MEMÒRIA

[417]

Sobre les condicions de resolubilitat de les equacions per radicals.[1]

Aquesta memòria[2] 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.[3] Heus ací el teorema que donem en la nostra anàlisi:

> 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] ÉMILE PICARD: Aquesta memòria, *Mémoire sur les conditions de résolubilité des équations par radicaux*,i *Des équations primitives qui sont solubles par radicaux* 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 2], 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.

[2] 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, 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.

[3] NTC: El grau de la qual és un nombre primer.

[418] PRINCIPIS

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

Definicions. Diem que una equació és reductible 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.

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.

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

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.

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*.

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.

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.

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

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.

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.

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

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.

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

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

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

LEMA II. Donada una equació arbitrària sense arrels múltiples, les arrels de la qual són $a, b, c, \dots$, 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 $A, B, C, \dots$, són nombres enters elegits convenientment.[4] □

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

En efecte, sigui

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

o bé

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

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:

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

que és simètrica en $b, c, d, \dots$. 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

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

[4] 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».

Hom jutjarà.

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

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

Siguin $V, V', V'', \dots,$ 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 $V - \varphi(a,b,c,\dots,d)$ 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 $b = f(V')$. □

PROPOSICIÓ I.

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

1. Tota funció de les arrels, invariant[6] per les substitucions del grup, és racionalment coneguda.

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

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

[5] 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.

[6] 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.

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

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

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.)

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:

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

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 $F = \psi V$, [423]
   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.

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.

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.

PROPOSICIÓ II

TEOREMA.[7] Suposem que, a una equació donada, se li adjunta l'arrel r d'una
[424] 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.

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

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

[7] 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.

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]

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.[8] □

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. □

PROPOSICIÓ V [426]

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

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.

[8] 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.

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.

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 extraccions d'arrels de
[427] grau inferior a p, conèixer-la no altera en res el grup de l'equació.

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).

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.

Adjuntem a l'equació el radical en qüestió; aleshores podrem raonar sobre el [428]
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. □

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

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:

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

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:

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

Aquest grup es descomposa, novament, en dos grups:

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

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

$$\begin{array}{l} abcd; \\ badc; \end{array}$$

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

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.

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 $r, r', r'', \dots,$ 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. □

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.) Així, el penúltim grup serà

[430]

$$(G) \qquad \left\{ \begin{array}{llllllll} x_0, & x_1, & x_2, & x_3, & \cdots & x_{n-3}, & x_{n-2}, & x_{n-1}, \\ x_1, & x_2, & x_3, & \cdots, & x_{n-3}, & x_{n-2}, & x_{n-1}, & x_0, \\ x_2, & x_3, & \multicolumn{2}{c}{\dots\dots\dots} & x_{n-2}, & x_{n-1}, & x_0, & x_1, \\ \multicolumn{8}{c}{\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots} \\ x_{n-2}, & x_{n-1}, & \multicolumn{3}{c}{\dots\dots\dots\dots\dots} & x_{n-5}, & x_{n-4}, & x_{n-3}, \\ x_{n-1}, & \multicolumn{4}{c}{\dots\dots\dots\dots\dots\dots\dots} & x_{n-4}, & x_{n-3}, & x_{n-2}, \end{array} \right.$$

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

Aleshores, el grup que el precedirà immediatament 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, $x_n = x_0,\ x_{n+1} = x_1, \dots,$ és clar que cada una de les substitucions del grup (G) s'obté col·locant 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 de contenir substitucions com ara [431]

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

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

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

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 $1\times2\times3\times\cdots\times(n-2)$ 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.

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, $x_k, \quad x_{fk}$, haurà de satisfer la condició

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

D'on, etc.

El teorema queda així demostrat. □

Exemple del teorema VII

[433]

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

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