APUNTS D'EQUACIONS ALGEBRAIQUES

XEVI GUITART

Resum. Apunts de l'assignatura Equacions Algebraiques de la Universitat de Barcelona, curs 2024-2025. No hi ha res d'original en aquestes notes; per a redactar-les he consultat diverses fonts, principalment [DF04], [DFX93], [Art91] i [Que]

Índex

Departament de Matemàtiques i Informàtica, Universitat de Barcelona, Catalunya
E-mail address: xevi.guitart@gmail.com.
Date: 12 de gener de 2025.

Introducció

En aquest curs estudiarem el que es coneix amb el nom de *teoria de Galois*, que estableix una connexió fonamental entre dos tipus d'objectes algebraics: els grups i els cossos.

La motivació històrica prové del problema de la resolubilitat d'equacions polinòmiques, que va ser un dels temes que més va mantenir ocupats els matemàtics entre els segles XVI i XIX. Per a l'equació de grau 2

$$x^2 + bx + c = 0$$

tenim la fórmula[1]

$$\frac{-b \pm \sqrt{b^2 - 4c}}{2}$$

que expressa les arrels en termes dels coeficients de l'equació i les operacions de sumar, restar, multiplicar, dividir i prendre arrels. Diem que l'equació quadràtica és *resoluble per radicals*.

Per a les equacions de grau 3 i grau 4 també hi ha fórmules anàlogues (les veurem als problemes). És a dir, les equacions de grau 3 i 4 són també resolubles per radicals.

En canvi, per a graus ≥ 5 l'equació general no és resoluble per radicals: no existeix una fórmula anàloga que doni les arrels d'un polinomi qualsevol de grau ≥ 5 com a expressions radicals dels coeficients. Sí que és cert que hi ha algunes equacions de graus ≥ 5 per a les quals sí que podem expressar les arrels per radicals (per exemple, $x^5 - 2 = 0$), però també n'hi ha d'altres (per exemple, $x^5 - 16x + 2 = 0$) per a les quals això no és possible.

Al llarg del curs veurem tots aquests resultats. La formulació moderna de l'estudi de les solucions d'equacions polinòmiques es fa a través de la teoria de cossos. Donat un polinomi $f(x) \in \mathbb{Q}[x]$ se li associa un cos K_f: és el cos més petit que conté les arrels de f. Per exemple, al polinomi $x^2 + 1 \in \mathbb{Q}[x]$ li associem el cos

$$\mathbb{Q}(i) := \{a + bi \colon a, b \in \mathbb{Q}\} \subseteq \mathbb{C}.$$

D'aquesta manera, els problemes sobre les arrels de f es tradueixen en problemes sobre el cos K_f corresponent.

El que fa la teoria de Galois és associar al cos K_f un grup finit, que s'anomena el grup de Galois de K_f i es denota per $\mathrm{Gal}(K_f/\mathbb{Q})$, i tradueix els problemes sobre el cos K_f a problemes sobre el grup $\mathrm{Gal}(K_f/\mathbb{Q})$. En particular, relacionat amb el problema de la resolubilitat d'equacions polinòmiques, veurem que un polinomi f és resoluble per radicals si i només si el grup $\mathrm{Gal}(K_f/\mathbb{Q})$ és resoluble[2].

Més en general, podem començar amb un polinomi $f \in F[x]$ amb coeficients en un cos F qualsevol. Aleshores el cos K_f que se li associa és un cos que conté F i novament conté totes les arrels de f. Es diu que K_f és una extensió de F. La teoria de Galois és l'estudi de les extensions de cossos obtingudes d'aquesta manera, i estableix una connexió fonamental entre la teoria d'aquestes extensions i la teoria de grups. Problemes complicats sobre extensions de cossos tenen una traducció sovint més tractable en termes dels grups associats.

El problema de la resolubilitat de les equacions polinòmiques va ser molt important al seu dia i va tenir un paper clau com a motor en el desenvolupament de la teoria de Galois. Però en la matemàtica moderna la importància de la teoria de Galois va molt més enllà de la seva aplicació a la resolubilitat d'equacions polinòmiques. L'objectiu del curs no és doncs només el problema de la resolubilitat per radicals, sinó estudiar pròpiament la teoria de Galois, que té un paper central i molt

[1] Exercici: si no heu vist mai d'on surt aquesta fórmula, demostreu-la.

[2] Recordem que un grup G és resoluble si existeix una cadena de subgrups $\{1\} = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n = G$ tal que G_i és normal en G_{i+1} i el quocient G_{i+1}/G_i és abelià per a tot $i = 0, 1, \ldots, n-1$.

destacat en la matemàtica actual amb aplicacions (d'ella o de generalitzacions seves) a la teoria de nombres, teoria d'anells, geometria algebraica, teoria de grups, topologia algebraica, criptografia, teoria de codis correctors d'errors, etc.

1. Fonaments de la teoria de cossos

En aquest primer capítol introduirem les nocions rellevants de la teoria d'extensions de cossos i en veurem algunes primeres propietats generals.

1.1. Definicions i primeres propietats.

Definició 1.1. Un *cos* F és un anell (commutatiu unitari) on tot element no nul és invertible pel producte i $1_F \neq 0_F$.

Com que tot element $\neq 0_F$ és invertible pel producte, el conjunt $F^\times := F \setminus \{0_F\}$ dotat amb l'operació producte del cos és un grup abelià. S'anomena el *grup dels invertibles* de F.

Definició 1.2. Un *morfisme de cossos* $\sigma\colon F \to K$ és un morfisme d'anells; és a dir: $\sigma(a+b) = \sigma(a)+\sigma(b)$, $\sigma(ab) = \sigma(a)\sigma(b)$ per a tot $a, b \in F$, i $\sigma(1_F) = 1_K$.

Remarca 1.3. A partir d'ara farem l'abús habitual de notació de denotar simplement per 1 l'element neutre pel producte d'un cos si el cos al qual pertany ja queda clar pel context; per exemple, la darrera propietat de la definició anterior seria $\sigma(1) = 1$. El mateix farem amb el 0.

Exemple 1.4.
(1) Alguns exemples de cossos que coneixem són $\mathbb{Q}$, $\mathbb{R}$ i $\mathbb{C}$. També per a cada primer p sabem que $\mathbb{Z}/p\mathbb{Z}$ és un cos que té p elements; una notació habitual per a aquest cos és $\mathbb{F}_p$. Més endavant veurem que per a tot primer p i tot $r \geq 1$ existeixen cossos de cardinal p^r. També veurem que si un cos té un nombre finit d'elements, aleshores el seu cardinal és p^r per a algun primer p i algun $r \geq 1$.
(2) Sigui R un domini d'integritat[3]. Aleshores el seu *cos de fraccions* $\mathrm{Fr}(R)$ és un cos. Recordem que el cos de fraccions és

$$\mathrm{Fr}(R) = \left\{ \frac{a}{b} \colon a, b \in R, b \neq 0 \right\} / \sim$$

on la relació $\sim$ és $\frac{a}{b} \sim \frac{c}{d}$ si $ad - bc = 0$. Per exemple, $\mathrm{Fr}(\mathbb{Z}) = \mathbb{Q}$. Si F és un cos, l'anell $F[x]$ de polinomis amb coeficients a F és un domini d'integritat, i definim $F(x) := \mathrm{Fr}(F[x])$; s'anomena el *cos de funcions racionals* en x amb coeficients a F.

Proposició 1.5.
(1) Els únics ideals d'un cos F són l'ideal (0) i l'ideal total F.
(2) Tot morfisme de cossos $\sigma\colon F \to K$ és injectiu.

Demostració.
(1) Sigui $I \subseteq F$ un ideal. Si $I \neq (0)$, aleshores existeix un element no nul $a \in I$. Com que F és un cos, a té un invers a^{-1} pel producte i, per ser I un ideal, tenim que $a^{-1}a$ pertany a I; és a dir, $1 \in I$ i, per tant, $I = F$.
(2) Sabem que el nucli $\ker(\sigma)$ és un ideal de F; com que $\sigma(1) = 1$, el nucli no és tot F i, per tant, ha de ser (0), amb la qual cosa σ és injectiu.

□

1.2. Característica d'un cos.

Si F és un cos i $n \in \mathbb{Z}_{>0}$, definim

$$n \cdot 1_F := 1_F + 1_F + \overset{n)}{\cdots} + 1_F.$$

[3] Recordem que això vol dir que R és un anell no nul sense divisors de 0 no nuls

Tenim un morfisme d'anells $f\colon \mathbb{Z} \to F$ definit de la manera següent:

$$f(n) = \begin{cases} n \cdot 1_F & \text{si } n > 0, \\ -(-n) \cdot 1_F & \text{si } n < 0, \\ 0_F & \text{si } n = 0. \end{cases}$$

El nucli $\ker(f)$ és doncs un ideal de $\mathbb{Z}$ i $\mathbb{Z}/\ker(f) \simeq \operatorname{Im}(f)$. Com que $\operatorname{Im}(f)$ és un subanell d'un cos, és un domini d'integritat i, per tant, $\ker(f)$ és un ideal primer. Si $\ker(f) = (0)$, diem que F és de *característica* 0. Si $\ker(f) \neq (0)$, aleshores és de la forma $\ker(f) = (p)$ per a cert nombre primer p; en aquest cas diem que F és de *característica* p. Denotem per $\operatorname{char}(F)$ la característica de F, que és 0 o un nombre primer p.

Si $\operatorname{char}(F) = 0$, aleshores f és injectiu i F conté un subanell isomorf a $\mathbb{Z}$. Com que F és un cos, també conté, doncs, un subcòs isomorf al cos de fraccions de $\mathbb{Z}$, és a dir, a $\mathbb{Q}$.

Si $\operatorname{char}(F) = p$, aleshores $p \cdot 1_F = 0_F$, i p és l'enter positiu més petit amb aquesta propietat (això és perquè p és el generador positiu de $\ker(f)$). És habitual referir-se a aquesta propietat com a "$p = 0$ a F". Observem també que F conté en aquest cas un subcòs isomorf a $\mathbb{F}_p$.

Definició 1.6. Si $\operatorname{char}(F) = 0$, diem que $\mathbb{Q}$ és el cos primer de F. Si $\operatorname{char}(F) = p$, diem que $\mathbb{F}_p$ és el cos primer de F.

Exemple 1.7. $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}(x)$, $\mathbb{R}(x), \mathbb{C}(x)$ són de característica 0; en canvi, $\mathbb{F}_p$ i $\mathbb{F}_p(x)$ són de característica p.

1.3. **Extensions de cossos.** Ja hem dit que una motivació per a la teoria de Galois és la resolució d'equacions polinòmiques amb coeficients en un cos. Ja sabem que molt sovint aquestes equacions no tenen solucions en el mateix cos on estan definits els coeficients, però sí que tenen solució en cossos més grans. Per exemple, $x^2 + 1$ no té arrels a $\mathbb{R}$, però sí a $\mathbb{C}$, que és un cos més gran. De manera natural, doncs, quan estudiem arrels de polinomis amb coeficients en un cos F, sovint hem de considerar cossos més grans que el mateix F. Això dóna lloc a la noció d'*extensió de cossos*, que és clau en la teoria de Galois.

Definició 1.8. Una extensió de cossos K/F és una inclusió de cossos $F \subseteq K$ (és a dir, F és un subcòs de K). Una subextensió de K/F és una extensió L/F amb $F \subseteq L \subseteq K$.

Observació 1.9. La notació K/F per a una extensió de cossos no s'ha de confondre amb el quocient. Sovint es dibuixa un diagrama de l'estil

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

per a indicar que K és una extensió de F.

Exemple 1.10. Tot cos és extensió del seu cos primer. Així doncs, tenim les extensions $\mathbb{R}/\mathbb{Q}$, $\mathbb{C}/\mathbb{Q}$, $\mathbb{F}_p(x)/\mathbb{F}_p$, etc. També sabem que $\mathbb{R}$ és un subcòs de $\mathbb{C}$; per tant, tenim també l'extensió $\mathbb{C}/\mathbb{R}$.

Exemple 1.11. Definim el subconjunt següent dels complexos:

$$\mathbb{Q}(i) := \{a + bi\colon a, b \in \mathbb{Q}\}.$$

És clar que $\mathbb{Q}(i)$ és un subanell de $\mathbb{C}$. Per a veure que n'és un subcòs, n'hi ha prou amb veure que l'invers pel producte d'un element no nul $a+bi \in \mathbb{Q}(i)$ també és de $\mathbb{Q}(i)$. Com que

$$(a+bi)^{-1} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i$$

també pertany a $\mathbb{Q}(i)$, tenim doncs que $\mathbb{Q}(i)$ és un cos. Tenim, així, les extensions $\mathbb{Q}(i)/\mathbb{Q}$ i $\mathbb{C}/\mathbb{Q}(i)$.

Una eina molt important en l'estudi de les extensions de cossos és l'àlgebra lineal. Si K/F és una extensió, podem dotar K d'una estructura d'espai vectorial:

- La suma de vectors és la suma a K; és a dir, si $u, v \in K$, definim la seva suma simplement com $u+v$, on $+$ és l'operació suma de K (com que K és un cos, hi ha definida una operació $+$).
- El producte per escalars de F és el producte a K; és a dir, si $\lambda \in F$ i $u \in K$, definim el producte simplement com λu, on prenem l'operació producte de K. Com que λ pertany a F i $F \subseteq K$, tenim que λu pertany a K i el producte per escalars està ben definit.

Proposició 1.12. Amb les operacions anteriors, K és un espai vectorial sobre F.

Demostració. Cal comprovar que les operacions de suma i producte per escalars satisfan els axiomes d'espai vectorial. Això és un exercici senzill, fent servir les propietats que satisfan aquestes operacions pel fet de ser K un cos. □

Definició 1.13. El *grau* d'una extensió K/F, denotat $[K\colon F]$, és la dimensió de K com a F-espai vectorial. Diem que K/F és finita si $[K\colon F] < \infty$ i que és infinita si $[K\colon F] = \infty$.

Exemple 1.14. $[\mathbb{C}\colon \mathbb{R}] = 2$, $[\mathbb{Q}(i)\colon \mathbb{Q}] = 2$, $[\mathbb{R}\colon \mathbb{Q}] = \infty$, $[\mathbb{Q}(t)\colon \mathbb{Q}] = \infty$ (ja que $1, t, t^2, t^3, \ldots$ són linealment independents).

1.4. **Un exemple molt important d'extensions: les obtingudes a partir de polinomis irreductibles.** Ara veurem que, donat un polinomi irreductible $f \in F[x]$, sempre existeix una extensió K/F on f té alguna arrel. Ja hem vist abans l'exemple prototípic d'aquesta situació: $x^2+1 \in \mathbb{R}[x]$ és irreductible i no té cap arrel a $\mathbb{R}$; en canvi, sí que té una (de fet, dues) arrels a $\mathbb{C}$. Comencem veient una manera de "construir" un cos isomorf a $\mathbb{C}$ de forma purament algebraica[4] i després generalitzarem aquest procés a altres cossos. La clau està a considerar l'aplicació següent, que és avaluar un polinomi en i:

$$\begin{array}{rccc} \phi\colon & \mathbb{R}[x] & \longrightarrow & \mathbb{C} \\ & f(x) & \longmapsto & f(i). \end{array}$$

És fàcil comprovar que ϕ és un morfisme d'anells i que ϕ és exhaustiu. Vegem ara que

$$\ker(\phi) = (x^2+1).$$

Clarament, $\phi(x^2+1) = 0$ i, per tant, $(x^2+1) \subseteq \ker(\phi)$. Per a l'altra inclusió, si $f \in \mathbb{R}[x]$ és tal que $f(i) = 0$, aleshores prenent la conjugació complexa i fent servir que f té coeficients reals veiem que $f(\bar{i}) = f(-i) = 0$. Per tant, $(x-i)(x+i) = x^2+1$ divideix f i $f \in (x^2+1)$. La conclusió és, doncs, que $\mathbb{R}[x]/(x^2+1) \simeq \mathbb{C}$.

Aquest procés es pot generalitzar per a donar resposta a aquesta pregunta: donat un cos F i un polinomi $f \in F[x]$ no constant, existeix alguna extensió K/F en la qual f té alguna arrel? La resposta és que sí, i ens la dóna la proposició següent. Fixem-nos que n'hi ha prou amb considerar

[4] És a dir, obtindrem un cos isomorf a $\mathbb{C}$, però no obtindrem cap de les altres propietats extres que coneixem de $\mathbb{C}$ (per exemple, que té una topologia).

el cas en què f sigui irreductible, ja que, si no ho fos, podríem prendre un factor irreductible de f (i una arrel d'aquest factor també seria una arrel de f).

Proposició 1.15. Sigui F un cos i $f(x) \in F[x]$ un polinomi irreductible. Existeix una extensió K de F tal que f té alguna arrel a K.

Demostració. Com que $F[x]$ és un domini d'ideals principals i $f(x)$ és irreductible, tenim que l'ideal $(f(x))$ és maximal. Per tant, el quocient $K = F[x]/(f(x))$ és un cos. Si $p(x) \in F[x]$, denotem per $\overline{p(x)}$ la classe de $p(x)$ a K. A dins de K hi tenim F com a subcòs: donat $a \in F$, la seva classe $\overline{a}$ pertany a K, i l'aplicació $a \mapsto \overline{a}$ és injectiva. D'ara en endavant, farem l'abús de notació de denotar $\overline{a}$ simplement per a si $a \in F$.

