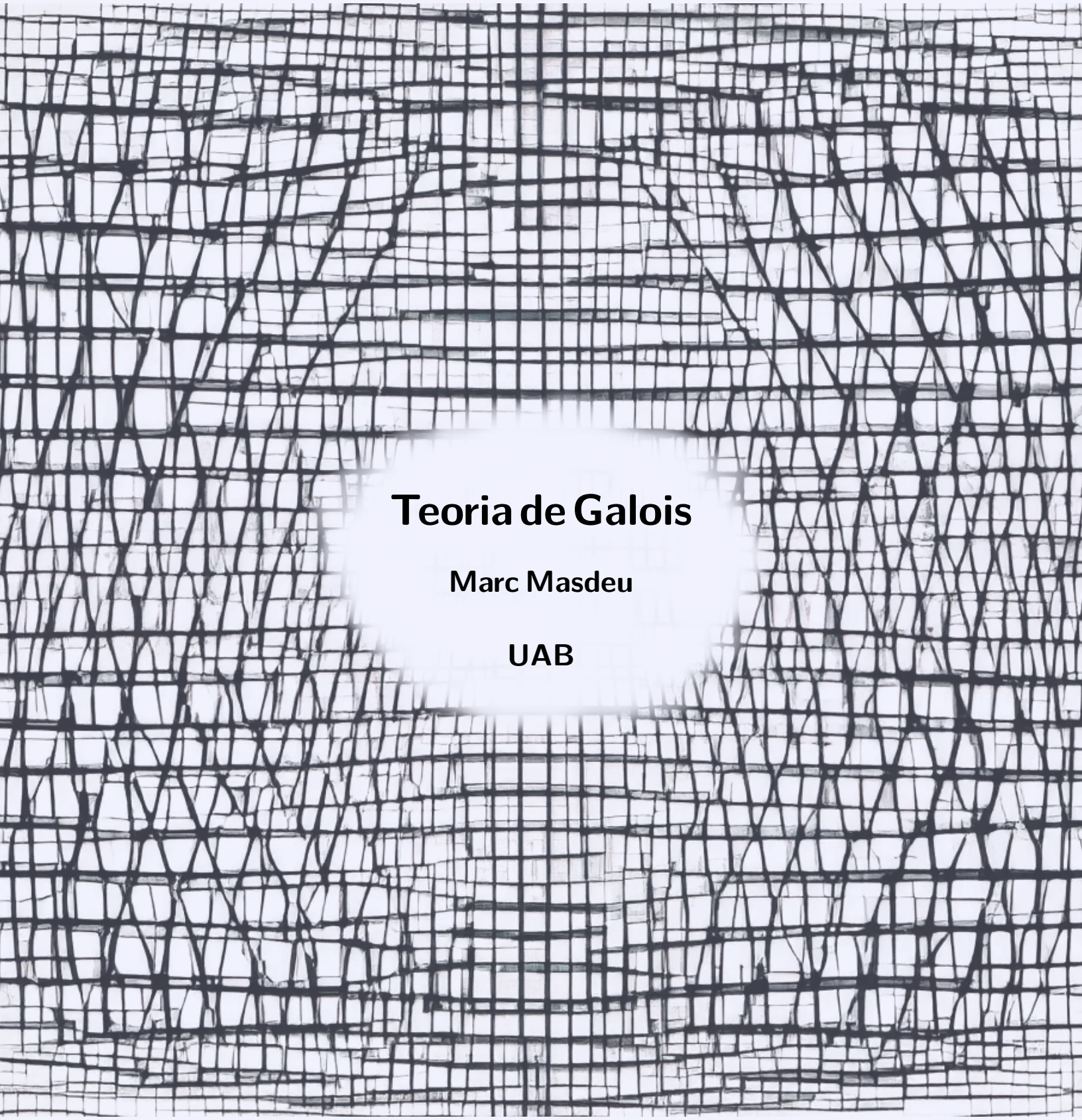


Teoria de Galois

Marc Masdeu

UAB

Índex

Introducció

Aquests són uns apunts de *Teoria de Galois*, pensats pel curs de 3r del Grau de Matemàtiques de la UAB.

L'assignatura de *Teoria de Galois* es cursa al primer semestre del tercer curs del Grau de Matemàtiques de la UAB. Consta de 6 crèdits, repartits en:

- Dues hores setmanals de teoria (15 setmanes), que actualment es fan seguides.
- Una hora setmanal de problemes (15 setmanes).
- Tres seminaris pràctics, de 2h cadascun.

El curs es pot dividir de manera natural en 15 sessions de dues hores. El temps efectiu de cadascuna d'aquestes sessions és de 100 minuts, i es pot pensar com una sèrie de 15 capítols.

L'estructura que s'ha seguit és essencialment la de Dummit and Foote (2004), però la demostració del teorema fonamental s'ha fet completament diferent, seguint un punt de vista proposat per Geck (2014). També s'ha canviat la presentació de l'existència de la clausura algebraica d'un cos arbitrari.

1. Vells coneguts

Començarem recordant les definicions i resultats bàsics que ja s'han vist a altres assignatures, com Fonaments o Estructures algebraiques. Donarem les definicions de cos, característica, cos primer, i veurem que aquest és o bé $\mathbb{F}_p$ per algun primer p, o bé $\mathbb{Q}$. A continuació introduïrem les extensions de cossos i el grau. Construirem el cos $F[x]/(p(x))$ associat a un polinomi irreductible $p(x) \in F[x]$, i veurem alguns exemples.

1.1 Convencions

En aquest curs, tots els anells seran commutatius, i assumirem sempre que tenen unitat. A més, demanarem que un morfisme d'anells enviï l'1 a l'1.

1.2 Característica d'un cos

Siguia A un anell qualsevol. Considerem el morfisme $\iota\colon \mathbb{Z} \to A$ definit com:

$$\iota(n) = \begin{cases} 1_A + 1_A + \cdots + 1_A & n \geq 0, \\ -(1_A + 1_A + \cdots + 1_A) & n < 0, \end{cases}$$

on les sumes tenen n termes. És fàcil comprovar que és un morfisme. A més, fent inducció en $|n|$ es demostra fàcilment que ι és l'únic morfisme $\mathbb{Z} \to A$. Per tant, a partir d'ara, qualsevol enter el podem pensar com a element d'un anell donat, i això no ens portarà cap confusió.

Com ja sabem, el nucli d'un morfisme d'anells és un ideal. Per tant, el nucli del morfisme $\iota_A\colon \mathbb{Z} \to A$ és un ideal de $\mathbb{Z}$ de la forma (n), amb $n \geq 0$.

Definició 1.2.1 — Característica. La *característica* d'un anell A és l'enter no negatiu n tal que $\iota_A = (n)$, i es denota per $\operatorname{char}(A)$.

Fixem-nos que si $\operatorname{char}(A) = n$, aleshores $na = 0$ per a tot $a \in A$.

Proposició 1.2.1 Sigui F un cos. Aleshores la seva característica és 0 o bé un primer p.

Demostració. Suposem que $\operatorname{char}(F) = n > 0$, i $n = ab$. Aleshores $(a1_A)(b1_A) = (ab)1_A = 0$. Com que F és un cos, això vol dir que $a1_A = 0$ o $b1_A = 0$. Si per exemple $a1_A = 0$, això significa que $n \mid a$. Com que $n = ab$, necessàriament $a = n$ i $b = 1$. Per tant, els únics divisors de n són trivials, i n és primer. ∎

Definició 1.2.2 — cos primer. El *cos primer* d'un cos F és el cos generat per 1_F. És o bé $\mathbb{Q}$ (si F té característica 0) o bé el cos $\mathbb{F}_p$ (si F té característica p).

1.3 Extensions

Quan K és un cos que conté un altre cos F, direm que K és una *extensió* de F, i escriurem K/F (no és cap mena de quocient!). Direm també que F és el *cos base* de l'extensió K/F. També farem servir el diagrama

$$\begin{array}{c} K \\ | \\ F. \end{array}$$

Com que un cos no té ideals propis, un morfisme de cossos $\iota\colon F \to K$ és sempre injectiu i, per tant, la imatge de ι és un subcos de K isomorf a F. A partir d'ara, a vegades identificarem F amb $\iota(F)$, i direm que K és una extensió de F.

Seguidament fem la següent observació clau: quan tenim una extensió K/F aleshores K esdevé automàticament un F-espai vectorial. Això ens permet definir:

Definició 1.3.1 — grau d'una extensió. El *grau* de l'extensió K/F és la dimensió de K com a F-espai vectorial, que escrivim com $[K\colon F]$. Direm que K/F és finita si té grau finit, i infinita si no.

En un diagrama de cossos, sovint indicarem que l'extensió té grau n així:

$$\begin{array}{c} K \\ {\scriptstyle n}\,| \\ F. \end{array}$$

Teorema 1.3.1 — Kronecker. Sigui $f(x) \in F[x]$ un polinomi. Aleshores existeix una extensió K/F tal que K té una arrel de $f(x)$.

Demostració. Considerem $K = F[x]/(g(x))$, on $g(x)$ és un factor irreductible qualsevol de $f(x)$. Sigui α la classe de x a K. Aleshores $g(\alpha) = 0$ i per tant $f(\alpha) = 0$. Els elements de K venen representats per $h(\alpha)$ on $h(x) \in F[x]$ són polinomis, que sempre podem pensar de grau menor al grau de $g(x)$ (per la divisió euclídea). D'altra banda, el fet que $g(x)$ sigui irreductible fa que K sigui un cos. En efecte, si $h(\alpha) \neq 0$, tenim que $g(x) \nmid h(x)$ i per tant $g(x)$ i $h(x)$ són coprimers. Per la identitat de Bézout, existeixen polinomis $a(x)$ i $b(x)$ tals que

$$a(x)g(x) + b(x)h(x) = 1,$$

i per tant $b(\alpha)h(\alpha) = 1$. És a dir, $h(\alpha)$ és invertible, amb invers $b(\alpha)$. ∎

El següent teorema ens diu que l'extensió donada pel teorema anterior té grau igual al grau del polinomi (per això s'ha triat el nom!) quan aquest és irreductible. De fet, ens dona una base de K com a F-espai vectorial.

Teorema 1.3.2 Sigui $f(x) \in F[x]$ un polinomi irreductible de grau n, i sigui $K = F[x]/(f(x))$. Sigui α la classe de x a K. Aleshores els elements $\{1, \alpha, \ldots, \alpha^{n-1}\}$ formen una F-base de K.

Demostració. Tot element de K té un representant de la forma $h(x) \in F[x]$. Dividint per $f(x)$, podem trobar un representant equivalent però de grau $< n$. Per tant, els elements $\{1, \alpha, \ldots, \alpha^{n-1}\}$

generen K com a F-espai vectorial. Cal veure que són linealment independents. Si hi hagués una relació de dependència lineal, voldria dir que hi hauria un polinomi $g(x) \in F[x]$ de grau $< n$ tal que $g(\alpha) = 0$. Però aleshores $g(x)$ hauria de ser un divisor de $f(x)$, que és impossible ja que $f(x)$ és irreductible. ■

L'aritmètica a $F[x]/(p(x))$ és molt explícita: els seus elements es poden expressar com a polinomis en α de grau menor que $n = \deg(p(x))$. Donats dos polinomis $a(\alpha)$ per $b(\alpha)$, podem considerar el residu $r(x)$ de dividir $a(x)b(x)$ per $p(x)$. Aleshores el producte $a(\alpha)b(\alpha)$ ve donat per l'element $r(\alpha)$. Per divir ens cal utilitzar la identitat de Bézout (exercici).

■ **Exemple 1.1** Potser l'exemple més conegut és el que s'obté de considerar el polinomi $x^2+1 \in \mathbb{R}[x]$, que és irreductible perquè no té arrels. El cos obtingut s'escriu $\mathbb{C}$, i la classe de x a $\mathbb{R}[x]/(x^2+1)$ s'escriu i. Com que $i^2+1=0$, tenim $i^2=-1$ i recuperem les fórmules habituals per treballar amb els nombres complexos.

De manera semblant, podem definir $\mathbb{Q}[x]/(x^2+1)$ (adjuntem una arrel de -1 als racionals), $\mathbb{Q}[x]/(x^2-2)$ (adjuntem un element α amb $\alpha^2=2$), o també $\mathbb{Q}[x]/(x^3-2)$. Es poden fer les operacions habituals (suma, resta, multplicació, divisió) en algun d'aquests cossos de manera molt explícita. Per exemple, $\mathbb{Q}[x]/(x^2-2)$ està format, com a conjunt, per tots els elements de la forma $a+b\alpha$, amb $a, b \in \mathbb{Q}$. La multiplicació ve donada pel fet que $\alpha^2 = 2$.

De manera semblant, $\mathbb{Q}[x]/(x^3-2) = \{a+b\beta+c\beta^2 \mid a,b,c \in \mathbb{Q}\}$, i hem de recordar que $\beta^3 = 2$ per simplificar el resultat de les multiplicacions. ■

■ **Exemple 1.2** Si considerem $\mathbb{F}_p$ el cos finit de p elements i un polinomi $f(x) \in \mathbb{F}_p[x]$ irreductible de grau n (suposant que existeixi!), aleshores obtenim un cos $K/\mathbb{F}_p$ de grau n. Té, per tant, p^n elements. Més endavant veurem, d'una manera bastant indirecta, que per qualsevol primer p i qualsevol enter $n \geq 1$ existeix un polinomi a $\mathbb{F}_p[x]$ irreductible de grau n (Teorema 9.3.1) ■

■ **Exemple 1.3** També podem fer extensions de cossos més "exòtics". Per exemple, podem prendre $k(t)$ com el cos de funcions racionals sobre un cos fixat k, i "afegir" una arrel quadrada de t (mitjançant el polinomi x^2-t). Els seus elements són de la forma $a(t)+b(t)\sqrt{t}$, on $a(t), b(t) \in k(t)$, i les operacions són les habituals. ■

Una altra manera de crear nous cossos és definir-los com subextensions d'una extensió donada. Sigui K/F una extensió, i fixem un conjunt $S \subseteq K$. Aleshores podem considerar el "mínim" subcos $L \subseteq K$ que conté F i tots els elements de S. S'anomena el *cos generat per S sobre F*, i escriurem $F(S)$. Si S és un conjunt finit format per $\alpha_1, \ldots, \alpha_n$ aleshores escriurem $F(\alpha_1, \ldots, \alpha_n)$ i direm que $F(S)$ és *finitament generat*. Un cas particular es dona és quan S conté un sol element: en aquest cas $F(\alpha)$ s'anomena una extensió *simple*, i l'element α s'anomena un *element primitiu* de l'extensió (que no és únic, en general!).

Teorema 1.3.3 — extensió simple. Sigui $f(x) \in F[x]$ un polinomi irreductible, i suposem que K/F és una extensió que conté una arrel α de $f(x)$. Aleshores hi ha un isomorfisme

$$F[x]/(f(x)) \cong F(\alpha).$$

Aquest isomorfisme és únic si demanem que $[x] \mapsto \alpha$.

Demostració. Tenim

$$\begin{aligned}\mathrm{Hom}_F(F[x]/(f(x)), F(\alpha)) &\cong \{\varphi \in \mathrm{Hom}_F(F[x], F(\alpha)) \mid \varphi(f) = 0\} \\ &\cong \{\beta \in F(\alpha) \mid f(\beta) = 0\} \neq \emptyset.\end{aligned}$$

Donat un morfisme φ, és automàticament un isomorfisme, fet que comprovem calculant graus de les extensions. ■

■ **Exemple 1.4** El cos $\mathbb{Q}(\sqrt{2}) \subset \mathbb{R}$ és isomorf a $\mathbb{Q}[x]/(x^2-2)$. Hi ha dos isomorfismes possibles, l'un identifica $[x] \leftrightarrow \sqrt{2}$ i l'altre $[x] \leftrightarrow -\sqrt{2}$.

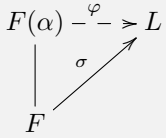
Considerem ara $\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$. Aquest cos també és isomorf a $\mathbb{Q}[x]/(x^3-2)$, però aquesta vegada només hi ha un isomorfisme possible, el que assigna $[x] \leftrightarrow \sqrt[3]{2}$. Això és així perquè el polinomi x^3-2 només té una arrel real. També hi ha un subcòs de $\mathbb{C}$ que és isomorf a $\mathbb{Q}[x]/(x^3-2)$, que és el generat per $\zeta_3\sqrt[3]{2}$, on $\zeta_3 = \frac{-1+i\sqrt{3}}{2}$ és una arrel cúbica de la unitat. Hi ha dos isomorfismes possibles, de fet, el que identifica $[x] \leftrightarrow \zeta_3\sqrt[3]{2}$ i el que identifica $[x] \leftrightarrow \zeta_3^{-1}\sqrt[3]{2}$. ■

R En els exemples, hem construit cossos que contenen una de les tres possibles arrels de x^3-2. Aquests són isomorfs, tal i com hem vist. El fet que un sigui subcos de $\mathbb{R}$ i l'altre de $\mathbb{C}$ té a veure amb anàlisi, no amb àlgebra. Algebraicament, no es poden distingir.

Acabem amb un teorema que ens servirà més endavant. Ens anirà bé fer servir la notació següent. Si $\sigma\colon F \to L$ és un morfisme de cossos i $f(x) \in F[x]$ és un polinomi qualsevol, escrivim $\sigma(f) \in L[x]$ per denotar el polinomi obtingut d'$f(x)$ aplicant σ als seus coeficients.

Teorema 1.3.4 — extensió de morfismes. Sigui $\sigma\colon F \to L$ un morfisme de cossos. Sigui $f(x) \in F[x]$ un polinomi irreductible. Aleshores l'aplicació $\varphi \mapsto \varphi(\alpha)$ indueix una bijecció

$$\mathrm{Hom}_\sigma(F(\alpha), L) \xrightarrow{\cong} \{\beta \in L \mid \sigma(f)(\beta) = 0\}.$$



Demostració.

$$\mathrm{Hom}_\sigma(F(\alpha), L) \cong \mathrm{Hom}_\sigma(F[x]/(f(x)), L) \cong \{\varphi \in \mathrm{Hom}_\sigma(F[x], L) \mid \varphi(f) = 0\},$$

i aquest últim conjunt és precisament $\{\beta \in L \mid \sigma(f)(\beta) = 0\}$. ■

2. Les Torres

Definirem elements algebraics i transcendents i el polinomi mínim d'un element algebraic, amb exemples. Enunciarem i demostrarem la fórmula de les torres, i com es comporta el grau en composicions de cossos.

2.1 Extensions algebraiques/transcendents

Considerem una extensió K/F.

Definició 2.1.1 — element algebraic. Diem que un element $\alpha \in K$ és *algebraic sobre* F si α és l'arrel d'un polinomi $f(x) \in F[x]$.

Diem que α és *transcendent sobre* F si no és algebraic.

L'extensió K/F és *algebraica* si tots els elements $\alpha \in K$ són algebraics sobre F.

Fixem-nos que si α és algebraic sobre F aleshores sabem que hi ha *algun* polinomi $f(x) \in F[x]$ que té α com a arrel. Però n'hi ha molts més, per exemple qualsevol múltiple de $f(x)$. El següent resultat ens permet assignar un polinomi *canònic* a cada element algebraic.

Proposició 2.1.1 Si α és algebraic sobre F, aleshores hi ha un únic polinomi **mònic** i **irreductible** $\mathrm{Irr}_{\alpha,F}(x)$ que té α com a arrel. A més, $f(x) \in F[x]$ té α com a arrel si i només si és un múltiple de $\mathrm{Irr}_{\alpha,F}(x)$.

Demostració. Sigui $g(x) \in F[x]$ un polinomi mònic amb α com a arrel, i amb grau mínim entre tots ells. Si es pogués trencar com $g(x) = g_1(x)g_2(x)$, aleshores α seria una arrel d'un dels $g_i(x)$, contradient la minimalitat del grau de $g(x)$.

Suposem que $f(x)$ satisfà $f(\alpha) = 0$. Dividint per $\mathrm{Irr}_{\alpha,F}(x)$, tenim

$$f(x) = \mathrm{Irr}_{\alpha,F}(x)q(x) + r(x),$$

i substituint a $x = \alpha$ tindrem $r(\alpha) = 0$. Per minimalitat, deduïm que $r(x) = 0$, com volíem. ■

Fixem-nos que, si $K/L/F$ és una torre d'extensions i $\alpha \in K$ és algebraic sobre F, aleshores també ho és sobre L, i a més $\mathrm{Irr}_{\alpha,L}(x)$ divideix $\mathrm{Irr}_{\alpha,F}(x)$ a $L[x]$.

Definició 2.1.2 — polinomi mínim. El polinomi $\mathrm{Irr}_{\alpha,F}(x)$ s'anomena el *polinomi mínim d'*α *sobre* F, i el seu grau s'anomena el *grau d'*α sobre F.

Posant junt tot el què hem vist fins ara, si prenem $\alpha \in K$ aleshores podem considerar la subextensió $F(\alpha)/F$. En aquest cas, $F(\alpha) \cong F[x]/(\mathrm{Irr}_{\alpha,F}(x))$ i per tant $[F(\alpha)\colon F] = \deg \alpha$.

■ **Exemple 2.1** El polinomi mínim de $\sqrt{2} \in \mathbb{R}$ sobre $\mathbb{Q}$ és $x^2 - 2$. Diem que $\sqrt{2}$ és un element *quadràtic* sobre $\mathbb{Q}$. De manera semblant, el polinomi mínim de $\sqrt[3]{2}$ és $x^3 - 2$. Aquests dos polinomis són irreductibles sobre $\mathbb{Q}$ per exemple per que són 2-Eisenstein. ■

Proposició 2.1.2 Si $[K\colon F] = n$ i $\alpha \in K$, aleshores $\deg \alpha \leq n$. En particular, tota extensió finita K/F és algebraica.

Demostració. Considerem els elements $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}, \alpha^n$. Com que n'hi ha $n+1$, hi ha d'haver una relació de dependència lineal entre ells, i això ens dona un polinomi $f(x) \in F[x]$ de grau $\leq n$ tal que $f(\alpha) = 0$. ■

No és cert que tota extensió algebraica sigui finita (en veurem exemples més endavant).

