Nota sobre la teoria de Galois clàssica

Agustí Reventós

2018

1 El grup de Galois d'un polinomi

L'objectiu d'aquesta nota és fer un breu resum de les idees més importants del treball original de Galois. Tot el que segueix està tret del magnific llibre *Teoria de Galois de les equacions algebraiques* de J. P. Tignol. Només necessitem saber que és un polinomi, què són les seves arrels i què és un grup de permutacions, coses totes elles estudiades a l'assignatura Fonaments de les Matemàtiques de primer curs del Grau de Matemàtiques a la UAB.

Considerem, per exemple, el polinomi

$$P(x) = x^5 - x^4 - 5x^3 + 5x^2 + 6x - 6.$$

Encara que els coeficients de $P(x)$ són racionals les arrels no ho són. De fet

$$P(x) = (x-1)(x^2-2)(x^2-3)$$

de manera que en aquest cas les arrels són

$$r_1 = 1, \quad r_2 = \sqrt{2}, \quad r_3 = -\sqrt{2}, \quad r_4 = \sqrt{3}, \quad r_5 = -\sqrt{3},$$

però actuarem de moment com si no les coneguéssim.

Escrivint

$$P(x) = (x-r_1)(x-r_2)(x-r_3)(x-r_4)(x-r_5)$$

i igualant coeficients tenim les 5 relacions fonamentals següents

1) $r_1 + r_2 + r_3 + r_4 + r_5 \in \mathbb{Q}$. [coeficient de x^4 canviat de signe]
2) $r_1r_2 + r_1r_3 + r_1r_4 + r_1r_5 + r_2r_3 + r_2r_4 + r_2r_5 + r_3r_4$ $+r_3r_5 + r_4r_5 \in \mathbb{Q}$. [coeficient de x^3]
3) $r_1r_2r_3 + r_1r_2r_4 + r_1r_2r_5 + r_1r_3r_4 + r_1r_3r_5 + r_1r_4r_5 + r_2r_3r_4$ $+r_2r_3r_5 + r_2r_4r_5 + r_3r_4r_5 \in \mathbb{Q}$. [coeficient de x^2 canviat de signe]

4) $r_1r_2r_3r_4 + r_1r_2r_3r_5 + r_1r_2r_4r_5 + r_1r_3r_4r_5 + r_2r_3r_4r_5 \in \mathbb{Q}$. [coeficient de x]

5) $r_1r_2r_3r_4r_5 \in \mathbb{Q}$. [terme independent canviat de signe]

Les cinc expressions de l'esquerra són les anomenades *funcions simètriques elementals* i tenen la propietat que són invariants per qualsevol permutació de les arrels.

Això vol dir que si $f(r_1, r_2, r_3, r_4, r_5)$ és una de les cinc funcions simètriques elementals anteriors i σ és una permutació de 5 elements, és a dir, $\sigma \in S_5$, llavors

$$f(r_1, r_2, r_3, r_4, r_5) = f(r_{\sigma(1)}, r_{\sigma(2)}, r_{\sigma(3)}, r_{\sigma(4)}, r_{\sigma(5)}).$$

La pregunta fonamental de la teoria de Galois és si entre les arrels d'un polinomi donat, a part d'haver-hi aquestes relacions que acabem d'escriure, n'hi ha més. Ens referim a relacions "essencialment" diferents a les anteriors, és a dir, que no siguin sumes, productes, quocients, etc de les anteriors.

Per exemple, en. el nostre cas tenim $r_2 + r_3 = 0$, que no és invariant per cap permutació que no permuti el 2 i el 3.

Per *relacions* ens referim a fraccions racionals de les arrels en valors a $\mathbb{Q}$. És a dir, una relació serà quelcom com

$$\frac{\text{polinomi en les 5 arrels}}{\text{polinomi en les 5 arrels}} \in \mathbb{Q}$$

Per exemple,

$$\frac{r_1^2 r_3 + r_5}{r_4 r_2^3} = q \in \mathbb{Q}$$

Així, si tinguéssim un polinomi de grau 5 com l'anterior i entre les 5 arrels *no hi hagués cap més relació* que les 5 donades per les funcions simètriques elementals, llavors podríem permutar lliurament les cinc arrels i aquesta permutació no tindria cap conseqüència. Totes les permutacions estarien permeses. Això vol dir que *el grup de Galois d'aquest hipotètic polinomi seria* S_5.