Afirmem que $\overline{x}$, la classe del polinomi x, és una arrel a K de $f(x)$. En efecte, si $f(x) = a_n x^n \cdots + a_1 x + a_0$, tenim les igualtats següents a K:

$$\begin{aligned} 0 = \overline{f(x)} = \overline{a_n x^n + \cdots a_1 x + a_0} &= \overline{a_n x^n} + \cdots + \overline{a_1 x} + \overline{a_0} \\ &= a_n \overline{x}^n + \cdots + a_1 \overline{x} + a_0 = f(\overline{x}), \end{aligned}$$

d'on veiem que $\overline{x} \in K$ és una arrel de f a K. □

Observació 1.16. Tan important com l'enunciat de la Proposició 1.15 és la seva demostració, ja que és constructiva; és a dir, no només sabem que hi ha extensions de F on f hi té arrels, sinó que també podem construir una extensió amb aquesta propietat: és la donada pel cos $K = F[x]/(f(x))$.

Així doncs, donat un polinomi irreductible $f(x) \in F[x]$ sabem que existeix una extensió K/F que conté com a mínim una arrel de f. Més endavant veurem que, de fet, existeix una extensió on f descompon completament com a producte de factors lineals; és a dir, que conté totes les arrels de f.

Proposició 1.17. Amb la notació de la Proposició 1.15 tenim que $[K\colon F] = n$ on n és el grau de f. Si posem $\alpha = \overline{x}$, una F-base de K és $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$.

Demostració. Tot element de $K = F[x]/(f(x))$ és de la forma $\overline{b(x)}$ per a un cert polinomi

$$b(x) = b_m x^m + \ldots b_1 x + b_0 \in F[x].$$

Per la divisió de polinomis tenim que

$$b(x) = q(x)f(x) + r(x) \text{ amb } \deg(r(x)) < n.$$

Si posem $r(x) = r_{n-1}x^{n-1} + \cdots + r_1 x + r_0$ amb els $r_i \in F$, tenim que

$$\overline{b(x)} = \overline{r(x)} = r_{n-1}\overline{x}^{n-1} + \cdots + r_1 \overline{x} + r_0 = r_{n-1}\alpha^{n-1} + \cdots + r_1 \alpha + r_0,$$

amb la qual cosa veiem que $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ genera K com a F-espai vectorial. Veiem que aquests elements són linealment independents: si no ho fossin, existiria una combinació lineal

$$c_{n-1}\alpha^{n-1} + \cdots + c_1 \alpha + c_0 = 0$$

amb algun $c_i \neq 0$. Aleshores, el polinomi $g(x) = c_{n-1}x^{n-1} + \cdots + c_1 x + c_0 \in F[x]$ seria un polinomi tal que $\overline{g(x)} = 0$ i, per tant, $g(x) \in (f(x))$. Com que $\deg(g) < \deg(f)$, tenim que necessàriament $g = 0$ i, per tant, tots els c_i han de ser 0. □

Així doncs, veiem que, si $f \in F[x]$ és irreductible, el cos $K = F[x]/(f)$ el podem pensar com

$$K = \{c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1}\colon c_i \in F\},$$

on α és un element tal que $f(\alpha) = 0$. Si $f, g \in F[x]$ i denotem per $\bar{f}, \bar{g}$ les seves classes mòdul (f), aleshores $\bar{f} + \bar{g} = \overline{f+g}$; és a dir, fem la suma $f + g$ i reduïm el resultat mòdul f. De manera semblant, podem multiplicar classes. També, si $\bar{g} \neq 0$, aleshores podem calcular $\bar{g}^{-1}$ de la manera següent: com que $g \notin (f)$ i f és irreductible tenim que $\gcd(f, g) = 1$ i per Bezout existeixen polinomis $a(x), b(x) \in F[x]$ tals que $a(x)f(x) + b(x)g(x) = 1$; aleshores, $\bar{b} = \bar{g}^{-1}$.

Exemple 1.18. (1) $\mathbb{C} \simeq \mathbb{R}[x]/(x^2+1)$.

(2) Sigui $f(x) = x^2 - 5 \in \mathbb{Q}[x]$, que és irreductible (5-Eisenstein). Posem $K = \mathbb{Q}[x]/(x^2-5)$. Tenim que $[K\colon \mathbb{Q}] = 2$ i $K = \{a + b\alpha\colon a, b \in \mathbb{Q}\}$ i $\alpha^2 = 5$. La suma i producte en aquest cos són:

$$(a + b\alpha) + (c + d\alpha) = (a + c) + (b + d)\alpha$$
$$(a + b\alpha)(c + d\alpha) = ac + 5bd + (ad + bc)\alpha.$$

Com que $\alpha^2 = 5$, a vegades es fa servir la notació $\sqrt{5}$ en comptes de α. És a dir que els elements de K són de la forma $a + b\sqrt{5}$ amb $a, b \in \mathbb{Q}$. Aquí $\sqrt{5}$ no vol dir el nombre real $\sqrt{5}$, sinó només un símbol que satisfà que el seu quadrat és 5.

(3) $F = \mathbb{Q}$ i $f(x) = x^3 - 7$. Aleshores,

$$\mathbb{Q}[x]/(f) = \{a + b\alpha + c\alpha^2\colon a, b, c \in \mathbb{Q}\}$$

on $\alpha^3 - 7 = 0$. Novament, podem operar en aquest cos amb les operacions habituals, només tenint en compte que $\alpha^3 = 7$.

(4) $F = \mathbb{F}_2$ i $f = x^2 + x + 1$. Aquest polinomi és irreductible a $\mathbb{F}_2[x]$, ja que té grau 2 i no té arrels a $\mathbb{F}_2$. Aleshores, $K = \mathbb{F}_2[x]/(x^2 + x + 1)$ és un cos amb $[K\colon \mathbb{F}_2] = 2$. Així doncs, té 2^2 elements. Els seus elements són de la forma $a + b\alpha$ amb $a, b \in \mathbb{F}_2$ i $\alpha^2 + \alpha + 1 = 0$. Com a exemple de com podem operar tenim que:

$$(\alpha + 1)\alpha = \alpha^2 + \alpha = \alpha + 1 + \alpha = 1.$$

1.5. **Grups d'automorfismes d'extensions.**

Definició 1.19. Siguin K/F i L/F extensions de cossos. Un morfisme de cossos $\sigma\colon K \to L$ tal que $\sigma_{|F} = \mathrm{id}$ (és a dir, tal que $\sigma(x) = x$ per a tot $x \in F$) s'anomena un *F-morfisme*; també es diu que σ és un *morfisme d'extensions*.

Definició 1.20. Un automorfisme de cossos $\sigma\colon K \to K$ (és a dir, un morfisme de cossos bijectiu) tal que $\sigma_{|F} = \mathrm{id}$ s'anomena un *F-automorfisme de K*; també s'anomena un *automorfisme de l'extensió K/F*.

Denotem per $\mathrm{Aut}(K/F)$ el conjunt de F-automorfismes de K:

$$\mathrm{Aut}(K/F) = \{\sigma\colon K \to K \mid \sigma \text{ és un morfisme de cossos bijectiu i } \sigma_{|F} = \mathrm{id}\}.$$

Aquest conjunt el podem dotar d'estructura de grup on l'operació és la composició: si $\sigma, \tau \in \mathrm{Aut}(K/F)$, definim $\sigma\tau = \sigma \circ \tau$. L'operació està ben definida, ja que la composició de F-automorfismes és un F-automorfisme, la identitat és el neutre per la composició, l'operació és associativa ja que la composició de funcions ho és, i finalment tot element té invers, ja que tot F-automorfisme té un invers per la composició que també és un F-automorfisme.

Com que K és un F-espai vectorial i $\sigma_{|F} = \mathrm{id}$, un element $\sigma \in \mathrm{Aut}(K/F)$ queda determinat per la imatge per σ d'una F-base de K: tot $x \in K$ és de la forma $x = \lambda_1\alpha_1 + \cdots + \lambda_n\alpha_n$, on els $\alpha_i \in K$ són d'una F-base de K i els λ_i són de F; aleshores, $\sigma(x) = \lambda_1\sigma(\alpha_1) + \cdots + \lambda_n\sigma(\alpha_n)$.

Exemple 1.21. (1) La conjugació complexa és un element de $\mathrm{Aut}(\mathbb{C}/\mathbb{R})$.

(2) Sigui $K = \mathbb{Q}[x]/(x^2-5)$, amb base $1, \alpha$ on $\alpha^2 - 5 = 0$. Si $\sigma \in \mathrm{Aut}(K/\mathbb{Q})$, fixem-nos que $\sigma(\alpha^2-5) = \sigma(0) = 0$ i, per tant, $\sigma(\alpha)^2-5 = 0$. És a dir, $\sigma(\alpha)$ és necessàriament una arrel de x^2-5 a K. Les dues úniques arrels són α i $-\alpha$. Es pot comprovar (tot i que més endavant veurem un resultat teòric que ens ho estalvia) que l'aplicació $\sigma : K \to K$ tal que $\sigma(\alpha) = -\alpha$ (i $\sigma(1) = 1$) és un automorfisme no trivial de K. L'altre únic automorfisme és la identitat, amb la qual cosa $\mathrm{Aut}(K/\mathbb{Q}) = \{\mathrm{id}, \sigma\}$. Com que $\sigma^2 = \mathrm{id}$, tenim que $\mathrm{Aut}(K/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}$.

(3) Sigui K un cos de característica $p > 0$. L'aplicació

$$\begin{array}{rccc} \mathrm{Fr}_p\colon & K & \longrightarrow & K \\ & \alpha & \longmapsto & \alpha^p \end{array}$$

és un morfisme de cossos. Clarament,

$$\mathrm{Fr}_p(\alpha\beta) = (\alpha\beta)^p = \alpha^p\beta^p = \mathrm{Fr}_p(\alpha)\mathrm{Fr}_p(\beta).$$

Pel que fa a la compatibilitat respecte de la suma, tenim que

$$\mathrm{Fr}_p(\alpha+\beta) = (\alpha+\beta)^p = \alpha^p + \sum_{i=1}^{p-1} \binom{p}{i} \alpha^{p-i}\beta^i + \beta^p = \mathrm{Fr}_p(\alpha) + \mathrm{Fr}_p(\beta).$$

La darrera igualtat és perquè p és primer i, per tant, $p \mid \binom{p}{i}$ per a tot $1 \leq i \leq p-1$; com que $p = 0$ a K, els termes del sumatori són 0.

A aquest morfisme se li diu el *morfisme* (o *l'endomorfisme*) *de Frobenius*. Com que per a tot $\alpha \in \mathbb{F}_p$ tenim que $\alpha^p = \alpha$ (pel teorema petit de Fermat), l'endomorfisme de Frobenius fixa el cos primer $\mathbb{F}_p$. Si $K/\mathbb{F}_p$ és finita, aleshores Fr_p és també exhaustiva i és doncs un automorfisme. Si $K/\mathbb{F}_p$ és infinita, aleshores això no és necessàriament cert; per exemple, per a $K = \mathbb{F}_p(x)$ tenim que Fr_p no és exhaustiu, ja que x no és de la imatge.

Remarca 1.22. A vegades al grup de F-automorfismes de K també se li diu grup de Galois de K/F i es denota per $\mathrm{Gal}(K/F)$. Hi ha una altra convenció terminològica (que és la que seguirem en aquestes notes) que reserva la terminologia de grup de Galois per a certes extensions que satisfan algunes propietats extres, i que s'anomenen *extensions de Galois*. Per tant, aquí parlarem en general del grup de F-automorfismes $\mathrm{Aut}(K/F)$, i quan K/F sigui de Galois, aleshores a aquest grup li direm el grup de Galois i el denotarem $\mathrm{Gal}(K/F)$.[5]

1.6. **Adjunció d'elements.**

Definició 1.23. Sigui K/F una extensió i $\alpha \in K$. Denotem per $F[\alpha]$ el menor subanell de K que conté F i α, i per $F(\alpha)$ el menor subcòs de K que conté F i α. Diem que $F(\alpha)$ és el cos obtingut adjuntant α a F.

Com que $F[\alpha]$ és un subanell que conté F i conté α i és tancat per la suma i el producte, conté tots els elements de la forma $a_0 + a_1\alpha + \cdots + a_n\alpha^n$ amb els $a_i \in F$. Així doncs,

$$F[\alpha] = \{a_0 + a_1\alpha + \cdots + a_n\alpha^n \colon a_i \in F, n \geq 0\} = \{f(\alpha) \colon f \in F[x]\},$$

[5] A la llista de problemes, però, se segueix l'altra convenció: es parla de grup de Galois $\mathrm{Gal}(K/F)$, fins i tot, per a extensions no necessàriament de Galois.

ja que el conjunt de la dreta és un subanell de K (en efecte, és la imatge del morfisme d'anells $F[x] \to K$ que envia $f(x)$ a $f(\alpha)$). Amb un raonament semblant, obtenim que

$$F(\alpha) = \left\{ \frac{a_0 + a_1\alpha + \cdots + a_n\alpha^n}{b_0 + b_1\alpha + \cdots + b_m\alpha^m} \colon m, n \geq 0, b_0 + b_1\alpha + \cdots + b_m\alpha^m \neq 0 \right\}.$$

Si $\alpha_1, \ldots, \alpha_r \in K$, definim $F[\alpha_1, \ldots, \alpha_r]$ com el menor subanell de K que conté F i els $\alpha_1, \ldots, \alpha_r$, i $F(\alpha_1, \ldots, \alpha_r)$ com el menor subcòs de K que conté F i els $\alpha_1, \ldots, \alpha_r$. Novament, $F[\alpha_1, \ldots, \alpha_r]$ és el conjunt d'expressions polinòmiques en $\alpha_1, \ldots, \alpha_r$ i coeficients a F, i $F(\alpha_1, \ldots, \alpha_r)$ el seu cos de fraccions.

Definició 1.24. Una extensió K/F és *finitament generada* si existeixen elements $\alpha_1, \ldots, \alpha_n$ tals que $K = F(\alpha_1, \ldots, \alpha_n)$. L'extensió és *simple* si està generada per un element, és a dir, si $K = F(\alpha)$ per a algun $\alpha \in K$.

Proposició 1.25. Sigui $f \in F[x]$ irreductible i K/F una extensió on f té una arrel α. Aleshores,

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

En particular, $[F(\alpha)\colon F] = \deg f$.

Demostració. Considerem el morfisme d'anells "avaluar en α":

$$\begin{array}{rccc} \varphi_\alpha\colon & F[x] & \longrightarrow & F(\alpha) \subseteq K \\ & a(x) & \longmapsto & a(\alpha). \end{array}$$

Com que $\varphi_\alpha(f) = f(\alpha) = 0$, tenim que $(f) \subseteq \ker\varphi_\alpha$. D'altra banda, si $p \in \ker(\varphi_\alpha)$, aleshores $p(\alpha) = 0$ i això implica que $\gcd(f, p) \neq 1$ (en efecte, si el màxim comú divisor fos 1 per Bezout existirien polinomis a i b tals que $a(x)f(x) + b(x)p(x) = 1$, i avaluant aquesta igualtat en $x = \alpha$ obtindríem $1 = 0$, cosa que no pot ser en un cos). Per tant, $\ker\varphi_\alpha = (f)$ i φ_α indueix un morfisme

$$\tilde{\varphi}_\alpha\colon F[x]/(f) \to F(\alpha).$$

Com que f és irreductible, $\mathrm{Im}(\tilde{\varphi}_\alpha) \simeq F[x]/(f)$ és un cos i, per tant, $\mathrm{Im}(\tilde{\varphi}_\alpha)$ és un subcòs de $F(\alpha)$ que conté F i conté α; això implica $F(\alpha) \subseteq \mathrm{Im}(\tilde{\varphi}_\alpha)$. Aquest fet prova que $\tilde{\varphi}_\alpha$ és exhaustiu i com que tots els morfismes de cossos són injectius, veiem, doncs, que és un isomorfisme. □

Observació 1.26. En la situació de la proposició anterior, per la Proposició 1.17 veiem que

$$F(\alpha) = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}\colon a_i \in F\},$$

on $n = \deg(f)$. En particular, en aquest cas tenim que $F[\alpha] = F(\alpha)$.

Exemple 1.27. (1) Posem $f(x) = x^2 - 5 \in \mathbb{Q}[x]$. Aquest polinomi no té cap arrel a $\mathbb{Q}$, però té arrels a $\mathbb{R}$. Posem $\sqrt{5}$ per a denotar l'arrel quadrada positiva de 5 a $\mathbb{R}$. Aleshores,

$$\mathbb{Q}(\sqrt{5}) = \{a + b\sqrt{5}\colon a, b \in \mathbb{Q}\}.$$

Fixem-nos en la diferència conceptual amb l'Exemple 1.18 (2). Allà hem construït un cos on f té una arrel, mentre que aquí partíem d'un cos que ja teníem (el cos dels reals) i on sabem que f té una arrel, i hem construït el cos més petit que conté aquesta arrel. Les dues construccions són formalment diferents, però la Proposició 1.25 ens diu que els cossos obtinguts en les dues construccions són isomorfs.