El següent resultat ens caracteritza com són les extensions quadràtiques d'un cos F de característica $\neq 2$.

Proposició 2.1.3 Sigui F un cos de característica $\neq 2$, i sigui K/F una extensió de grau 2. Aleshores existeix $\delta \in K \setminus F$ tal que $\delta^2 = D \in F$ i $K = F(\delta)$. Escriurem que $K = F(\sqrt{D})$.

Demostració. Prenem $\alpha \in K \setminus F$. Per tant, α satisfà un polinomi de grau dos, que podem suposar mònic, posem $f(x) = x^2 + bx + c$ amb $b, c \in F$. Observem que $F(\alpha) = K$, ja que $F(\alpha)$ és una extensió de grau 2 dins de K. Sigui $\delta = \alpha + b/2$. Aleshores és fàcil veure que δ és una arrel del polinomi $g(x) = x^2 - D$, on $D = b^2 - 4c$. Per tant, $F(\alpha) = F(\delta) = F(\sqrt{D})$. ■

2.2 Torres de cossos

En aquesta secció considerem torres $L/K/F$. Ens interessa relacionar les dues extensions L/K i K/F amb l'extensió total L/F.

Proposició 2.2.1 Sigui K/F una extensió, i sigui V un K-espai vectorial. Aleshores

$$\dim_F V = [K\colon F] \dim_K V.$$

Demostració. Sigui $\{v_i\}_{i \in I}$ una K-base de V, i sigui $\{\alpha_j\}_{j \in J}$ una base de K sobre F. Aleshores és fàcil comprovar que el conjunt $\{\alpha_j v_i\}_{i \in I, j \in J}$ forma una F-base de V. ■

Teorema 2.2.2 — fórmula de les torres. Si $F \subseteq K \subseteq L$, aleshores

$$[L\colon F] = [L\colon K][K\colon F].$$

Si un costat de l'equació és infinit, aleshores l'altre també.

Demostració. Es dedueix directament del lema anterior. ■

Corol · lari 2.2.3 Si L/F és una extensió finita i K/F és una subextensió (és a dir, $K \subseteq L$) aleshores $[K\colon F]$ divideix $[L\colon F]$.

Per exemple, el corol · lari anterior ens permet deduïr que $\sqrt{2}$ no pertany a cap extensió de grau senar.

Exercici 2.1 Demostreu que el polomi $x^3 - \sqrt{2}$ és irreductible sobre $\mathbb{Q}(\sqrt{2})$, fent servir la torre $\mathbb{Q}(\sqrt[6]{2})/\mathbb{Q}(\sqrt{2})/\mathbb{Q}$. ■

El següent lema senzill ens permetrà construir qualsevol extensió finitament generada de manera iterativa:

Lema 2.2.4 Si α i β són elements de K/F, aleshores $F(\alpha, \beta) = (F(\alpha))(\beta)$.

Demostració. El cos $F(\alpha, \beta)$ conté $F(\alpha)$. Com que també conté β, tenim $F(\alpha)(\beta) \subseteq F(\alpha, \beta)$ per minimalitat de $F(\alpha)(\beta)$.

Recíprocament, com que el cos $F(\alpha)(\beta)$ conté a F, a α i a β, aleshores per minimalitat de $F(\alpha, \beta)$ tenim que $F(\alpha, \beta) \subseteq F(\alpha)(\beta)$. ■

Exercici 2.2 Calculeu el grau de l'extensió $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$, i doneu-ne una base. ■

Teorema 2.2.5 L'extensió K/F és finita si i només si $K = F(S)$ on S és un conjunt finit d'elements algebraics.

Demostració. Suposem K/F finita de grau n, i sigui S el conjunt (finit) format per una base de K sobre F. Aleshores $K = F(S)$, i els elements $\alpha \in S$ són tots algebraics, ja que $[F(\alpha) : F]$ divideix n i en particular el grau és finit.

Recíprocament, si $K = F(S)$ amb S un conjunt finit d'elements algebraics, aleshores podem obtenir K adjuntant successivament els elements de S, i cada extensió és finita. ■

Corol · lari 2.2.6 Si α i β són algebraics sobre F, aleshores també ho són $\alpha \pm \beta$, $\alpha\beta$ i α/β (si $\beta \neq 0$).

Corol · lari 2.2.7 Si L/F és una extensió qualsevol, aleshores el conjunt K d'elements de L que són algebraics sobre F forma un subcos $L/K/F$.

Per exemple, podem considerar $\bar{\mathbb{Q}} \subseteq \mathbb{C}$, el conjunt de tots els complexos algebraics, o també $\bar{\mathbb{Q}} \cap \mathbb{R}$, el conjunt dels reals algebraics. Aquests cossos són enumerables (tenen un conjunt d'elements enumerable) i per tant són més petits que $\mathbb{R}$ i que $\mathbb{C}$. D'aquest fet obtenim que hi ha (molts) elements de $\mathbb{R}$ que no són algebraics. En canvi, sovint és difícil demostrar que un real donat (per exemple π) és transcendent.

Teorema 2.2.8 Si K/F és una extensió algebraica i L/K també, aleshores L/F és algebraica.

Demostració. Sigui $\alpha \in L$. Per tant, α satisfà un polinomi $f(x) \in K[x]$. Sigui S el conjunt (finit) format pels coeficients de $f(x)$. Com que K/F és algebraica, els elements de S són tots

algebraics i per tant l'extensió $F(S)/F$ és finita. Considerem el cos $F(\alpha, S)$. Tenim:

$$[F(\alpha, S)\colon F] = [F(\alpha, S)\colon F(S)][F(S)\colon F].$$

El primer terme és menor o igual que el grau del polinomi $f(x)$, ja que podem pensar $f(x) \in F(S)$ i α n'és una arrel. El segon terme és finit, com hem dit. Per tant $F(\alpha, S)$ és una extensió finita, i això vol dir que α és algebraic sobre F. ■

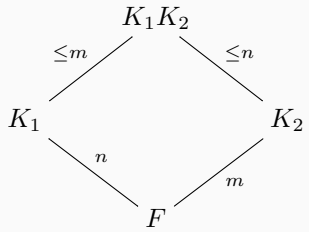
2.3 Compositum de cossos

Recordem que donats dos cossos K_1/F i K_2/F, el seu *compost* (o *compositum*) K_1K_2/F és el mínim cos que conté tant a K_1 com a K_2. També es pot pensar com la intersecció de tots els cossos L/F que contenen el conjunt $K_1 \cup K_2$.

Proposició 2.3.1 Siguin K_1/F i K_2/F dues extensions contingudes a K. Aleshores

$$[K_1K_2\colon F] \leq [K_1\colon F][K_2\colon F].$$

La igualtat es dona si i només si una base de K_1/F segueix essent linealment independent sobre K_2 (o a l'inrevés). A més, tenim:



Demostració. Cal veure que els productes $\alpha\beta$ on α i β recorren bases respectives de K_1/F i de K_2/F generen K_1K_2/F. N'hi ha prou amb veure que les combinacions lineal d'aquests elements formen un cos, que és una observació senzilla. ■

Fixem-nos que, si m i n són coprimers, aleshores per la fórmula de les torres tenim $[K_1K2\colon K_1] = m$ i $[K_1K_2\colon K_2] = n$. En general, però les desigualtats del diagrama anterior seran estrictes.

3. Regle i Compàs

Parlarem de tres problemes de la Grècia clàssica sobre construccions amb regle no marcat i compàs: la quadratura del cercle, la trisecció de l'angle i la duplicació del cub. Caracteritzarem els nombres constructibles, i veurem que aquests problemes no tenen solució. Veurem també que si el regle és marcat aleshores podem trisecar l'angle i també duplicar el cub.

3.1 El problema

Els grecs es van interessar molt per les construccions amb dos instruments molt simples: per una banda, el que habitualment s'anomena regle, i que vol dir simplement un regle sense cap mena de marca. Ens permet, donats dos punts del pla, traçar la recta que els uneix. El segon instrument és el compàs. Donats dos punts podem fixar l'obertura, i donat un tercer punt (que pot coincidir o no amb els anteriors) podem traçar un arc de circumferència amb el radi fixat prèviament, i el centre aquest tercer punt.

Hi ha tres problemes clàssics que ens proposem estudiar:

1. "Duplicació del cub": donat un cub, podem construir-ne un altre de volum exactament el doble?
2. "Trisecció de l'angle": donat un angle θ, podem construir l'angle $\theta/3$?
3. "Quadratura del cercle": donat un cercle, podem construir un quadrat d'àrea igual a la del cercle donat?

Donada una longitud inicial (que definirem com a 1), direm que un nombre real α és *constructible* si podem construir un segment de longitud α mitjançant una successió finita d'operacions amb regle i compàs. Tenim els quatre tipus d'operacions següents:

1. Unir dos punts per una recta.
2. Trobar el punt d'intersecció de dues rectes.
3. Dibuixar un cercle amb centre i radi donats.
4. Trobar els punts d'intersecció d'una recta amb un cercle, o de dos cercles.

3.2 La (no) solució

Comencem veient que els nombres constructibles són un cos.

Proposició 3.2.1 Els nombres constructibles formen un subcos de $\mathcal{C} \subseteq \mathbb{R}$.

Demostració. Cal donar construcions de la suma, resta, producte i divisió de nombres ja construïts. Mentre que la suma i la resta són òbvies, la multiplicació i divisió es poden obtenir aplicant proporcionalitat, com aquí sota.

■

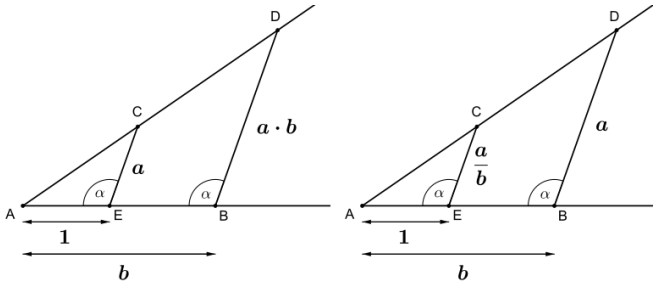
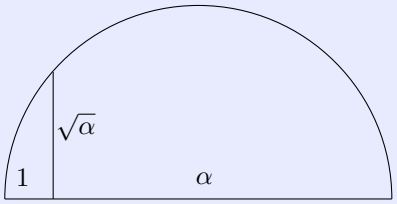


Figura 3.1: Multiplicació i divisió.

És fàcil veure que també podem prendre arrels quadrades, com s'indica al següent exercici.

Exercici 3.1 Demostreu que si el diàmetre de la circumferència és $\alpha + 1$, aleshores el segment vertical indicat mesura $\sqrt{\alpha}$.



■

Fent servir l'equació d'un cercle de radi (x_0, y_0) i radi r

$$(x - x_0)^2 + (y - y_0)^2 = r^2,$$

podem veure que les coordenades de la intersecció amb una recta (posem amb equació $ax+by = c$) pertanyen al cos $\mathbb{Q}(x_0, y_0, r, a, b, c)$. També podem comprovar-ho pel cas de la intersecció de dos cercles. Resumint si α és construcible en n passos a partir de punts en un cos F, aleshores hi ha una successió de cossos

$$F = F_0 \subseteq F_1 \subseteq F_2 \subseteq F_n,$$

amb $[F_{i+1} : F_i] \leq 2$, tals que $\alpha \in F_n$. En particular, α és un nombre algebraic sobre F de grau una potència de 2.

D'aquí en deduïm directament el següent teorema (on haurem d'assumir que π és transcendent, cosa que no demostrem).

Teorema 3.2.2 Els tres problemes clàssics no són resolubles.

Demostració. Per la duplicació d'un cub de costat 1 ens caldria construir $\sqrt[3]{2}$, que té grau 3 i, per tant, no és constructible.

Si un angle θ és constructible, aleshores fàcilment veiem que $\cos(\theta)$ i $\sin(\theta)$ també són constructibles. Veurem que $\alpha = 2\cos(\pi/9)$ no és constructible. Com que $\cos(\pi/3) = 1/2$, a partir de la fórmula de l'angle triple obtenim

$$\alpha^3 - 3\alpha - 1 = 0.$$

El polinomi $x^3 - 3x - 1$ és irreductible (substituint $x - 2$ obtenim un polinomi 3-Eistenstein) i per tant α té grau 3 i no és constructible.

Finalment, per la quadratura del cercle de radi 1 hauríem de construïr un quadrat de costat $\sqrt{\pi}$. Però aleshores també podríem construir π, que és transcendent (com hem dit, no ho demostrem). ■

Més endavant estudiarem quins angles són constructibles. De fet, tenim el següent:

Teorema 3.2.3 Sigui t un enter. L'angle de t graus (no radians!) és constructible si i només si t és un múltiple de 3.

Demostració. Hi ha construccions molt antigues del pentàgon regular (72°), ja que

$$\cos(72°) = \frac{1}{4}\sqrt{5} - \frac{1}{4},$$

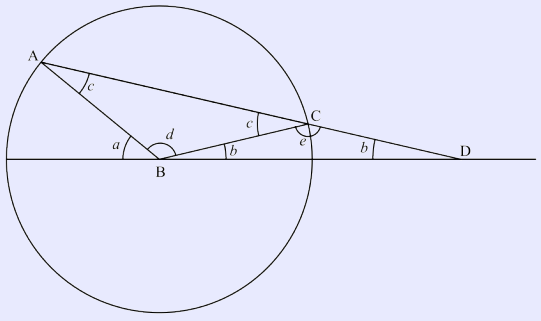
i encara més del triangle equilàter (30°), ja que $\cos(30°) = \sqrt{2}/2$. Com que podem bisectar qualsevol angle, també podem construir 18° i 15°. Finalment, com que $3 = 18 - 15$ també podem construir l'angle de 3°. És clar que no podem construir ni 2° ni 1°, perquè aleshores podríem construir també qualsevol múltiple d'aquests i, per tant, podríem construir 20°, que ja sabem que no és possible. ■

3.3 Construccions amb regle marcat i compàs

És important adonar-se que amb molt poc més aleshores algunes construccions clàssiques esdevenen molt senzilles. Aquí veurem que si el regle té dues marques a una distància qualsevol, aleshores podem trisecar l'angle i duplicar el cub.

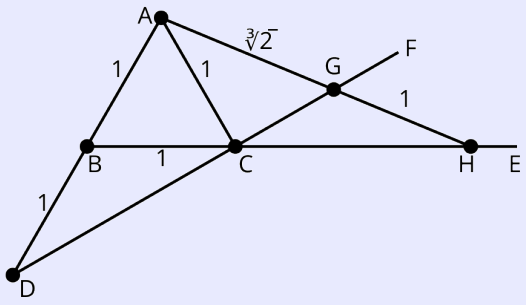
Exercici 3.2 — Trisecció d'un angle. En el dibuix d'aquí sota, s'ha començat amb un angle a amb centre B. Suposem que el regle té dues marques a una certa distància, que serà la nostra unitat. Fem un cercle de radi aquesta unitat, i tracem una recta pel punt A de manera que les dues marques del regle estiguin una sobre el cercle (punt C) i l'altra sobre la recta donada (punt D).

Demostreu que l'angle b és igual a $\frac{a}{3}$.



■

Exercici 3.3 — Duplicació del cub. Demostreu que el costat AG del dibuix de sota mesura $\sqrt[3]{2}$.



■

4. Normalitat

El cos de descomposició d'un polinomi juga un paper destacat al llarg del curs. Aquí el definirem, i en demostrarem l'existència i unicitat (llevat d'isomorfisme). Aprofitarem per definir extensions normals (aquelles que són cos de descomposició d'un conjunt de polinomis).

Com a aplicació, s'introduiran els polinomis i cossos ciclotòmics, i ho lligarem amb la demostració de l'existència i unicitat de cossos finits de cardinal potència d'un primer.

També veurem les clausures algebraiques, i una construcció (seguint Artin (2014) i Jelonek (1993)). Això ens permetrà (assumint el teorema fonamental de l'àlgebra, que demostrarem més endavant) pensar els elements algebraics sobre $\mathbb{Q}$ dins dels complexos.

4.1 Cossos de descomposició

Diem que un polinomi $f(x) \in F[x]$ *descomposa completament* en una extensió K/F si es pot escriure com a producte de polinomis de grau 1.

Definició 4.1.1 — cos de descomposició. Una extensió K/F és un *cos de descomposició* del polinomi $f(x) \in F[x]$ si $f(x)$ descomposa completament a K i no ho fa en cap subextensió $K/K'/F$.

Teorema 4.1.1 — existència del cos de descomposició. Sigui $f(x) \in F[x]$. Aleshores existeix un cos de descomposició K/F de $f(x)$.

Demostració. Farem inducció en el grau d'f, essent el cas $n = 1$ trivial. Suposem l'enunciat cert per tots els polinomis de grau \$ < n\$ definits sobre qualsevol cos, i ho demostrarem per $f(x) \in F[x]$ de grau n. Pel Teorema @ref{thm:kronecker}, hi ha una extensió L/F que conté una arrel $\alpha \in L_0$ de $f(x)$. Dividint per $(x - \alpha)$ obtenim un polinomi $f_0(x) \in L_0[x]$ de grau $n - 1$. Per hipòtesi d'inducció, existeix una extensió L/L_0 on $f_0(x)$ (i per tant també $f(x)$) descomposa completament. Aleshores podem prendre per K/F la intersecció de totes les subextensions $L/K'/F$ on $f(x)$ descomposa completament. Per construcció, K/F és un cos de descomposició de $f(x)$. ■

Fixem-nos que cada vegada que adjuntem una arrel d'un polinomi de grau n, aquest polinomi tindrà un cofactor com a molt de grau $n - 1$. Així, per obtenir un cos de descomposició en el pitjor dels casos haurem de fer una extensió de grau $n(n-1)(n-2)\cdots 2 \cdot 1 = n!$.

Podem fer servir la fórmula de les torres per demostrar una versió més forta d'aixecament de morfismes.

Teorema 4.1.2 — teorema d'aixecament d'isomorfismes. Sigui K/F una extensió finita, i sigui

L/F una extensió. Aleshores:

$$|\operatorname{Hom}_F(K,L)| \leq [K\colon F].$$

Demostració. Farem inducció en el grau $n = [K\colon F]$. Quan $n = 1$, el resultat és trivial. En general, prenem un element $\alpha \in K \setminus F$ i fem servir la fórmula de les torres i 1.3.4. El cardinal de $\operatorname{Hom}_F(F(\alpha), L)$ és igual al nombre d'arrels d'$\operatorname{Irr}_{\alpha,F}(x)$ a L, que com a molt és $[F(\alpha)\colon F]$.

En tot cas, si $\tilde{\sigma}$ és un d'aquests morfismes, com que $[K\colon F(\alpha)] < [K\colon F]$ podem aplicar la hipòtesi d'inducció i $\tilde{\sigma}$ es pot aixecar a com a molt $[K\colon F(\alpha)]$ morfismes a L. ■

Revisant la demostració anterior, obtenim els dos següent corol · laris.

Corol · lari 4.1.3 Siguin K/F i L/F extensions d'un cos F. Si existeix $\alpha \in K$ tal que $\operatorname{Irr}_{\alpha,F}(x)$ no té cap arrel a L, aleshores no existeix cap F-morfisme $K \to L$.

Corol · lari 4.1.4 Suposem que tot polinomi irreductible a F amb una arrel a K descomposa completament a L. Aleshores

$$|\operatorname{Hom}_F(K,L)| = [K\colon F].$$

Proposició 4.1.5 — unicitat del cos de descomposició. Siguin K/F i K'/F dos cossos de descomposició de $f(x) \in F[x]$. Aleshores $K \cong K'$.

Demostració. Prenem $L = K'$ al Teorema 4.1.2 i en repetim la demostració. A cada pas, podem prendre com a α una arrel de $f(x)$ i sempre obtindrem arrels a K' perquè $f(x)$ hi trenca completament. ■

■ **Exemple 4.1** El cos de descomposició de x^2-2 és $\mathbb{Q}(\sqrt{2})$. Considerem el polinomi $(x^2-2)(x^2-3)$. En aquest cas, el seu cos de descomposició ha de contenir $\mathbb{Q}(\sqrt{2})$ i $\mathbb{Q}(\sqrt{3})$ i, per tant, el seu grau ha de ser parell i més gran que 2. Sigui $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, que és un cos de grau 4. El polinomi factoritza com $(x-\sqrt{2})(x+\sqrt{2})(x-\sqrt{3})(x+\sqrt{3})$ i per tant K és el cos de descomposició que busquem.

Un cas una mica més interessant és el del polinomi $x^3 - 2$. El seu cos de descomposició ha de contenir $\alpha = \sqrt[3]{2}$, però quan fem la divisió obtenim:

$$x^3 - 2 = (x-\alpha)(x^2 + \alpha x + \alpha^2).$$

Fixem-nos que si α i β són dues arrels diferents de $x^3 - 2$ en el cos de descomposició $L/\mathbb{Q}$, aleshores $(\alpha/\beta)^3 = 1$. Per tant, α/β satisfà el polinomi $(x^3-1)/(x-1) = x^2 + x + 1$, que ja sabem que és irreductible a $\mathbb{Q}$. Per tant, L ha de contenir també ζ_3, i obtenim finalment que $L = \mathbb{Q}(\alpha, \zeta_3)$, que és un cos de grau 6 sobre $\mathbb{Q}$.

Finalment, observem que a vegades el cos de descomposició pot ser de grau més petit que el polinomi amb què comencem. Per exemple, el cos de descomposició de $x^4 + 4$ és simplement $\mathbb{Q}(i)$, que té grau 2. ■

■ **Exemple 4.2 — cossos ciclotòmics.** Calculem el cos de descomposició del polinomi $x^n - 1$. Les seves arrels s'anomenen *arrels n-èssimes de la unitat*. En els complexos les arrels són els nombres $e^{\frac{2\pi i}{n}}$, amb $n = 0, \ldots, n-1$. Per tant $\mathbb{C}$ conté el cos de descomposició de $x^n - 1$. En general, si $K/\mathbb{Q}$ és un cos de descomposició de $x^n - 1$, aleshores podem veure que aquestes formen un grup amb la multiplicació que, de fet, és cíclic. Diem que una arrel de la unitat ζ_n és *primitiva* si és un generador d'aquest grup. Si en fixem una, les altres primitives són de la forma ζ_n^a, amb a coprimer amb n. Hi ha, doncs, $\varphi(n)$ arrels primitives.