Com saber, doncs, si hi ha o no més relacions entre les arrels que les donades per les funcions simètriques elementals?

El grup de Galois $Gal(P/\mathbb{Q})$ del polinomi P, sobre $\mathbb{Q}$, és el grup format per les permutacions de les arrels que podem fer de manera que quedin inalterades totes les possibles relacions entre elles. Aquesta descripció del grup de Galois, tot i que correcte, no és massa útil ja que com no coneixem aquestes relacions no el podríem pas calcular.

A l'assignatura de Teoria de Galois veureu el següent impressionant resultat que justifica la definició que acabem de donar.

Teorema 1.1 (**Proposició 1** de la memòria de Galois)**.** *Sigui $f(r_1, \ldots, r_5)$ una fracció racional (quocient de polinomis) de les arrels d'un polinomi amb coeficients racionals. Llavors*

$$f(r_1, \ldots, r_5) \in \mathbb{Q}$$

si i només si

$$f(r_1, r_2, r_3, r_4, r_5) = f(r_{\sigma(1)}, r_{\sigma(2)}, r_{\sigma(3)}, r_{\sigma(4)}, r_{\sigma(5)}).$$

per a tota $\sigma \in Gal(P/\mathbb{Q})$.

Podeu canviar el 5 per n.

2 Teorema de l'element primitiu

Una eina fonamental en la teoria de Galois, que s'utilitza fortament per demostrar el teorema anterior, és l'anomenat *element primitiu*.

L'element primitiu V és una certa combinació lineal de les arrels, hàbilment trobada (no entro en més detalls, és el **Lema 2** de la memòria de Galois[1]), de la forma doncs

$$V = a_1 r_1 + a_1 r_1 + a_1 r_1 + a_1 r_4 + a_5 r_5, \quad a_i \in \mathbb{Q}$$

i té la propietat increïble de que *tota arrel és una fracció racional de V*. És a dir,

$$r_i = \frac{\text{polinomi en } V}{\text{polinomi en } V}$$

Escriurem

$$r_i = f_i(V).$$

En el nostre exemple prenem

$$V = r_2 + r_4 = \sqrt{2} + \sqrt{3}.$$

[1]Es demostra que sempre existeix un tal V, no únic de cap manera, per un argument no constructiu, de manera que a la pràctica es busca aquest V una mica a ull.

Fent unes manipulacions no massa complicades veiem que

$$\begin{aligned} r_1 &= 1 \\ r_2 &= \frac{V^2-1}{2V} \\ r_3 &= \frac{1-V^2}{2V} \\ r_4 &= \frac{V^2+1}{2V} \\ r_5 &= -\frac{V^2+1}{2V} \end{aligned}$$

Així doncs les fraccions racionals $f_i(X)$ són

$$\begin{aligned} f_1(X) &= 1, \\ f_2(X) &= \frac{X^2-1}{2X} = -f_3(X), \\ f_4(X) &= \frac{X^2+1}{2X} = -f_5(X). \end{aligned}$$

Teorema 2.1 (**Lema 3** de la memòria de Galois)**.** *Existeix un únic polinomi mònic irreductible, amb coeficients a* $\mathbb{Q}$*, que té* V *com arrel. Es diu que és el* polinomi mínim de V*.*

En el nostre exemple es pot veure, fent una mica de càlculs, que V és arrel del polinomi

$$x^4 - 10x^2 + 1 = 0.$$

I es pot veure també fàcilment que aquest polinomi és irreductible sobre $\mathbb{Q}$ i per tant és el polinomi mínim de V.

El fet de que aquest polinomi mínim tingui grau 4 voldrà dir, com ara veurem, que el grup de Galois $Gal(P/\mathbb{Q})$ tindrà 4 elements.

Teorema 2.2 (**Lema 4** de la memòria de Galois)**.** *Siguin* $V_1 = V, V_2, \ldots, V_m$ *les arrels del polinomi mínim de* V *i siguin* $r_i = f_i(V)$ *les* n *arrels de* $P(x)$*. Llavors, per tot* $j = 1, \ldots, m$*, els elements* $f_i(V_j)$ *són, en algun ordre, les arrels* $r_1, \ldots, r_n$ *del polinomi donat* $P(x)$*.*

Ja podem escriure quines són les permutacions que formen el grup de Galois.