(2) $f(x) = x^3 - 2 \in \mathbb{Q}[x]$. Posem $\sqrt[3]{2}$ per a denotar l'arrel cúbica de 2 a $\mathbb{R}$. Aleshores,

$$\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2 : a, b, c \in \mathbb{Q}\}.$$

Sabem que f té dues altres arrels a $\mathbb{C}$: $e^{\frac{2\pi i}{3}}\sqrt[3]{2}$ i $e^{\frac{4\pi i}{3}}\sqrt[3]{2}$. Podem considerar també, per exemple, el cos $\mathbb{Q}(e^{\frac{2\pi i}{3}}\sqrt[3]{2})$. Aquest cos és certament diferent de $\mathbb{Q}(\sqrt[3]{2})$ (un està contingut a $\mathbb{R}$ i l'altre no), però, en canvi, com a cossos són isomorfs.

Fixem-nos que les diferents arrels d'un polinomi són indistingibles des del punt de vista algebraic, ja que generen cossos isomorfs. El resultat següent fa una mica més precís aquest fet.

Proposició 1.28. Sigui $\varphi\colon F \to F'$ un isomorfisme de cossos i sigui $f(x) \in F[x]$ irreductible. Denotem per $f'(x) \in F'[x]$ el polinomi que obtenim aplicant φ als coeficients de f. Sigui α una arrel de f en una extensió de F, i sigui α' una arrel de f' en una extensió de F'. Aleshores, existeix un isomorfisme $\tilde{\varphi}\colon F(\alpha) \xrightarrow{\simeq} F'(\alpha')$ tal que $\tilde{\varphi}(\alpha) = \alpha'$ i que estén φ (és a dir, $\tilde{\varphi}_{|F} = \varphi$).

Demostració. El morfisme φ indueix un isomorfisme d'anells $\varphi\colon F[x] \to F'[x]$ tal que $\varphi((f)) = (f')$. Passant al quocient tenim un isomorfisme $F[x]/(f) \to F'[x]/(f')$. Per la Proposició 1.25 el cos de l'esquerra és isomorf a $F(\alpha)$ i el de la dreta a $F'(\alpha')$. Composant els isomorfismes obtenim $\tilde{\varphi}$. □

Observació 1.29. Sigui f un polinomi irreductible i sigui α una arrel de f en una extensió. Considerem l'extensió $F(\alpha)/F$. Fixem-nos que si $\sigma \in \mathrm{Aut}(F(\alpha)/F)$, aleshores $\sigma(\alpha)$ és necessàriament una arrel de f, ja que

$$f(\sigma(\alpha)) = \sigma(f(\alpha)) = \sigma(0) = 0.$$

Per tant, si f no té cap altra arrel a $F(\alpha)$ a part de α, l'únic F-automorfisme de $F(\alpha)$ és la identitat i, per tant, $\mathrm{Aut}(F(\alpha)/F) = \{1\}$ és el grup trivial. La Proposició 1.28, d'altra banda, ens diu que per a cada arrel β de f en $F(\alpha)$ existeix[6] un $\sigma \in \mathrm{Aut}(F(\alpha)/F)$ tal que $\sigma(\alpha) = \beta$.

1.7. **Extensions algebraiques.**

Definició 1.30. Sigui K/F una extensió. Un element $\alpha \in K$ és *algebraic sobre* F si és arrel d'algun polinomi no nul de $F[x]$, i és *transcendent sobre* F en cas contrari. L'extensió K/F és *algebraica* si tot element de K és algebraic sobre F, i és *transcendent* en cas contrari (és a dir, si existeix algun element de K transcendent sobre F).

Exemple 1.31.
(1) $\sqrt{5}$ és algebraic sobre $\mathbb{Q}$, ja que $\sqrt{5}$ és arrel del polinomi $x^2 - 5$. De fet, l'extensió $\mathbb{Q}(\sqrt{5})/\mathbb{Q}$ és algebraica: l'element $a+b\sqrt{5}$ és arrel del polinomi $x^2-2ax+a^2-5b^2 \in \mathbb{Q}[x]$.
(2) A $\mathbb{Q}(x)$, l'element x és transcendent sobre $\mathbb{Q}$.
(3) Els nombres reals π i e són transcendents sobre $\mathbb{Q}$. Això no és evident i cal demostrar-ho (la demostració no és excessivament complicada, però no la farem aquí). També se sap que e^π és transcendent, però, en canvi, no se sap si π^e ho és (i tampoc si $e\pi$ o $e + \pi$ ho són). Fixem-nos que $\mathbb{Q}[x]$ és numerable i, com que cada polinomi té un nombre finit d'arrels, el conjunt de nombres complexos que són algebraics sobre $\mathbb{Q}$ també és numerable. En canvi, $\mathbb{R}$ i $\mathbb{C}$ no són numerables. En aquest sentit, "la majoria" de nombres reals o complexos són transcendents sobre $\mathbb{Q}$ (però demostrar que un nombre concret és transcendent sol ser complicat).

[6] De fet, la proposició ens diu que hi ha un F-morfisme $\sigma\colon F(\alpha) \to F(\beta)$; fixem-nos que si $\beta \in F(\alpha)$, aleshores $F(\beta) \subseteq F(\alpha)$, i com que per la proposició 1.25 tenen la mateix dimensió, tenim que $F(\alpha) = F(\beta)$.

Observació 1.32. Si $L/K/F$ és una torre d'extensions i $\alpha \in L$ és algebraic sobre F, aleshores també ho és sobre K, ja que α és arrel d'un polinomi amb coeficients a F i, en particular, a K.

Proposició 1.33. Si K/F és finita, aleshores és algebraica.

Demostració. Posem $n = [K\colon F]$ i prenem un element $\alpha \in K$. Els elements $1, \alpha, \alpha^2, \alpha^3, \ldots, \alpha^n$ són $n+1$ elements en un espai de dimensió n i, per tant, són linealment dependents. Existeixen, doncs, elements $a_i \in F$ no tots nuls tals que $a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0$. Aleshores, α és arrel del polinomi $a_0 + a_1x + \cdots + a_nx^n \in F[x]$. □

Proposició 1.34 (i definició)**.** Si $\alpha \in K$ és algebraic sobre F, aleshores existeix un únic polinomi mònic $\mathrm{Irr}(\alpha, F)(x) \in F[x]$ que és irreductible i té α com a arrel. S'anomena el *polinomi irreductible de α sobre F* i té la propietat que si $f \in F[x]$ és tal que $f(\alpha) = 0$, aleshores $\mathrm{Irr}(\alpha, F) \mid f$. També, és el polinomi mònic de grau més petit que té α com a arrel.

Demostració. Sigui $\varphi_\alpha\colon F[x] \to K$ el morfisme d'anells avaluar en α, que envia $f(x)$ a $f(\alpha)$. Tenim, doncs, que $\mathrm{Im}(\varphi_\alpha)$ és un subanell de K i, en particular, un domini d'integritat. Com que $F[x]/\ker(\varphi_\alpha) \simeq \mathrm{Im}(\varphi_\alpha)$, veiem que $\ker(\varphi_\alpha)$ és un ideal primer de $F[x]$, que a més és no nul, ja que α és algebraic. L'anell $F[x]$ és un domini d'ideals principals (i, en particular, un domini de factorització única) i, per tant, els elements primers no nuls són irreductibles. Així doncs, $\ker(\varphi_\alpha)$ és principal generat per un polinomi irreductible; definim, doncs, $\mathrm{Irr}(\alpha, F)(x)$ com el generador mònic de $\ker(\varphi_\alpha)$, que és clar que satisfà les propietats de l'enunciat. □

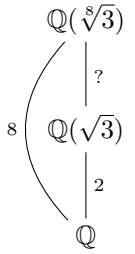
Definició 1.35. Si α és algebraic sobre F, definim el seu grau sobre F com el grau del polinomi $\mathrm{Irr}(\alpha, F)(x)$.

Observació 1.36. Si α és algebraic sobre F, aleshores per la Proposició 1.25 tenim que

$$F[x]/(\mathrm{Irr}(\alpha, F)(x)) \simeq F(\alpha).$$

En particular, $\deg(\alpha) = [F(\alpha)\colon F]$.

Exemple 1.37. Considerem l'extensió $\mathbb{Q}(\sqrt[8]{3})/\mathbb{Q}$. Tenim que $\mathrm{Irr}(\sqrt[8]{3}, \mathbb{Q})(x) = x^8 - 3$, ja que aquest és un polinomi mònic irreductible que té $\sqrt[8]{3}$ com a arrel. El grau de $\sqrt[8]{3}$ sobre $\mathbb{Q}$ és 8. Fixem-nos que $(\sqrt[8]{3})^4 = \sqrt{3}$, amb la qual cosa $\sqrt{3} \in \mathbb{Q}(\sqrt[8]{3})$. Tenim, doncs, inclusions de cossos $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{3}) \subseteq \mathbb{Q}(\sqrt[8]{3})$. Sovint es posa en forma de diagrama:



on els nombres indiquen el grau de l'extensió. Acabem de veure que $[\mathbb{Q}(\sqrt[8]{3})\colon \mathbb{Q}] = 8$ i és fàcil veure que $[\mathbb{Q}(\sqrt{3})\colon \mathbb{Q}] = 2$. El grau $[\mathbb{Q}(\sqrt[8]{3})\colon \mathbb{Q}(\sqrt{3})]$ és ≤ 4, ja que $\sqrt[8]{3}$ és arrel del polinomi $x^4 - \sqrt{3} \in \mathbb{Q}(\sqrt{3})[x]$. El grau és 4 si i només si aquest polinomi és irreductible, cosa que es podria demostrar directament però no és del tot evident. Però això ho deduirem del resultat següent, que és molt útil a la pràctica i ens estalvia de fer càlculs com aquest.

Proposició 1.38 (Multiplicativitat dels graus)**.** Siguin $F \subseteq K \subseteq L$ cossos. Aleshores

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

on la igualtat val també en el cas en què algun dels termes és infinit.

Demostració. Farem la demostració en el cas en què tots els graus involucrats siguin finits; deixem el cas en què algun d'ells és infinit com a exercici.

Posem, doncs, $[L\colon K] = m$ i $[K\colon F] = n$. Sigui $\{\alpha_i\}_{i=1,\dots,m}$ una K-base de L i $\{\beta_j\}_{j=1,\dots,n}$ una F-base de K. Aleshores, afirmem que

$$\{\alpha_i\beta_j\colon 1 \leq i \leq m,\ 1 \leq j \leq n\}$$

és una F-base de L. Si veiem això, ja hem acabat perquè, aleshores, $[L\colon F] = mn = [L\colon K][K\colon F]$.

Per a veure que són un sistema de generadors, prenem $\alpha \in L$. Aleshores, $\alpha = \sum a_i\alpha_i$ per a certs $a_i \in K$. Ara cada a_i el podem escriure com $a_i = \sum b_{ij}\beta_j$ per a certs $b_{ij} \in F$. Per tant, $\alpha = \sum_{i,j} b_{ij}\alpha_i\beta_j$.

Per a veure que són linealment independents, suposem que existeixi alguna combinació lineal

$$\sum_{i,j} b_{ij}\alpha_i\beta_j = 0,\ \text{amb } b_{ij} \in F.$$

Reagrupant la suma, tenim que $\sum_{i=1}^{m}(\sum_{j=1}^{n} b_{ij}\beta_j)\alpha_i = 0$, on cada terme $(\sum_{j=1}^{n} b_{ij}\beta_j)$ pertany a K. Com que els α_i són K-linealment independents, tenim que $(\sum_{j=1}^{n} b_{ij}\beta_j) = 0$ per a tot i. Com que els β_j són F-linealment independents tenim que $b_{ij} = 0$ per a tot i, j. □

Exemple 1.39. Amb aquesta fórmula veiem que $[\mathbb{Q}(\sqrt[8]{3})\colon \mathbb{Q}(\sqrt{3})] = 4$ i, en particular, que $x^4 - \sqrt{3}$ és irreductible a $\mathbb{Q}(\sqrt{3})[x]$.

Corol·lari 1.40. Si $F \subseteq K \subseteq L$, aleshores $[L\colon K] \mid [L\colon F]$ i $[K\colon F] \mid [L\colon F]$.

Sovint convé utilitzar la multiplicativitat dels graus en torres d'extensions, que s'obté aplicant repetidament el cas d'una única subextensió de la Proposició 1.38

Corol·lari 1.41. En una torre d'extensions

$$F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_{n-1} \subseteq F_n$$

tenim que $[F_n\colon F_0] = [F_n\colon F_{n-1}][F_{n-1}\colon F_{n-2}]\dots[F_1\colon F_0]$.

Recordem que K/F és finitament generada si $K = F(\alpha_1, \dots, \alpha_n)$ per a certs $\alpha_i \in K$.

Lema 1.42. $F(\alpha, \beta) = F(\alpha)(\beta)$.

Demostració. Com que $\alpha, \beta \in F(\alpha)(\beta)$, tenim que $F(\alpha, \beta) \subseteq F(\alpha)(\beta)$. D'altra banda, $F(\alpha) \subseteq F(\alpha, \beta)$ i $\beta \in F(\alpha, \beta)$; per tant, $F(\alpha)(\beta) \subseteq F(\alpha, \beta)$. □

Observació 1.43. Això prova que tota extensió finitament generada $F(\alpha_1, \dots, \alpha_n)$ s'obté com una torre d'extensions

$$F \subseteq F(\alpha_1) \subseteq F(\alpha_1, \alpha_2) \subseteq \cdots \subseteq F(\alpha_1, \dots, \alpha_n),$$

en què cada cos és una extensió simple de l'anterior.

Proposició 1.44. K/F és finita si, i només si, és algebraica i finitament generada.

Demostració. Suposem que K/F és finita. Per la Proposició 1.33 és algebraica. Si $\alpha_1, \dots, \alpha_n$ és una F-base de K, aleshores $K = F(\alpha_1, \dots, \alpha_n)$ així que també és finitament generada.

Suposem ara que K/F és algebraica i finitament generada i veiem que és finita. Per les observacions 1.32 i 1.43 tenim una torre d'extensions

$$F = F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_{n-1} \subseteq F_n = K$$

en què cada cos és una extensió simple de l'anterior. Si $F_{i+1} = F_i(\alpha_i)$, com que α_i és algebraic sobre F_i, per l'Observació 1.36 tenim que $[F_{i+1}\colon F_i] = \deg(\alpha_i)$. Pel Corol·lari 1.41 tenim que

$$[K\colon F] = [F_n\colon F_{n-1}][F_{n-1}\colon F_{n-2}] \dots [F_1\colon F_0] < \infty.$$

□

Observació 1.45. De fet, a la demostració hem vist que si $\alpha_1, \dots, \alpha_n$ són algebraics sobre F, aleshores $F(\alpha_1, \dots, \alpha_n)/F$ és finita.

Proposició 1.46. Si α i β són algebraics sobre F, aleshores $\alpha + \beta$, $\alpha - \beta$, $\alpha\beta$ i α/β (si $\beta \neq 0$) són algebraics.

Demostració. Tots aquests elements pertanyen a $F(\alpha, \beta)$, que és una extensió finita de F i, per tant, algebraica. □

Corol·lari 1.47. Si K/F és una extensió i denotem per E el conjunt d'elements de K que són algebraics sobre F, aleshores E és un cos.

Exemple 1.48. Podem considerar el conjunt de nombres complexos que són algebraics sobre $\mathbb{Q}$, que es denota habitualment per $\overline{\mathbb{Q}}$. Hem vist, doncs, que tenim inclusions de cossos $\mathbb{Q} \subseteq \overline{\mathbb{Q}} \subseteq \mathbb{C}$.

Proposició 1.49. Si tenim una torre d'extensions $L/K/F$, aleshores L/F és algebraica si i només si L/K i K/F ho són.

Demostració. Si L/F és algebraica és clar que L/K i K/F ho són. Vegem la implicació contrària. Sigui $\alpha \in L$ i sigui $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in K[x]$ un polinomi tal que $f(\alpha) = 0$. Considerem el cos $E = F(a_0, \dots, a_n)$. Aleshores, α és algebraic sobre E (ja que f té coeficients a E) i, per tant, $E(\alpha)/E$ és finita. Com que els a_i són algebraics sobre F (ja que K/F és algebraica) tenim que E/F és finita. Així doncs, $E(\alpha)/F$ és finita i, en particular, algebraica; per tant, α és algebraic sobre F. □

Proposició 1.50. Si K/F és algebraica, tot F-morfisme $\sigma\colon K \to K$ és un F-automorfisme.

Demostració. Sabem que σ és injectiva. Si K/F és finita amb $[K\colon F] = n$, aleshores σ és una aplicació lineal injectiva entre dos F-espais vectorials de dimensió n i, per tant, és també exhaustiva. Si K/F és infinita, donat $\alpha \in K$, posem $\alpha = \alpha_1, \alpha_2, \dots, \alpha_r$ les arrels a K de $f = \mathrm{Irr}(\alpha, F)$. Fixem-nos que σ envia arrels de f a arrels de f, ja que

$$f(\sigma(\alpha_i)) = \sigma(f(\alpha_i)) = \sigma(0) = 0.$$

Per tant, si posem $K' = F(\alpha_1, \dots, \alpha_r)$, tenim que $\sigma(K') \subseteq K'$. Ara, K'/F és algebraica i finitament generada; per tant, és finita, i $\sigma_{|K'}\colon K' \to K'$ és exhaustiva pel cas d'extensions finites. Així doncs, $\alpha = \alpha_1$ pertany a la imatge de σ i veiem que σ és exhaustiva. □

1.8. **Composició de cossos.**

Definició 1.51. Sigui K un cos i siguin L_1/K i L_2/K extensions de K contingudes en un cos $\overline{K}$. La composició de L_1 i L_2, denotada L_1L_2, és el subcòs de $\overline{K}$ més petit que conté L_1 i L_2.