Anomenem *cos ciclotòmic n-èssim$ al cos $\mathbb{Q}(\zeta_n)$, que és el cos de descomposició de $x^n - 1$: si adjuntem ζ_n, automàticament totes les seves potències pertanyen a aquest cos. A l'episodi 5.3 aprendrem com calcular el grau d'aquest cos, però –a tall d'espòiler– podem veure fàcilment que quan $n = p$ és primer, aleshores

$$x^p - 1 = (x-1)(x^{p-1} + x^{p-1} + \cdots + x + 1),$$

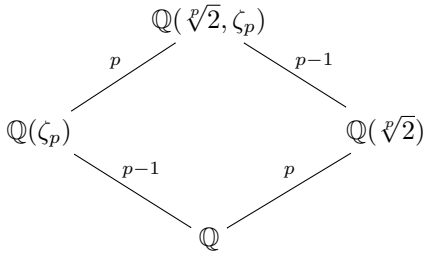
i ja hem vist que el polinomi $\Phi_p(x) = x^{p-1} + x^{p-1} + \cdots + x + 1$ és irreductible. Per tant, tenim

$$[\mathbb{Q}(\zeta_p) \colon \mathbb{Q}] = p - 1.$$

■

■ **Exemple 4.3** Calcularem ara el cos de descomposició de $x^p - 2$, on p és un primer. Si anomenem α una arrel d'aquest polinomi, aleshores les altres arrels són de la forma $\alpha\zeta$, on ζ és una arrel p-èssima de la unitat. Podem veure fàcilment que el cos de descomposició és $L = \mathbb{Q}(\sqrt[p]{2}, \zeta_p)$.

Tenim la torre $L/\mathbb{Q}(\zeta_p)/\mathbb{Q}$ i $L/\mathbb{Q}(\zeta_p)$ té grau com a molt p, ja que està generada per $\sqrt[p]{2}$. Per tant, es té la desigualtat $[L \colon \mathbb{Q}] \leq p(p-1)$. Com que L té subcossos de grau p i de grau $p-1$, aquests dos nombres divideixen el grau de l'extensió total i, com que són coprimers, en deduim que el grau és exactament $p(p-1)$. Ho podem il · lustrar amb el diagrama següent:



■

4.2 Extensions normals

Acabem explicant el concepte d'extensió normal, i les seves propietats bàsiques.

Definició 4.2.1 — extensió normal. Una extensió algebraica K/F es diu *normal* si tot polinomi irreductible $f(x) \in F[x]$ que té una arrel a K trenca completament a K.

Dit d'una altra manera K/F és normal si per tot $\alpha \in K$ el seu polinomi mínim sobre F descomposa completament a K. D'entrada, sembla difícil demostrar que una extensió donada K/F és normal, ja que cal veure una propietat per possiblement infinits polinomis. Veurem ara que les extensions normals tenen una caracterització més senzilla. En particular, el cos de descomposició d'un polinomi és sempre una extensió normal.

Proposició 4.2.1 Una extensió K/F és normal si i només si K és el cos de descomposició d'un conjunt $S \subset F[x]$ de polinomis de F.

Demostració. Suposem que K/F és normal. Per cada element $\alpha \in K$, denotem per $f_\alpha(x) = \mathrm{Irr}_{\alpha,F}(x)$. Aleshores K és el cos de descomposició del conjunt $S = \{f_\alpha(x) \mid \alpha \in K\}$.

Recíprocament, si K és el cos de descomposició d'un conjunt S i $f(x) \in F[x]$ té una arrel $\alpha \in K$, aleshores sense perdre generalitat podem suposar que $f(x)$ és irreductible. Considerem el conjunt $\Sigma \subset K$ d'elements de K que són arrels de polinomis a S. Podem trobar un subconjunt finit S_0 i el seu corresponent conjunt d'arrels Σ_0 tals que $\alpha \in F(\Sigma_0)$. Però aleshores $F(\Sigma_0)$ és un cos de descomposició d'un polinomi (el que s'obté multiplicant tots els polinomis de S_0 i extraient-ne la part lliure de quadrats). Per tant, $f(x)$ descomposa completament a $F(\Sigma_0)$ i per tant també a K. ■

Proposició 4.2.2 Sigui $L/K/F$ una torre. Si L/F és normal, aleshores L/K també ho és.

Demostració. Trivial: si L/F és el cos de descomposició d'un conjunt de polinomis S, també ho és del mateix conjunt pensat com a conjunt de polinomis amb coeficients a K. ■

5. Polinomis (In)separables

Definim la noció de separabilitat d'un polinomi, i posem algun exemple. Introduïm el morfisme de Frobenius, que ens permet definir cossos perfectes. Aprofitem per parlar del grau de separabilitat/inseparabilitat d'una extensió, i la factorització d'aquesta.

Finalment, donem l'existència i unicitat dels cossos finits, i estudiem els polinomis ciclotòmics.

5.1 Separabilitat de polinomis i extensions

Sigui F un cos.

Definició 5.1.1 — separabilitat. Un polinomi $f(x) \in F[x]$ és *separable* si les seves arrels (en un cos de descomposició) són totes diferents. Si $f(x)$ no és separable diem que $f(x)$ és *inseparable*.

Fixem-nos que la definició no depèn del cos de descomposició que ens triem, per unicitat llevat d'isomorfisme. De fet, podem caracteritzar la separabilitat de $f(x)$ sense haver de considerar cap cos de descomposició:

Proposició 5.1.1 Un polinomi $f(x)$ té una arrel múltiple α si i només si α és una arrel de $f'(x)$. En particular, $f(x)$ és separable si i només si $\mathrm{mcd}(f(x), f'(x)) = 1$.

Demostració. Si $f(x) = (x-\alpha)g(x)$, aleshores $f'(x) = g(x) + (x-\alpha)g'(x)$ i, per tant, $f'(\alpha) = 0$ si i només si $g(\alpha) = 0$, si i només si $f(x) = (x-\alpha)^2 h(x)$. ■

Corol · lari 5.1.2 Si $f(x) \in F[x]$ és irreductible i F té característica 0, aleshores f és separable. En general, un polinomi $f(x) \in F[x]$ és separable si i només si és producte de diferents polinomis irreductibles.

Demostració. Si $f(x)$ té una arrel múltiple α, aleshores $h(x) = \mathrm{mcd}(f(x), f'(x))$ és un múltiple de $(x-\alpha)$ que divideix $f(x)$, i per tant $f(x)$ no pot ser irreductible. ■

■ **Exemple 5.1** El polinomi $x^n - 1$ té derivada nx^{n-1} i per tant, si $n \neq 0$ a F aleshores $x^n - 1$ és separable, i en aquest cas hi ha n arrels de la unitat diferents a F. En canvi, si F és de característica $p \mid n$, aleshores cada arrel de $x^n - 1$ és múltiple. ■

Ja hem estudiat el problema de separabilitat en característica 0, que és molt senzill. Ens centrarem ara en característica p, així que sigui F un cos de característica finita p. Pensem en què pot anar malament per tal que un polinomi irreductible $f(x) \in F[x]$ sigui inseparable. Cal que la seva derivada tingui factors en comú amb $f(x)$, i això només pot passar si la derivada és 0.

Lema 5.1.3 Sigui $f(x) \in F[x]$ amb $\text{char}(F) = p$. Si $f'(x) = 0$, aleshores hi ha un polinomi $f_1[x] \in F[x]$ tal que $f(x) = f_1(x^p)$.

En particular, observem que si $f(x) \in F[x]$ és inseparable, aleshores el seu grau és un múltiple de p.

Proposició 5.1.4 Sigui $f(x) \in F[x]$ amb $\text{char}(F) = p$ un polinomi irreductible. Aleshores hi ha un únic $k \geq 0$ i un únic polinomi irreductible i separable $g(x) \in F[x]$ tal que

$$f(x) = g(x^{p^k}).$$

Demostració. Iterem el procediment del lema anterior fins que el polinomi que obtenim és separable. Seguirà essent irreductible, i ja haurem acabat. ■

Definició 5.1.2 — grau de separabilitat. Sigui $f(x) \in F[x]$ amb $\text{char}(F) = p$ un polinomi irreductible. El *grau de separabilitat* de $f(x)$ és el grau de $g(x)$ en la proposició anterior, i el denotem per $\deg_s f(x)$.

El *grau d'inseparabilitat* és l'enter p^k que hi apareix, i el denotem per $\deg_i f(x)$.

Observem que $\deg f(x) = \deg_s f(x) \deg_i f(x)$.

Proposició 5.1.5 Sigui F un cos de característica p. Aleshores l'aplicació $a \mapsto a^p$ és un morfisme de cossos $F \to F$.

Demostració. Només cal veure que $(a+b)^p = a^p + b^p$ i que $(ab)^p = a^p b^p$. La primera igualtat es veu fent servir que p divideix a $\binom{p}{i}$ per a $1 \leq i \leq p-1$, i la segona és trivial. ■

El morfisme de la proposició anterior s'anomena el *morfisme de Frobenius*. Observem que si $\mathbb{F}$ és un cos finit, aleshores el morfisme de Frobenius és un isomorfisme (només cal comptar), però en general no és cert. Per exemple, la imatge de Frobenius a $F = \mathbb{F}_p(t)$ és $\mathbb{F}_p(t^p)$.

Proposició 5.1.6 Sigui $\mathbb{F}$ és un cos de característica p tal que el morfisme de Frobenius és exhaustiu. Aleshores tot polinomi irreductible sobre $\mathbb{F}$ és separable.

Demostració. Suposem que $f(x)$ fos inseparable. Aleshores $f(x) = f_1(x^p)$ per algun $f_1(x) \in \mathbb{F}[x]$. Els coeficients de f_1 són potències de p, i aleshores podem escriure

$$f_1(x) = a_m^p x^m + a_{m-1}^p x^{m-1} + \cdots a_1^p x + a_0^p.$$

Per tant, tenim

$$f(x) = f_1(x^p) = a_m^p x^{pm} + a_{m-1}^p x^{p(m-1)} + \cdots a_1^p x^p + a_0^p = \left(a_m x^m + a_{m-1} x^{m-1} + \cdots a_1 x + a_0\right)^p,$$

que contradiu el fet que $f(x)$ sigui irreductible. ■

Aquesta definició ens servirà per unificar els dos casos on la separabilitat no és problemàtica.

Definició 5.1.3 — cos perfecte. Un cos F és *perfecte* si té característica 0 o bé el morfisme de Frobenius és exhaustiu.

Corol · lari 5.1.7 Si F és perfecte, aleshores tot polinomi irreductible a $F[x]$ és separable.

Finalment, podem introduir el concepte d'extensió separable.

Definició 5.1.4 — extensió separable. Una extensió K/F és *separable* si tot element de K és arrel d'un polinomi separable sobre F.

Corol · lari 5.1.8 Tota extensió finita d'un cos perfecte és separable. En particular, els cossos finits són separables.

Corol · lari 5.1.9 Sigui F un cos de característica p, i sigui K/F una extensió finita tal que $p \nmid [K\colon F]$. Aleshores K/F és separable.

Demostració. Sigui $\alpha \in K$, i considerem $\mathrm{Irr}_{\alpha,F}(x)$. Com que el seu grau és un divisor de $[K\colon F]$, no pot ser divisible per p i, per tant, és separable. ■

Més endavant ens serà útil saber que que la separabilitat es comporta bé en torres. ::: {.lemma} Sigui $L/K/F$ una torre. Si L/F és separable, aleshores L/K i K/F també ho són. ::: ::: {.proof} Si L/F aleshores K/F és separable, trivialment. Per veure que L/K també ho és, observem simplement que per tot $\alpha \in L$, el polinomi $\mathrm{Irr}_{\alpha,K}(x)$ és un divisor (a $K[x]$) del polinomi $\mathrm{Irr}_{\alpha,F}(x)$. :::

Més endavant veurem que el recíproc també és cert, però per ara no ens caldrà.

5.2 Applicació : cossos finits

L'objectiu és demostrar l'existència de cossos finits d'ordre qualsevol potència d'un primer, i veure que són únics (llevat d'isomorfisme).

Teorema 5.2.1 — Existència i unicitat de cossos finits. Per tot primer p i tot $n \geq 1$, hi ha un únic (llevat d'isomorfisme) cos finit d'ordre p^n, que denotarem per $\mathbb{F}_{p^n}$. A més, si $\mathbb{F}$ és un cos finit de característica p, aleshores és isomorf a $\mathbb{F}_{p^n}$ per alguna $n \geq 1$.

Demostració. Sigui $n \geq 1$, i fixem-nos que el polinomi $f(x) = x^{p^n} - x \in \mathbb{F}_p[x]$ té derivada -1 i, per tant, és separable. Si α i β són dues arrels qualssevol, aleshores $\alpha\beta$ i $\alpha + \beta$ també són arrels. Per tant, el conjunt L format per les p^n arrels forma un subcos del cos de descomposició de $f(x)$ i, per tant, com que L conté totes les arrels, ha de ser el propi cos de descomposició. Com que L té p^n elements, té grau n sobre $\mathbb{F}_p$, i per tant hem vist que hi ha cossos finits de grau n per qualsevol $n \geq 1$.

Sigui ara $\mathbb{F}$ un cos finit qualsevol de característica p. Com que és un espai vectorial sobre el seu cos primer $\mathbb{F}_p$, ha de tenir p^n elements per algun $n \geq 1$. Fixem-nos que $\mathbb{F}^\times$ és un grup d'ordre $p^n - 1$ i, per tant $\alpha^{p^n-1} = 1$ per tot $\alpha \in \mathbb{F}$. Per tant α és una arrel de $x^{p^n} - x$ i $\mathbb{F}$ està contingut al cos de descomposició d'aquest polinomi. Mirant el nombre d'elements, veiem que és igual al cos de descomposició. ■

Fixem-nos que encara no hem sabut demostrar que existeixen polinomis irreductibles a $\mathbb{F}_p[x]$ de qualsevol grau. El que ens caldria és demostrar que l'extensió $\mathbb{F}_{p^n}/\mathbb{F}_p$ és *simple*, és a dir, que s'obté adjuntant l'arrel d'un polinomi irreductible. Això ho veurem més endavant, al Teorema **??**.

5.3 Polinomis Ciclotòmics

L'objectiu principal és demostrar que l'extensió ciclotòmica $\mathbb{Q}(\zeta_n)$ té grau $\varphi(n)$ (la phi d'Euler). Per això, introduïrem els polinomis ciclotòmics, veurem que són irreductibles i mònics i tenen coeficients enters.

Sigui μ_n el grup de les arrels n-èssimes de la unitat, que podem pensar dins de $\mathbb{C}$. Com a grup abstracte, és isomorf a $\mathbb{Z}/n\mathbb{Z}$ (un cop fixem una arrel primitiva ζ_n):

$$\mathbb{Z}/n\mathbb{Z} \to \mu_n, \quad a \mapsto \zeta_n^a.$$

Ja hem observat que les arrels primitives són exactament les de la forma ζ_n^a amb a coprimer amb n i que, per tant, n'hi ha $\varphi(n)$. Fixem-nos també que si $d \mid n$ aleshores $\mu_d \subseteq \mu_n$. Però fixem-nos que si $\zeta \in \mu_n$, aleshores ζ és una arrel primitiva d-èssima per algun $d \mid n$.

Definició 5.3.1 — polinomi ciclotòmic. El *polinomi ciclotòmic n-èssim* $\Phi_n(x)$ és el polinomi de grau $\varphi(n)$ que té per arrels les arrels primitives de la unitat:

$$\Phi_n(x) = \prod_{\substack{1 \le a \le n \\ \mathrm{mcd}(a,n)=1}} (x - \zeta_n^a).$$

Tenim la factorització

$$x^n - 1 = \prod_{\zeta \in \mu_n} (x - \zeta) = \prod_{d \mid n} \Phi_d(x).$$

En particular, comparant graus tenim la identitat

$$n = \sum_{d \mid n} \varphi(d).$$

A més, fixem-nos que la fórmula anterior ens permet calcular els polinomis ciclotòmics de manera recursiva, dividint pels factors coneguts:

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{\substack{d \mid n \\ d < n}} \Phi_d(x)}. \tag{5.1}$$

Els primers valors són, per exemple:

$$\begin{aligned}
\Phi_1(x) &= x - 1 & \Phi_2(x) &= x + 1 \\
\Phi_3(x) &= x^2 + x + 1 & \Phi_4(x) &= x^2 + 1 \\
\Phi_5(x) &= x^4 + x^3 + x^2 + x + 1 & \Phi_6(x) &= x^2 - x + 1 \\
\Phi_7(x) &= x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 & \Phi_8(x) &= x^4 + 1 \\
\Phi_9(x) &= x^6 + x^3 + 1 & \Phi_{10}(x) &= x^4 - x^3 + x^2 - x + 1
\end{aligned}$$

Lema 5.3.1 Els polinomis $\Phi_n(x)$ són mònics de grau $\varphi(n)$ i tenen coeficients enters.

Demostració. L'únic que ens cal veure és que $\Phi_n(x)$ té coeficients enters. Això es veu fàcilment per inducció en n i l'algoritme de divisió, fent servir la fórmula (5.1). ■

Amb una mica més de feina podem veure que també són irreductibles.

Teorema 5.3.2 Els polinomis $\Phi_n(x)$ són irreductibles.

Demostració. Prenem $n \geq 3$, i escrivim una factorització $\Phi_n(x) = f(x)g(x)$ amb $f(x)$ i $g(x)$ mònics a $\mathbb{Z}[x]$, i amb $f(x)$ irreductible de grau com a mínim 2. L'objectiu és demostrar que $f(x) = \Phi_n(x)$, és a dir, que tota arrel primitiva n-èssima és arrel de $f(x)$. Sigui doncs ζ una arrel n-èssima primitiva que sigui arrel de $f(x)$, i veurem que ζ^a també és arrel de $f(x)$ per a tot a coprimer amb n. N'hi ha prou amb veure-ho per $a = p$ un primer no dividint n, perquè aleshores podem iterar l'argument.

Com que ζ^p és una arrel primitiva de la unitat, ha de ser una arrel de $f(x)$ o de $g(x)$. Si $g(\zeta^p) = 0$, aleshores ζ és una arrel de $g(x^p)$. Per tant, a $\mathbb{Z}[x]$ tenim

$$g(x^p) = f(x)h(x).$$

Reduïnt mòdul p i fent servir el "Freshman's dream", tenim

$$(\bar{g}(x))^p = \bar{f}(x)\bar{h}(x) \text{ a } \mathbb{F}_p[x].$$

D'aquí en deduïm que $\bar{f}(x)$ i $\bar{g}(x)$ tenen un factor comú a $\mathbb{F}_p[x]$. Per tant, $\bar{\Phi}_n(x) = \bar{f}(x)\bar{g}(x)$ té un factor repetit, i com que $\Phi_n(x)$ divideix $x^n - 1$, també $x^n - 1$ té un factor repetit a $\mathbb{F}_p[x]$. Però ja hem vist que aquest polinomi no té factors repetits, i per tant tenim una contradicció. ■

Corol · lari 5.3.3 El cos ciclotòmic $\mathbb{Q}(\zeta_n)$ té grau $\varphi(n)$ sobre $\mathbb{Q}$.

6. La clausura algebraica

En aquest episodi demostrem l'existència i unicitat de la clausura algebraica d'un cos. Aprofitarem també per estudiar els polinomis ciclotòmics.

TODO: reorganitzar-ho.

6.1 La clausura algebraica

Definició 6.1.1 — clausura algebraica. Diem que $\bar{F}/F$ és una *clausura algebraica* d'F si $\bar{F}/F$ és algebraica i tot polinomi $f(x) \in F[x]$ descomposa completament a $\bar{F}$.

Definició 6.1.2 — algebraicament tancat. Un cos F és *algebraicament tancat* si és una clausura algebraica sobre si mateix. És a dir, si tot polinomi $f(x) \in F[x]$ té alguna arrel a F.

Aviat veurem que tot cos té alguna clausura algebraica, i que hi ha cossos algebraicament tancats. Veurem primer que les clausures algebraiques són algebraicament tancades.

Proposició 6.1.1 Sigui $\bar{F}/F$ una clausura algebraica de F. Aleshores $\bar{F}$ és algebricament tancat.

Demostració. Considerem un polinomi $f(x) \in \bar{F}[x]$, i considerem l'extensió $\bar{F}(\alpha)$ obtinguda adjuntant una arrel de $f(x)$ a $\bar{F}$. Aleshores $\bar{F}(\alpha)/\bar{F}/F$ és una torre algebraica, i per tant l'extensió total és algebraica. En particular, α és algebraic sobre F i, per tant, $\alpha \in \bar{F}$, com volíem demostrar. ■

El següent resultat ens permet trobar una clausura algebraica de qualsevol subcos d'un cos algebraicament tancat.

Proposició 6.1.2 Sigui K/F una extensió, i suposem que K és algebraicament tancada. Aleshores la subextensió $\bar{F}/F$ formada pels elements de K que són algebraics sobre F és una clausura algebraica de F .

Demostració. L'extensió $\bar{F}/F$ és algebraica per definició. Donat un polinomi $f(x) \in F[x]$, aquest trencarà completament a K en producte de polinomis de la forma $x - \alpha$. Però cadascun dels α és algebraic sobre F i, per tant, és un element de $\bar{F}$. Per tant $f(x)$ ja trencava completament a $\bar{F}[x]$, i per tant $\bar{F}$ és una clausura algebraica de F. ■

Cap al final del curs veurem una demostració del següent teorema, que també es pot demostrar amb mètodes analítics.