N'hi ha justament m, el grau del polinomi mínim de l'element primitiu. I són les següents:

Definició 2.3. *El grup de Galois és el grup format per les permutacions següents:*

$$\boxed{\sigma_j : r_i = f_i(V_1) \longrightarrow f_i(V_j), \qquad j = 1, \ldots, m.}$$

Observem que $\sigma_1 = id$.
En el nostre exemple les arrels de $x^4 - 10x^2 + 1$ són

$$\begin{aligned} V &= \sqrt{2} + \sqrt{3} \\ V_2 &= \sqrt{2} - \sqrt{3} \\ V_3 &= -\sqrt{2} + \sqrt{3} \\ V_4 &= -\sqrt{2} - \sqrt{3} \end{aligned}$$

Anem a calcular els valors $f_i(V_j)$ que necessitem per descriure les permutacions del grup de Galois. Com $\sigma_1 = id$ podem suposar $j = 2, 3, 4$, i com $f_1(V_j) = 1$ podem suposar $i = 2, 3, 4, 5$.
Amb la notació habitual per descriure les permutacions tenim

$$\sigma_2 = \begin{pmatrix} r_1 & r_2 & r_3 & r_4 & r_5 \\ f_1(V_2) & f_2(V_2) & f_3(V_2) & f_4(V_2) & f_5(V_2) \end{pmatrix}$$
$$\sigma_3 = \begin{pmatrix} r_1 & r_2 & r_3 & r_4 & r_5 \\ f_1(V_3) & f_2(V_3) & f_3(V_3) & f_4(V_3) & f_5(V_3) \end{pmatrix}$$
$$\sigma_4 = \begin{pmatrix} r_1 & r_2 & r_3 & r_4 & r_5 \\ f_1(V_4) & f_2(V_4) & f_3(V_4) & f_4(V_4) & f_5(V_4) \end{pmatrix}$$

Calculem σ_2. [Recordem que $f_2 = -f_3$ i $f_4 = -f_5$].

$$\begin{aligned} f_2(V_2) &= \frac{V_2^2 - 1}{2V_2} = \frac{(\sqrt{2} - \sqrt{3})^2 - 1}{2(\sqrt{2} - \sqrt{3})} = \frac{2 - \sqrt{2}\sqrt{3}}{\sqrt{2} - \sqrt{3}} = \sqrt{2} = r_2 \\ f_3(V_2) &= r_3 \\ f_4(V_2) &= \frac{(\sqrt{2} - \sqrt{3})^2 + 1}{2(\sqrt{2} - \sqrt{3})} = -\sqrt{3} = r_5 \\ f_5(V_2) &= r_4 \end{aligned}$$

Calculem σ_3.

$$
\begin{aligned}
f_2(V_3) &= \frac{V_3^2-1}{2V_3} = \frac{(-\sqrt{2}+\sqrt{3})^2-1}{2(-\sqrt{2}+\sqrt{3})} = \frac{2-\sqrt{2}\sqrt{3}}{-\sqrt{2}+\sqrt{3}} = -\sqrt{2} = r_3 \\
f_3(V_3) &= r_2 \\
f_4(V_3) &= \frac{(-\sqrt{2}+\sqrt{3})^2+1}{2(-\sqrt{2}+\sqrt{3})} = r_4 \\
f_5(V_3) &= r_5
\end{aligned}
$$

Calculem σ_4.

$$
\begin{aligned}
f_2(V_4) &= \frac{V_4^2-1}{2V_4} = \frac{(-\sqrt{2}-\sqrt{3})^2-1}{2(-\sqrt{2}-\sqrt{3})} = \frac{2+\sqrt{2}\sqrt{3}}{-\sqrt{2}-\sqrt{3}} = -\sqrt{2} = r_3 \\
f_3(V_4) &= r_2 \\
f_4(V_4) &= \frac{(-\sqrt{2}-\sqrt{3})^2+1}{2(-\sqrt{2}-\sqrt{3})} = r_5 \\
f_5(V_4) &= r_4
\end{aligned}
$$

