algebra*. http://www-dimat.unipv.it/~rosso/didattica.html.

Scharlau, W. (1982). «Uveröffentlichte algebraische Arbeiten Richard Dedekind aus seiner Göttinger Zeit 1855-1858». *Archive for History of Exact Sciences*, 27: p. 335–367.

Stillwell, J. (1994). *Elements of Algebra*. Springer-Verlag, Berlín.

Tannery, P. (1908). *Manuscrits d'Évariste Galois*. Gauthier-Villars, París.

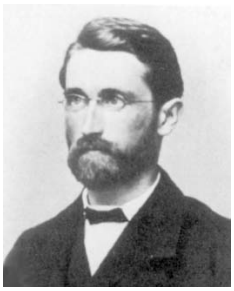
Teixidor, J. and Vaquer, J. (1968). *Curso de matemáticas*. Universitat de Barcelona, Barcelona.

Tignol, J.-P. (2001). *Galois theory of algebraic equations*. World Scientific, Singapur. ISBN 978-9810245412.

Waring, E. (1770). *Meditationes algebraicae*. Archdeacon, Cambridge. Vegeu http://books.google.es/books/about/Meditationes_Algebraicae.html?id=1MNbAAAAQAAJ&redir_esc=y.
Pel que fa al teorema de les funcions simètriques, vegeu http://archive.numdam.org/ARCHIVE/NAM/NAM_1849_1_8_/NAM_1849_1_8__76_0/NAM_1849_1_8__76_0.pdf.

Índex de Noms

Cramer, Gabriel
[Geneva, Suïssa, 1704 –
Bagnols-sur-Cèze, França, 1752],
18, 49



Dedekind, Richard
[Braunschweig, ducat de Brunswick, Alemanya, 6 d'octubre de 1831 –
Braunschweig, ducat de Brunswick, Alemanya, 12 de febrer de 1916],
56

Descartes, René
[La Haye, Turena francesa, França, 1596 –
Stockholm, Suècia, 1650],
52

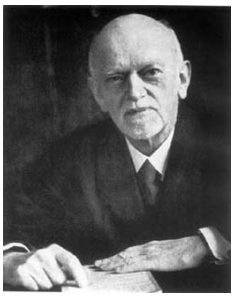
Euclides
[?, ∼365 aC-Alexandria –
∼275 aC],
10

Euler, Leonhard
[Basel, Suïssa, 1707 –
Saint Petersburg, Imperi Rus, 1783],
52

Fermat, Pierre
[Beaumont-de-Lomagne, França, 17 d'agost de 1601 – Castres, França, 12 de gener de 1665],
61

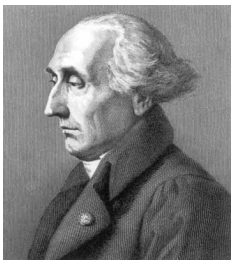
Galois, Evariste
[Bourg-la-Reine, França, 25 d'octubre de 1811 – Paris, França, 31 de maig de 1832],
2–16, 21–27, 30, 32, 36, 38, 43–45, 47, 52, 53, 57, 59, 62

Gauss, Carl Friedrich
[Braunschweig, Alemanya, 30 d'abril de 1777 – Göttingen, Alemanya, 23 de febrer de 1855],
6, 12



Hilbert, David
[Königsberg, Prússia Oriental, avui Kaliningrad, Rússia, 23 de gener de 1862 – Göttingen, Alemanya, 14 de febrer de 1943],
12

Jordan, Camille
[Lyon, França, 5 de gener de 1838 – Paris, França, 22 de gener de 1922],
10



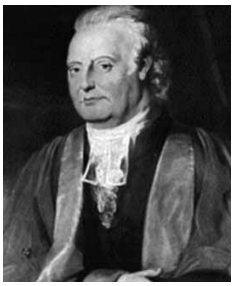
Lagrange, Joseph-Louis
[Torino, Itàlia, 25 de gener de 1736 –
Paris, França, 10 d'abril de 1813],
7, 12, 17, 20, 25, 28, 47, 49, 51

Liouville, Joseph
[Saint Omer, França, 24 de març de 1809 –
Paris, França, 8 de setembre de 1882],
2, 38, 39

Ruffini, Paolo
[Valentano, Itàlia, 22 de setembre de 1765 –
Modena, Itàlia, 10 de maig de 1822],
7, 10, 15

Vandermonde, Alexandre-Théophile
[Paris, França, 28 de febrer de 1735 –
Paris, França, 1 de gener de 1796],
52

Viète, François
[Fontenay-le-Comte, Vendée, França, 1540 –
Paris, França, 23 de febrer de 1603],
28



Waring, Edward
[Old Heath, Shropshire, Anglaterra, 1734 – Pontesbury, Shropshire, Anglaterra, 15 d'agost de 1798],
12

Índex de Termes

Professor emèrit de la
Universitat de Barcelona
josepplaicarrera@gmail.com

Publicat el 19 de desembre de 2016