Teorema 6.1.3 — Teorema Fonamental de l'Àlgebra. El cos $\mathbb{C}$ dels nombres complexos és algebraicament tancat

Com a conseqüència, podrem clausures algebraiques de qualsevol extensió subextensió $\mathbb{C}/F/\mathbb{Q}$. En particular, el cos $\bar{\mathbb{Q}}$ format pels complexos algebraics és una clausura algebraica de $\mathbb{Q}$.

Donat un cos qualsevol F, tenim ara l'objectiu de construir una clausura algebraica $\bar{F}/F$. Intuitivament almenys, la idea és de considerar, per cada polinomi $g(x) \in F[x]$, un cos F_g que contingui totes les arrels de g. Aleshores hauríem de prendre el compositum de tots aquests cossos. El problema és que per fer el compositum hem de prendre una intersecció de molts cossos, i no està clar on viuen aquests cossos (la intersecció de conjunts només té sentit quan aquests conjunts són subconjunts d'un conjunt fixat). Fixem-nos que si només consideréssim un nombre finit de polinomis $g_1(x), \ldots, g_n(x)$ aleshores podríem prendre el cos de descomposició del producte $g_1(x) \cdots g_n(x)$.

Teorema 6.1.4 — existència de clausura algebraica. Sigui F un cos. Aleshores existeix una clausura algebraica $\bar{F}/F$.

Demostració. Considerem un conjunt $\mathcal{U} \supset F$ de cardinal estrictament superior a $\mathcal{N} = \max(\aleph_0, |K|)$.

Sigui

$$X = \{K \subseteq L \subseteq S \mid L/K \text{ és una extensió algebraica de } K\},$$

amb la relació d'ordre

$$K_2 > K_1 \iff K_2/K_1 \text{ és una extensió algebraica.}$$

Com que tota cadena té un element maximal (prenem la unió de totes les extensions), el lema de Zorn ens diu que hi ha un element maximal a X, que anomenarem $\bar{F}$. Només ens cal veure que $\bar{F}/F$ és una clausura algebraica. Sigui $f(x) \in F[x]$ un polinomi no constant, i suposem que no té cap zero a $\bar{F}$. Podem construir una extensió $L/\bar{F}$ on $f(x)$ tingui un zero. Aleshores L/F és algebraica, i per tant

$$|\bar{F}| \leq |L| \leq \mathcal{N}.$$

Per tant, $|S \setminus \bar{K}| = |S| > |L \setminus \bar{K}|$. Això fa que existeixi una aplicació (de conjunts) injectiva $i\colon L \to S$ tal que $i(x) = x$ si $x \in \bar{F}$. Podem doncs transportar l'estructura de cos de L a $i(L)$ i obtenim un nou element maximal $L > \bar{F}$, contradient la maximalitat de $\bar{F}$. ■

Una demostració alternativa: ::: {.proof} Presentem una demostració alternativa que amaga una mica més els problemes amb la teoria de conjunts. Gràcies a la Proposició 6.1.2, n'hi ha prou amb construir una extensió K/F algebraicament tancada.

Per cada polinomi mònic no constant $f = f(x) \in F[x]$, considerem una variable x_f. Tenim l'anell de polinomis en infinites variables $F[\{x_f\}]$, i hi podem considerar l'ideal I generat pels polinomis $f(x_f)$.

Veurem que I no és el total i que, per tant, està contingut en un ideal maximal $\mathcal{M}$. El quocient l'anomenem K_1, que és una extensió de F que conté **una arrel** de cada polinomi amb coeficients a F. Podem iterar el procés (començant amb K_1 en comptes de amb F) per obtenir K_2/K_1, una extensió on tot polinomi amb coeficients a K_1 té una arrel, i així construim una successió de cossos de la qual en podem prendre la seva "unió" K. Donat un polinomi $f(x) \in K[x]$, tots els seus coeficients viuen necessàriament a K_n i, per tant, $f(x)$ té alguna arrel a K_{n+1} i, per tant a K.

Ens queda per veure que I és un ideal propi. Suposem que no i arribarem a contradicció. Suposem que tenim una relació

$$g_1 f_1(x_{f_1}) + g_2 f_2(x_{f_2}) + \cdots + g_k f_k(x_{f_k}) = 1, \quad g_i \in F[\{x_f\}].$$

En total, aquesta relació només involucra un nombre finit de variables. Les hi posem nom: denotem $x_1 = x_{f_1}$, i així successivament fins a $x_k = x_{f_k}$. Després anomenem $x_{k+1}, \ldots, x_r$ la resta de variables que apareixen en els polinomis g_i, de manera que podem reescriure la relació anterior com

$$g_1(x_1, \ldots, x_r) f_1(x_1) + g_2(x_1, \ldots, x_r) f_2(x_2) + \cdots + g_k(x_1, \ldots x_r) f_k(x_k) = 1.$$

Prenem ara una extensió finita F'/F que contingui una arrel α_i de $f_i(x)$ per cada i. La relació anterior particularitza, si fem $x_i = \alpha_i$ per $i = 1, \ldots, k$ i $x_i = 0$ per $i > k$, a $0 = 1$, que és una contradicció. Això acaba la demostració. :::

Veurem ara la unicitat de la clausura algebraica.

Teorema 6.1.5 Sigui K/F una extensió algebraica, i sigui L/F una extensió algebraicament tancada. Aleshores existeix un F-morfisme $K \to L$.

Demostració. Considerem el conjunt de tots els morfismes $\varphi\colon K' \to L$, on $F \subseteq K' \subseteq K$. Aquest conjunt té un ordre parcial: $\varphi \leq \psi$ si i només si ψ extén φ. Podem aplicar fàcilment el lema de Zorn per obtenir un element maximal $\varphi\colon K' \to L$. Cal veure que $K' = K$. Però si no ho fos, podem prendre un element $\alpha \in K \setminus K'$, i estendre el morfisme φ a $K'(\alpha)$, ja que L té una arrel del polinomi mínim d'α, contradient la maximalitat de K'. ■

Corol · lari 6.1.6 — unicitat de la clausura algebraica. Siguin K/F i L/F clausures algebraiques de F. Aleshores $K \cong L$.

Demostració. Apliquem el teorema anterior i obtenim un F-morfisme $\varphi\colon K \to L$, que és injectiu. Sigui $\beta \in L$ un element qualsevol, i sigui $f(x)$ el seu polinomi mínim sobre F. Com que K és algebraicament tancat, conté totes les arrels de $f(x)$, i φ indueix una aplicació injectiva (i per tant exhaustiva) entre elles. Així, hi ha alguna arrel $\alpha \in K$ tal que $\varphi(\alpha) = \beta$, i hem demostrat que φ és exhaustiu. ■

R L'existència i unicitat de clausures algebraiques fou demostrada per Steinitz el 1910, i la demostració era molt més llarga i complicada (unes 20 pàgines).
També es pot demostrar (però ens cal teoria que veurem una mica més endavant) que el cos K_1 que apareix a la demostració anterior ja és algebraicament tancat, així que no caldria fer tots els altres infinits passos. La demostració d'aquest fet no és senzilla, fa servir el teorema de l'element primitiu (vegeu 10), i separa els casos de característica 0 i característica p.

7. Automorfismes

Començarem definint els automorfismes d'una extensió. Veurem que formen un grup, i que cada subgrup té associat el cos dels elements fixos per aquest. Veurem també que els automorfismes envien cada element α a una arrel de $\mathrm{Irr}(\alpha, x)$, i demostrarem que en una extensió normal el cardinal del grup d'automorfismes està fitat pel grau de l'extensió. Així, podrem definir una extensió de Galois com aquella on la fita s'assoleix.

7.1 Definició

Sigui K un cos. Un *automorfisme* de K és simplement un isomorfisme de K a K, i el grup d'automorfismes de K (amb la composició) s'escriu $\mathrm{Aut}(K)$.

Si $\alpha \in K$, diem que $\sigma \in \mathrm{Aut}(K)$ *fixa* α si $\sigma(\alpha) = \alpha$. Més en general, si S és un subconjunt de K, diem que $\sigma \in \mathrm{Aut}(K)$ *fixa* S si $\sigma(x) = x$ per a tot $x \in S$.

Fixem-nos també que tot automorfisme fixa el cos primer de K (exercici). En particular, $\mathrm{Aut}(\mathbb{Q}) = \mathrm{Aut}(\mathbb{F}_p) = 1$.

Un cas important de subconjunt S es dona quan tenim una extensió de cossos K/F. En aquest cas, escrivim $\mathrm{Aut}(K/F)$ com el grup d'automorfismes que fixen F (que és un subgrup d'$\mathrm{Aut}(K)$):

$$\mathrm{Aut}(K/F) = \{\sigma \in \mathrm{Aut}(K) \mid \sigma(x) = x \, \forall x \in F\}.$$

Proposició 7.1.1 Sigui K/F una extensió, i sigui $\alpha \in K$ un element algebraic sobre F. Aleshores per tot $\sigma \in \mathrm{Aut}(K/F)$ envia α a una arrel $\sigma(\alpha)$ de $\mathrm{Irr}(\alpha, F)(x)$.

Demostració. Com que $\mathrm{Irr}(\alpha, F)(x)$ té coeficients a F i σ és un morfisme de cossos, tenim

$$\mathrm{Irr}(\alpha, F)(\sigma(\alpha)) = \sigma(\mathrm{Irr}(\alpha, F)(\alpha)) = \sigma(0) = 0.$$

■

Corol · lari 7.1.2 Sigui $f(x) \in F[x]$ un polinomi irreductible i K/F és una extensió. Aleshores tot automorfisme $\sigma \in \mathrm{Aut}(K/F)$ permuta les arrels de $f(x)$ a K.

Corol · lari 7.1.3 Sigui K/F una extensió algebraica. Aleshores $\mathrm{Hom}_F(K, K) = \mathrm{Aut}(K/F)$.

Demostració. Sigui $\sigma \colon K \to K$ un morfisme que fixa F. Ja sabem que és injectiu, però volem veure que és exhaustiu. Si K/F és una extensió finita això ja ho sabem (per àlgebra lineal), però aquí ho volem veure en general. Sigui $\beta \in K$ qualsevol element. Considerem el conjunt

$$B = \{\text{arrels de } \mathrm{Irr}_{\beta,F}(x) \text{ a } K\}.$$

Aleshores σ indueix una aplicació injectiva al conjunt finit B i, per tant, també exhaustiva. Per tant hi ha $\alpha \in B \subseteq K$ tal que $\sigma(\alpha) = \beta$. ■

Aquests resultats ens permeten descriure el grup d'automorfismes d'extensions algebraiques considerant com actuen aquests automorfismes en els elements que generen l'extensió, ja que tot automorfisme quedarà únicament determinat per aquesta acció. En particular, quan K/F és finita el nombre d'automorfismes també serà finit.

■ **Exemple 7.1** Calculem $\mathrm{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{1, \sigma\}$ i $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/QQ) = 1$. ■

7.2 Cossos fixos

Fixem K un cos. Hem vist com associar a cada subcos $F \subseteq K$ un subgrup $\mathrm{Aut}(K/F)$ d'$\mathrm{Aut}(K)$. Prenem ara la direcció oposada. Associarem a cada subgrup d'automorfismes una certa extensió. Concretament, si $S \subseteq \mathrm{Aut}(K)$ és un subconjunt, podem considerar aquells elements de K que són fixos per tots els elements de S. És molt fàcil veure que aquest conjunt, que escriurem K^S i anomenarem el *cos fix per* S, és un subcos de K (exercici). Fixem-nos també que

$$K^S = K^{\langle S \rangle},$$

on $\langle S \rangle$ és el subgrup d'$\mathrm{Aut}(K)$ generat per S (el subgrup més petit que conté S). Per tant, normalment considerarem només cossos fixos per subgrups d'$\mathrm{Aut}(K)$ i no perdrem generalitat.

Lema 7.2.1 Sigui K un cos. - Si $F1 \subseteq F_2 \subseteq K$, aleshores $\mathrm{Aut}(K/F_2) \leq \mathrm{Aut}(K/F_1)$. - Si $H_1 \leq H_2 \leq \mathrm{Aut}(K)$, aleshores $K^{H_2} \subseteq K^{H_1}$.

Demostració. Trivial. ■

Lema 7.2.2 Sigui F un cos infinit, i sigui V un F-espai vectorial, i siguin $V_1, \ldots, V_r$ subespais propis. Aleshores $V \neq \bigcup V_i$.

Demostració. Fem inducció en la dimensió n de V. El cas $n = 1$ és trivial, així que podem assumir-ho cert per tot F-espai vectorial de dimensió $\leq n-1$ i ho demostrarem per V. Triem un subespai $U \subset V$ de dimensió $n-1$ diferent de tots els V_i (aquí utilitzem que F és infinit). Aleshores apliquem inducció als subespais $U \cap V_i$ d'U, i obtenim un element d'U que ja ens serveix. ■

R El lema també és cert quan V és de dimensió infinita (exercici), però no ens caldrà per les aplicacions.

Proposició 7.2.3 Sigui K/F una extensió finita, i siguin $K_1, \ldots, K_r$ subextensions diferents de K. Aleshores hi ha algun element de K que no pertany a cap dels K_i.

Demostració. Si F és infinit, ja estem pel lema anterior. Fem doncs el cas on F és finit. En aquest cas K també és finit, posem que té p^n elements. Aleshores els K_i també són finits, i

tenen p^i elements cadascun. Com que tots són diferents i hi ha un únic cos finit de cada cardinal, la unió dels K_i té com a molt

$$\sum_{j=0}^{n-1} p^j = \frac{p^n - 1}{p - 1}$$

elements, que és menor que p^n. ■

Teorema 7.2.4 Sigui K/F una extensió finita. Aleshores

$$|\operatorname{Aut}(K/F)| \leq [K\colon F].$$

En particular, $\operatorname{Aut}(K/F)$ és un grup finit.

Demostració. Suposem que $\operatorname{Aut}(K/F)$ conté $\sigma_1 = 1, \ldots, \sigma_n$ automorfismes diferents. Per cada $i \neq j$, considerem el conjunt

$$\operatorname{Eq}_{\sigma_i,\sigma_j} = \{x \in K \mid \sigma_i(x) = \sigma_j(x)\}.$$

És fàcil veure que $\operatorname{Eq}_{\sigma_i,\sigma_j} \subsetneq K$ i que $\operatorname{Eq}_{\sigma_i,\sigma_j}$ és un cos. Aplicant la proposició anterior, hi ha algun $\alpha \in K$ que no està en cap dels $\operatorname{Eq}_{\sigma_i,\sigma_j}$. El polinomi mínim d'$\alpha$ sobre F té arrels $\alpha, \sigma_2(\alpha), \ldots, \sigma_{n+1}(\alpha)$, que són totes diferents. Per tant $[F(\alpha)\colon F] \geq n$. Però $F(\alpha)$ és una subextensió de K i, per tant $[K\colon F] \geq n$. ■

Donarem un nom doncs a aquelles extensions que tinguin el nombre màxim d'automorfismes que permet aquesta fita.

Definició 7.2.1 — extensió de Galois. Sigui K/F una extensió finita. Diem que K *és Galois sobre* F (o que K/F és una *extensió de Galois*) si $|\operatorname{Aut}(K/F)| = [K\colon F]$. En aquest cas, escriurem $\operatorname{Gal}(K/F) = \operatorname{Aut}(K/F)$.

Corol·lari 7.2.5 Sigui K/F una extensió finita i Galois. Aleshores $K^{\operatorname{Gal}(K/F)} = F$.

Demostració. Escrivim $G = \operatorname{Gal}(K/F)$, i sigui $M = K^G \supseteq F$. Tenim, per definició, que $G = \operatorname{Aut}(K/M)$. Per tant, $[K\colon F] = |G| \leq [K\colon M]$, del que en deduim $F = M$. ■

Corol·lari 7.2.6 Sigui K/F una extensió finita i Galois. Aleshores hi ha un polinomi irreductible i separable $f(x) \in F[x]$ de grau $[K\colon F]$ que descomposa completament a K.

Demostració. Sigui $n = [K\colon F] = |\operatorname{Gal}(K/F)|$. A la demostració del teorema, prenem tots els n automorfismes, obtenint $\alpha \in K$ tal que $F(\alpha) = F$. El seu polinomi mínim $f(x) \in F[x]$ és irreductible, de grau n i té per arrels $\{\sigma(\alpha) \mid \sigma \in \operatorname{Aut}(K/F)\}$. Per tant té n arrels totes diferents, com volíem. ■

Les dues propietats de les extensions de Galois de fet les caracteritzen. Vegem una quarta caracterització d'aquestes extensions:

Teorema 7.2.7 — Caracterització d'extensions de Galois. Sigui K/F una extensió finita i sigui $G = \mathrm{Aut}(K/F)$. Aleshores els següents enunciats són equivalents: 1. $|G| = [K\colon F]$. 2. $F = K^G$. 3. K/F és normal i separable. 4. Hi ha un polinomi $f(x) \in F[x]$ irreductible i separable de grau $[K\colon F]$ que descomposa completament a K.

Demostració. Ja hem vist 1 $\implies$ 2 i 1 $\implies$ 4. Fixem-nos també que 4 $\implies$ 3 és obvi. - 2 $\implies$ 3: Suposem que $K = F(\alpha_1, \ldots, \alpha_m)$, i considerem el conjunt finit

$$B = \{\sigma(\alpha_i) \mid \sigma \in G, i = 1, \ldots, m\}.$$

Fixem-nos que no sabem quants elements exactament conté B. En tot cas, considerem el polinomi separable

$$f(x) = \prod_{\beta \in B} (z - \beta).$$

Observem que $\sigma(f) = f$ per a tot $\sigma \in G$ i, per tant, $f \in K^G[x] = F[x]$. Finalment, α_i és arrel de $f(x)$ per a tot $i = 1, \ldots, m$ i concloem que K és el cos de descomposició de $f(x)$.

- 3 $\implies$ 1: Suposem que K/F és el cos de descomposició d'un polinomi separable $f(x) \in F[x]$. Com s'ha indicat al Corol · lari 4.1.4, a cada pas podem prendre per α una arrel del polinomi $f(x)$ i per tant tindrem la igualtat.

■

R Suposem que K/F és de Galois, i sigui $\alpha \in K$ una arrel del polinomi $f(x)$ que apareix a la condició (4). Aleshores $K = F(\alpha)$. Veiem doncs que tota extensió finita de Galois és primitiva. Més endavant veurem que només cal que K/F sigui separable.

Si K/F és una extensió de Galois i $\alpha \in K$, els elements $\sigma(\alpha)$ (on $\sigma \in \mathrm{Gal}(K/F)$) s'anomenen *conjugats de Galois* d'α sobre F. Si $K/M/F$ és una subextensió, el cos $\sigma(M)$ s'anomena el conjugat de M per σ.

8. El Teorema Fonamental

Enunciem i demostrem el teorema fonamental de la teoria de Galois. Acabarem amb diversos exemples concrets d'extensions, il · lustrant la correspondència de Galois.

8.1 Preliminars

Proposició 8.1.1 Sigui K una cos qualsevol. Sigui $G \leq \mathrm{Aut}(K)$ un subgrup finit, i sigui $F = K^G$. Aleshores K és Galois sobre F, i $\mathrm{Gal}(K/F) = G$.

Demostració. Per definició d'F, tenim $G \leq \mathrm{Aut}(K/F)$, i només ens cal veure la igualtat. El teorema ens diu que $|G| = [K\colon F]$, i ja hem vist $|\mathrm{Aut}(K/F)| \leq [K\colon F]$. Per tant:

$$[K\colon F] = |G| \leq |\mathrm{Aut}(K/F)| \leq [K\colon F].$$

Per tant, totes les desigualtats són igualtats i, en particular $|G| = |\mathrm{Aut}(K/F)|$. ■

Corol · lari 8.1.2 Si G_1 i G_2 són subgrups diferents d'$\mathrm{Aut}(K)$, aleshores $K^{G_1} \neq K^{G_2}$.

Demostració. Trivial. ■

8.2 La correspondència de Galois

Sigui K/F una extensió finita de Galois. A cada subextensió K/M li podem associar el seu grup de Galois, $\mathrm{Gal}(K/M)$. També podem associar a cada subgrup $H \leq \mathrm{Gal}(K/F)$ el cos fix K^H. El següent resultat ens diu que aquestes dues operacions són inverses mútuament.

Teorema 8.2.1 Sigui K/F finita Galois. Aleshores $M \mapsto \mathrm{Gal}(K/M)$ i $H \mapsto K^H$ estableixen una bijecció

$$\{ \text{ subextensions } K/M/F\} \overset{1\colon 1}{\longleftrightarrow} \{ \text{ subgrups } H \leq \mathrm{Gal}(K/F)\}.$$

A més el grau $[M\colon F]$ es correspon amb l'ordre d'H.

Demostració. Hem de veure: 1. $K^{\mathrm{Gal}(K/M)} = M$. Això és automàtic a partir de la proposició i del Corol · lari 7.2.5. 2. $\mathrm{Gal}(K/K^H) = H$. Escrivim $M = K^H$. Ja sabem que K/M és de Galois, i $|\mathrm{Gal}(K/M)| = [K\colon M]$. A més, per definició tenim $H \leq \mathrm{Gal}(K/M)$. Hem de demostrar la igualtat: donat $\tau \in \mathrm{Gal}(K/M)$, veurem que $K = \bigcup_{\sigma\in H} \mathrm{Eq}(\sigma,\tau)$. Pel Lema 7.2.3, algun dels $\mathrm{Eq}(\sigma,\tau)$ ha de ser tot K, i això ens diu que $\tau \in H$. Per tant, només ens cal comprovar que per tot $\alpha \in K$, hi ha algun $\sigma \in H$ tal que $\sigma(\alpha) = \tau(\alpha)$. Considerem el polinomi

$$f(x) = \prod_{\sigma\in H} (x - \sigma(\alpha)) \in K[x].$$

Fixem-nos que $\sigma(f) = f$ per tot $\sigma \in H$ i per tant $f(x) \in K^H[x] = M[x]$. Com que τ fixa M, tenim que $\tau(f) = f$. Però aleshores $\tau(\alpha)$ ha de ser una arrel de f, és a dir, $\tau(\alpha) = \sigma(\alpha)$ per algun $\sigma \in H$, com volíem. ■

Hem vist que si $K/M/F$ és Galois aleshores K/M també ho és. Què podem dir de l'extensió M/F?