Proposició 1.52. L_1L_2 és la intersecció de tots els cossos L tals que $L \subseteq \overline{K}$ i $L_1 \subseteq L$, $L_2 \subseteq L$.

Demostració. És directa, utilitzant el fet que la intersecció de dos cossos que contenen L_1 i L_2 és un cos que conté L_1 i L_2. □

Exemple 1.53. $\mathbb{Q}(\sqrt{2})\mathbb{Q}(\sqrt{3}) = \mathbb{Q}(\sqrt{2},\sqrt{3})$. La prova és senzilla: per una banda, $\sqrt{2},\sqrt{3} \in \mathbb{Q}(\sqrt{2})\mathbb{Q}(\sqrt{3})$ i, per tant, $\mathbb{Q}(\sqrt{2},\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2})\mathbb{Q}(\sqrt{3})$; per l'altra, $\mathbb{Q}(\sqrt{2},\sqrt{3})$ és un cos que conté $\mathbb{Q}(\sqrt{2})$ i $\mathbb{Q}(\sqrt{3})$ i, per tant, conté $\mathbb{Q}(\sqrt{2})\mathbb{Q}(\sqrt{3})$.

Proposició 1.54. Si $[L_1\colon K] < \infty$ i $[L_2\colon K] < \infty$, aleshores $[L_1L_2\colon K] \leq [L_1\colon K][L_2\colon K]$.

Demostració. És un exercici de la llista. □

1.9. **Cossos de descomposició.** Hem vist que per a $f \in F[x]$ no constant existeix una extensió K de F que conté una arrel de f. Ara veurem que, de fet, existeix una extensió que conté totes les arrels de f.

Definició 1.55. Una extensió K de F es diu que és un *cos de descomposició* d'un polinomi $f \in F[x]$ no constant si f descompon completament (com a producte de factors de grau 1) a K, i no ho fa en cap subextensió de K. De manera anàloga, es defineix un cos de descomposició d'un conjunt de polinomis.

Proposició 1.56. Sigui F un cos i $f \in F[x]$ no constant. Existeix una extensió K de F on f descompon completament.

Demostració. Farem inducció sobre $n = \deg(f)$. Si $n = 1$ és evident, suposem l'enunciat cert per a n i vegem-ho per a $n+1$. Sigui K_1/F un cos on f té una arrel α (que sabem que existeix per la Proposició 1.15). Aleshores, $f(x) = (x-\alpha)g(x)$ amb $g \in K_1[x]$ i $\deg(g) = n$. Per hipòtesi d'inducció, existeix una extensió K/K_1 on g descompon completament, i per tant f també descompon completament a K. □

Proposició 1.57. Donat $f \in F[x]$ no constant, existeix un cos de descomposició de f.

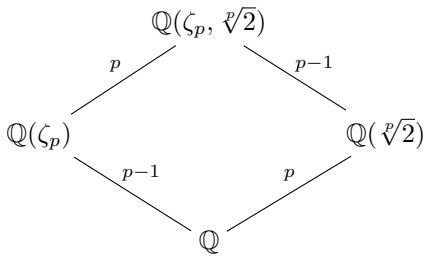
Demostració. Sigui K/F una extensió on f descompon completament. Un cos de descomposició de f és la intersecció de tots els cossos E amb $F \subseteq E \subseteq K$ tals que f descompon completament a E. Alternativament, si $\alpha_1,\ldots,\alpha_n$ són les arrels de f a K, aleshores $F(\alpha_1,\ldots,\alpha_n)$ és un cos de descomposició de f. □

Observació 1.58. Fixem-nos que de la demostració de les dues proposicions anteriors es dedueix que si K és un cos de descomposició de f sobre F, aleshores $[K\colon F] \leq n!$ on $n = \deg(f)$.

Exemple 1.59. $f(x) = x^4 - 2 \in \mathbb{Q}[x]$. Les arrels de f a $\mathbb{C}$ són $\sqrt[4]{2}, -\sqrt[4]{2}, i\sqrt[4]{2}, -i\sqrt[4]{2}$. Per tant un cos de descomposició de f és $\mathbb{Q}(\sqrt[4]{2}, i\sqrt[4]{2})$. Aquest cos també es pot escriure com a $\mathbb{Q}(\sqrt[4]{2}, i)$.

Exemple 1.60. $f(x) = x^n - 1 \in \mathbb{Q}[x]$. Si posem $\zeta_n = e^{\frac{2\pi i}{n}}$, les arrels són ζ_n^k amb $0 \leq k \leq n-1$. Per tant un cos de descomposició és $\mathbb{Q}(\zeta_n)$.

Exemple 1.61. $f(x) = x^p - 2 \in \mathbb{Q}[x]$, on p és primer; les arrels són $\sqrt[p]{2}\zeta_p^k$ amb $0 \leq k \leq p-1$. Un cos de descomposició és, doncs, $K = \mathbb{Q}(\zeta_p, \sqrt[p]{2})$. Sabem alguns subcossos de K:



Els graus es justifiquen de la manera següent: $[\mathbb{Q}(\zeta_p)\colon \mathbb{Q}] = p-1$, ja que[7]

$$\mathrm{Irr}(\zeta_p, \mathbb{Q}) = x^{p-1} + x^{p-2} + \cdots + x + 1.$$

$[\mathbb{Q}(\sqrt[p]{2})\colon \mathbb{Q}] = p$ ja que $\mathrm{Irr}(\sqrt[p]{2}, \mathbb{Q}) = x^p - 2$. Per tant, $[K\colon \mathbb{Q}]$ és divisible per p i $p-1$, i com que són coprimers, de fet, és divisible per $p(p-1)$. Ara bé, $K = \mathbb{Q}(\sqrt[p]{2})\mathbb{Q}(\zeta_p)$ i, per tant,

$$[K\colon \mathbb{Q}] \leq [\mathbb{Q}(\sqrt[p]{2})\colon \mathbb{Q}][\mathbb{Q}(\zeta_p)\colon \mathbb{Q}] = p(p-1).$$

Això prova que $[K\colon \mathbb{Q}] = p(p-1)$ i els graus que falten al diagrama surten, doncs, de la multiplicativitat dels graus en torres d'extensions. Fixem-nos que, en particular, això demostra que el polinomi $x^p - 2$ és irreductible a $\mathbb{Q}(\zeta_p)$, cosa que no és evident d'entrada.

Proposició 1.62. Sigui $\varphi\colon F \to F'$ un isomorfisme de cossos i sigui $f \in F[x]$ i $f' \in F'[x]$ el polinomi obtingut aplicant φ a f. Sigui K un cos de descomposició de f i K' un de f'. Aleshores, existeix un isomorfisme $\tilde{\varphi}\colon K \to K'$ tal que $\tilde{\varphi}_{|F} = \varphi$.

Demostració. Inducció sobre $n = \deg f$. Si $n = 1$, aleshores $K = F$ i $K' = F'$ i l'enunciat és trivial. Suposem l'enunciat cert per a polinomis de grau $n-1$ i provem-lo per a un f de grau n. Si tots els factors irreductibles de f tenen grau 1, aleshores $K = F$ i $K' = F'$ i l'enunciat és cert; podem suposar, doncs, que f té algun factor irreductible g de grau ≥ 2, i denotem per $g' = \varphi(g)$. Sigui $\alpha \in K$ una arrel de g i $\alpha' \in K'$ una arrel de g' (que en particular és arrel també de f'). Per la Proposició 1.28 sabem que existeix un isomorfisme

$$\varphi'\colon F(\alpha) \to F'(\alpha') \quad \text{tal que } \varphi'_{|F} = \varphi \text{ i } \varphi'(\alpha) = \alpha'.$$

Tenim, doncs, descomposicions

$$f(x) = (x-\alpha)f_1(x) \quad f'(x) = (x-\alpha')f_1'(x),$$

amb $f_1 \in F(\alpha)[x]$ i $f_1' \in F'(\alpha')[x]$ i on $f_1' = \varphi'(f_1)$. Podem aplicar, doncs, la hipòtesi d'inducció a φ', els polinomis f_1 i f_1' que són de grau $n-1$ i les extensions $K/F(\alpha)$ i $K'/F'(\alpha')$ (clarament K és un cos de descomposició de $f_1(x)$ sobre $F(\alpha)$ i K' ho és de $f_1'(x)$ sobre $F'(\alpha')$). Per tant, existeix un isomorfisme $\tilde{\varphi}\colon K \longrightarrow K'$ tal que $\tilde{\varphi}_{|F(\alpha)} = \varphi'$. Aleshores, $\tilde{\varphi}_{|F} = \varphi'_{|F} = \varphi$, que és el darrer que ens faltava comprovar. □

Corol·lari 1.63. Si K_1 i K_2 són dos cossos de descomposició de f sobre F, aleshores K_1 i K_2 són F-isomorfs.

Demostració. Prenem $K = K_1$, $K' = K_2$ i $\varphi = \mathrm{id}$ en la proposició anterior. □

[7] En efecte, ζ_p és arrel de $f_p(x) = \frac{x^p-1}{x-1} = x^{p-1} + x^{p-2} + \cdots + x + 1$. Aquest polinomi és irreductible perquè ho és $f_p(x+1) = x^{p-1} + \sum_{i=2}^{p-1} \binom{p}{i} x^{i-1} + p$, ja que és p-Eisenstein.

1.10. **Clausures algebraiques i cossos algebraicament tancats.**

Definició 1.64. Un cos $\overline{F}$ és una clausura algebraica de F si $\overline{F}/F$ és algebraica i tot polinomi de $F[x]$ descompon completament a $\overline{F}$.

Definició 1.65. Un cos K és algebraicament tancat si tot polinomi no constant de $K[x]$ té alguna arrel a K.

Observació 1.66. Si K és algebraicament tancat, aleshores tot $f \in K[x]$ té totes les arrels a K. En particular, no existeixen extensions algebraiques de K no trivials, i el propi K és una clausura algebraica de K.

Proposició 1.67. Sigui F un cos i $\overline{F}$ una clausura algebraica de F. Aleshores $\overline{F}$ és algebraicament tancat.

Demostració. Sigui $f(x) \in \overline{F}[x]$ no constant i α una arrel de f (en un cos de descomposició de f). Aleshores $\overline{F}(\alpha)/\overline{F}$ és algebraica. Com que $\overline{F}/F$ és algebraica, per la Proposició 1.49 $\overline{F}(\alpha)/F$ és algebraica. Per tant, α és arrel d'un polinomi amb coeficients a F i pertany a $\overline{F}$. □

Proposició 1.68. Donat un cos F, existeix un cos algebraicament tancat que conté F.

Demostració. Associem a cada polinomi $f \in F[x]$ no constant una indeterminada x_f i considerem l'anell de polinomis $F[\dots, x_f, \dots]$ amb variables indexades per aquests polinomis. Sigui I l'ideal generat pels polinomis de la forma $f(x_f)$ amb $f \in F[x] \setminus F$. Afirmem que $I \subsetneq F[\dots, x_f, \dots]$. En efecte, si es tingués la igualtat existirien polinomis $g_i \in F[\dots, x_f, \dots]$ i $f_i \in I$ tals que

$$g_1 f_1(x_{f_1}) + \dots g_n f_n(x_{f_n}) = 1. \tag{1.1}$$

Sigui K/F una extensió que contingui arrels α_i dels f_i. Posant $x_{f_i} = \alpha_i$ i fent 0 les altres variables que apareguin als g_i a (1.1), obtenim $0 = 1$, que és absurd.

Per tant, I està contingut en un ideal maximal $\mathcal{M}$ (aquí s'utilitza l'axioma de l'elecció). Aleshores $K_1 = F[\dots, x_f, \dots]/\mathcal{M}$ és un cos que conté F, i per construcció, tot $f \in F[x]$ no constant té una arrel en K_1 (la classe de x_f).

Ara repetim la construcció amb K_1 en lloc de F, i obtenim una extensió K_2/K_1 tal que tot polinomi no constant a $K_1[x]$ té una arrel a K_2. Continuant així, tenim una torre d'extensions

$$F = K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_n \subseteq K_{n+1} \subseteq \cdots$$

amb la propietat que tot $f \in K_i[x]$ no constant té una arrel en $K_{i+1}[x]$.

Posem $K = \cup_i K_i$, que és un cos[8]. Veiem que K és algebraicament tancat. Sigui $f \in K[x]$. Com que f té un nombre finit de coeficients, existeix un índex n tal que $f \in K_n[x]$. Aleshores, f té una arrel en K_{n+1} i, per tant, té una arrel en K. □

Proposició 1.69. Sigui K un cos algebraicament tancat que conté F. El cos $\overline{F}$ format pels elements de K que són algebraics sobre F és una clausura algebraica de F.

Demostració. $\overline{F}/F$ és algebraica per definició. Sigui $f \in F[x]$. Aleshores, f descompon completament a K. Siguin $\alpha_1, \dots, \alpha_n$ les arrels de f a K. Com que els α_i són algebraics sobre F, són de $\overline{F}$, de manera que f descompon completament a $\overline{F}$. □

[8] La unió de cossos no és un cos en general –per això cal considerar la composició– però sí que ho és en el cas d'una torre d'extensions.

Exemple 1.70. El Teorema Fonamental de l'Àlgebra afirma que $\mathbb{C}$ és algebraicament tancat[9]. Per tant, el cos $\overline{\mathbb{Q}}$ format pels nombres complexos que són algebraics sobre $\mathbb{Q}$ és una clausura algebraica de $\mathbb{Q}$.

Proposició 1.71 (Extensió de morfismes a un cos algebraicament tancat)**.** Sigui $\sigma\colon F \to K$ un morfisme amb K algebraicament tancat. Si E/F és algebraica aleshores existeix una extensió $\tilde{\sigma}\colon E \to K$ de σ.

Demostració. Fem primer el cas en què $E = F(\alpha)$ és simple. Posem $f = \mathrm{Irr}(\alpha, F)$; aleshores $\sigma(f) \in K[x]$ descompon completament a K i, en particular, té alguna arrel $\beta \in K$. L'aplicació

$$\begin{array}{ccc} F(\alpha) & \longrightarrow & K \\ g(\alpha) & \longmapsto & \sigma(g)(\beta) \end{array}$$

és un morfisme que estén σ (cf. Proposició 1.28).

El cas general és una aplicació estàndard del Lema de Zorn. Considerem

$$A = \{(L, \sigma_L)\colon F \subseteq L \subseteq E \text{ i } \sigma_L \text{ estén } \sigma\}.$$

En aquest conjunt hi posem un ordre parcial definint que $(L_1, \sigma_{L_1}) \leq (L_2, \sigma_{L_2})$ si $L_1 \subseteq L_2$ i σ_{L_2} estén σ_{L_1}. Ara, si $\{(L_i, \sigma_{L_i})\}_{i\in I}$ és una cadena, definim $L' = \cup L_i$ i $\sigma'\colon L' \to L'$ per $\sigma'(x) = \sigma_{L_i}(x)$ si $x \in L_i$. Aleshores, (L', σ') és una fita superior de la cadena, i pel Lema de Zorn existeix un element maximal (M, σ_M) de A. Aleshores $M = E$, ja que altrament prenent $\alpha \in E \setminus M$ pel cas simple podríem estendre σ_M a $M(\alpha)$ contradient el fet que (M, σ_M) és maximal. Aleshores $\tilde{\sigma} = \sigma_M$ és l'extensió buscada. □

Corol·lari 1.72. Si $\overline{F}$ i $\overline{F}'$ són dues clausures algebraiques de F, aleshores són F-isomorfes.

Demostració. La inclusió $\sigma\colon F \to \overline{F}$ s'estén a $\tilde{\sigma}\colon \overline{F}' \to \overline{F}$, i la inclusió $\tau\colon F \to \overline{F}'$ s'estén a $\tilde{\tau}\colon \overline{F} \to \overline{F}'$. Per la Proposició 1.50 la composició $\tilde{\sigma} \circ \tilde{\tau}\colon \overline{F} \to \overline{F}$ és un F-automorfisme i, per tant, $\tilde{\sigma}$ és exhaustiva i és, doncs, un F-isomorfisme. □

Si F és un cos, denotarem per $\overline{F}$ una clausura algebraica de F. En general, no serà única, però pel resultat anterior és única llevat de F-isomorfisme.

[9] Veurem més endavant una demostració d'aquest teorema.

2. Extensions algebraiques de cossos: normalitat i separabilitat

Sigui K/F una extensió algebraica i per a simplificar suposem-la simple, diguem $K = F(\alpha)$. Sigui $f = \operatorname{Irr}(\alpha, F)$ i $d = \deg f$, de manera que $[K\colon F] = d$. Sigui $\{\alpha_1, \alpha_2, \dots, \alpha_n\}$ el conjunt d'arrels de f a K, on podem suposar que $\alpha_1 = \alpha$.