Resumint,

$$
\sigma_2 = \begin{pmatrix} r_1 & r_2 & r_3 & r_4 & r_5 \\ r_1 & r_2 & r_3 & r_5 & r_4 \end{pmatrix}
$$
$$
\sigma_3 = \begin{pmatrix} r_1 & r_2 & r_3 & r_4 & r_5 \\ r_1 & r_3 & r_2 & r_4 & r_5 \end{pmatrix}
$$
$$
\sigma_4 = \begin{pmatrix} r_1 & r_2 & r_3 & r_4 & r_5 \\ r_1 & r_3 & r_2 & r_5 & r_4 \end{pmatrix}
$$

Amb la notació de cicles que s'utilitza a Fonaments tenim

$$
\begin{aligned}
\sigma_2 &= (4,5) \\
\sigma_3 &= (2,3) \\
\sigma_4 &= (2,3)(4,5)
\end{aligned}
$$

Observeu que $\{id, \sigma_2, \sigma_3, \sigma_4\}$ és un subgrup de S_5.

3 Bézout

El fet bàsic subjacent a tota la teoria de Galois és aquest resultat, propi de l'assignatura de Fonaments.

Teorema 3.1. *Siguin $P(x), S(x)$ dos polinomis amb $S(x)$ irreductible sobre $\mathbb{Q}$. Llavors si $P(x)$ té una arrel de $S(x)$ (a $\mathbb{C}$) les té totes.*

Demostració. El màxim comú divisor de $P(x)$ i $S(x)$ és 1 o $S(x)$. Si és $S(x)$ hem acabat. Si és 1 Bézout ens diu que existeixen polinomis $a(x), b(x)$ tals que

$$aP + bS = 1,$$

per tant P i S no poden tenir cap arrel en comú. □

En teoria de Galois ens cal aquest resultat per a fraccions racionals, és a dir,

Teorema 3.2. *Sigui $P(x)$ una fracció racional i sigui $S(x)$ un polinomi irreductible sobre $\mathbb{Q}$. Llavors si $P(x)$ s'anul·la sobre una arrel de $S(x)$ s'anul·la sobre totes.*

4 Relació entre permutar arrels i les arrels del polinomi mínim de l'element primitiu

Tenir una relació entre les arrels de $P(x)$ vol dir tenir una expressió racional del tipus $f(r_1, \ldots, r_n) = q \in \mathbb{Q}$.

Com $r_i = f_i(V)$ l'anterior expressió s'escriu com $g(V) = q$ on

$$g(X) = f(f_1(X), \ldots, f_n(X)).$$

Equivalentment, V és arrel de la fracció racional donada per $g(X) - q$.

Com aquesta fracció racional admet l'arrel V admet totes les arrels del polinomi mínim de V, per tant $g(V_j) = q$, $j = 1, \ldots, m$.

Les permutacions de les arrels que provenen del grup de Galois canvien $r_i = f_i(V)$ per $f_i(V_j)$.

Per tant si fem aquest tipus de permutació a $f(r_1, \ldots, r_n)$ obtindrem

$$f(f_1(V_j), f_2(V_j), \ldots, f_n(V_j)) = g(V_j)$$

valor constant igual a q. Hem fet una permutació de les arrels que ha deixat invariant la relació entre elles!

Exemple 4.1. Per exemple, en el polinomi considerat a l'inici d'aquesta nota, si ens inventem una relació racional entre les arrels, com ara

$$f(r_1, r_2, r_3, r_4, r_5) = \frac{r_2^2}{r_4^2} = \frac{f_2(V)^2}{f_4(V)} = \frac{(V^2-1)^2}{(V^2+1)^2} = \frac{2}{3}$$

podem dir que V és arrel de la fracció racional

$$\frac{(X^2-1)^2}{(X^2+1)^2}-\frac{2}{3}$$

cosa que es comprova fàcilment.

Observem que és evident que l'expressió racional r_2^2/r_4^2 que ens hem inventat és invariant per les permutacions $\sigma_2=(4,5)$, $\sigma_3=(2,3)$ i $\sigma_4=\sigma_2\circ\sigma_3$ que conformen el grup de Galois.

Però el que volem veure és que $g(V_j)$ és constant.

Com a l'expressió de $g(X)$ només apareixen quadrats ja és clar que $g(V_1)=g(V_4)$ i $g(V_2)=g(V_3)$. A més

$$g(V_4)=\frac{[(\sqrt{2}+\sqrt{3})^2-1]^2}{[(\sqrt{2}+\sqrt{3})^2+1]^2}=\frac{[(\sqrt{2}-\sqrt{3})^2-1]^2}{[(\sqrt{2}-\sqrt{3})^2+1]^2}=g(V_2).$$

5 Equació general de cinquè grau

Què volem dir quan diem "equació general" (del grau que sigui)?