Proposició 8.2.2 Sigui $K/M/F$ una torre amb K/F Galois, posem $G = \mathrm{Gal}(K/F)$. Aleshores són equivalents:

1. M/F és Galois.
2. $H = \mathrm{Gal}(K/M)$ és un subgrup normal de G.
3. $\sigma(M) \subseteq M$ per a tot $\sigma \in G$.

En aquest cas, $\mathrm{Gal}(M/F) \cong G/H$.

Demostració. Sigui $H = \mathrm{Gal}(K/M)$. 1 $\implies$ 2: Sigui $\sigma \in G$. Si $\alpha \in M$ té polinomi mínim $f(x) \in F[x]$, aleshores σ en permuta les seves arrels i, en particular, $\sigma(\alpha) \in M$. Per tant σ restringeix a un morfisme de M, que ja hem vist que és un automorfisme. Hem construit doncs una aplicació $G \to H$, i és fàcil comprovar que és un morfisme de grups. El seu nucli és doncs un subgrup normal, format per aquells automorfismes $\sigma \in G$ que fixen M, és a dir, és justament $\mathrm{Gal}(K/M)$.

2 $\implies$ 3: Sigui $\sigma \in G$. Per definició, $\sigma(M) \in K^{\tilde{H}}$, on $\tilde{H} = \sigma H \sigma^{-1}$. Com que H és normal $\tilde{H} = H$ i $K^{\tilde{H}} = K^H = M$.

3 $\implies$ 1: escrivim $M = F(\alpha_1, \dots \alpha_n)$, i considerem

$$B = \{\sigma(\alpha_i) \mid \sigma \in G, i = 1, \dots, n\}.$$

Aleshores $f(x) = \prod_{\beta in B}(x - \beta)$ és un polinomi separable amb coeficients a F. La hipòtesi és que $B \subseteq M$ i, per tant, M és el cos de descomposició de f. ■

8.3 Operacions de reticle

Per acabar d'entendre bé la correspondència de Galois, relacionem operacions conegudes entre cossos i entre grups. ::: {.proposition name=" "} Sigui K/F Galois amb $G = \mathrm{Gal}(K/F)$. Sigui M_1 i M_2 dues subextensions, amb $H_i = \mathrm{Gal}(K/M_i)$. Aleshores:

1. $\mathrm{Gal}(K/M_1M_2) = H_1 \cap H_2$, i
2. $\mathrm{Gal}(K/(M_1 \cap M_2)) = \langle H_1, H_2 \rangle$. ::: ::: {.proof} Directa, per definició. :::

Podem resumir tot l'episodi en un sol resultat:

Teorema 8.3.1 — Teorema fonamental de la teoria de Galois. Sigui K/F una extensió de Galois finita amb grup de Galois G. Hi ha una bijecció entre

$$\{\text{subcossos } K/M/F\} \overset{1:1}{\longleftrightarrow} \{subgrups H \leq G\}$$

donada per $M \mapsto H = \mathrm{Gal}(K/M)$ i $H \mapsto M = K^H$ que satisfà:

1. (gira les inclusions) $M_1 \subseteq M_2$ si i només si $H_2 \leq H_1$.

2. (preserva els graus) $[K\colon M] = |H|$ i $[M\colon F] = [G\colon H]$.
3. (preserva normalitat) M/F és Galois si i només si H és normal en G.
4. (gira els reticles) $M_1M_2 \leftrightarrow H_1 \cap H_2$ i $M_1 \cap M_2 \leftrightarrow \langle H_1, H_2\rangle$.

8.4 Examples

Calculem alguns exemples, com $\mathbb{Q}(\sqrt{2},\sqrt{3})$, el cos de descomposició de $\sqrt[3]{2}$, $\mathbb{Q}(\sqrt{2}+\sqrt{3})$, o el cos de descomposició de $\mathbb{Q}(\sqrt[8]{2},\zeta_8)$ de $\sqrt[8]{2}$.

És important adonar-se que no n'hi ha prou en assignar valors als generadors d'una extensió per definir un automorfisme, ja que hi pot haver relacions amagades entre els generadors. Per exemple, si $\theta = \sqrt[8]{2}$, tenim $\theta^4 = \zeta_8 + \zeta_8^{-1}$ i per tant no totes les tries $\theta \mapsto \theta\zeta_8^i$ i $\zeta_8 \mapsto \theta_8^j$ amb j senar donen lloc a automorfismes.

9. Cossos Finits

Aplicarem el teorema fonamental de la teoria de Galois a l'estudi complet des cossos finits i les seves extensions. Sabem que per cada potència de primer p^n hi ha un únic cos amb p^n elements, que anomenem $\mathbb{F}_{p^n}$.

9.1 Grup de Galois

Ja vam definir $\mathbb{F}_{p^n}$ com el cos de descomposició del polinomi $x^{p^n} - x \in \mathbb{F}_p[x]$. Per tant, l'extensió $\mathbb{F}_{p^n}/\mathbb{F}_p$ és de Galois.

Lema 9.1.1 El grup $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ és cíclic d'ordre n, generat per l'automorfisme de Frobenius

$$\sigma\colon \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}, \quad \alpha \mapsto \sigma(\alpha) = \alpha^p.$$

Demostració. Fixem-nos que σ és un automorfisme, perquè és un endomorfisme injectiu d'un grup finit. També tenim $\sigma^i(x) = x^{p^i}$, i per tant σ té ordre n a $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$. Com que l'ordre d'aquest grup és $n = [\mathbb{F}_{p^n} : \mathbb{F}_p]$, obtenim el resultat. ■

9.2 Subcossos

El teorema fonamental ens diu que els subcossos de $\mathbb{F}_{p^n}$ estan en correspondència amb els subgrups de $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle\sigma\rangle$. Sabem de teoria de grups que per cada divisor $d \mid n$ hi ha exactament un subgrup d'índex d, que és el generat per σ^d. A més, tots els subgrups són normals (perquè és un grup abelià). Per tant, tenim:

Proposició 9.2.1 Si $d \mid n$, aleshores $\mathbb{F}_{p^d}$ és un subcos de $\mathbb{F}_{p^n}$. Recíprocament, si $\mathbb{F} \subseteq \mathbb{F}_{p^n}$ és un subcos, és de Galois, i $\mathbb{F} \cong \mathbb{F}_{p^d}$ amb $d \mid n$.

Vegem una aplicació fàcil d'aquest resultat: ::: {.corollary} El polinomi irreductible $\Phi_8(x) = x^4 + 1 \in \mathbb{Z}[x]$ és reductible mòdul qualsevol primer p. ::: ::: {.proof} Per $p = 2$, tenim $x^4 + 1 = (x+1)^4$. Suposem ara p senar. Com que $8 \mid p^2 - 1$ (mirem els quadrats senars mòdul 8), tenim que $x^8 - 1 = (x^4 - 1)(x^4 + 1)$ divideix a $x^{p^2-1} - 1$ a $\mathbb{Z}[x]$. Per tant, $x^4 + 1$ divideix també a $x^{p^2} - x$. Això vol dir que les arrels de $x^4 + 1$ viuen totes a $\mathbb{F}_{p^2}$. Però si fos irreductible, generaria una extensió de grau 4, contradicció. :::

9.3 Polinomis irreductibles

Ja hem vist que tota extensió de Galois és simple. Obtenim, per tant:

Proposició 9.3.1 L'extensió $\mathbb{F}_{p^n}/\mathbb{F}_p$ és simple. Equivalentment, per cada $n \geq 1$ existeix un

polinomi $f(x) \in \mathbb{F}_p[x]$ irreductible de grau n.

Podem trobar una fórmula explícita pel nombre de polinomis irreductibles de grau n. Ens caldrar primer demostrar un resultat útil sobre la factorització de $x^{p^n} - x \in \mathbb{F}_p[x]$.

Proposició 9.3.2 El polinomi $x^{p^n} - x$ és el producte de tots els polinomis irreductibles de grau d, per tots els $d \mid n$.

Demostració. Sigui $f(x)$ un polinomi irreductible de grau $d \mid n$. Aleshores l'extensió generada per f és de grau d sobre $\mathbb{F}_p$ i per tant és $\mathbb{F}_{p^d}$. Per tant, $f(x)$ és un divisor de $x^{p^d} - x$, que al seu torn divideix $x^{p^n} - x$.

Recíprocament, suposem que $f(x)$ és un factor irreductible de $x^{p^n} - x$, podem de grau d. Aleshores l'extensió que genera és un subcos de $\mathbb{F}_{p^n}$ i, per tant, té grau $d \mid n$. ■

Corol · lari 9.3.3 El nombre de polinomis irreductibles de grau n a $\mathbb{F}_p[x]$ és:

$$\Psi(n) = \frac{1}{n} \sum_{d|n} \mu(d) p^{n/d},$$

on μ és la funció de Möbius.

Demostració. Comptant els graus dels polinomis de la proposició anterior, obtenim

$$p^n = \sum_{d|n} d\Psi(d).$$

El resultat s'obté aplicant la fórmula d'inversió de Möbius. ■

9.4 La clausura algebraica d'$\mathbb{F}_p$

Ja hem vist que $\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^n}$ si i només si $d \mid n$. Per tant, donades dues extensions d'$\mathbb{F}_p$ com ara $\mathbb{F}_{p^n}$ i $\mathbb{F}_{p^m}$, podem pensar-les dins de $\mathbb{F}_{p^{nm}}$. Així, podem prendre la unió de totes elles i obtenir la clausura algebraica de manera explícita:

Proposició 9.4.1 Tenim

$$\overline{\mathbb{F}}_p = \bigcup_{n \geq 1} \mathbb{F}_{p^n}.$$

10. Element Primitiu

El primer objectiu és demostrar el teorema de l'element primitiu. Recordem que una extensió K/F és simple si hi ha algun $\alpha \in K$ tal que $K = F(\alpha)$.

Teorema 10.0.1 — caracterització d'extensions simples. Una extensió K/F és simple si i només si hi ha finites subextensions $K/M/F$.

Demostració. Suposem que $K = F(\alpha)F$ és simple, i sigui $f(x) = \mathrm{Irr}_{\alpha,F}(x)$. Considerem una subextensió $K/M/F$. Aleshores $g(x) = \mathrm{Irr}_{\alpha,M}(x)$ és un divisor de $f(x)$ pensats a $K[x]$. Sigui $M' \subseteq M$ l'extensió generada sobre F pels coeficients de $g(x)$. Com que $\mathrm{Irr}_{\alpha,M}(x) = \mathrm{Irr}_{\alpha,M'}(x)$, tenim $[K\colon M] = [K\colon M']$ i per tant $M = M'$. En conclusió, els subcossos M estan generats per coeficients dels factors irreductibles de $f(x)$ pensat com a polinomi a $K[x]$ i, per tant, n'hi ha un nombre finit.

Recíprocament, suposem que K/F té un nombre finit de subcossos. Gràcies a la Proposició 7.2.3, hi ha algun $\alpha \in K$ que no pertany a cap dels subcossos de K. Per tant, $F(\alpha) = K$. ■

10.1 El teorema de l'element primitiu

Amb aquesta caracterització i tot el què sabem fins ara podem demostrar fàcilment el teorema de l'element primitiu.

Teorema 10.1.1 — Element Primitiu. Si una extensió K/F és finita i separable, aleshores existeix $\gamma \in K$ tal que $K = F(\gamma)$.

Demostració. Sigui L/K una extensió tal que L/F sigui Galois. Per exemple, podem prendre el compositum de tots els cossos de descomposició dels polinomis mínims d'un conjunt de generadors de K/F. Aleshores L/F és primitiva i, pel criteri anterior, hi ha un nombre finit de subcossos de L. En particular, hi ha un nombre finit de subcossos de K i, un altre cop pel criteri anterior, l'extensió K/F és primitiva. ■

Podem generalitzar una mica aquest teorema:

Teorema 10.1.2 Suposem que $K = F(\alpha, \beta)$ i β és separable sobre F. Aleshores existeix $\gamma \in K$ tal que $K = F(\gamma)$.

Demostració. Si F és un cos finit, aleshores $F(\alpha, \beta)$ també és un cos finit i per tant sabem que és simple. Suposem doncs que F és infinit, i escrivim $f(x)$ i $g(x)$ pels polinomis mínims d'α i β, respectivament. Sigui $L/F(\alpha, \beta)$ un cos de descomposició per $f(x)g(x)$, i escrivim $\alpha = \alpha_1, \alpha_2, \dots \alpha_r$ per les arrels de $f(x)$ a L i $\beta = \beta_1, \beta_2, \dots, \beta_s$ per les arrels de $g(x)$ a L. Per cada i i per cada $j \neq 1$, l'equació

$$\alpha_i + X\beta_j = \alpha + X\beta_j$$

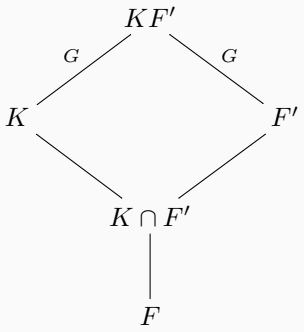
només té la solució $X = \frac{\alpha_i - \alpha}{\beta - \beta_j}$ (el denominador no és zero perquè $g(x)$ és separable). Per tant, com que F és infinit podem prendre $t \in F$ que no sigui cap de les solucions anteriors, i definim $\gamma = \alpha + t\beta$. Veurem que $F(\alpha, \beta) = F(\gamma)$. N'hi ha prou amb veure que $\beta \in F(\gamma)$, perquè aleshores $\alpha = \gamma - t\beta$ també hi serà. Considerem els polinomis a $g(x)$ i $h(x) = f(\gamma - tx)$ a $F(\gamma)$. Observem que $g(\beta) = 0$ i $h(\beta) = f(\gamma - t\beta) = f(\alpha) = 0$. Però les altres arrels de $g(x)$ són les β_j amb $j > 1$, i $h(\beta_j) \neq 0$ en aquest cas. Per tant, $\mathrm{mcd}(g(x), h(x)) = (x - \beta)$ i en deduim que $\beta \in F(\gamma)$, com volíem. ■

10.2 Galois i compositum d'extensions

Estudiem ara com es comporta la propietat de ser Galois quan prenem compositums.

Suposem que tenim extensions K/F i F'/F.

Proposició 10.2.1 Si K/F és de Galois, aleshores KF' és de Galois sobre F' i la restricció indueix un isomorfisme $\mathrm{Gal}(KF'/F') \cong \mathrm{Gal}(K/K \cap F')$:



En particular, si F'/F és finita, aleshores

$$[KF' : F] = \frac{[K : F][F' : F]}{[K \cap F' : F]}.$$

Demostració. Sabem que K és el cos de descomposició d'un polinomi separable $f(x) \in F[x]$. Aleshores, KF' és el cos de descomposició del mateix polinomi $f(x)$ ara pensat com a polinomi a $F'[x]$. Considerem ara el morfisme restricció

$$\varphi\colon \mathrm{Gal}(KF'/F') \to \mathrm{Gal}(K/F).$$

Està ben definit: donat $\sigma \in \mathrm{Gal}(KF'/F')$, com que F és un subcos de F' també fixa els elements de F, i per tant la seva restricció a K dona lloc a un element de $\mathrm{Gal}(K/F)$. Calcularem el nucli i la imatge de φ.

Si $\sigma \in \mathrm{Gal}(KF'/F')$, i suposem que $\sigma|_K = 1$, vol dir que σ fixa K. Com que també fixava F', fixa tot KF' i per tant és la identitat a $\mathrm{Gal}(KF'/F')$. Així doncs, φ és injectiva.

Sigui $H = \mathrm{Im}(\varphi) \leq \mathrm{Gal}(K/F)$ la imatge, i sigui $M = K^H$ el seu subcos fix. Volem veure que $M = K \cap F'$, i això ens donarà el resultat gràcies a la correspondència de Galois. Si $\sigma \in H$, aleshores σ fixa F'. Per tant, $K \cap F' \subseteq M$. D'altra banda, el compositum MF' és fix per tot $\sigma \in \mathrm{Gal}(KF'/F')$, ja que aquest σ fixa els elements de F' i en els elements de K hi actua via la restricció. Pel teorema fonamental, $MF' = F'$ i, per tant $M \subseteq F'$, d'on en traiem $K \cap F' = M$.

La fórmula final s'obté comptant graus d'extensions. ■

R Considerem $F = \mathbb{Q}$, $K = \mathbb{Q}(\sqrt[3]{2})$ (el nostre prototipus d'extensió no normal) i $F' = \mathbb{Q}(\zeta_3\sqrt[3]{2})$, on ζ_3 és una arrel cúbica primitiva de la unitat. Tenim $[K\colon F] = [F'\colon F] = 3$, i $KF' = \mathbb{Q}(\zeta_3, \sqrt[3]{2})$ té grau 6, per tant la igualtat no és certa si cap de les extensions inicials és de Galois.

Estudiem ara el cas on les dues extensions inicials són de Galois.

Proposició 10.2.2 Siguin K_1/F i K_2/F dues extensions de Galois amb grups G_1 i G_2. Aleshores K_1K_2/F i $K_1 \cap K_2/F$ són Galois, i la restricció a K_1 i a K_2 indueix un isomorfisme

$$\mathrm{Gal}(K_1K_2/F) \cong H = \{(\sigma,\tau) \in G_1 \times G_2 \mid \sigma|_{K_1\cap K_2} = \tau|_{K_1\cap K_2}\}.$$

En particular, si $K_1 \cap K_2 = F$, aleshores

$$\mathrm{Gal}(K_1K_2/F) \cong G_1 \times G_2.$$

Demostració. Suposem que K_i és el cos de descomposició del polinomi separable $f_i(x) \in F[x]$. Aleshores K_1K_2 és el cos de descomposició de la part lliure de quadrats de $f_1(x)f_2(x)$ i per tant K_1K_2 és Galois sobre F. Sigui ara $f(x)$ un polinomi irreductible a $F[x]$ amb una arrel a $K_1 \cap K_2$. Aleshores totes les arrels de $f(x)$ són a K_1 i també a K_2 i, per tant, a $K_1 \cap K_2$. Per tant, $K_1 \cap K_2$ és Galois.

Considerem ara l'aplicació

$$\varphi\colon \mathrm{Gal}(K_1K_2/F) \to G_1 \times G_2, \quad \sigma \mapsto (\sigma|_{K_1}, \sigma|_{K_2}).$$

És clarament injectiva, i per tant només ens cal estudiar la imatge. Clarament està continguda dins d'H, i per tant n'hi ha prou amb calcular els ordres. Pel primer teorema d'isomorfisme,

$$|\operatorname{Im}(\varphi)| = |\mathrm{Gal}(K_1K_2/F)| = [K_1K_2\colon F].$$

D'altra banda, fixem-nos que per cada $\sigma \in \mathrm{Gal}(K_1/F)$ hi ha $|\mathrm{Gal}(K_2/K_1 \cap K_2)|$ elements $\tau \in \mathrm{Gal}(K_2/K_1 \cap K_2)$ que satisfan $(\sigma,\tau) \in H$. Per tant:

$$|H| = |G_1||\mathrm{Gal}(K_2/K_1 \cap K_2)| = |G_1|\frac{|G_2|}{\mathrm{Gal}(K_1 \cap K_2/F)}$$

i la fórmula de la proposició anterior ens demostra $|H| = |\operatorname{Im}(\varphi)|$. ■

Podem demostrar un cert recíproc:

Proposició 10.2.3 Suposem que K/F és una extensió de Galois, i $G = \mathrm{Gal}(K/F) = G_1 \times G_2$. Aleshores K és el compositum de dues extensions de Galois K_1/F i K_2/F amb $K_1 \cap K_2 = F$ i grups de Galois G_1 i G_2, respectivament.

Demostració. Definim $K_1 = K^{G_1}$ i $K_2 = K^{G_2}$. Aleshores $K_1 \cap K_2$ correspon a $\langle G_1, G_2\rangle = G$, per tant $K_1 \cap K_2 = F$. El compositum correspon amb $G_1 \cap G_2 = 1$, i per tant $K_1K_2 = K$. ■

Corol · lari 10.2.4 — clausura de Galois. Sigui K/F una extensió finita separable. Aleshores hi ha una extensió $E/K/F$ tal que E/F és Galois$, i és mínima en el sentit que si E'/K és una extensió amb E'/F Galois, tenim $E \subseteq E'$. Aquesta extensió s'anomena la *clausura de Galois* de K/F.

Demostració. Ja sabem que hi ha extensions de K que són Galois (prenem el cos de descomposició dels polinomis mínims d'un conjunt de generadors de K). El cos E buscat és llavors la intersecció de totes les extensions E'/K tals que E'/F és Galois. Hem vist que aquesta intersecció serà Galois. ■

11. Extensions Abelianes i ciclotòmiques

En aquest apartat estudiem les extensions ciclotòmiques, i veiem que $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ és canònicament isomorf a $(\mathbb{Z}/n\mathbb{Z})^\times$. Com a aplicació, veurem com construir polígons regulars amb regle i compàs. Veurem que només és possible per polígons regulars de n costats quan φn és una potència de 2. Això passa si i només si n és producte d'una potència de dos i de primers de Fermat diferents.