Ja hem vist (Observació 1.29) que si $\sigma \in \operatorname{Aut}(K/F)$, aleshores

$$f(\sigma(\alpha)) = \sigma(f(\alpha)) = 0,$$

de manera que $\sigma(\alpha) \in \{\alpha_1, \dots, \alpha_n\}$. D'altra banda, també hem vist que per a tot $i = 1, \dots, n$ existeix $\sigma_i \in \operatorname{Aut}(K/F)$ tal que $\sigma_i(\alpha) = \alpha_i$. Com que un F-automorfisme de K queda unívocament determinat per la imatge de α, veiem que $\operatorname{Aut}(K/F) = \{\sigma_1, \dots, \sigma_n\}$ i, en particular, $\#\operatorname{Aut}(K/F) = n$. Com que $n \leq d$, tenim doncs que $\#\operatorname{Aut}(K/F) \leq [K\colon F]$, i la desigualtat pot ser estricta per dos motius:

(1) El polinomi $f = \operatorname{Irr}(\alpha, F)$ no descompon completament a K;
(2) El polinomi $f = \operatorname{Irr}(\alpha, F)$ té arrels repetides (és a dir, amb multiplicitat > 1).

En el primer cas, direm que K/F no és normal, i en el segon, que K/F no és separable. Les extensions per a les quals la teoria de Galois és satisfactòria són aquelles que no tenen aquests inconvenients; és a dir, que són normals i separables. En aquest capítol introduïm i estudiem amb detall aquestes dues propietats de les extensions algebraiques. Ho farem per a extensions algebraiques arbitràries (no necessàriament simples), tot i que acabarem veient que tota extensió finita separable és simple; així doncs, en el cas que ens interessa en la teoria de Galois, sempre treballarem amb extensions que podrem suposar simples.

2.1. **Extensions normals.**

Definició 2.1. Una extensió algebraica K/F és *normal* si per a tot $\alpha \in K$ el polinomi $\operatorname{Irr}(\alpha, F)$ descompon completament a K. També es diu que K és normal sobre F.

Exemple 2.2. Per $d \in \mathbb{Q}^\times \setminus (\mathbb{Q}^\times)^2$ l'extensió quadràtica $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ és normal. En efecte, donat $\alpha = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ tenim que α és arrel del polinomi

$$f_\alpha(x) = (x - (a + b\sqrt{d}))(x - (a - b\sqrt{d})) = x^2 - 2ax + a^2 - b^2 d \in \mathbb{Q}[x].$$

Per tant, $\operatorname{Irr}(\alpha, \mathbb{Q}) \mid f_\alpha$ i, com que f_α descompon completament a $\mathbb{Q}(\sqrt{d})$, veiem que $\operatorname{Irr}(\alpha, \mathbb{Q})$ també. En particular, $\operatorname{Irr}(\sqrt{d}, \mathbb{Q})$ té les dues arrels a $\mathbb{Q}(\sqrt{d})$, que són $\sqrt{d}$ i $-\sqrt{d}$.

Fixem-nos que per l'Observació 1.29 hi ha un $\sigma \in \operatorname{Aut}(\mathbb{Q}(\sqrt{2}/\mathbb{Q}))$ tal que $\sigma(\sqrt{2}) = -\sqrt{2}$. De fet, aquest és l'únic automorfisme no trivial i, per tant, $\operatorname{Aut}(\mathbb{Q}(\sqrt{d})/\mathbb{Q}) = \{1, \sigma\}$.

Exemple 2.3. Més en general, si F és un cos qualsevol i $a \in F$, aleshores $F(\sqrt{a})$ és normal sobre F.

Exemple 2.4. $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ no és normal, ja que $\operatorname{Irr}(\sqrt[3]{2}, \mathbb{Q}) = x^3 - 2$ i les altres dues arrels d'aquest polinomi no viuen a $\mathbb{Q}(\sqrt[3]{2})$ (ja que no són reals i $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$). De nou, per l'Observació 1.29 veiem que $\operatorname{Aut}(\mathbb{Q}(\sqrt[3]{2}))/\mathbb{Q} = \{1\}$.

En aquests dos exemples veiem la relació entre la propietat de normalitat i els automorfismes de l'extensió. De manera una mica imprecisa, i que ja anirem precisant, una extensió que no és normal té pocs automorfismes.

Proposició 2.5. Sigui K/F una extensió algebraica i $\overline{K}$ una clausura algebraica de K. Les propietats següents són equivalents:

(1) K/F és normal.
(2) K és el cos de descomposició d'un conjunt de polinomis S de $F[x]$.
(3) Per a tot F-morfisme $\sigma\colon K \to \overline{K}$ es té que $\sigma(K) = K$.

Demostració. (1) $\Rightarrow$ (2): Com que per a tot $\alpha \in K$ les arrels de $\mathrm{Irr}(\alpha, F)$ pertanyen a K, K és el cos de descomposició de $\{\mathrm{Irr}(\alpha, F)\}_{\alpha\in K}$.

(2) $\Rightarrow$ (3): Denotem per A el conjunt de totes les arrels dels polinomis de S. Aleshores $K = F(A)$. Sigui $\alpha \in A$ i $\sigma\colon K \to \overline{K}$. Aleshores $\sigma(\alpha) \in A$, ja que si α és arrel de f tenim que $f(\sigma(\alpha)) = \sigma(f(\alpha)) = 0$. Per tant, $\sigma\colon K \to K$ és un F-morfisme i, com que K/F és algebraic, serà un automorfisme.

(3) $\Rightarrow$ (1): Sigui $\alpha \in K$ i β una arrel de $\mathrm{Irr}(\alpha, F)$ a $\overline{K}$. Volem veure que $\beta \in K$. L'aplicació

$$\begin{array}{rccc} \sigma\colon & F(\alpha) & \longrightarrow & \overline{K} \\ & f(\alpha) & \longmapsto & f(\beta) \end{array}$$

és un F-morfisme amb imatge $F(\beta)$. Com que $\overline{K}$ és algebraicament tancat i K/F algebraica, per la Proposició 1.71 σ s'estén a $\sigma\colon K \to \overline{K}$. Per (3) sabem que $\sigma(K) = K$ i, per tant, $\beta \in \sigma(K) = K$. □

La caracterització (2) és molt útil. Per exemple, ens permet provar el resultat següent de manera fàcil.

Proposició 2.6. Si $K = F(A)$ i per a tot $\alpha \in A$ el polinomi $\mathrm{Irr}(\alpha, F)$ descompon completament a K, aleshores K/F és normal.

Demostració. K és el cos de descomposició del conjunt de polinomis $\{\mathrm{Irr}(\alpha, F)\}_{\alpha\in A}$. □

Proposició 2.7. Sigui $L/K/F$. Si L/F és normal, aleshores també ho és L/K.

Demostració. Si L és el cos de descomposició d'un conjunt $S \subseteq F[x]$, també és cos de descomposició dels mateixos polinomis pensats com a polinomis de $K[x]$. □

Definició 2.8. Donada K/F algebraica, una clausura normal és una extensió N/K tal que N/F és normal i és minimal amb aquesta propietat (és a dir, si $K \subseteq N' \subseteq N$ amb N'/F normal, aleshores $N' = N$).

Proposició 2.9. N/K és una clausura normal de K/F si, i només si, N és un cos de descomposició de $\{\mathrm{Irr}(\alpha, F)\}_{\alpha\in K}$.

Demostració. Exercici. □

Proposició 2.10. Si K/F és finita amb $K = F(\alpha_1, \ldots, \alpha_n)$, aleshores una clausura normal de K és el cos de descomposició del polinomi $\prod_{i=1}^{n} \mathrm{Irr}(\alpha_i, F)$. En particular, la clausura normal de K/F és única llevat de F-isomorfisme.

Demostració. Exercici. □

Exemple 2.11. $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ no és normal, ja que les arrels de $\mathrm{Irr}(\sqrt[4]{2}, \mathbb{Q}) = x^4 - 2$ són $\sqrt[4]{2}, -\sqrt[4]{2}, i\sqrt[4]{2}, -i\sqrt[4]{2}$. Per tant, la clausura normal és $\mathbb{Q}(\sqrt[4]{2}, i)$. Fixem-nos que tenim una torre d'inclusions

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt[4]{2}) \subseteq \mathbb{Q}(\sqrt[4]{2}, i),$$

on $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ i $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ són normals, però $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ no és normal. És a dir, una extensió normal d'una extensió normal pot no ser normal.

Proposició 2.12 (Extensió de morfismes en cossos normals)**.** Sigui K/F una extensió algebraica normal i E/F una subextensió (és a dir, $F \subseteq E \subseteq K$). Tot F-morfisme $\sigma\colon E \to K$ s'estén a un F-morfisme $\tilde{\sigma}\colon K \to K$ (en particular $\tilde{\sigma} \in \mathrm{Aut}(K/F)$.

Demostració. Posem $\overline{K}$ una clausura algebraica de K. Aleshores $\sigma\colon E \to K \subseteq \overline{K}$ s'estén, per la Proposició 1.71, a $\tilde{\sigma}\colon K \to \overline{K}$. Com que K és normal, $\tilde{\sigma}(K) = K$ i, per tant, tenim $\tilde{\sigma}\colon K \to K$. Com que K/F és algebraica, $\tilde{\sigma}$ és un automorfisme. □

2.2. **Extensions separables.**

Definició 2.13. Un polinomi $f(x) \in F[x]$ es diu separable si totes les seves arrels en un cos de descomposició són simples (és a dir, de multiplicitat 1). Es diu inseparable en cas contrari.

Observació 2.14. Aquesta noció no depèn del cos de descomposició escollit, ja que tots ells són isomorfs.

Definició 2.15. Sigui K/F algebraica. Diem que $\alpha \in K$ és separable sobre F si $\mathrm{Irr}(\alpha, F)$ és separable. Diem que K/F és separable si tot $\alpha \in K$ és separable sobre F i que K/F és inseparable en cas contrari.

Proposició 2.16. Si $L/K/F$ i $\alpha \in L$ és separable sobre F, aleshores també ho és sobre K.

Demostració. Això és perquè $\mathrm{Irr}(\alpha, K) \mid \mathrm{Irr}(\alpha, F)$. □

Exemple 2.17.
(1) $x^2 + 1 \in \mathbb{Q}[x]$ és separable.
(2) $x^2 + 1 \in \mathbb{F}_2[x]$ és inseparable, ja que $x^2 + 1 = (x+1)^2$. Més en general, si $a \in \mathbb{F}_p$, $x^p + a$ és inseparable a $\mathbb{F}_p$ ja que $x^p + a = (x+a)^p$.
(3) Sigui $F = \mathbb{F}_p(t)$ i $f(x) = x^p - t \in F[x]$. Aquest polinomi és irreductible (és t-Eisenstein). Sigui α una arrel de f en un cos de descomposició; aleshores $\alpha^p = t$. Per tant:
$$x^p - t = x^p - \alpha^p = (x - \alpha)^p$$
d'on veiem que f té una única arrel amb multiplicitat p i és inseparable. Fixem-nos que si posem $K = F(\alpha)$, aleshores $\mathrm{Aut}(K/F) = \{1\}$, ja que tot $\sigma \in \mathrm{Aut}(K/F)$ envia α a una arrel de f, però l'única arrel de f és α. El fet que K l'hem obtingut adjuntant α i $\mathrm{Irr}(\alpha, F)$ no és separable té com a conseqüència que K/F no té automorfismes no trivials. Això és un fet general, que anirem precisant: les extensions que no són separables, tenen "pocs automorfismes".

Definició 2.18. Donat $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in F[x]$ definim el seu derivat com a
$$f'(x) = n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \cdots + a_1.$$

Les propietats següents es comproven fàcilment a partir de la definició:
- $(f+g)' = f' + g'$.
- $(fg)' = f'g + fg'$.
- $(af)' = af'$ si $a \in F$.

Lema 2.19. Sigui K/F una extensió i $f, g \in F[x]$. Aleshores $\gcd(f,g) = 1$ a $F[x]$ si i només si $\gcd(f,g) = 1$ a $K[x]$.

Demostració. És una conseqüència de l'algoritme d'Euclides, que calcula $\gcd(f,g)$ fent les operacions a F, fins i tot si pensem f i g com a polinomis de $K[x]$. □

Proposició 2.20. Un polinomi f és separable si i només si $\gcd(f, f') = 1$.

Demostració. Si f no és separable, aleshores $f(x) = (x-\alpha)^2 g(x)$ per a cert $\alpha \in K$ i $g(x) \in K[x]$. Aleshores $f'(x) = 2(x-\alpha)g(x) + (x-\alpha)^2 g'(x)$ i, per tant, $(x-\alpha) \mid \gcd(f, f')$.

D'altra banda, si $(x-\alpha) \mid \gcd(f, f')$, aleshores posant $f(x) = (x-\alpha)g(x)$ tenim que $f'(x) = g(x) + (x-\alpha)g'(x)$; com que $f'(\alpha) = 0$, veiem que $g(\alpha) = 0$ i, aleshores, $(x-\alpha) \mid g$ amb la qual cosa $(x-\alpha)^2 \mid f$. □

Proposició 2.21. Si $\mathrm{char}(F) = 0$, aleshores tot $f \in F[x]$ irreductible és separable.

Demostració. Si $\mathrm{char}(F) = 0$, tenim que $\deg(f') < \deg(f)$ i $f' \neq 0$. Per tant, $\gcd(f', f) = 1$. □

Corol·lari 2.22. Tota extensió algebraica d'un cos de característica 0 és separable.

Proposició 2.23. Sigui F de característica $p > 0$. Un polinomi irreductible $f \in F[x]$ és inseparable si, i només si, $f(x) = g(x^p)$ per a algun $g \in F[x]$.

Demostració. Com que f és irreductible $\gcd(f', f)$ només pot ser 1 o f (llevat d'unitats a $F[x]$). Si $f' \neq 0$, com que $\deg(f') < \deg(f)$, aleshores és 1. Per tant, si f és inseparable necessàriament $f' = 0$. Si posem

$$f(x) = a_n x^n + \cdots + a_1 x + a_0,$$

veiem que els únics coeficients no nuls són, doncs, aquells en què l'exponent és múltiple de p; per tant, $f(x) = g(x^p)$ per a algun g.

D'altra banda, és directe veure que si $f(x) = g(x^p)$, aleshores $f' = 0$ i, per tant, $\gcd(f', f) = f$. □

El resultat següent fa precís el comentari informal de l'Exemple 2.17 (3).

Proposició 2.24. Sigui K/F finita de grau n i N/K una extensió tal que N/F és normal. El nombre de F-morfismes $\sigma\colon K \to N$ és menor o igual que n, amb igualtat si i només si K/F és separable.

Demostració. Farem la prova per inducció sobre n. Si $n = 1$, el resultat és evident; suposem-lo cert per a extensions de grau $< n$ i provem-lo per a una extensió K/F de grau n. Sabem que per $\alpha \in K \setminus F$ el polinomi $\mathrm{Irr}(\alpha, F)$ descompon completament a N, ja que N/F és normal; posem $\alpha = \alpha_1, \ldots, \alpha_r$ les seves arrels. Fixem-nos que $r \leq [F(\alpha)\colon F]$ amb igualtat si, i només si, α és separable sobre F. Per a cada $i = 1, \ldots, r$ tenim un F-morfisme:

$$\begin{array}{rccc} \tilde{\tau}_i\colon & F(\alpha) & \longmapsto & N \\ & f(\alpha) & \longmapsto & f(\alpha_i). \end{array}$$

Com que N/F és normal i $N/F(\alpha)$ algebraica, per la Proposició 2.12 s'estenen a $\tau_i\colon N \to N$ amb $\tau_i(\alpha) = \alpha_i$.

Ara considerem $N/F(\alpha)$. Com que $N/F(\alpha)$ és normal i $s = [K\colon F(\alpha)] < n$, per hipòtesi d'inducció existeixen $t \leq s$ $F(\alpha)$-morfismes $K \to N$ amb igualtat si i només si $K/F(\alpha)$ és separable. Anomenem-los $\sigma_1, \ldots, \sigma_t$. Per a $i = 1, \ldots, r$ i $j = 1, \ldots, s$ tenim un F-morfisme $\tau_i \circ \sigma_j\colon K \to N$. D'aquests n'hi ha $rt \leq [K\colon F(\alpha)][K\colon F(\alpha)] = [K\colon F]$.

Veiem ara que tot F-morfisme $\sigma\colon K \to N$ és de la forma $\tau_i \circ \sigma_j$ pera algun i i per a algun j. Sabem que $\sigma(\alpha) = \alpha_i$ per a algun i i, per tant, $\tau_i^{-1} \circ \sigma$ fixa α. Això vol dir que $\tau_i^{-1} \circ \sigma$ és un $F(\alpha)$-morfisme i, per tant, $\tau_i^{-1} \circ \sigma = \sigma_j$ per a algun j. Tenim doncs que $\sigma = \tau_i \circ \sigma_j$.

D'altra banda els $\tau_i \circ \sigma_j$ són tots ells diferents: $\tau_i \circ \sigma_j(\alpha) = \alpha_i$ ja que σ_j és un $F(\alpha)$-morfisme; si $\tau_i \circ \sigma_j = \tau_{i'} \circ \sigma_{j'}$, aleshores $\tau_i = \tau_{i'}$ i, com que els τ's són automorfismes, $\sigma_j = \sigma_{j'}$.