Ens referim a un polinomi on els coeficients són lletres. Com que necessitem que els coeficients del polinomi estiguin en un cos considerem que

$$P(x)=x^5-s_1x^4+s_2x^3-s_3x^2+s_4x-s_5$$

és un polinomi a coeficients $F=\mathbb{C}(s_1,\ldots,s_5)$ (fraccions racionals en aquestes variables i coeficients complexos). Expressions del tipus is_2^5/s_3, etc.

5.1 Polinomi resoluble per radicals

Suposem R,F cossos amb $F\subset R$. Diem que R és una *extensió radical* de F d'altura 1 si existeix

a) un nombre primer p,

b) un element $a\in F$ que no és la potència p-èssima de cap element de F,

c) un element $u\in R$ tal que $u^p=a$

tals que

$$R=F(u).$$

L'extensió radical d'altura h es defineix ara per inducció.

Definició 5.1. *Un polinomi $P(x)$, amb coeficients en un cert cos F, es diu que és* resoluble per radicals *si hi ha una extensió radical de F, de l'altura que sigui, que conté una arrel de $P(x)$.*

Podem dir doncs que l'equació *general* de cinquè grau és resoluble per radicals si hi ha una extensió radical R de $F = \mathbb{C}(s_1, \ldots, s_5)$ que conté una arrel de $P(x)$.

5.2 Invariància per permutacions de les arrels p-èssimes

Per estudiar la resolubilitat per radicals[2] començarem amb una observació senzilla.

Siguin $u, a \in \mathbb{C}(x_1, \ldots, x_n)$ és a dir, quocients de polinomis en les variables x_i.

Per exemple,

$$u = \frac{x_1^2 x_3 + x_3^2 x_1}{5\, i\, x_2^3}, \quad a = u^p$$

on $p \in \mathbb{N}$.

És evident que si u és invariant per una certa permutació (en aquest exemple u és invariant per $\sigma = (1,3)$) llavors a també és invariant per aquesta permutació.

El que no és tan evident, i de fet és fals, és al revés. Si $a = u^p$ es pot donar el cas de ser a invariant per una certa permutació i $u = \sqrt[p]{a}$ no.

Exemple 5.2. Exemple trivial: $u = x_1 - x_2$ no és invariant per $\sigma = (1,2)$ en canvi $a = u^2$ sí que és invariant. És a dir, el fet de que un element sigui invariant no vol dir que la seva arrel p-èssima ho sigui. I anar traient arrels p-èssimes és el que haurem de fer per resoldre una equació per radicals.

Exemple 5.3. Exemple no tant trivial[3]

$$u = x_1 + \omega x_3 + \omega^2 x_2, \quad \omega^3 = 1.$$

Observem que ω és una arrel cúbica de la unitat. Les arrels de la unitat juguen un paper fonamental en la teoria de Galois.

[2]Que la quíntica general no és resoluble és d'Abel. En aquesta secció no segueixo doncs el treball de Galois. Per saber quines equacions de cinquè grau són resolubles per radicals sí que hem de seguir Galois.

[3]Aquest exemple és meu! Els experts es fotaran a riure suposo.

Clarament u no és invariant per $\sigma = (1,2,3)$. En canvi u^3 sí que ho és ja que

$$\begin{aligned} u^3 &= 3x_1x_2x_3 \\ &+ 3\omega(x_1^2x_3 + x_3^2x_2 + x_1x_2^2) \\ &+ x_1^3 + x_2^3 + x_3^3 \\ &+ 3\omega^2(x_1^2x_2 + x_1x_3^2 + x_3x_2^2) \end{aligned}$$

Tenim doncs un exemple d'un element $a \in \mathbb{C}(x_1, \ldots, x_n)$ invariant per una certa permutació i en canvi la seva arrel cúbica no.

Si ara volgués millorar aquest exemple 'meu' però que u^3 a més de ser invariant per σ fos també invariant per una altra permutació, seria molt difícil. Feina he tingut en pensar aquest exemple on intervé només una permutació. De fet tenim el següent resultat, no massa difícil de demostrar, que té com corol·lari força directe la no resolubilitat de la quíntica.