11.1 Grup de Galois dels cossos ciclotòmics

Sigui $n \geq 2$ i considerem el cos ciclotòmic $\mathbb{Q}(\zeta_n)$. Volem estudiar $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. Per cada $a \in \mathbb{Z}$ coprimer amb n, definim l'aplicació

$$\sigma_a \colon \mathbb{Q}(\zeta_n) \to \mathbb{Q}(\zeta_n), \quad \zeta_n \mapsto \zeta_n^a.$$

Teorema 11.1.1 L'aplicació $a \mapsto \sigma_a$ indueix un isomorfisme

$$\psi \colon (\mathbb{Z}/n\mathbb{Z})^\times \to \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}).$$

Demostració. Ja sabem que $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ té exactament $\varphi(n)$ elements. Si σ és un d'aquests automorfismes, sabem que ve determinat per on envia ζ_n, que és una arrel del polinomi ciclotòmic $\Phi_n(x)$. Per tant, $\sigma(\zeta_n)$ és una arrel n-èssima primitiva de la unitat i doncs ha de ser ζ_n^a per alguna a coprimera amb n. Així veiem que $\sigma_a \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ i ψ és una aplicació ben definida i a més exhaustiva, per tant bijectiva. A més, ψ és un morfisme de grups, ja que

$$(\sigma_a\sigma_b)(\zeta_n) = \sigma_a(\zeta_n^b) = (\zeta_n^b)^a = \zeta_n^{ab} = \sigma_{ab}(\zeta_n).$$

■

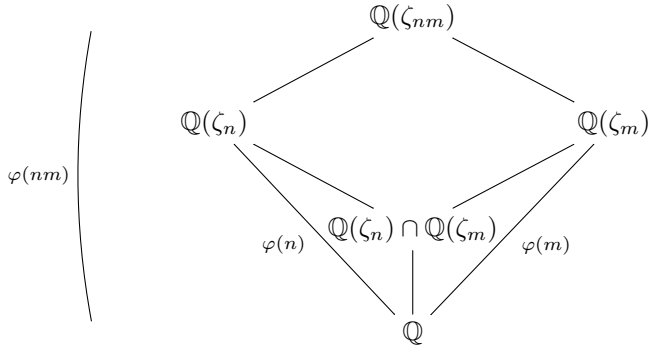
Fixem-nos que en particular tenim exemples d'extensions cícliques de grau $p-1$ per qualsevol primer p. També tenim una versió més conceptual del teorema xinès dels residus, que escrivim en el cas de dos factors per estalviar notació.

Proposició 11.1.2 Si n i m són coprimers, aleshores $\mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\zeta_m) = \mathbb{Q}$, $\mathbb{Q}(\zeta_n, \zeta_m) = \mathbb{Q}(\zeta_{nm})$, i

$$\mathrm{Gal}(\mathbb{Q}(\zeta_{nm})/\mathbb{Q}) \cong \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}).$$

Demostració. Tenim òbviament $\mathbb{Q}(\zeta_n) \subseteq \mathbb{Q}(\zeta_{nm})$ i $\mathbb{Q}(\zeta_m) \subseteq \mathbb{Q}(\zeta_{nm})$. Per tant el compositum també és un subcos. Però aquest compositum conté $\zeta_n\zeta_m$ i, per tant obtenim $\mathbb{Q}(\zeta_n, \zeta_m) = \mathbb{Q}(\zeta_{nm})$.

El diagrama



i la fórmula de les torres ens permet deduir que $\mathbb{Q}(\zeta_n)\cap\mathbb{Q}(\zeta_m)=\mathbb{Q}$. Per la Proposició 10.2.2, tenim $\mathrm{Gal}(\mathbb{Q}(\zeta_{mn})/\mathbb{Q})\cong\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})\times\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. ■

El següent lema ens permet trobar generadors dels subcossos de $\mathbb{Q}(\zeta_p)$ quan p és un primer. En aquest cas, la base formada pels elements $\zeta_p,\zeta_p^2,\ldots,\zeta_p^{p-1}$ és molt convenient (s'anomena una *base normal*) ja que els seus elements són els conjugats d'un de sol, per exemple ζ_p. Això és així perquè els elements d'aquesta base són tots ells arrels primitives, i els automorfismes de $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ les permuten.

Lema 11.1.3 Sigui p un primer, i sigui $H\leq\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ un subgrup. Aleshores

$$\theta_H=\sum_{\sigma\in H}\sigma(\zeta_p)$$

és un generador del cos fix d'H. L'element θ_H s'anomena un *període* de ζ_p.

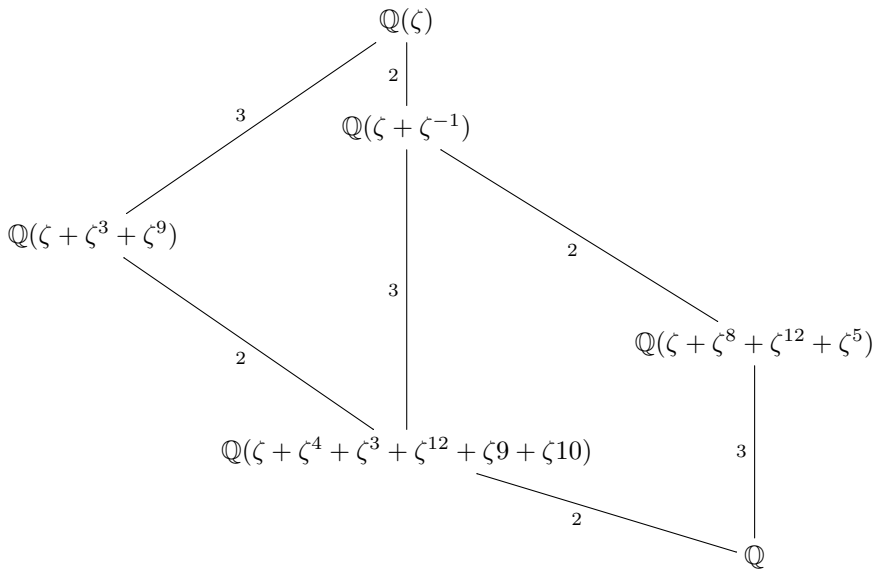
Demostració. Sigui $G=\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$. Primer de tot, observem que per tot $\tau\in H$, aleshores $\tau\theta_H=\theta_H$, ja que els summands simplement es permuten. Per tant, θ_H és un element del cos fix d'H. Pels comentaris del paràgraf anterior, $\tau(\theta_H)$ és una suma d'elements de la base normal, per qualsevol $\tau\in G$. Així, si $\tau\in G\setminus H$ i es donés el cas que $\tau(\theta_H)=\theta_H$, tindríem $\tau(\zeta_p)=\sigma(\zeta_p)$ per algun $\sigma\in H$. Però els automorfismes estan determinats per la seva acció a ζ_p, i per tant $\tau=\sigma$. Concloem que θ_H no és fix per cap automorfisme fora d'H, i per tant genera el cos fix per H. ■

■ **Exemple 11.1** Calcularem el reticle de subcossos de $\mathbb{Q}(\zeta_{13})$, fent servir el lema anterior. Hem de calcular $G=\mathrm{Gal}(\mathbb{Q}(\zeta_{13})/QQ)\cong(\mathbb{Z}/13\mathbb{Z})^\times$, que és un grup cíclic de 12 elements. Per exemple, un generador és el 2, ja que $2^4\equiv 3 \pmod{13}$ i $2^6\equiv 12 \pmod{13}$. Es correspon al generador de G que anomenarem σ, amb $\sigma(\zeta_p)=\zeta_p^2$.

Els subgrups no trivials de G tenen ordres 2, 3, 4 i 6, i venen generats per σ^6, σ^4, σ^3 i σ^2, respectivament. Aleshores podem calcular els θ_H corresponents, que són:

$$\begin{aligned}\zeta+\sigma^6(\zeta)&=\zeta+\zeta^{2^6}=\zeta+\zeta^{-1}\\ \zeta+\sigma^4(\zeta)+\sigma^8(\zeta)&=\zeta+\zeta^3+\zeta^9\\ \zeta+\sigma^3(\zeta)+\sigma^6(\zeta)+\sigma^9(\zeta)&=\zeta+\zeta^8+\zeta^{12}+\zeta^5\\ \zeta+\sigma^2(\zeta)+\sigma^4(\zeta)+\sigma^6(\zeta)+\sigma^8(\zeta)+\sigma^{10}(\zeta)&=\zeta+\zeta^4+\zeta^3+\zeta^{12}+\zeta 9+\zeta 10.\end{aligned}$$

Obtenim, finalment, el següent reticle de subcossos:



■

11.2 Extensions abelianes

Podem fer servir el què hem vist per demostrar el següent resultat. Necessitarem un resultat d'aritmètica:

Proposició 11.2.1 Sigui $m \geq 1$ un enter positiu. Aleshores existeixen infinits primers p tals que $p \equiv 1 \pmod{m}$.

Demostració. Ens caldà fer servir que $\Phi_m \in \mathbb{Z}[x]$ és mònic, i $\Phi_m(0) = 1$.

Suposem, donats $p_1, \ldots, p_k$ congruents amb 1 mòdul m. Trobarem un primer més gran que tots ells, que també serà $\equiv 1 \pmod{m}$. Considerem el producte $M = \ell m p_1 p_2 \cdots p_k$ on ℓ és suficientment gran com per què

$$T = \Phi_m(M) > 0.$$

Considerem un primer p que divideixi aquesta quantitat T. Com que $T \equiv 1 \pmod{M}$, el primer p no és cap dels p_i, i tampoc divideix m. Per definició, $\Phi_m(M) \equiv 0 \pmod{p}$, i per tant $M^m \equiv 1 \pmod{p}$. De fet, si $n \mid m$ amb $n < m$ aleshores $M^n \neq 1 \pmod{p}$ (per què?). Pel petit teorema de Fermat, $p - 1 \mid M$, és a dir, que $p \equiv 1 \pmod{M}$. Acabem de construir un nou primer congruent amb 1 mòdul M, com volíem. ■

Teorema 11.2.2 — realització de grups abelians. Sigui G un grup finit abelià. Aleshores hi ha una extensió $K/\mathbb{Q}$ continguda dins d'un cos ciclotòmic tal que $\mathrm{Gal}(K/\mathbb{Q}) \cong G$.

Demostració. Tot grup abelià és producte de cíclics:

$$G \cong C_{n_1} \times C_{n_2} \times \cdots \times C_{n_k}.$$

Per la proposició anterior, existeixen primers diferents $p_1, p_2, \ldots, p_k$ tals que $p_i \equiv 1 \pmod{n_i}$. Considerem $n = p_1 p_2 \cdots p_k$. Aleshores, tenim

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/(p_1-1))^\times \times (\mathbb{Z}/(p_2-1))^\times \times \cdots \times (\mathbb{Z}/(p_k-1))^\times.$$

Com que n_i divideix $p_i - 1$, hi ha un subgrup $H_i \leq C_{p_i-1}$ d'índex n_i per cada i, i el quocient per $H_1 \times H_2 \times \cdots \times H_k$ és isomorf a G. Per la correspondència de Galois, hi ha un subcos de $\mathbb{Q}(\zeta_n)$ que realitza G. ■

Els cossos ciclotòmics són exemples d'extensions de Galois amb grup abelià. En general, una extensió K/F es diu que té la propietat P si és de Galois i el seu grup de Galois té la propietat P. Per exemple, tenim la següent definició:

Definició 11.2.1 — extensió abeliana. Una extensió K/F és *abeliana* si K/F és de Galois i $\mathrm{Gal}(K/F)$ és un grup abelià.

El resultat anterior té un recíproc que no podem demostrar aquí:

Teorema 11.2.3 — Kronecker-Weber. Sigui $K/\mathbb{Q}$ una extensió finita abeliana. Aleshores K està contingut en una extensió ciclotòmica.

En general, és avui un problema obert el determinar quins grups apareixen quan com a grups de Galois d'extensions $K/\mathbb{Q}$. Ja hem vist que tots els grups abelians apareixen, però hi ha grups (per exemple $\mathrm{PSL}_2(\mathbb{F}_{125})$) pels quals no s'ha demostrat encara que hi apareguin. Aquest problema s'anomena el **problema invers de la teoria de Galois**.

11.3 Constructibilitat de polígons regulars

Com a aplicació dels cossos ciclotòmics, estudiarem quins polígons regulars es poden construir amb regle i compàs. Ja hem vist que un nombre real α és construible si i només si $\mathbb{Q}(\alpha)$ està contingut en un cos K obtingut a partir de $\mathbb{Q}$ a partir d'un nombre finit d'extensions quadràtiques.

Construir un polígon de n costats és equivalent a construir les arrels n-èssimes de la unitat ζ_n, que al seu torn és equivalent a construir la seva part real $x = \frac{1}{2}(\zeta_n + \zeta_n^{-1})$. Com que $\zeta_n^2 - 2x\zeta_n + 1 = 0$, el cos $\mathbb{Q}(zeta_n)$ és una extensió de grau 2 sobre $\mathbb{Q}(x)$ (aquesta última és real, mentre que $\mathbb{Q}(\zeta_n)$ no). Per tant, si volem que el cos $\mathbb{Q}(x)$ estigui dins de K ens cal en particular que el seu ordre $\varphi(n)/2$ sigui potència de 2, és a dir, que $\varphi(n)$ sigui potència de 2.

Recíprocament, si $\varphi(n)$ és una potència de 2, aleshores $\mathbb{Q}(x)$ té ordre una potència de 2. Prenent successivament subgrups d'índex 2 i fent servir la correspondència de Galois, obtenim una successió

$$\mathbb{Q} = K_0 \subset K_1 \subset \cdots \subset K_m = \mathbb{Q}(x), \quad [K_i \colon K_{i-1}] = 2,$$

i per tant x és constructible. D'aquí tenim la següent caracterització. Recordem que un primer p es diu *primer de Fermat* si $p - 1$ és una potència de 2.

Teorema 11.3.1 — construcció de polígons regulars. Sigui n un enter positiu. Aleshores el polígon regular de n costats és constructible amb regle i compàs si i només si n és de la forma

$$n = 2^k p_1 \cdots p_r,$$

on $k \geq 0$ i p_i són primers de Fermat diferents.

Demostració. Escrivim n com a producte de potències de primers diferents

$$n = 2^k q_1^{e_1} q_2^{e_2} \cdots q_r^{e_r}, \quad q_i \text{ senar.}$$

Aleshores tenim la fórmula coneguda

$$\varphi(n) = 2^{k-1} \prod_{i=1}^{r} (q_i - 1) q_i^{e_i - 1}.$$

Ja veiem que cal que $e_i = 1$ per tot i si volem que $\varphi(n)$ sigui potència de 2. A més, cal que $q_i - 1$ sigui potència de 2 per a tot i, és a dir que q_i sigui un primer de Fermat. ■

Només es coneixen cinc primers de Fermat: $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65537$. En general, si p és un primer de Fermat aleshores $p = 2^{2^i} + 1$ per algun $i \geq 0$. Els nombres $F_i = 2^{2^i} + 1$ s'anomenen *nombres de Fermat*. Sembla poc probable que hi hagi infinits primers de Fermat, però és encara un problema obert.

La següent expressió dona (en principi) una manera de construir un 17-gon regular amb regle i compàs.

$$\cos \frac{2\pi}{17} = \frac{1}{16} \left(\sqrt{17} - 1 + \sqrt{34 - 2\sqrt{17}} \right) + \frac{1}{8} \left(\sqrt{17 + 3\sqrt{17} - \sqrt{34 - 2\sqrt{17}} - 2\sqrt{34 + 2\sqrt{17}}} \right).$$

12. Grups de Polinomis

En aquest episodi estudiem els grups de Galois de polinomis separables, i veurem una demostració del Teorema Fonamental de l'Àlgebra.

12.1 Grup de Galois d'un polinomi

Definició 12.1.1 — grup de Galois d'un polinomi. Sigui $f(x) \in F[x]$ un polinomi separable amb coeficients a un cos F. El *grup de Galois d'*$f(x)$ és el grup de Galois del cos de descomposició de $f(x)$, que escriurem $\mathrm{Gal}(f)$.

Sigui K/F una extensió de Galois. Aleshores K és el cos de descomposició d'un polinomi separable $f(x) \in F[x]$. Com que les arrels de $f(x)$ generen K/F, tot element de $\mathrm{Gal}(K/F)$ ve determinat per on envia cadascuna de les arrels de $f(x)$, que necessàriament és una altra arrel. Així, si etiquetem les arrels de $f(x)$ com $\alpha_1, \ldots, \alpha_n$, obtenim un morfisme de grups injectiu

$$\mathrm{Gal}(K/F) \hookrightarrow S_n,$$

que ens permet pensar $\mathrm{Gal}(K/F)$ com un subgrup de S_n. De fet, si $f(x)$ no és irreductible i factoritza com

$$f(x) = f_1(x) \cdots f_k(x),$$

possiblement amb repetició, i $\deg(f_i(x)) = n_i$, aleshores

$$\mathrm{Gal}(K/F) \hookrightarrow S_{n_1} \times \cdots S_{n_k},$$

ja que els elements de $\mathrm{Gal}(K/F)$ permuten les arrels de cadascun dels $f_i(x)$ per separat.

R [] Suposem que $f(x)$ és irreductible. Aleshores el subgrup de $G \leq S_n$ que obtenim com a imatge de $\mathrm{Gal}(K/F)$ és *transitiu*: donats i, j, hi ha un element $g \in G$ tal que $g(i) = j$. Així, no tots els subgrups de S_n són possibles grups de Galois.

■ **Exemple 12.1** Calculem els grups de Galois $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ i $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ com a subgrups de S_4 i S_3, respectivament. ■

12.2 El grup de Galois del polinomi genèric

Fixem un cos F, i considerem el cos $F(s_1, \ldots, s_n)$, on s_i són indeterminades. Els elements d'aquest cos són quocients de polinomis en les variables s_i (s'anomenen funcions racionals). Considerem el polinomi

$$f(x) = x^n - s_1 x^{n-1} + s_2 x^{n-2} + \cdots + (-1)^n s_n \in F(s_1, \ldots, x_n),$$

que té arrels $x_1, \ldots, x_n$ que satisfan

$$\begin{aligned} s_1 &= x_1 + x_2 + \cdots + x_n \\ s_2 &= x_1x_2 + x_1x_3 + \cdots x_{n-1}x_n \\ &\cdots \\ s_n &= x_1x_2 \cdots x_n. \end{aligned}$$

El polinomi $f(x)$ s'anomena el *polinomi general de grau n*.

Teorema 12.2.1 El polinomi general de grau n és separable sobre $F(s_1, \ldots, s_n)$, amb grup de Galois S_n.

Demostració. El cos de descomposició del polinomi general de grau n $f(x)$ és justament $F(x_1, \ldots, x_n)$. Suposem que $p(t_1, \ldots, t_n)$ fos un polinomi en n variables i coeficients a F tal que $p(x_1, \ldots, x_n) = 0$. Aleshores podem prendre el producte de $p(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)})$ amb σ variant per tot S_n, i obtenim un polinomi simètric $\tilde{p}$ tal que $\tilde{p}(x_1, \ldots, x_n) = 0$. Però això donaria una relació no trivial entre $s_1, \ldots, s_n$, contradicció. ■

Aquest resultat es pot interpretar com que un polinomi "genèric" de grau n tindrà grup de Galois S_n. Tot i així, cal anar amb compte amb el significat de "genèric": per exemple, els grups de Galois d'un polinomi irreductible sobre un cos finit sempre és cíclic, així que no serà S_n si $n > 3$. Sí que és cert però que la "majoria" de polinomis sobre $\mathbb{Q}$ tenen grup de Galois S_n (en un cert sentit de "majoria").

Definició 12.2.1 — discriminant. El *discriminant* d'un polinomi de grau n amb arrels $x_1, \ldots, x_n$ és

$$\operatorname{disc}(f(x)) = \prod_{i<j}(x_i - x_j)^2.$$

Com que el discriminant és un polinomi simètric en les arrels de $f(x)$, es pot expressar en termes dels seus coeficients. En particular, el discriminant del polinomi general és un element $D \in F(s_1, \ldots, s_n)$.

Teorema 12.2.2 Sigui $f(x) \in F[x]$. Aleshores $\operatorname{Gal}(f)$ és un subgrup del grup alternat A_n si i només si $\operatorname{disc}(f(x))$ és el quadrat d'un element de F.

Demostració. Siguin $x_1, \ldots, x_n$ les arrels de $f(x)$, i sigui $D = \operatorname{disc}(f(x))$. Aleshores $\sqrt{D} = \prod_{i<j}(x_i - x_j)$ és un element del cos de descomposició de $f(x)$. Un element $\sigma \in S_n$ té signe parell si i només si preserva $\sqrt{D}$ (per definició del signe). Per tant, $\sqrt{D}$ és un element de F si i només si tot element de $\operatorname{Gal}(f)$ té signe parell, si i només si $\operatorname{Gal}(f)$ és un subgrup d'A_n. ■

12.3 El teorema fonamental de l'àlgebra

Demostrarem que $\mathbb{C} = \mathbb{R}(i)$ és algebraicament tancat, fent servir aquest fet bàsic sobre $\mathbb{R}$, que es demostra amb el teorema del valor mig:

Proposició 12.3.1 No hi ha cap extensió de $\mathbb{R}$ finita de grau senar > 1.

Demostració. És equivalent a veure que tot polinomi de grau senar amb coeficients reals té una arrel real. ■

Lema 12.3.2 No hi ha cap extensió de grau 2 de $\mathbb{C}$.

Demostració. Hem de veure que l'arrel quadrada d'un nombre complex també és complex. Això és un exercici senzill. Per exemple, si $\alpha = a + bi$, aleshores una arrel quadrada és de la forma

$$\sqrt{\frac{a+\sqrt{a^2+b^2}}{2}} \pm i\sqrt{\frac{-a+\sqrt{a^2+b^2}}{2}}.$$

■

Teorema 12.3.3 — Teorema Fonamental de l'Àlgebra. Sigui $K/\mathbb{R}$ una extensió finita. Aleshores $[K:\mathbb{R}] \leq 2$.

Demostració. Podem suposar (prenent la clausura de Galois) que $K/\mathbb{R}$ és finita Galois. Sigui $G = \mathrm{Gal}(K/\mathbb{R})$, i sigui $H \leq G$ un subgrup de 2-Sylow. Pel TFTG, el grau $[K^H:\mathbb{R}]$ és senar. Per tant, $K^H = \mathbb{R}$ i això vol dir que $H = G$, és a dir, que G és un 2-grup (té ordre una potència de 2).