Finalment, si K/F és separable, aleshores val la igualtat, ja que llavors $r = [F(\alpha)\colon F]$ i $t = s$. I si K/F no és separable, aleshores no val la igualtat, ja que llavors podem prendre $\alpha \in K$ inseparable sobre K i tenim que $r < [F(\alpha)\colon F]$ amb la qual cosa $rt < [K\colon F]$. □

Proposició 2.25. Una extensió algebraica simple $F(\alpha)/F$ és separable si, i només si, α és separable.

Demostració. Denotem per m el nombre de F-morfismes de $F(\alpha)$ en una clausura normal N de F. Sabem que m és el nombre d'arrels de $\mathrm{Irr}(\alpha, F)$ en N. Per tant, α és separable si i només si $m = \deg(\alpha)$, és a dir, si i només si $m = [F(\alpha)\colon F]$. D'altra banda, per la proposició anterior $F(\alpha)/F$ és separable si i només si $m = [F(\alpha)\colon F]$. □

Proposició 2.26. Sigui $K/E/F$ una torre d'extensions algebraiques. Aleshores K/F és separable si, i només si, K/E i E/F són separables.

Demostració. Exercici (pista: feu primer el cas en què K/F és finita, i vegeu que el cas general es redueix a aquest). □

2.3. **Extensions simples.**

Teorema 2.27 (Teorema de l'element primitiu)**.** Tota extensió K/F finita i separable és simple.

Demostració. Si F és un cos finit ho veurem més endavant. Suposem ara que F té un nombre infinit d'elements. Donats $\alpha, \beta \in K$, trobarem un $\gamma \in K$ tal que $F(\alpha, \beta) = F(\gamma)$. Si veiem això ja ho tindrem, perquè K/F és finita i, per tant, $K = F(\delta_1, \delta_2, \ldots, \delta_n)$ i obtenim el resultat per inducció.

Posem $f = \mathrm{Irr}(\alpha, F)$ i $g = \mathrm{Irr}(\beta, F)$. Posem també $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n$ les arrels de f i $\beta = \beta_1, \beta_2, \ldots, \beta_m$ les arrels de g en un cos de descomposició, que són totes elles diferents per la hipòtesi de separabilitat. Com que F és infinit, existeix $\lambda \in F$ tal que

$$\lambda \neq \frac{\alpha_1 - \alpha_i}{\beta_j - \beta_1} \quad \text{per a tot } \ i \ \text{ i per a tot } j \neq 1. \tag{2.1}$$

Posem $\gamma = \alpha + \lambda\beta$. Clarament $F(\gamma) \subseteq F(\alpha, \beta)$. Per a veure la inclusió contrària, n'hi ha prou de veure que $\beta \in F(\gamma)$ (ja que llavors $\alpha = \gamma - \lambda\beta \in F(\gamma)$). Posem $h = \mathrm{Irr}(\beta, F(\gamma))$. Aleshores $h \mid g$ i, per tant, les seves arrels només poden estar entre els β_i. També tenim que $h \mid f(\gamma - \lambda x)$, ja que $f(\gamma - \lambda\beta) = f(\alpha) = 0$. Per tant, les arrels de h també són arrels de $f(\gamma - \lambda x)$. Si algun β_j amb $j > 1$ és arrel de $f(\gamma - \lambda x)$, aleshores $\gamma - \lambda\beta_j$ seria arrel de f i, per tant, $\gamma - \lambda\beta_j = \alpha_i$ per a algun i, però això és una contradicció amb (2.1). La conclusió, doncs, és que l'única arrel de h és $\beta = \beta_1$. Com que h és separable i no té arrels amb multiplicitat > 1, veiem que h té grau 1 i, per tant, $h = x - \beta$; com que h té coeficients a $F(\gamma)$, això implica que β pertany a $F(\gamma)$. □

3. Teoria de Galois

Recordem que $\mathrm{Aut}(K/F)$ denota el grup dels F-automorfismes de K. Fixem-nos que si K/F és normal, aleshores

$$\mathrm{Aut}(K/F) = \{F\text{-morfismes } K \to \overline{K}\}.$$

Observació 3.1. Si $F \subseteq E \subseteq K$, aleshores $\mathrm{Aut}(K/E)$ és un subgrup de $\mathrm{Aut}(K/F)$.

Definició 3.2. Sigui G un subgrup de $\mathrm{Aut}(K/F)$. El cos fix de G és

$$K^G = \{x \in K : \sigma(x) = x \text{ per a tot } \sigma \in G\}.$$

És fàcil veure que K^G és un subcòs de K que conté F. Tenim, doncs, aplicacions $\mathcal{F}$ i $\mathcal{G}$:

$$\begin{array}{ccc} \{\text{subcossos } E \text{ amb } F \subseteq E \subseteq K\} & \longleftrightarrow & \{\text{subgrups } H \leq \mathrm{Aut}(K/F)\} \\ E & \xrightarrow{\mathcal{G}} & \mathrm{Aut}(K/E) \\ K^H & \xleftarrow{\mathcal{F}} & H \end{array} \tag{3.1}$$

Proposició 3.3. Les aplicacions $\mathcal{F}$ i $\mathcal{G}$ satisfan les propietats següents:

(1) Si $E_1 \subseteq E_2$, aleshores $\mathrm{Aut}(K/E_2) \leq \mathrm{Aut}(K/E_1)$.
(2) Si $H_1 \leq H_2$, aleshores $K^{H_2} \subseteq K^{H_1}$.
(3) $E \subseteq \mathcal{F}(\mathcal{G}(E))$, és a dir, $E \subseteq K^{\mathrm{Aut}(K/E)}$.
(4) $H \leq \mathcal{G}(\mathcal{F}(H))$, és a dir, $H \leq \mathrm{Aut}(K/K^H)$.

Demostració. Són directes a partir de les definicions. □

El Teorema Fonamental de la teoria de Galois ens dirà que si K/F és finita, normal i separable, aleshores $\mathcal{F} \circ \mathcal{G} = \mathrm{id}$ i que $\mathcal{G} \circ \mathcal{F} = \mathrm{id}$.

3.1. Extensions de Galois.

Definició 3.4. Una extensió finita[10] K/F és de Galois si és normal i separable.

Proposició 3.5. Una extensió finita K/F és de Galois si i només si K és el cos de descomposició d'un polinomi separable $f \in F[x]$.

Demostració. És conseqüència directa de la caracterització de normalitat de la Proposició 2.5 (2) i de la caracterització de separabilitat de la Proposició 2.25. □

Definició 3.6. Si K/F és de Galois, aleshores el grup $\mathrm{Aut}(K/F)$ s'anomena grup de Galois de l'extensió i es denota $\mathrm{Gal}(K/F)$.

Proposició 3.7. Si K/F és Galois i E/F és una subextensió, aleshores K/E és Galois.

Demostració. És conseqüència de la Proposició 2.7 i la Proposició 2.16. □

Proposició 3.8. Si K/F és de Galois, aleshores $F = K^{\mathrm{Gal}(K/F)}$.

[10] També hi ha una teoria de Galois per a extensions infinites, però nosaltres només farem el cas d'extensions finites i, per tant, ja incorporem la condició de finitud en la definició d'extensió de Galois.

Demostració. Ja sabem que $F \subseteq K^{\mathrm{Gal}(K/F)}$. Sigui ara $\alpha \in K^{\mathrm{Gal}(K/F)}$; veurem que, de fet, $F(\alpha) = F$ i això ja ens diu que $\alpha \in F$. Sigui

$$\sigma\colon F(\alpha) \longrightarrow K$$

un F-morfisme; com que K/F és normal, σ estén a $\tilde{\sigma} \in \mathrm{Gal}(K/F)$ per la Proposició 2.12. Ara $\tilde{\sigma}_{|F} = \mathrm{id}$ i $\tilde{\sigma}(\alpha) = \alpha$ (ja que $\alpha \in K^{\mathrm{Gal}(K/F)}$). Així doncs $\tilde{\sigma}_{|F(\alpha)} = \mathrm{id}$ i, per tant, $\sigma = \mathrm{id}$. Tenim doncs que només hi ha un únic F-morfisme $F(\alpha) \to K$ i com que K/F és normal i $F(\alpha)$ separable, això vol dir que $[F(\alpha)\colon F] = 1$ per la Proposició 2.24. □

Proposició 3.9. Si K/F és de Galois, aleshores $\mathcal{F} \circ \mathcal{G} = \mathrm{id}$.

Demostració. Si K/F és Galois, aleshores K/E és Galois per a tota subextensió E/F per la Proposició 3.7. Aplicant el resultat anterior a K/E tenim que $E = E^{\mathrm{Gal}(K/E)}$. □

Proposició 3.10. Sigui K/F finita. Aleshores, $|\operatorname{Aut}(K/F)| \leq [K\colon F]$, amb igualtat si i només si K/F és Galois.

Demostració. Aplicant la Proposició 2.24 amb $N = \overline{K}$, sabem que el nombre de F-morfismes $\sigma\colon K \to \overline{K}$ és $\leq [K\colon F]$, amb igualtat si i només si K/F és separable. Com que tot $\sigma \in \operatorname{Aut}(K/F)$ és un F-morfisme $K \to \overline{K}$, això ja ens mostra que $|\operatorname{Aut}(K/F)| \leq [K\colon F]$.

Veiem ara la segona afirmació de l'enunciat. En primer lloc, si K/F és Galois, tot F-morfisme $\sigma\colon K \to \overline{K}$ pertany a $\sigma \in \mathrm{Gal}(K/F)$, per ser K/F normal; i n'hi ha exactament $[K\colon F]$, per ser K/F separable. Per tant, si K/F és Galois, aleshores $|\mathrm{Gal}(K/F)| = [K\colon F]$.

D'altra banda, si K/F no és Galois, aleshores no és normal o no és separable. si K/F no és separable, d'aquests F-morfismes de K en $\overline{K}$ n'hi ha menys que $[K\colon F]$. Si K/F no és normal, existeix un F-morfisme $\sigma\colon K \to \overline{K}$ tal que $\sigma(K) \neq K$, i per tant, $\sigma \notin \operatorname{Aut}(K/F)$. En tots dos casos, $|\operatorname{Aut}(K/F)| < [K\colon F]$. □

Teorema 3.11 (Teorema d'Artin)**.** Sigui K/F una extensió finita i $G \leq \operatorname{Aut}(K/F)$. Posem $E = K^G$. Aleshores, K/E és de Galois i $\mathrm{Gal}(K/E) = G$.

Demostració. Com que K/F és finita, K/E també ho és i, en particular, és algebraica. Veiem ara que K/E és normal i separable. Posem $G = \{\sigma_1, \ldots, \sigma_n\}$, prenem $\alpha \in K$ i considerem el conjunt $A = \{\sigma_1(\alpha), \ldots, \sigma_n(\alpha)\}$. Fixem-nos que $\alpha \in A$, ja que G conté la identitat. En aquest conjunt poden haver-hi elements repetits; és a dir, si posem $r = |A|$, pot ser que $r < n$. Denotem per $\alpha_1, \ldots, \alpha_r$ els elements de A (un d'ells és α, podem suposar que $\alpha_1 = \alpha$). Fixem-nos que, com que G és un grup, per a tot $\sigma \in G$ tenim que

$$\{\sigma(\alpha_1), \ldots, \sigma(\alpha_r)\} = \{\sigma\sigma_1(\alpha), \ldots, \sigma\sigma_n(\alpha)\} = \{\alpha_1, \ldots, \alpha_r\}. \tag{3.2}$$

Definim el polinomi

$$p(x) = (x - \alpha_1) \cdots (x - \alpha_r) = x^r + a_{r-1}x^{r-1} + \cdots + a_1 x + a_0 \in K[x].$$

La igualtat de conjunts (3.2) implica que $\sigma(p) = p$ per a tot $\sigma \in G$ i, per tant, que els a_i pertanyen a E. Veiem, doncs, que α és arrel d'un polinomi separable $p(x) \in E[x]$ que descompon completament i, per tant, K/E és normal i separable.

Provem ara que $\mathrm{Gal}(K/E) = G$. Tenim que $G \leq \mathrm{Gal}(K/E)$ i, com que K/E és Galois, $|\mathrm{Gal}(K/E)| = [K\colon E]$. Si veiem que que $|G| = [K\colon E]$, tindrem que $|G| = |\mathrm{Gal}(K/E)|$ i haurem acabat. Com que $G \subseteq \mathrm{Gal}(K/E)$, tenim que $|G| \leq |\mathrm{Gal}(K/E)| = [K\colon E]$. Per a l'altra desigualtat, sigui $\alpha \in K$. Aleshores, $[E(\alpha)\colon E] \leq |G|$, ja que hem vist abans que α és arrel d'un polinomi amb coeficients a E de grau $\leq |G|$. Prenem $\alpha \in K$ de grau màxim sobre E. Afirmem que

$K = E(\alpha)$. En efecte, si $\beta \in K$, aleshores pel Teorema de l'Element Primitiu $E(\alpha, \beta) = E(\gamma)$, però $[E(\gamma)\colon E] = [E(\alpha)\colon E]$ per la maximalitat del grau; com que $E(\alpha) \subseteq E(\gamma)$, veiem que $E(\alpha) = E(\gamma)$ i $\beta \in E(\alpha)$. Així doncs, $[K\colon E] = [E(\alpha)\colon E] \leq |G|$. □

Observació 3.12. El Teorema d'Artin, de fet, és cert en una versió una mica més general, que diu que si K és un cos, G és un subgrup finit dels automorfismes de K i $E = K^G$, aleshores K/E és Galois i $\mathrm{Gal}(K/E) = G$. L'únic que ens ha faltat provar d'aquest resultat més general és que K/E és finita.

Corol·lari 3.13. Si K/F és de Galois, aleshores $\mathcal{G} \circ \mathcal{F} = \mathrm{id}$.

Demostració. Si $H \leq \mathrm{Gal}(K/F)$ i posem $E = K^H$, tenim que K/E és finita i pel Teorema d'Artin $\mathrm{Gal}(K/E) = H$. □

Lema 3.14. Sigui K/F de Galois i E un cos intermedi. Per a tot $\sigma \in \mathrm{Gal}(K/F)$ tenim que $\sigma(E)$ és un altre cos intermedi i $\mathrm{Gal}(K/\sigma(E)) = \sigma\,\mathrm{Gal}(K/E)\sigma^{-1}$.

Demostració. És clar que si $F \subseteq E \subseteq K$, aleshores $F \subseteq \sigma(E) \subseteq K$. Vegem la igualtat $\mathrm{Gal}(K/\sigma(E)) = \sigma\,\mathrm{Gal}(K/E)\sigma^{-1}$.

- [$\supseteq$] Si $x \in E$ i $\tau \in \mathrm{Gal}(K/E)$, aleshores $(\sigma\tau\sigma^{-1})(\sigma(x)) = \sigma(x)$ o sigui que $\sigma\tau\sigma^{-1} \in \mathrm{Gal}(K/\sigma(E))$.
- [$\subseteq$] Si $\tau \in \mathrm{Gal}(K/\sigma(E))$, aleshores per un argument semblant veiem que $\sigma^{-1}\tau\sigma \in \mathrm{Gal}(K/E)$; per tant, $\tau \in \sigma\,\mathrm{Gal}(K/E)\sigma^{-1}$.

□

Proposició 3.15. Si K/F és Galois i E/F és una subextensió, aleshores E/F és Galois si i només si $\mathrm{Gal}(K/E) \trianglelefteq \mathrm{Gal}(K/F)$.

Demostració. E/F és separable (cf. Corol·lari 2.26) i, per tant, E/F és Galois si i només si E/F és normal. Com que K/F és Galois, tot F-morfisme $\sigma_0\colon E \to K$ s'aixeca a $\sigma \in \mathrm{Gal}(K/F)$. Per tant, E/F és normal si i només si $\sigma(E) = E$ per a tot $\sigma \in \mathrm{Gal}(K/F)$. Per la injectivitat de $\mathcal{G}$, això és si i només si $\mathrm{Gal}(K/E) = \mathrm{Gal}(K/\sigma(E))$ per a tot $\sigma \in \mathrm{Gal}(K/F)$. Pel Lema 3.14 això és si i només si $\mathrm{Gal}(K/E) = \sigma\,\mathrm{Gal}(K/E)\sigma^{-1}$ per a tot $\sigma \in \mathrm{Gal}(K/F)$, és a dir, si i només si $\mathrm{Gal}(K/E)$ és normal. □

Proposició 3.16. Si K/F és Galois i E és un cos intermedi amb E/F Galois, aleshores

$$\mathrm{Gal}(E/F) \simeq \mathrm{Gal}(K/F)/\,\mathrm{Gal}(K/E). \tag{3.3}$$

Demostració. Si $\sigma \in \mathrm{Gal}(K/F)$ podem considerar $\sigma_{|E}$, la seva restricció a E. Com que E/F és normal, $\sigma(E) = E$ i, per tant, $\sigma_{|E}$ pertany a $\mathrm{Gal}(E/F)$. L'aplicació

$$\begin{array}{ccc} \mathrm{Gal}(K/F) & \longrightarrow & \mathrm{Gal}(E/F) \\ \sigma & \longmapsto & \sigma_{|E} \end{array}$$

és un morfisme de grups exhaustiu (cf. Proposició 2.12) amb nucli $\mathrm{Gal}(K/E)$. L'isomorfisme de l'enunciat surt doncs del primer teorema d'isomorfisme per a grups. □

3.2. **Teorema Fonamental.**

Teorema 3.17 (Teorema Fonamental de la Teoria de Galois)**.** Si K/F és de Galois finita, aleshores les aplicacions $\mathcal{F}$ i $\mathcal{G}$ de (3.1) són bijeccions i inverses una de l'altra. A més, aquestes aplicacions satisfan les propietats següents:

(1) Si els subcossos E_1 i E_2 es corresponen amb els subgrups H_1, H_2, aleshores $E_1 \subseteq E_2$ si i només si $H_2 \leq H_1$.
(2) Si H es correspon amb E, aleshores $[K\colon E] = |H|$ i $[E\colon F] = [\mathrm{Gal}(K/F)\colon H]$.
(3) Si H es correspon amb E, aleshores K/E és de Galois amb $\mathrm{Gal}(K/E) = H$.
(4) E és de Galois sobre F si i només si $\mathrm{Gal}(K/E) \trianglelefteq \mathrm{Gal}(K/F)$ i, aleshores,

$$\mathrm{Gal}(E/F) \simeq \mathrm{Gal}(K/F)/\mathrm{Gal}(K/E).$$

(5) Si els subcossos E_1 i E_2 es corresponen amb els subgrups H_1, H_2, aleshores $H_1 \cap H_2$ es correspon amb E_1E_2 (la composició de E_1 i E_2), i $E_1 \cap E_2$ es correspon amb H_1H_2 (el subgrup generat per H_1 i H_2).