Teorema 5.4. *Siguin $u, a \in \mathbb{C}(x_1, \ldots, x_n)$ i suposem $u^p = a$, p primer i suposem $n \geq 5$.*[4] *Si a és invariant per $\sigma = (1,2,3)$ i $\tau = (3,4,5)$ llavors u (i.e. la seva arrel p-èssima) també és invariant per σ i τ.*

Demostració.[5]Recordem que u i a són quocients de polinomis en les variables x_i i la notació $\sigma(a)$ vol dir l'element de $\mathbb{C}(x_1, \ldots, x_n)$ que s'obté en permutar les x_i que apareixen a l'expressió de a segons indica σ (és a dir, $x_1 \to x_2 \to x_3 \to x_1$).

Per exemple, si $a = x_1 - x_2$ llavors $\sigma(a) = x_2 - x_3$ i $\tau(a) = a$.

Aplicant σ a la igualtat $a = u^p$ tenim

$$\sigma(a) = \sigma(u^p) = \sigma(u)^p$$

i com a és invariant per σ tenim $u^p = \sigma(u)^p$ o equivalentment

$$(\frac{\sigma(u)}{u})^p = 1,$$

és a dir, $\sigma(u)/u$ és una arrel p-èssima de la unitat. Escriurem

$$\sigma(u) = \omega_\sigma u.$$

Com $\sigma^3 = id$ (σ és un cicle d'ordre 3) tenim

$$u = \sigma^3(u) = \omega_\sigma\sigma^2(u) = \omega_\sigma^2\sigma(u) = \omega_\sigma^3 u$$

[4]Que p sigui primer no és massa important, una cosa tècnica per a la demostració.

[5]Tignol, pàgina 225.

i per tant ω_σ és una arrel cúbica de la unitat, $\omega_\sigma^3 = 1$.

El mateix argument demostra que

$$\tau(u) = \omega_\tau u, \qquad \omega_\tau^3 = 1.$$

(Tant aplicar σ com τ a u és només multiplicar!)

Com

$$\sigma \circ \tau = (1,2,3,4,5), \qquad \sigma^2 \circ \tau = (1,3,4,5,2)$$

són cicles d'ordre 5 tenim

$$(\omega_\sigma \omega_\tau)^5 = (\omega_\sigma^2 \omega_\tau)^5 = 1$$

d'on es dedueix fàcilment que

$$\omega_\sigma = \omega_\tau = 1,$$

per tant u és invariant per σ i per τ. □

No podríem tenir una situació semblant a la del teorema **??** però per a $n = 4$? El número 5 de τ no podria aparèixer però potser seria cert un resultat com el següent

Teorema 5.5 (Resultat fals)**.** *Siguin $u, a \in \mathbb{C}(x_1, \ldots, x_4)$ i suposem $u^p = a$, p primer. Si a és invariant per $\sigma = (1,2,3)$ i $\tau = (3,4)$ llavors u (i.e. la seva arrel p-èssima) també és invariant per σ i τ.*

Contraexemple. Si revisem la demostració anterior aplicada a aquest cas arribem a que ha de ser $\omega_\sigma = 1$ i $\omega_\tau = \pm 1$. Aquest canvi de signe fa que les coses no funcionin.

Sigui

$$u = \prod_{1 \le i < j \le 4} (x_i - x_j)$$

Llavors és clar que $a = u^2$ (que és el Discriminant) és invariant per σ i τ, en canvi u no és invariant per τ ja que

$$\begin{aligned} \tau(u) &= \tau\Big((x_1 - x_2)(x_1 - x_3)(x_1 - x_4)(x_2 - x_3)(x_2 - x_4)(x_3 - x_4)\Big) \\ &= (x_1 - x_2)(x_1 - x_4)(x_1 - x_3)(x_2 - x_4)(x_2 - x_3)(x_4 - x_3) \\ &= -u. \end{aligned}$$

Tenim doncs un contraexemple a l'enunciat del teorema. □

6 Abel

Diu Tignol (p.219):

> *El primer pas a la prova d'Abel (que no apareix a la prova de Ruffini) és demostrar que l'extensió radical R de $F = \mathbb{C}(s_1, \ldots, s_5)$ es pot suposar continguda a $K = \mathbb{C}(r_1, \ldots, r_5)$, on r_i són les arrels de $P(x)$.*

Observem que $F \subset K$ ja que els coeficients s_i són funcions simètriques elementals de les arrels.