Suposem doncs que $|G| \geq 4$, i arribarem a una contradicció. En aquest cas, hi ha subgrups $H_2 \leq H_1 \leq G$ amb $[G:H_i] = 2^i$. En termes de cossos fixos, hi ha una extensió de grau 2 de $K^{H_1} = \mathbb{C}$, que contradiu el lema anterior. ■

13. Arrels i radicals

Definirem què vol dir que un polinomi sigui resoluble per radicals, i veurem que és equivalent a què el seu grup de Galois sigui resoluble. D'aquí en podrem deduir que els polinomis generals de grau ≥ 5 no són resolubles per radicals i, per tant, no existeix una fórmula que expressi les arrels d'un polinomi en termes dels seus coeficients. També es mostrarà un exemple concret d'un polinomi de grau 5 sobre $\mathbb{Q}$ amb grup de Galois S_5.

13.1 Caràcters

En aquesta secció demostrarem un resultat d'àlgebra lineal que ens caldrà més endavant.

Definició 13.1.1 Un *caràcter* χ d'un grup G amb valors en un cos L és un morfisme de grups

$$\chi\colon G \to L^\times.$$

Podem pensar un caràcter χ com una funció $G \to L$. Les funcions de G a L formen un L-espai vectorial, de manera òbvia. El següent resultat és degut a Dedekind.

Teorema 13.1.1 — Independència lineal dels caràcters. Siguin $\chi_1, \ldots, \chi_n$ caràcters de G diferents. Aleshores són linealment independents, és a dir, no hi ha cap combinació lineal no trivial $a_1\chi_1 + \cdots + a_n\chi_n$ que doni lloc a la funció idènticament zero.

Demostració. Suposem (reordenant, si cal) que podem escriure

$$a_1\chi_1 + \cdots a_m\chi_m = 0,$$

amb tots els $a_i \neq 0$ (observem $m \leq n$) i amb m mínim. Obtindrem una relació de dependència amb menys termes, arribant així a contradicció.

Prenem $g_0 \in G$ tal que $\chi_1(g_0) \neq \chi_m(g_0)$. Aleshores tenim

$$a_1\chi_1(g) + \cdots a_m\chi_m(g) = 0,$$

i

$$a_1\chi_1(g_0g) + \cdots a_m\chi_m(g_0g) = 0.$$

Multiplicant la primera equació per $\chi_m(g_0)$ i restant-li la segona obtenim, per a tot g,

$$a_1(\chi_m(g_0) - \chi_1(g_0))\chi_1(g) + \cdots a_{m-1}(\chi_m(g_0) - \chi_{m-1}(g_0))\chi_{m-1}(g) = 0.$$

Com que el primer coeficient és diferent de zero, tenim una relació no trivial amb $m-1$ termes, contradicció. ∎

Un cas particular que ens interessa aquí prové de considerar un morfisme no trivial de cossos $\sigma\colon K \to L$, que indueix un morfisme de grups entre les unitats $\sigma\colon K^\times \to L^\times$ (aquesta restricció ja conté tota la informació que ens cal de σ, perquè ja sabem que $\sigma(0) = 0$). Aleshores σ esdevé un caràcter del grup $G = K^\times$, i per tant tenim el següent:

Corol · lari 13.1.2 Si $\sigma_1, \ldots, \sigma_n$ són morfismes diferents de K a L, aleshores són linealment independents com a funcions de K.

13.2 Extensions cícliques

Definició 13.2.1 — extensió cíclica. Una extensió K/F és *cíclica* si és Galois amb grup de galois cíclic.

Escriurem μ_n pel grup de les arrels n-èssimes de la unitat (en una clausura algebraica), i també escriurem $\sqrt[n]{a}$ per una arrel del polinomi $x^n - a$.

Proposició 13.2.1 Sigui F és un cos de característica no divisora de n que conté μ_n. Aleshores si $a \in F$ l'extensió $F(\sqrt[n]{a})$ és cíclica de grau un divisor de n.

Demostració. Escrivim $K = F(\sqrt[n]{a})$. Com que $\mu_n \subseteq F$, K és el cos de descomposició de $x^n - a$ i per tant és Galois. Sigui $\alpha = \sqrt[n]{a}$ una arrel fixada. Aleshores tot $\sigma \in \mathrm{Gal}(K/F)$ porta α a $\alpha\zeta_\sigma$, on $\zeta_\sigma \in \mu_n$ és una arrel n-èssima de la unitat que depèn de σ. Obtenim així una aplicació

$$\chi_a \colon \mathrm{Gal}(K/F) \to \mu_n, \quad \sigma \mapsto \zeta_\sigma = \frac{\sigma(\alpha)}{\alpha}.$$

Fixem-nos que χ_a no depèn de quina arrel α hem triat de $x^n - a$. Qualsevol altra arrel seria de la forma $\alpha\zeta$, i $\sigma(\alpha\zeta)/(\alpha\zeta) = \sigma(\alpha)/\alpha$ perquè σ fixa les arrels de la unitat. Fent servir això, és fàcil veure que aquesta aplicació és un morfisme de grups (és a dir, que $\zeta_{\sigma\tau} = \zeta_\sigma\zeta_\tau$), i el seu nucli està format per aquelles σ que fixen $\sqrt[n]{a}$, és a dir per la identitat. Per tant, $\mathrm{Gal}(K/F)$ és isomorf a un subgrup del grup cíclic μ_n, com volíem veure. ■

El recíproc resulta ser cert.

Proposició 13.2.2 Sigui F és un cos de característica no divisora de n que conté μ_n, i sigui K/F una extensió cíclica de grau n. Aleshores $K = F(\sqrt[n]{a})$ per algun $a \in F$.

Demostració. Escrivim $G = \langle\sigma\rangle$. Donat $\alpha \in K$ i $\zeta \in \mu_n$, definim la *resolvent de Lagrange* com

$$[\alpha, \zeta] = \sum_{i=0}^{n-1} \zeta^i \sigma^i(\alpha).$$

Fixem-nos que, com que σ fixa ζ, tenim:

$$\begin{aligned}\sigma([\alpha,\zeta]) &= \sum_{i=0}^{n-1} \zeta^i \sigma^{i+1}(\alpha) \\ &= \zeta^{-1}[\alpha,\zeta],\end{aligned}$$

i repetint el procés tenim $\sigma^i([\alpha,\zeta]) = \zeta^{-i}[\alpha,\zeta]$. També tenim que $\sigma([\alpha,\zeta]^n) = \zeta^{-n}[\alpha,\zeta]^n = [\alpha,\zeta]^n$. Per tant $[\alpha,\zeta]^n$ és un element de F. Si fixem una arrel primitiva ζ el Corol · lari 13.1.2 ens diu que els automorfismes $1, \sigma, \ldots, \sigma^{n-1}$ són linealment independents, i per tant que hi ha un element $\alpha \in K$ tal que $[\alpha,\zeta] \neq 0$. Com que $\sigma^i([\alpha,\zeta]) = \zeta^{-i}[\alpha,\zeta]$, aquest element no pot viure en cap subcos propi de K. Per tant, $K = F([\alpha,\zeta])$. A més, $[\alpha,\zeta]^n \in F$, per tant $K = F(\sqrt[n]{a})$ per algun $a \in F$, com volíem veure. ■

13.3 Solubilitat per radicals

Considerarem només cossos de característica zero, encara que n'hi hauria prou amb evitar les característiques que divideixin el grau de les extensions que prendrem.

Definició 13.3.1 — element resoluble per radicals. Un element α algebraic sobre F es diu que *es pot expressar amb radicals*, o *resoluble per radicals*, si $\alpha \in K$ on K es pot obtenir mitjançant una cadena d'extensions

$$F = K_0 \subset K_1 \subset \cdots \subset K_r = K, \quad K_{i+1} = K_i(\sqrt[n_i]{a_i}).$$

Direm que K és una *extensió radical* d'F.

Definició 13.3.2 — polinomi resoluble per radicals. Diem que un polinomi $f(x) \in F[x]$ és *resoluble per radicals* si totes les seves arrels són resolubles per radicals.

Com que afegir les arrels de la unitat dona lloc a una extensió radical, podem assumir sempre que F té les arrels de la unitat que vulguem. Per tant, podrem identificar extensions radicals amb extensions cícliques.

Lema 13.3.1 El compositum d'un nombre finit d'extensions radicals és una extensió radical.

Demostració. N'hi ha prou amb considerar el compositum de dues extensions radicals

$$F = K_0 \subset K_1 \subset \cdots \subset K_r = K \tag{13.1}$$
$$F = L_0 \subset L_1 \subset \cdots \subset L_s = L \tag{13.2}$$
$$\tag{13.3}$$

Fem inducció en $s \geq 0$, on el cas $s = 0$ és trivial. Considerem aleshores la

$$F = K_0L_1 \subseteq K_1L_1 \subseteq \cdots \subseteq KL_1.$$

Cadascuna de les extensions que hi apareixen és radical, per tant KL_1 és radical. Ara tenim l'extensió KL_1/F radical, i per hipòtesi d'inducció l'extensió KL/KL_1 és radical, per tant KL/F també ho és. ∎

Lema 13.3.2 Si α pertany a una extensió radical K/F, aleshores α pertany a una extensió radical K'/F on les extensions successives són cícliques.

Demostració. Prenem la clausura de Galois $L/K/F$ i considerem, per cada $\sigma \in \mathrm{Gal}(L/F)$, la cadena

$$F = \sigma(K_0) \subset \sigma(K_1) \subset \cdots \subset \sigma(K_r) = \sigma(K).$$

Les extensions intermitges també són simples radicals, generades per $\sigma(\sqrt[n_i]{a_i})$, que és una arrel polinomi $x^{n_i} - \sigma(a_i)$ amb coeficients a $\sigma(K_i)$. El compositum dels $\sigma(K)$ és L, i pel lema anterior L/F és radical.

Finalment, hem d'adjuntar totes les arrels n_i-èssimes que apareguin a la cadena radical per L/F, obtenint un nou cos F'. Composant amb la cadena per L/F obtenim:

$$F \subseteq F' = F'L_0 \subseteq F'L_1 \subseteq \cdots \subseteq F'L_r = F'L.$$

El primer sant és abelià i per tant es pot trencar en una cadena cíclica. Els altres salts són radicals simples però ara tenim les arrels del a unitat disponibles, i per tant sabem que són cícliques, i hem acabat. ■

Recordem que un grup finit G és *resoluble* si hi ha una cadena de subgrups

$$1 = G_r \leq G_{r-1} \leq \cdots \leq G_0 = G, \quad G_i/G_{i-1} \text{ cíclic.}$$

(es pot canviar cíclic per abelià, ja que donat un grup abelià sempre es pot trobar una cadena cíclica). També cal recordar que si $N \trianglelefteq G$ aleshores G és resoluble si i només si N i G/N ho són.

Teorema 13.3.3 — Galois. El polinomi $f(x)$ és resoluble per radicals si i només si $\mathrm{Gal}(f)$ és un grup resoluble.

Demostració. Suposem que $f(x)$ és resoluble per radicals. Cada arrel és resoluble i per tant està continguda en una extensió radical. El compositum de totes aquestes extensions, posem K/F, també és radical. Si prenem els subgrups de Galois $G_i = \mathrm{Gal}(K_i/F)$ de cadascun dels cossos de la cadena, com que $\mathrm{Gal}(K_{i+1}/K_i) = G_i/G_{i+1}$ és cíclic per tot i, en deduïm que $\mathrm{Gal}(K/F)$ és resoluble.

Recíprocament, suposem que $f(x)$ té cos de descomposició K/F, i que $G = \mathrm{Gal}(f) = \mathrm{Gal}(K/F)$ és resoluble. Els cossos fixos d'una cadena demostrant la resolubilitat de G donen lloc a una cadena d'extensions cícliques. Podem obtenir una nova cadena de cossos composant-la amb una extensió F'/F on s'adjuntin totes les arrels de la unitat necessàries. Aleshores les noves extensions intermitges són radicals simples, i per tant les arrels d'$f(x)$ estan contingudes en una extensió radical $F'K$. ■

Corol · Iari 13.3.4 El polinomi general de grau n no és resoluble per radicals, per cap $n \geq 5$.

Demostració. Cal saber que S_n no és resoluble per $n \geq 5$. ■

Aquest teorema diu que no podem trobar una fórmula general només fent servir radicals per les arrels d'una equació de grau $n \geq 5$. Però això no vol dir que no hi hagi polinomis pels quals no es pugui fer! Per exemple, $x^n - a$ és resoluble per radicals per qualsevol a, trivialment. Veurem ara com podem trobar polinomis de grau primer amb grup de Galois S_p.

Proposició 13.3.5 Sigui $f(x) \in \mathbb{Q}[x]$ un polinomi irreductible de grau p amb exactament $p-2$ arrels reals. Aleshores $\mathrm{Gal}(f) \cong S_p$.

Demostració. Sigui $G = \mathrm{Gal}(f)$, que el pensem com a subgrup de S_p. Siguin α i $\bar{\alpha}$ les dues arrels complexes de f. Com que f és irreductible de grau p, el cos de descomposició K té grau múltiple de p. Per tant, $|G|$ és divisible per p. Els únics elements de S_p d'ordre p són els p-cicles, així que G conté un p-cicle.

D'altra banda, la conjugació complexa restringeix a un element de G que fixa les arrels reals i intercanvia les dues arrels complexes. Per tant G conté una transposició. És un senzill exercici de permutacions demostrar que un p-cicle i una transposició qualsevol generen S_p quan p és primer. ■

Podem aplicar el resultat anterior al polinomi $f(x) = x^5 - 4x - 2$. Com que és 2-Eisenstein, és irreductible. A més, la seva derivada és $5x^4 - 4$, que té zeros a $x = \pm\frac{\sqrt{2}}{\sqrt[4]{5}}$. Deduïm que $f(x)$ té exactament tres zeros reals, que de fet podem aproximar: $-1.24359639\ldots, -0.50849948\ldots, 1.51851215\ldots$. Per tant, $\mathrm{Gal}(f) \cong S_5$, i concloem que no hi ha una fórmula per les arrels de $x^5 - 4x - 2$ que només faci servir arrels n-èssimes.

14. Càlcul explícit de grups de Galois

Hem vist com calcular el grup de Galois de polinomis de la forma $x^n - a$. En general, però, calcular el grup de Galois d'un polinomi donat és una tasca difícil. Ens conformarem doncs amb estudiar completament els polinomis de graus 3 i 4, i farem servir tot el que hem après per trobar fórmules per les seves arrels.

14.1 Polinomis cúbics

Trobarem la solució de la cúbica fent servir el què hem après fins ara. Primer determinarem el seu grup de Galois. Assumirem que la característica de F no és 2. Això ens cal perquè en general per un polinomi separable $f(x)$ de grau n tenim $\mathrm{Gal}(f) \leq A_n$ si i només si $\sqrt{\mathrm{disc}(f(x))} \in F$.

Sigui doncs $f(x) \in F[x]$ un polinomi separable de grau 3. Resulta que el discriminant ja determina el grup de Galois.

Teorema 14.1.1 Si $\mathrm{disc}(f(x))$ és un quadrat a F, aleshores $\mathrm{Gal}(f)$ és A_3. Si no, aleshores $\mathrm{Gal}(f) = S_3$.

Demostració. Els únics subgrups transitius de S_3 són S_3 i A_3, i ja sabem que $\sqrt{\mathrm{disc}(f)} \in F$ si i només si $\mathrm{Gal}(f) \leq A_3$. ■

R Si $f(x) \in Q[x]$ té $\mathrm{Gal}(f) = A_3$ aleshores totes les seves arrels generen el mateix cos cúbic. Com que com a mínim una de les arrels és real, totes ho han de ser. Però el recíproc no és cert. Per exemple, el polinomi $x^3 - 4x - 1$ té tres arrels reals, però el seu grup de Galois és S_3 perquè té discriminant 229, que no és un quadrat perfecte. Les seves tres arrels generen tres subcossos diferents de $\mathbb{R}$.

R La condició que f és irreductible és important! El polinomi $x^3-2x+1 = (x-1)(x^2+x-1)$ té discriminant 5 però grup de Galois A_3, mentre que el polinomi $x^3 - 7x - 6 = (x + 1)(x + 2)(x - 3)$ té discrimiant 20^2 i grup de Galois S_3.

Podem fer el resultat del teorema anterior més explícit. Si $\Delta = \mathrm{disc}(f(x))$ és el quadrat d'un element d'F, aleshores el cos de descomposició d'$f(x)$ s'obté simplement adjuntant una arrel α d'$f(x)$, i el cos que s'obté és Galois amb grup cíclic d'ordre 3. En canvi, si Δ no és un quadrat aleshores el cos de descomposició és $F(\alpha, \sqrt{D})$. Els generadors del grup de Galois són σ i τ,

$$\sigma(\theta) = \theta', \quad \sigma(\sqrt{\Delta}) = \sqrt{\Delta},$$

amb θ' una altra arrel d'$f(x)$, i

$$\tau(\theta) = \theta, \quad \tau(\sqrt{\Delta}) = -\sqrt{\Delta}.$$

Considerem ara un polinomi cubic reduït $f(x) = x^3 + px + q \in \mathbb{Q}[x]$. Donat un polinomi cúbic qualsevol, es pot posar en aquesta forma fent un canvi (completant el quadrat) sobre $\mathbb{Q}$, i al final podem recuperar les arrels originals desfent el canvi. Ja hem vist que el cos de descomposició és una extensió A_3 sobre $\mathbb{Q}(\sqrt{\Delta})$. Denotem per α, β, γ les tres arrels de $f(x)$, que satisfan que $\alpha + \beta + \gamma = 0$. Si adjuntem una arrel cúbica de la unitat $\zeta = \zeta_3$, aquesta extensió serà radical de grau 3, amb generador donat per la resolvent de Lagrange. Considerem doncs els elements

$$\begin{aligned}[\alpha, 1] &= \alpha + \beta + \gamma = 0\\ \theta_+ = [\alpha, \zeta] &= \alpha + \zeta\beta + \zeta^2\gamma\\ \theta_- = [\alpha, \zeta^2] &= \alpha + \zeta^2\beta + \zeta\gamma.\end{aligned}$$

Com que $1 + \zeta + \zeta^2 = 0$, tenim:

$$\begin{aligned}\theta_+ + \theta_- &= 3\alpha\\ \zeta^2\theta_+ + \zeta\theta_- &= 3\beta\\ \zeta\theta_+ + \zeta^2\theta_- &= 3\gamma.\end{aligned}$$

Per tant, si podem expressar θ_+ i θ_- en termes dels coeficients de $f(x)$ ja estarem.

Ja sabem en general que els cubs de les resolvents, $\theta_\pm^3$, viuen al cos base $\mathbb{Q}(\zeta, \sqrt{\Delta})$. Expandim $\theta_\pm^3$ i $\sqrt{\Delta} = (\alpha - \beta)(\alpha - \gamma)(\beta - \gamma)$ en termes de les arrels, i fent servir la teoria dels polinomis simètrics arribem a les expressions

$$\begin{aligned}\theta_+^3 &= \frac{-27q + 3\sqrt{-3\Delta}}{2}\\ \theta_-^3 &= \frac{-27q - 3\sqrt{-3\Delta}}{2}\end{aligned}$$

(hem triat els noms fent servir $\pm$ justament per això). Obtenim les solucions de la cúbica extraient les arrels cúbiques d'aquestes expressions. Fixem-nos que hi ha tres possibles arrels cúbiques en cada cas, i semblaria que obtindriem 9 solucions, que no té sentit. Però θ_+ i θ_- no són independents, ja que ja sabem que quan n'adjuntem una ja obtenim l'extensió total de grau 6. De fet, un càlcul semblant al què hem fet per trobar $\theta_\pm^3$ ens dona l'equació $\theta_+\theta_- = -3p$, i per tant només hem de triar una de les arrels cúbiques.

Finalment, si fem servir que $\Delta = -4p^3 - 27q^2$, i escrivim $C_\pm = \frac{1}{3}\sqrt[3]{\theta_\pm}$, tenim

$$\alpha = C_+ + C_-, \quad \beta = \zeta C_+ + \zeta^- 1 C_-, \quad \gamma = \zeta^- 1 C_+ + \zeta C_-,$$

amb $\zeta = \frac{-1+\sqrt{-3}}{2}$.

14.2 Polinomis quàrtics

Sigui $f(x) = x^4 + px^2 + qy + r \in F[x]$ un polinomi de grau 4 en forma reduïda i arrels $\alpha_1, \alpha_2, \alpha_3, \alpha_4$. Sigui $G = \mathrm{Gal}(f)$.

Suposem primer que $f(x)$ és reductible. Si té una arrel racional, aleshores estem en el cas del polinomi cúbic de l'apartat anterior. D'altra banda, si $f(x)$ és producte de dos quadràtics, aleshores el seu cos de descomposició és $K = F(\sqrt{D_1}, \sqrt{D_2})$, on els D_i són els discriminants dels polinomis quadràtics. Si el producte D_1D_2 és un quadrat perfecte, aquesta extensió s'anomena

biquadràtica, i G és isomorf a $V_4 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Si el producte és un quadrat perfecte, aleshores $K = F(\sqrt{D_1})$ és una extensió quadràtica.

Considerem ara el cas de $f(x)$ irreductible. Aleshores G és un subgrup transitiu de S_4, i hi ha les següents possibilitats: - S_4, - \$A_44, - $D_{2\times 4} = \{1, (1324), (12)(34), (1423), (13)(24), (14)(23), (12), (34)\}$ i els seus 3 conjugats, - $V_4 = \{1, (12)(34), (13)(24), (14)(23)\}$, o - $C_4 = \{1, (1234), (13)(24), (1432)\}$ i els seus 3 conjugats.

Considerem els elements

$$\begin{aligned}\theta_1 &= (\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4)\\ \theta_2 &= (\alpha_1 + \alpha_3)(\alpha_2 + \alpha_4)\\ \theta_3 &= (\alpha_1 + \alpha_4)(\alpha_2 + \alpha_3),\end{aligned}$$

tenim una acció de S_4 en el conjunt $\{\theta_1, \theta_2, \theta_3\}$, i el subgrup que els fixa tots tres és precisament V_4. Fixem-nos que les funcions simètriques elementals en els θ_i són fixes per tot G, i per tant viuen al cos base. Obtenim així el polinomi

$$h(x) = (x - \theta_1)(x - \theta_2)(x - \theta_3) = x^3 - 2px^2 + (p^2 - 4r)x + q^2,$$

que s'anomena la *resolvent cúbica* de $f(x)$. Comprant les definicions dels discriminants per $f(x)$ i $h(x)$, veiem que $\operatorname{disc}(f(x)) = \operatorname{disc}(h(x))$. En particular, trobem:

$$\Delta = \operatorname{disc}(f(x)) = \operatorname{disc}(h(x)) = -4p^3q^2 + 16p^4r - 27q^4 + 144pq^2r - 128p^2r^2 + 256r^3.$$

El següent resultat ens classifica G segons aquesta informació.