Demostració. La primera afirmació és la Proposició 3.9 i el Teorema d'Artin. Les propietats (1), (3) i (4) també les hem demostrat. Queden només les propietats (2) i (5), que són senzilles i deixem com a exercici. □

Observació 3.18. Del fet que $\mathcal{F}$ i $\mathcal{G}$ siguin inverses una de l'altra, juntament amb les propietats (1) i (5), es dedueix que el reticle de subcossos de K/F i el reticle de subgrups de $\mathrm{Gal}(K/F)$ són duals (un diagrama és igual que l'altre girat cap per avall, ja que la correspondència gira les inclusions).

Exemple 3.19. Considerem $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. És el cos de descomposició de $(x^2-2)(x^2-3)$ sobre $\mathbb{Q}$ i, per tant, $K/\mathbb{Q}$ és Galois. Tenim que $[K\colon \mathbb{Q}] = 4$. Per a veure-ho, fixem-nos que

$$[K\colon \mathbb{Q}] = [K\colon \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2})\colon \mathbb{Q}];$$

clarament $[\mathbb{Q}(\sqrt{2})\colon \mathbb{Q}] = 2$ i $[K\colon \mathbb{Q}(\sqrt{2})] \leq 2$ (ja que $K = \mathbb{Q}(\sqrt{2})(\sqrt{3})$ i $\sqrt{3}$ satisfà el polinomi x^2-3 que té coeficients a $\mathbb{Q}(\sqrt{2})$). Si $[K\colon \mathbb{Q}(\sqrt{2})]$ fos 1, tindríem que $K = \mathbb{Q}(\sqrt{2})$ i, en particular, que $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$ cosa que ràpidament es veu que no pot ser. Per tant, $[K\colon \mathbb{Q}(\sqrt{2})] = 2$ i $[K\colon \mathbb{Q}] = 4$.

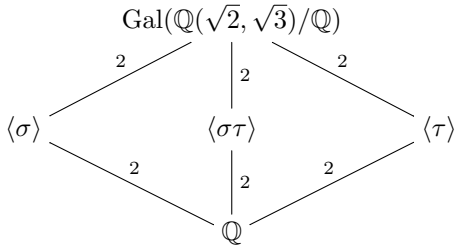
D'aquí veiem que $|\mathrm{Gal}(K/\mathbb{Q})| = 4$. Tot $s \in \mathrm{Gal}(K/\mathbb{Q})$ satisfà que $s(\sqrt{2}) = \pm\sqrt{2}$ i $s(\sqrt{3}) = \pm\sqrt{3}$; això dóna 4 possibles automorfismes:

$$\mathrm{id}\colon \begin{matrix}\sqrt{2}\mapsto\sqrt{2}\\ \sqrt{3}\mapsto\sqrt{3}\end{matrix} \qquad \sigma\colon \begin{matrix}\sqrt{2}\mapsto-\sqrt{2}\\ \sqrt{3}\mapsto\sqrt{3}\end{matrix} \qquad \tau\colon \begin{matrix}\sqrt{2}\mapsto\sqrt{2}\\ \sqrt{3}\mapsto-\sqrt{3}\end{matrix} \qquad \rho\colon \begin{matrix}\sqrt{2}\mapsto-\sqrt{2}\\ \sqrt{3}\mapsto-\sqrt{3}.\end{matrix}$$

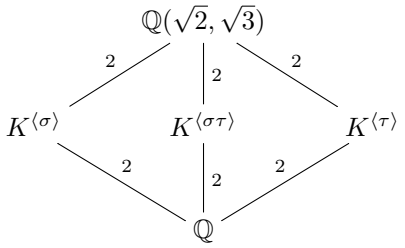
Com que $|\mathrm{Gal}(K/\mathbb{Q})| = 4$, de fet totes aquestes aplicacions sabem que són automorfismes de K (altrament caldria comprovar-ho). Fixem-nos que $\sigma\tau = \rho$, per tant,

$$\mathrm{Gal}(K/\mathbb{Q}) = \{1, \sigma, \tau, \sigma\tau\},$$

és a dir, que $\mathrm{Gal}(K/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. El reticle de subgrups de $\mathrm{Gal}(K/\mathbb{Q})$ és



Pel teorema fonamental, això ens dóna el diagrama de subcossos de K:



Aquí per a raonar que $K^{\langle\sigma\rangle} = \mathbb{Q}(\sqrt{3})$, fixem-nos que clarament $\mathbb{Q}(\sqrt{3}) \subseteq K^{\langle\sigma\rangle}$; ara, pel teorema fonamental $[K^{\langle\sigma\rangle}\colon \mathbb{Q}] = [\mathrm{Gal}(K/\mathbb{Q})\colon \langle\sigma\rangle] = 2$ i obtenim la igualtat. La resta de cossos s'obtenen igual.

Exemple 3.20. Sigui K el cos de descomposició de $f = x^3 - 2 \in \mathbb{Q}[x]$. Les arrels de f són $\sqrt[3]{2}$, $\rho\sqrt[3]{2}$ i $\rho^2\sqrt[3]{2}$, on $\rho = \frac{1}{2}(-1 + \sqrt{-3})$ és una arrel tercera primitiva de la unitat. Veiem doncs que

$$K = \mathbb{Q}(\sqrt[3]{2}, \rho\sqrt[3]{2}, \rho^2\sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2}, \rho) = \mathbb{Q}(\sqrt[3]{2}, \sqrt{-3}).$$

Com que K és la composició de $\mathbb{Q}(\sqrt[3]{2})$ i $\mathbb{Q}(\sqrt{-3})$, de graus 3 i 2 respectivament, tenim que $[K\colon \mathbb{Q}] = 6$. Tot $s \in \mathrm{Gal}(K/\mathbb{Q})$ satisfà que

$$s(\sqrt[3]{2}) = \begin{cases} \sqrt[3]{2} \\ \rho\sqrt[3]{2} \\ \rho^2\sqrt[3]{2} \end{cases} \qquad s(\sqrt{-3}) = \begin{cases} \sqrt{-3} \\ -\sqrt{-3}. \end{cases}$$

Com que tot $s \in \mathrm{Gal}(K/\mathbb{Q})$ està completament determinat per on envia $\sqrt[3]{2}$ i $\sqrt{-3}$, això dóna 6 possibles automorfismes. Com que, de fet, $|\mathrm{Gal}(K/\mathbb{Q})| = 6$, veiem que totes les opcions són automorfismes (altrament, s'hauria de comprovar). Definim dos automorfismes concrets:

$$\sigma\colon \begin{array}{ccc} \sqrt[3]{2} & \mapsto & \rho\sqrt[3]{2} \\ \sqrt{-3} & \mapsto & \sqrt{-3} \end{array} \qquad \tau\colon \begin{array}{ccc} \sqrt[3]{2} & \mapsto & \sqrt[3]{2} \\ \sqrt{-3} & \mapsto & -\sqrt{-3}. \end{array}$$

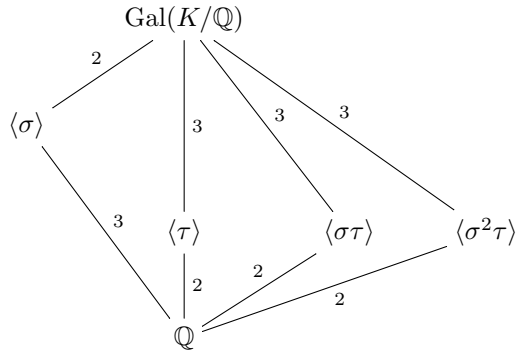
Fixem-nos que $\sigma(\rho) = \rho$ i $\tau(\rho) = \frac{1}{2}(-1 - \sqrt{-3}) = \rho^2$. Amb això podem calcular σ^2 i σ^3:

$$\sigma^2\colon \begin{array}{ccc} \sqrt[3]{2} & \mapsto & \rho^2\sqrt[3]{2} \\ \sqrt{-3} & \mapsto & \sqrt{-3} \end{array} \qquad \sigma^3\colon \begin{array}{ccc} \sqrt[3]{2} & \mapsto & \rho^3\sqrt[3]{2} = \sqrt[3]{2} \\ \sqrt{-3} & \mapsto & \sqrt{-3}. \end{array}$$

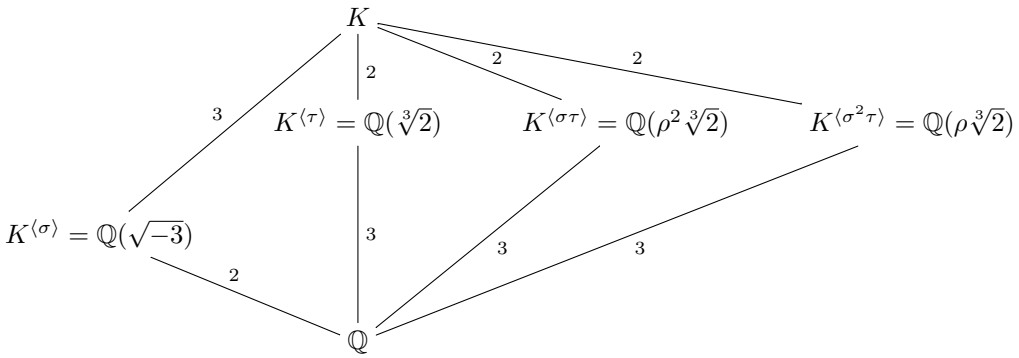
d'on veiem que $\sigma^3 = 1$. De manera semblant, podem calcular que $\sigma^2 = 1$ i que $\sigma\tau = \tau\sigma^2$. Per tant,

$$\mathrm{Gal}(K/\mathbb{Q}) = \langle \sigma, \tau \mid \sigma^3 = 1, \tau^2 = 1, \sigma\tau = \tau\sigma^2 \rangle \simeq \mathrm{D}_6 \simeq \mathrm{S}_3.$$

El diagrama de subgrups és:



Pel teorema fonamental, això ens dóna el diagrama de subcossos de K:



Per a provar que els cossos fixos són aquests, podem procedir com a l'exemple anterior. Per exemple, és clar que $\mathbb{Q}(\sqrt{-3}) \subseteq K^{\langle\sigma\rangle}$, i pel teorema fonamental sabem que $[K^{\langle\sigma\rangle}\colon \mathbb{Q}] = 2$; com que $[\mathbb{Q}(\sqrt{-3}\colon \mathbb{Q})] = 2$, veiem la igualtat. Els altres subcossos es fan de manera semblant.

4. Algunes aplicacions de la teoria de Galois

4.1. **Cossos finits.** Com a exemple d'aplicació de la teoria d'extensions de cossos i la teoria de Galois veurem el cas dels cossos finits. Els cossos finits tenen molta importància, tant interna a les matemàtiques (teoria de nombres, teoria de grups i representacions, combinatòria...) com a l'enginyeria (criptografia, teoria de codis correctors d'errors, generació de nombres pseudoaleatoris...).

Definició 4.1. Un cos finit és un cos que té un nombre finit d'elements.

Ja coneixem alguns exemples de cossos finits: si p és un nombre primer, aleshores l'anell $\mathbb{Z}/p\mathbb{Z}$ dels enters mòdul p és un cos finit que té p elements, i que es denota habitualment per $\mathbb{F}_p$.

Proposició 4.2. Si K és un cos finit, aleshores $|K| = p^r$ per a algun primer p i algun $r \in \mathbb{Z}_{\geq 1}$.

Demostració. K té característica p per a algun primer p (altrament, contindria $\mathbb{Q}$, que no pot ser perquè K és finit) i, per tant, conté $\mathbb{F}_p$. Com que K és finit, la dimensió de K sobre $\mathbb{F}_p$ és finita, diguem-li r, i posem $\alpha_1, \ldots, \alpha_r$ una $\mathbb{F}_p$-base de K. Aleshores,

$$K = \{a_1\alpha_1 + \cdots + a_r\alpha_r \colon a_i \in \mathbb{F}_p\}$$

i, per tant, $|K| = p^r$. □

A partir d'ara en aquesta secció p sempre denotarà un primer, r un enter ≥ 1 i $q = p^r$.

Proposició 4.3. Existeix un cos de cardinal q. Tots els cossos de cardinal q són isomorfs.

Demostració. Considerem $f = x^q - x \in \mathbb{F}_p[x]$. Com que $f' = qx^{q-1} - 1 = -1$, tenim que $\gcd(f, f') = 1$ i f és separable i té q arrels diferents en un cos de descomposició. Sigui K un cos de descomposició de f. Aleshores, K conté les q arrels de f, i de fet, el conjunt d'aquestes arrels és un cos. Per a veure-ho, hem de provar que si α, β són arrels de f, aleshores $\alpha\beta$, α/β amb $\beta \neq 0$, $\alpha + \beta$ i $\alpha - \beta$ també ho són. Clarament, si $\alpha^q = \alpha$ i $\beta^q = \beta$, tenim que $(\alpha\beta)^q = \alpha\beta$, i de manera semblant es veu que α/β també n'és arrel. Per a $\alpha + \beta$, com que K és de característica p, per l'Exemple 1.21 (2) tenim que

$$(\alpha + \beta)^p = \alpha^p + \beta^p.$$

Aplicant aquesta propietat repetidament, obtenim que

$$(\alpha + \beta)^q = \alpha^q + \beta^q = \alpha + \beta$$

i, per tant, $\alpha + \beta$ també és arrel de f; de manera similar es veu $\alpha - \beta$. Així doncs, K és el conjunt d'arrels de f i, per tant, $|K| = q$.

D'altra banda, si K' és un altre cos de cardinal q, el grup multiplicatiu de K' té cardinal $q - 1$ i tot $\alpha \in K' \setminus \{0\}$ satisfà que $\alpha^{q-1} = 1$ i, per tant, que $\alpha^q = \alpha$. És a dir, α és arrel de f. Com que 0 també és arrel de f, tenim que tots els elements de K' són arrels de f i K' és, doncs, un cos de descomposició de f. Per tant, $K' \simeq K$ ja que tots els cossos de descomposició de f són isomorfs. □

És habitual fer un abús de notació i denotar per $\mathbb{F}_q$ un cos de cardinal q. Com que tots els cossos de cardinal q són isomorfs, aquesta notació no és excessivament ambigua (tot i que ja veurem que l'isomorfisme no és únic quan $r > 1$).

Proposició 4.4. $\mathbb{F}_q/\mathbb{F}_p$ és de Galois.

Demostració. Ho hem vist a la demostració de la proposició anterior, ja que $\mathbb{F}_q$ és el cos de descomposició de $x^q - x \in \mathbb{F}_p[x]$ que és separable. □

Proposició 4.5. Tot subgrup finit G del grup multiplicatiu $F^\times$ d'un cos F és cíclic.

Demostració. Com que G és abelià, pel teorema de classificació de grups abelians finits tenim que

$$G \simeq \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$$

amb $n_i > 1$ i $n_1 \mid n_2 \mid \cdots \mid n_k$. Tot element de G té, doncs, ordre dividint n_k i, per tant, és arrel del polinomi $x^{n_k} - 1$. Així doncs, el polinomi $x^{n_k} - 1$ té almenys $n_1 \cdots n_k$ arrels a F; si $k > 1$, aquest nombre és més gran que el grau n_k, cosa que no pot ser. Per tant, $k = 1$ i G és cíclic. □

Corol·lari 4.6. $\mathbb{F}_q^\times$ és cíclic.

Corol·lari 4.7. $\mathbb{F}_q$ és simple. En particular, existeix un polinomi irreductible de grau r amb coeficients a $\mathbb{F}_p$.

Demostració. Pel resultat anterior $\mathbb{F}_q^\times$ és cíclic. És a dir, existeix $\alpha \in \mathbb{F}_q$ tal que $\mathbb{F}_q^\times = \{1, \alpha, \ldots, \alpha^{q-2}\}$. Aleshores tenim que $\mathbb{F}_q = \mathbb{F}_p(\alpha)$, i $\operatorname{Irr}(\alpha, \mathbb{F}_p)$ és irreductible de grau r. □

L'automorfisme de Frobenius (cf. 1.21)

$$\begin{array}{rccc} \operatorname{Fr}_p\colon & \mathbb{F}_q & \longrightarrow & \mathbb{F}_q \\ & \alpha & \longmapsto & \alpha^p. \end{array}$$

és un element de $\operatorname{Gal}(\mathbb{F}_q/\mathbb{F}_p)$. Recordem que en la notació d'aquesta secció $q = p^r$.