L'observació de Tignol vol dir que les arrels p-èssimes que anem adjuntant a F podem suposar que són elements de K, que és el més natural per similitud a fer extensions de $\mathbb{Q}$ adjuntat elements de $\mathbb{C}$.[6]

Això dóna lloc al teorema d'Abel dels irracionals naturals (que no demostrem aquí).

Teorema 6.1 (Irracionalitats naturals)**.** *Sigui $F = \mathbb{C}(s_1, \ldots, s_5)$ i $K = \mathbb{C}(r_1, \ldots, r_5)$. Si un element $v \in K$ pertany a una extensió radical de F, existeix una extensió radical R de F, amb $v \in R$, tal que*

$$F \subset R \subset K.$$

Teorema 6.2. *Sigui R una extensió radical de $F = \mathbb{C}(s_1, \ldots, s_5)$ continguda a $K = \mathbb{C}(r_1, \ldots, r_5)$. Si $n \geq 5$ tots els elements de R són invariants per $\sigma = (1, 2, 3)$ i $\tau = (3, 4, 5)$.*

Demostració. És un corol·lari del Teorema **??**. En efecte, podem pensar que R l'hem construït adjuntant arrels p-èssimes,

$$F \subset F(\sqrt[p]{a}) \subset F(\sqrt[p]{a})(\sqrt[q]{b}) \ldots$$

fins arribar a R. En cada pas adjuntem un element u tal que u^p (algun primer) pertany al cos anterior, és dir, $a \in F$, $b \in F(\sqrt[p]{a})$, etc. Com $a \in F$ i les funcions simètriques elementals s_i (els coeficients del polnomi) són invariants per qualsevol permutació de les arrels, a és invariant per qualsevol permutació i en particular per les permutacions σ, τ del teorema **??**. Per tant, per aquest mateix teorema, $\sqrt[p]{a}$ és invariant també per σ i τ. Així tots els elements de $F(\sqrt[p]{a})$ són invariants per σ i τ i continuem el procés fina arribar a R.

Observeu que els elements de R són fraccions racionals en les arrels r_i i σ i τ se suposa que actuen sobre aquestes arrels, i.e. $\sigma(r_1) = r_2, \sigma(r_2) = r_3, \sigma(r_3) = r_1$. $\square$

[6] Si volem passar de $\mathbb{Q}$ a $\mathbb{Q}[\sqrt{2}]$ suposem ni que sigui implícitament $\mathbb{Q} \subset \mathbb{C}$ per tenir un lloc on visqui $\sqrt{2}$.

Teorema 6.3. *L'equació general de cinquè grau no és resoluble per radicals.*

Demostració. Hauríem d'especificar el cos però és suficient demostrar que no és resoluble per radicals a $F = \mathbb{C}(s_1, \ldots, s_5)$ (això implica que no és resoluble per radicals sobre cossos més petits com ara $\mathbb{Q}(s_1, \ldots, s_5)$).

Suposem, per reducció a l'absurd, que hi ha una extensió radical R de F que conté una arrel r_i del polinomi general.

Pel teorema **??**, i amb la mateixa notació, podem suposar que tenim

$$F \subset R \subset K$$

i per tant, pel teorema **??** tot els elements de R són invariants per σ i τ. Com $\sigma \circ \tau = (r_1, r_2, r_3, r_4, r_5)$ no podem tenir $r_i \in R$, per cap i, ja que r_i no és invariant per $\sigma \circ \tau$. $\square$

7 Resolubilitat i grup de Galois

Per saber quines equacions de grau ≥ 5 es poden resoldre per radicals (que la general no es pugui resoldre no vol dir que no n'hi hagi altres que sí que es poden resoldre) donem sense comentaris la **Proposició 5** de la memòria de Galois.

Teorema 7.1 (**Proposició 5** de Galois)**.** *Sigui P un polinomi sobre un cos F i suposem que les arrels, en algun cos que contingui F són totes diferents. L'equació $P(x) = 0$ és completament*[7] *resoluble per radicals sobre F si i només si el grup de Galois $Gal(P/F)$ conté una successió de subgrups*

$$Gal(P/F) = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_t = \{id\}$$

tal que, per $i = 1, \ldots, t$, G_i és un subgrup normal d'index primer de G_{i-1}.

[7] Totes les arrels són expressions radicals dels coeficients.