Teorema 14.2.1

1. Si $h(x)$ és irreductible, aleshores:
2. Si Δ no és un quadrat, $G = S_4$.
3. Si Δ és un quadrat, $G = A_4$.
4. Si $h(x)$ té exactament una arrel a F, aleshores:
5. Si $f(x)$ és irreductible a $F(\sqrt{\Delta})$, aleshores $G = D_{2\times 4}$.
6. Si no, aleshores $G = C_4$.
7. Si $h(x)$ té tres arrels a F, aleshores $G = V_4$.

Demostració. Si $h(x)$ és irreductible i D no és un quadrat, aleshores $G \not\leq A_4$ i $\operatorname{Gal}(h(x)) = S_3$. Per tant, $|G|$ és divisible per 6 i l'unica possibilitat és S_4.

Si $h(x)$ és irreductible i D és un quadrat, aleshores $G \leq A_4$, i a més $\operatorname{Gal}(h(x)) = A_3$, per tant $3 \mid |G|$ i l'única possibilitat és A_4.

Si $h(x)$ té tres arrels a F, aleshores G fixa θ_i per $i = 1, 2, 3$, i per tant $G \leq V$, d'on en treiem $G = V$

Finalment, si $h(x)$ té exactament una arrel, posem $\theta_1 \in F$, aleshores G fixa θ_1 però no intercanvia $\theta_2 \leftrightarrow \theta_3$. Això vol dir que $G \leq D_{2\times 4}$ i $G \not\leq V$. Per tant, $G = D_{2\times 4}$ o $G = C_4$. Per distingir-los, podem observar que $D_{2\times 4} \cap A_4 = V_4$ i $C_4 \cap A_4 = \{1, (13)(24)\}$, i aquest segon no és transitiu en les arrels de $f(x)$. Per tant el segon cas passa justament quan $h(x)$ factoritza sobre $F(\sqrt{\Delta})$, i ja hem cobert tots els casos. ■

Veiem ara com trobar les arrels explícitament, en el cas que $F = \mathbb{Q}$. Sigui K/F el cos de descomposició de $f(x)$, i sigui $E = \mathbb{Q}(\theta_1, \theta_2, \theta_3)$ el cos de descomposició de la resolvent cúbica $h(x)$. Aleshores $\mathrm{Gal}(K/E) \cong V_4$ i és per tant una extensió biquadràtica. Això vol dir que podem trobar les arrels α_i en termes d'arrels quadrades d'expressions en les θ_j. En aquest cas, com que $(\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4) = \theta_1$ i $(\alpha_1 + \alpha_2) + (\alpha_3 + \alpha_4) = 0$, obtenim la primera fila de la següent taula. Les altres files es fan igual:

$$\begin{aligned} \alpha_1 + \alpha_2 &= \sqrt{-\theta_1}, & \alpha_3 + \alpha_4 &= -\sqrt{-\theta_1}, \\ \alpha_1 + \alpha_3 &= \sqrt{-\theta_2}, & \alpha_2 + \alpha_4 &= -\sqrt{-\theta_2}, \\ \alpha_1 + \alpha_4 &= \sqrt{-\theta_3}, & \alpha_2 + \alpha_3 &= -\sqrt{-\theta_3}. \end{aligned}$$

Les arrels quadrades no són independents, ja que el producte $\sqrt{-\theta_1}\sqrt{-\theta_2}\sqrt{-\theta_3} = -q$ i per tant un cop triades dues arrels la tercera ja ve determinada. Amb aquestes sis equacions podem aïllar les α_i, per exemple $\alpha_1 = \frac{1}{2}(\sqrt{-\theta_1} + \sqrt{-\theta_2} + \sqrt{-\theta_3})$. Les θ_j són arrels d'una cúbica, que ja sabem resoldre.

15. Teoria de Galois infinita

Farem un esbós de com cal modificar els enunciats per adaptar el teorema fonamental de la Teoria de Galois a extensions infinites.

15.1 Definicions

Sigui K/F una extensió algebraica arbitraria. Per definir què vol dir *Galois*, no ens anirà bé mirar el cardinal d'$\mathrm{Aut}(K/F)$, perquè en general serà un grup infinita. En canvi, una de les caracteritzacions que hem trobat sí que generalitza bé.

Definició 15.1.1 L'extensió K/F és una *extensió de Galois* si és normal i separable. És a dir, si per tot $\alpha \in K$ el polinomi $\mathrm{Irr}_{\alpha,F}(x)$ descomposa completament a K en factors simples.

■ **Exemple 15.1** Podem donar els exemples de $\bar{\mathbb{Q}}/\mathbb{Q}$, de $\mathbb{Q}(\zeta_{p^\infty})$ i de $\bar{\mathbb{F}}_p/\mathbb{F}_p$. ■

Definició 15.1.2 — grup de Galois. Si K/F és de Galois, alhores el seu *grup de Galois* és el grup $\mathrm{Gal}(K/F)$ format pels automorfismes de K que fixen F.

Suposem a partir d'ara que L/K és un extensió de Galois (que pot ser infinita).

Lema 15.1.1 Sigui E/F una subextensió de L/K. Aleshores L/E també és de Galois.

Demostració. Sigui $\alpha \in L$. Aleshores $\mathrm{Irr}_{\alpha,E}(x)$ és un divisor de $\mathrm{Irr}_{\alpha,F}(x)$. Per tant, és separable i té totes les arrels a L. ■

Necessitem el següent resultat tècnic. ::: {.proposition} Sigui $K/M/F$ una subextensió, i sigui $\tilde{\sigma}\colon M \to K$ un F-morfisme. Aleshores existeix $\sigma \in \mathrm{Gal}(K/F)$ tal que $\sigma|_M = \tilde{\sigma}$. ::: ::: {.proof} Fem servir el Lema de Zorn. Donada una cadena d'extensions, podem prendre prendre com a element maximal la unió d'aquestes, i $\tilde{\sigma}$ hi extén. Si $\sigma'\colon L' \to L$ és l'element maximal donat per Zorn, volem veure que $L' = L$. Si no ho fos, prenem $\alpha \in L \setminus L'$ i extenem (ho podem fer perquè estem en el cas finit), cosa que és una contradicció.

Veiem que l'extensió σ és exhaustiva fent servir que permuta les arrels del polinomi mínim de qualsevol element. :::

Lema 15.1.2 Sigui E/F una subextensió finita i Galois de K. Aleshores la restricció indueix un morfisme de grups

$$\mathrm{res}\colon \mathrm{Gal}(K/F) \to \mathrm{Gal}(E/F)$$

que és exhaustiu.

Demostració. Només cal observar que si $\sigma \in \mathrm{Gal}(K/F)$ aleshores $\sigma(E) = E$, ja que σ permuta les arrels del polinomi mínim de qualsevol element d'E, i aquestes viuen totes a E. La proposició anterior ens dona l'exhaustivitat. ■

Donat un subgrup $H \leq \mathrm{Gal}(K/F)$, podem considerar el cos fix K^H. També donat una subcos $K/M/F$, podem considerar el subgrup $\mathrm{Gal}(K/M) \leq \mathrm{Gal}(K/F)$.

■ **Exemple 15.2** Considerem l'extensió de Galois infinita $\bar{\mathbb{F}}_p/\mathbb{F}_p$, i l'automorfisme $\pi\colon \bar{\mathbb{F}}_p \to \bar{\mathbb{F}}_p$, que envia $x \mapsto x^p$. El cos fix per π és $\mathbb{F}_p$. Veurem que $\mathbb{F}_p$ no està generat per π i per tant el teorema fonamental de la teoria de Galois no pot ser cert en aquest context.

Construirem un element de $\sigma \in \mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p)$ tal que $\sigma \neq \pi^n$ per cap n. Considerem l'extensió $M = \bigcup_{n\geq 1} \mathbb{F}_{p^{2n+1}}$, que és infinita i no conté $\mathbb{F}_{p^2}$, per tant no és tot $\bar{\mathbb{F}}_p$. Prenem $\alpha \in \bar{\mathbb{F}}_p \setminus M$ i considerem una arrel β conjugada d'α sobre M. Hi ha un element de $\mathrm{Gal}(M'/M)$ que envia $\alpha \mapsto \beta$ (M' el cos de descomposició de $\mathrm{Irr}_{\alpha,M}(x)$) i per tant, pel l'exhaustivitat de la restricció, trobem $\sigma \in \mathrm{Gal}(\bar{\mathbb{F}}_p/M)$ que envia $\alpha \mapsto \beta$. El cos fix per σ conté M, que és un cos infinit. En canvi, per cada n el cos fix per π^n és el cos finit de p^n elements. Per tant $\sigma \neq \pi^n$. ■

En l'apartat següent veurem com corregir aquest problema, que és que hi ha massa subgrups de subgrups, i no tots es poden correspondre a subextensions. Per tant, la solució consistirà en restringir els possibles subgrups que considerem.

15.2 La topologia de Krull

Ajuntant tots els morfismes restricció de l'apartat anterior, obtenim una aplicació

$$\iota\colon \mathrm{Gal}(K/F) \to \prod_{E/F \text{ finita Galois}} \mathrm{Gal}(E/F).$$

Aquest morfisme de grups és injectiu, ja que tot $\alpha \in K$ viu en una extensió finita i Galois (per exemple, la clausura de Galois de $F(\alpha)/F$). La imatge de ι està formada per aquells elements $(\sigma_E)_E$ del producte cartesià tals que $(\sigma_E)|_{E'} = \sigma_{E'}$ per a tota parella de subextensions finites Galois $E' \subset E$.

Els grups que apareixen a la dreta són tots finits, i podem considerar la topologia discreta en cadascun d'ells. Aleshores podem posar la topologia del producte en el producte (infinit), i com que $\mathrm{Gal}(K/F)$ s'identifica amb un subconjunt, li podem donar la topologia del subespai.

Definició 15.2.1 — topologia de Krull. La *topologia de Krull* a $\mathrm{Gal}(K/F)$ és la topologia obtinguda amb el procediment anterior.

Proposició 15.2.1 Els conjunts

$$U_{\sigma,E} = \{\tau \in \mathrm{Gal}(K/F) \mid \tau|_E = \sigma|_E\},$$

on E recorre les subextensions finites Galois E/F formen una base d'entorns de σ.

Demostració. Veiem primer que si E_0/F és una subextensió finita Galois aleshores U_{σ,E_0} és un obert. El conjunt

$$V_{\sigma,E_0} = \{\sigma|_{E_0}\} \times \prod_{E\neq E_0} \mathrm{Gal}(K/E) \subseteq \prod \mathrm{Gal}(K/E)$$

és un obert, i satisfà

$$\iota(U_{\sigma,E_0}) = V_{\sigma,E_0} \cap \iota(\mathrm{Gal}(K/F)).$$

Ara només ens cal veure que, donat un obert qualsevol V, podem trobar σ i E_0 tal que $U_{\sigma,E_0} \subseteq V$. N'hi ha prou amb veure-ho per una base d'oberts del producte, és a dir, podem pensar que $\iota(V)$ és de la forma

$$\iota(V) = V_{E_1} \times V_{E_2} \times \cdots V_{E_k} \times \prod_{E \neq E_i} \mathrm{Gal}(K/E).$$

Prenem $\sigma \in V \subseteq \mathrm{Gal}(K/F)$ i considerem $E_0 = E_1E_2 \cdots E_k$. Aleshores

$$\iota(\sigma) \in \iota(U_{\sigma,E_0}) \subseteq \{\sigma|_{E_1}\} \times \{\sigma|_{E_2}\} \times \cdots \times \{\sigma|_{E_1}\} \times \prod_{E \neq E_i} \mathrm{Gal}(E/F).$$

■

Proposició 15.2.2 El grup $\mathrm{Gal}(K/F)$ és tancat a $\prod_{E/F} \mathrm{Gal}(E/F)$.

Demostració. Sigui $(\sigma_E)_E$ un element del producte que no ve de $\mathrm{Gal}(K/F)$. Això vol dir que hi ha extensions finites $E_0 \subseteq E_1$ tals que $(\sigma_{E_1})|_{E_0} \neq \sigma_{E_0}$. Aleshores el conjunt

$$\{\sigma_{E_0}\} \times \{\sigma_{E_1}\} \times \prod_{E \neq E_0, E_1} \mathrm{Gal}(E/K)$$

és un obert que conté $(\sigma_E)_E$ i no interseca la imatge de $\mathrm{Gal}(K/F)$. ■

Corol · lari 15.2.3 El grup $\mathrm{Gal}(K/F)$ és compacte.

Demostració. Pel teorema de Tychonoff, el producte infinit és compacte, i un subespai tancat d'un compacte és compacte. ■

Això ens permet donar una condició necessària per ser grup de Galois d'una subextensió:

Proposició 15.2.4 Sigui M/F una subextensió de L/K. Aleshores $\mathrm{Gal}(K/M)$ és tancat a $\mathrm{Gal}(K/F)$.

Demostració. Veurem que el complementari és obert. Sigui $\sigma \in \mathrm{Gal}(K/F) \setminus \mathrm{Gal}(K/M)$. Per tant, existeix $\alpha \in M \setminus F$ tal que $\sigma(\alpha) \neq \alpha$. Sigui E/F una extensió finita Galois que contingui α. Aleshores

$$U_{\sigma,E} \subseteq \mathrm{Gal}(K/F) \setminus \mathrm{Gal}(K/M).$$

En efecte, si $\tau \in U_{\sigma,E}$, vol dir que $\tau(\alpha) \neq \alpha$, i per tant $\tau \notin \mathrm{Gal}(K/M)$. ■

A l'apartat següent veurem que aquesta condició també és suficient.

15.3 El teorema

Teorema 15.3.1 — teorema fonamental de la teoria de Galois infinita. Sigui K/F una extensió de

Galois. La correspondència de Galois estableix una bijecció entre els subcossos $K/M/F$ i els subgrups *tancats* de $\mathrm{Gal}(K/F)$.

Demostració. L'únic que no és obvi és el fet, donat un subgrup tancat H, si definim $M = K^H$ aleshores $\mathrm{Gal}(K/M) = H$. De fet, la inclusió $\supseteq$ és trivial, i només cal veure $\subseteq$.

Sigui $\sigma \in \mathrm{Gal}(K/M)$. Veurem que $U_{\sigma,E} \cap H \neq \emptyset$ per tota extensió finita Galois E/F. Això voldrà dir que $\sigma \in \overline{H}$ i, com que H és tancat, $\sigma \in H$.

Per veure que $U_{\sigma,E} \cap H \neq \emptyset$, considerem el cos $E' = EM$, que és una extensió finita Galois de M. N'hi haurà prou amb veure $U_{\sigma,E'} \cap H \neq \emptyset$, ja que $U_{\sigma,E'} \subseteq U_{\sigma,E}$. En aquest cas, la restricció $H \to \mathrm{Gal}(E'/M)$ és exhaustiva. Per tant tenim $\mathrm{res}(H) = \mathrm{res}(\mathrm{Gal}(K/M))$. És a dir, per tot $\sigma \in \mathrm{Gal}(K/M)$, hi ha $\tau \in H$ tal que $\sigma|_{E'} = \tau|_{E'}$. Per tant, $\tau \in U_{\sigma,E'} \cap H$. ■

La correspondència de Galois gira els reticles (la demostració és igual que en el cas finit), i a més satisfà les següents propietats:

Proposició 15.3.2

1. Un subgrup tancat $H \leq \mathrm{Gal}(K/F)$ és obert si i només si té índex finit, i aleshores
$$[\mathrm{Gal}(K/F) \colon H] = [K^H \colon F].$$
2. Un subgrup tancat $H \leq \mathrm{Gal}(K/F)$ és normal si i només si K^H/F és Galois, i aleshores
$$\mathrm{Gal}(K^H/F) \cong \mathrm{Gal}(K/F)/H.$$

Demostració.

1. Si H és d'índex finit, llavors $\mathrm{Gal}(K/F) = \bigcup_\sigma \sigma(H)$, on σ recorre un conjunt (finit) de representants de les classes laterals d'H (assumim que un dels representants és 1). Per tant, el complementari d'H està format per una unió finita de tancats (σ és tancada, perquè és un automorfisme continu) i per tant és un tancat (i H és un obert).

Recíprocament, si H és obert llavors el complementari és tancat i per tant compacte (ja hem vist que $\mathrm{Gal}(K/F)$ és compacte). Tenim un recobriment per oberts del complementari com a $\bigcup_{\sigma \neq 1} \sigma(H)$ i, per compacitat, hi ha un subrecobriment finit. Això vol dir que $\mathrm{Gal}(K/F)$ és una unió finita de classes laterals d'H i per tant H té índex finit. 2. Definim $E = K^H$. Donats automorfismes $\sigma, \tau \in \mathrm{Gal}(K/F)$, i donat $\alpha \in K$, tenim

$$\tau\alpha = \alpha \iff \sigma\tau\sigma^{-1}(\sigma\alpha) = \sigma(\alpha).$$

Per tant, $\mathrm{Gal}(K/\sigma(E)) = \sigma\,\mathrm{Gal}(K/E)\sigma^{-1} = \sigma H \sigma^{-1}$. D'aquí en traiem que H és normal si i només si $\sigma(E) = E$ per tot $\sigma \in \mathrm{Gal}(K/F)$, i això és equivalent a que E/F sigui Galois. L'isomorfisme es demostra igual que en el cas finit.

■

■ **Exemple 15.3 — grup de Galois de $\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}$.** Considerem la unió infinita $K = \bigcup_{n\geq 1} \mathbb{Q}(\zeta_{p^n})$. Es té un morfisme injectiu

$$\iota \colon \mathrm{Gal}(K/\mathbb{Q}) \hookrightarrow \prod_{n\geq 1} \mathrm{Gal}(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}) \cong \prod_{n\geq 1} (\mathbb{Z}/p^n\mathbb{Z})^\times,$$

on la última identificació ve de fer correspondre $a_n \in (\mathbb{Z}/p^n\mathbb{Z})^\times$ amb $\sigma_{a_n}\colon \zeta_{p^n} \mapsto \zeta_{p^n}^{a_n}$. La imatge de ι està formada per aquells elements $(\sigma_{a_n})_n$ del producte que són compatibles amb la restricció.

$$\sigma_{a_{n+1}}(\zeta_{p^{n+1}}) = \zeta_{p^{n+1}}^{a_{n+1}} \implies \sigma_{a_{n+1}}(\zeta_{p^n}) = \zeta_{p^n}^{a_{n+1}},$$

i per tant la condició de ser compatible amb la restricció és equivalent a la condició $a_{n+1} \equiv a_n \pmod{p^n}$. Concloem que

$$\mathrm{Gal}(K/\mathbb{Q}) \cong \{(a_n)_{n\geq 1} \in \prod_{n\geq 1} (\mathbb{Z}/p^n\mathbb{Z})^\times \mid a_{n+1} \equiv a_n \pmod{p^n}\} = \mathbb{Z}_p^\times,$$

on el grup $\mathbb{Z}_p^\times$ és el grup d'unitats de l'anell dels enters p-àdics. Fixem-nos que aquest grup és no-numerable, mentre que hi ha una quantitat numerable de subcossos de K. ∎

∎ **Exemple 15.4 — grup de Galois de $\bar{\mathbb{F}}_p/\mathbb{F}_p$.** Considerem en aquest cas l'extensió $\bar{\mathbb{F}}_p/\mathbb{F}_p$, on $\bar{\mathbb{F}}_p = \bigcup_{n\geq 1} \mathbb{F}_{p^n}$. Tenim un morfisme injectiu

$$\iota\colon \mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p) \hookrightarrow \prod_{n\geq 1} \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong \prod_{n\geq 1} \mathbb{Z}/n\mathbb{Z},$$

fent correspondre $a \in \mathbb{Z}/n\mathbb{Z}$ amb la potència del Frobenius π^a. Si $n \mid m$, hi ha el morfisme de restricció

$$\mathrm{Gal}(\mathbb{F}_{p^m}/\mathbb{F}_p) \to \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p),$$

que es correspon amb l'aplicació natural $\mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$. Per tant,

$$\mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p) \cong \{(a_n)_n \in \prod_{n\geq 1} \mathbb{Z}/n\mathbb{Z} \mid \forall n \mid m, a_m \equiv a_n \pmod{n}\} = \hat{\mathbb{Z}},$$

on $\hat{Z} \cong \prod_p \mathbb{Z}_p$ és la *completació finita* dels enters. ∎

Bibliografia

Artin, Michael. 2014. *Algebra / Michael Artin.* 2nd ed., new international ed. Edinbourgh Gate, Harlow, Essex: Pearson.

Dummit, David S., and Richard M. Foote. 2004. *Abstract Algebra.* 3rd ed. New York: Wiley.

Geck, Meinolf. 2014. "On the Characterization of Galois Extensions." *Amer. Math. Monthly* 121 (7): 637–39. https://doi.org/10.4169/amer.math.monthly.121.07.637.

Jelonek, Zbigniew. 1993. "A Simple Proof of the Existence of the Algebraic Closure of a Field." *Univ. Iagel. Acta Math.*, no. 30: 131–32.

Rotman, Joseph J. 2015. *Advanced Modern Algebra. Part 1.* Third. Vol. 165. Graduate Studies in Mathematics. American Mathematical Society, Providence, RI. https://doi.org/10.1090/gsm/165.

Weintraub, Steven H. 2021. "The Theorem of the Primitive Element." *Amer. Math. Monthly* 128 (8): 753–54. https://doi.org/10.1080/00029890.2021.1944757.