Proposició 4.8. $\operatorname{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ és cíclic d'ordre r generat per Fr_p.

Demostració. Com que $[\mathbb{F}_q\colon \mathbb{F}_p] = r$ sabem que $|\operatorname{Gal}(\mathbb{F}_q/\mathbb{F}_p)| = r$. Clarament $\operatorname{Fr}_p^i(\alpha) = \alpha^{p^i}$ per a tot $i \geq 1$; en particular, $\operatorname{Fr}_p^r(\alpha) = \alpha^{p^r} = \alpha$ i, per tant, $\operatorname{Fr}_p^r = \mathrm{id}$. Cap altra potència Fr_p^i amb $1 \leq i < r$ és la identitat, perquè això voldria dir que $\alpha^{p^i} = \alpha$ per a tot $\alpha \in \mathbb{F}_q$, la qual cosa implicaria que el polinomi $x^{p^i} - x$ té p^r arrels a $\mathbb{F}_q$. □

Corol·lari 4.9. $\mathbb{F}_q$ conté $\mathbb{F}_{p^d}$ si i només si $d \mid r$.

Demostració. Pel teorema fonamental de la teoria de Galois els subcossos de $\mathbb{F}_q$ es corresponen amb els subgrups de $\operatorname{Gal}(\mathbb{F}_q/\mathbb{F}_p) \simeq \mathbb{Z}/r\mathbb{Z}$, i la dimensió del subcòs sobre $\mathbb{F}_p$ coincideix amb l'índex del subgrup. Ara, hi ha un subgrup de $\mathbb{Z}/r\mathbb{Z}$ d'índex d si i només si $d \mid r$, i en aquest cas només n'hi ha un. □

Proposició 4.10. El polinomi $x^q - x$ és el producte de tots els polinomis mònics irreductibles a $\mathbb{F}_p[x]$ de grau divisor de r.

Demostració. Sigui f un factor irreductible de $x^q - x \in \mathbb{F}_p[x]$. Com que $\mathbb{F}_q$ és un cos de descomposició de $x^q - x$, conté una arrel α de f. Aleshores, $\mathbb{F}_p(\alpha)$ és un subcòs de $\mathbb{F}_q$ de grau d i pel Corol·lari 4.9 tenim que $d \mid r$. Per tant, tot factor irreductible de $x^q - x$ té grau dividint r.

D'altra banda, sigui $f \in \mathbb{F}_p[x]$ un polinomi irreductible de grau r, i sigui α una arrel de f en una extensió. Com que $[\mathbb{F}_p(\alpha)\colon \mathbb{F}_p] = r$, $\mathbb{F}_p(\alpha)$ és el cos de descomposició de $x^q - x$ i, per tant, α és arrel de $x^q - x$, amb la qual cosa veiem que $f \mid x^q - x$. Utilitzant que si $d \mid r$ el polinomi $x^{p^d} - x$ divideix[11] $x^q - x$, veiem que si f és un polinomi irreductible de grau $d \mid r$, aleshores divideix $x^{p^d} - x$ i per tant també $x^q - x$.

Finalment, com que $x^q - x$ és separable, no té cap factor repetit i és, doncs, el producte de tots els polinomis mònics irreductibles a $\mathbb{F}_p[x]$ de grau dividint r. □

[11] Això ho deixem com a exercici.

Hem vist que $\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^r}$ si i només si $d \mid r$. En particular, donats dos cossos finits $\mathbb{F}_{p^n}$ i $\mathbb{F}_{p^m}$, existeix un altre cos finit que els conté: $\mathbb{F}_{p^{nm}}$. Per tant, la unió $\cup_{n\geq 1}\mathbb{F}_{p^n}$ és un cos que conté totes les extensions finites de $\mathbb{F}_p$.

Proposició 4.11. $\overline{\mathbb{F}}_p = \cup_{n\geq 1}\mathbb{F}_{p^n}$.

4.2. **Cossos Ciclotòmics.** El subcòs dels nombres complexos generat sobre $\mathbb{Q}$ per $\zeta_n = e^{\frac{2\pi i}{n}}$ s'anomena *cos ciclotòmic n-èssim.* L'extensió $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ és de Galois (ja que és el cos de descomposició de x^n-1). En aquest capítol estudiarem aquest tipus de cossos i veurem que $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$.

Denotem per μ_n el conjunt d'arrels n-èssimes de la unitat; és a dir, les arrels de $x^n - 1$. Sabem que

$$\mu_n = \{\zeta_n^a \colon 0 \leq a \leq n-1\},$$

i en particular $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\mu_n)$. El conjunt μ_n és un grup amb el producte i tenim un isomorfisme

$$\begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} & \longrightarrow & \mu_n \\ a & \longmapsto & \zeta_n^a. \end{array}$$

Si $d \mid n$, aleshores $\mu_d \subseteq \mu_n$ i, per tant, $\mathbb{Q}(\zeta_d) \subseteq \mathbb{Q}(\zeta_n)$. També tenim que ζ_n^a és una arrel n-èssima de la unitat, i que és primitiva si i només si $(a, n) = 1$.

Definició 4.12. El polinomi ciclotòmic n-èssim és el polinomi que té per arrels les arrels n-èssimes primitives de la unitat:

$$\Phi_n(x) = \prod_{\substack{0\leq a<n \\ (a,n)=1}} (x - \zeta_n^a).$$

Com que les arrels de $x^n - 1$ són les arrels n-èssimes de la unitat i tota arrel n-èssima és primitiva d'ordre d per a algun $d \mid n$ tenim que

$$x^n - 1 = \prod_{d\mid n} \Phi_d(x). \tag{4.1}$$

Comparant graus, això ens dóna la identitat

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

La fórmula (4.1) ens permet calcular alguns polinomis ciclotòmics de manera recurrent. També, per $n = p$ primer obtenim que

$$\Phi_p = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1.$$

Ja hem vist que Φ_p pertany a $\mathbb{Z}[x]$ i és irreductible; ara veurem que el mateix és cert per a Φ_n amb n no necessàriament primer.

Proposició 4.13. $\Phi_n(x)$ és mònic, té coeficients enters i grau $\varphi(n)$.

Demostració. Clarament és mònic i té grau $\varphi(n)$. Per a veure que té coeficients enters, fem inducció sobre n. El cas $n = 1$ és clar. Suposem-ho cert, doncs, per a Φ_m amb $m < n$. Per (4.1) tenim que

$$x^n - 1 = \Phi_n(x) \cdot f(x),$$

on $f(x)$ és un polinomi mònic amb coeficients enters. Per tant,

$$\Phi_n(x) = \frac{x^n - 1}{f(x)}$$

i per l'algoritme de divisió veiem que $\Phi_n(x)$ també és mònic i té coeficients enters. □

Proposició 4.14. $\Phi_n(x)$ és irreductible a $\mathbb{Q}[x]$. En particular, $[\mathbb{Q}(\zeta_n)\colon \mathbb{Q}] = \varphi(n)$.

Demostració. Pel Lema de Gauss n'hi ha prou veient que és irreductible a $\mathbb{Z}[x]$. Si no ho fos, hi hauria una factorització

$$\Phi_n(x) = f(x)g(x) \quad \text{amb } f(x), g(x) \in \mathbb{Z}[x] \text{ mònics},$$

i on podem suposar que $f(x)$ és irreductible a $\mathbb{Z}[x]$ (i, per tant, a $\mathbb{Q}[x]$). Sigui ζ una arrel n-èssima primitiva que sigui arrel de f, i sigui p un primer que no divideix n. Aleshores ζ^p també és una arrel n-èssima primitiva i, per tant, és arrel de $f(x)$ o de $g(x)$. Veiem que no pot ser arrel de $g(x)$. Si ho fos, ζ seria arrel de $g(x^p)$ i, per tant, $f(x)$, que és el polinomi irreductible de ζ, dividiria $g(x^p)$. Tindríem, doncs,

$$g(x^p) = f(x)h(x) \text{ a } \mathbb{Z}[x]$$

i reduint mòdul p:

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

com que $\bar{g}(x^p) = (\bar{g}(x))^p$ veiem que necessàriament $\bar{f}$ i $\bar{g}$ tenen un factor en comú. Per tant, $\bar{\Phi}_n(x) = \bar{f}(x)\bar{g}(x)$ té una arrel múltiple a $\overline{\mathbb{F}}_p$ i, com que és un factor de $x^n - 1$, tenim que $x^n - 1$ també té una arrel múltiple. Però si $p \nmid n$, $x^n - 1$ és separable (ja que $\gcd(nx^{n-1}, x^n - 1) = 1$) i hem arribat, doncs, a una contradicció.

Per tant, ζ^p és una arrel de $f(x)$. Com que això val per a tota arrel ζ de f, repetint el procés amb ζ^p per a altres primers veiem que ζ^a és arrel de $f(x)$ per a tot a coprimer amb n. És a dir, $f(x) = \Phi_n(x)$. □

Sabem que $|\operatorname{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})| = \varphi(n)$. Tot $\sigma \in \operatorname{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ envia ζ_n a una altra arrel n-èssima primitiva de la unitat; és a dir, $\sigma(\zeta_n) = \zeta_n^a$ amb $1 \leq a < n$ i $(a, n) = 1$. Com que hi ha $\varphi(n)$ possibilitats per a a, totes aquestes aplicacions són automorfismes de $\mathbb{Q}(\zeta_n/\mathbb{Q})$ i, de fet, són tots. Podem dir encara més, i és que podem concretar quina és l'estructura d'aquest grup de Galois.

Proposició 4.15. L'aplicació

$$\begin{array}{ccc} (\mathbb{Z}/n\mathbb{Z})^\times & \longrightarrow & \operatorname{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \\ a \pmod n & \longmapsto & \sigma_a, \end{array}$$

on σ_a és l'automorfisme tal que $\sigma_a(\zeta_n) = \zeta_n^a$, és un isomorfisme de grups.

Demostració. L'aplicació és clarament injectiva i, com que la sortida i l'arribada tenen el mateix cardinal. és també exhaustiva. Per a veure que és un morfisme de grups, cal comprovar que $\sigma_{ab} = \sigma_a\sigma_b$, cosa que és immediata, ja que $\sigma_a\sigma_b(\zeta_n) = \sigma_a(\zeta_n^b) = \zeta_n^{ab}$. □

Observació 4.16. Una extensió de Galois K/F es diu *abeliana* si $\operatorname{Gal}(K/F)$ és un grup abelià. Amb aquesta terminologia, $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ és, doncs, una extensió abeliana.

Hem vist que tot grup de la forma $(\mathbb{Z}/n\mathbb{Z})^\times$ és el grup de Galois d'una extensió $K/\mathbb{Q}$. El mateix és cert per a tot grup finit abelià: si G és un grup finit abelià, aleshores existeix una extensió de Galois $K/\mathbb{Q}$ tal que $\mathrm{Gal}(K/\mathbb{Q}) \simeq G$.[12] No se sap si el resultat és cert per a un grup finit qualsevol. Aquest és un problema obert i molt important, que s'anomena el Problema Invers de la teoria de Galois.[13]

Relacionat amb el resultat que el grup de Galois d'una extensió ciclotòmica és abelià, també es coneix el resultat següent que dóna una mena de recíproc.

Teorema 4.17 (Teorema de Kronecker–Weber)**.** Si $K/\mathbb{Q}$ és una extensió abeliana, aleshores K està contingut en un cos ciclotòmic.

La demostració d'aquest teorema s'escapa dels objectius del curs, però el resultat és molt rellevant ja que dóna una descripció completa de les extensions abelianes de $\mathbb{Q}$; de fet, aquest resultat és el punt de partida del que s'anomena Teoria de Cossos de Classes, que estudia extensions abelianes de cossos F amb $[F\colon \mathbb{Q}] < \infty$.

4.3. **Problemes clàssics de construccions amb regle i compàs.** El llenguatge algebraic d'extensions de cossos que hem desenvolupat es pot aplicar per a resoldre alguns problemes clàssics de construccions amb regle i compàs plantejats pels grecs. Per exemple:

- Trisecció d'angles: És possible trisecar un angle qualsevol només amb regle i compàs?[14]
- Quadratura del cercle: Donat un cercle, és possible construir un quadrat que tingui la mateixa àrea emprant només regle i compàs?

Amb l'ajuda de la teoria d'extensions algebraiques veurem que la resposta a aquestes preguntes és negativa. Primer formalitzarem la noció de "*construir amb regle i compàs*".

Treballarem al pla $\mathbb{R}^2$. Habitualment partirem d'alguns objectes geomètrics ja construïts (per exemple, dos punts), i a partir d'aquí en construirem de nous amb les construccions següents, que són les que es poden fer amb regle i compàs:

a) Si dos punts estan construïts, podem traçar la recta que els uneix. Aquesta recta la considerarem construïda.
b) Si dos punts estan construïts, podem traçar el cercle amb centre un dels punts i que passa per l'altre. Aquest cercle el considerarem construït.
c) Els punts d'intersecció de rectes i cercles construïts també els considerarem construïts.

A partir d'aquestes construccions bàsiques, en podem fer d'altres:

1) Si P és un punt construït i L una recta construïda, aleshores podem construir la recta que passa per P i és perpendicular a L.

   La construcció és diferent segons si el punt pertany a la recta o no. Si $P \notin L$, el procés és el de la Figura 1; si $P \in L$, és el de la Figura 2.
2) Si P és un punt construït i L una recta construïda, aleshores podem construir la recta que passa per P i és paral·lela a L. Això és aplicar dos cops la construcció anterior.

---

[12] El motiu és que tot grup finit abelià és isomorf a un quocient d'un grup de la forma $(\mathbb{Z}/n\mathbb{Z})^\times$ per algun n; la prova no és complicada, però utilitza que per a tot n existeixen infinits primers $p \equiv 1 \pmod{n}$, un cas particular del Teorema de la Progressió Aritmètica de Dirichlet.

[13] `https://en.wikipedia.org/wiki/Inverse_Galois_problem`

[14] Recordem que sí que es poden bisecar angles amb regle i compàs, amb un mètode senzill que aprenem a l'escola; sembla una pregunta natural doncs si també es poden trisecar.

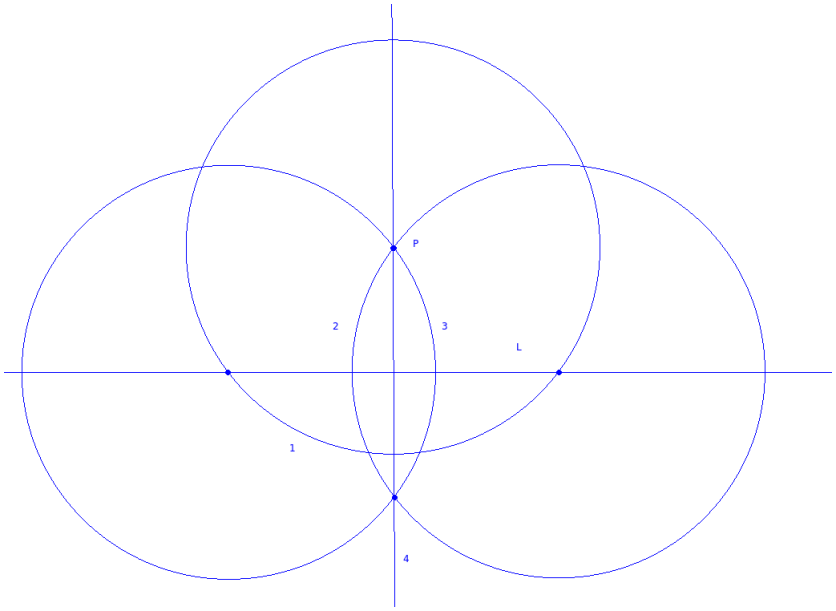


FIGURA 1. Recta perpendicular a L que passa per P quan $P \notin L$. Els nombres indiquen l'odre amb què cal construir cada element.

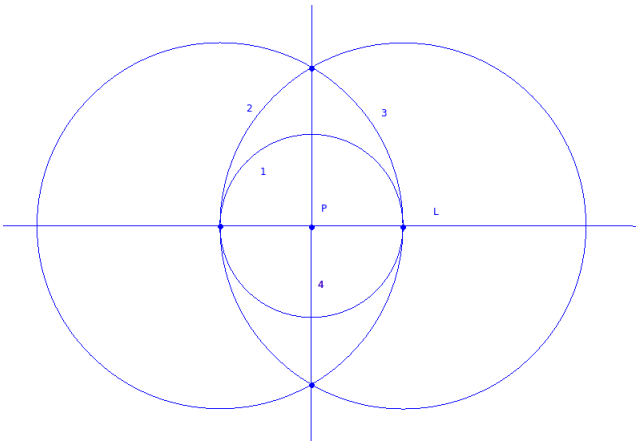


FIGURA 2. Recta perpendicular a L que passa per p quan $P \in L$.

3) Donat $P \in L$ i dos punts A i B construïts, podem construir un punt $Q \in L$ tal que $d(P,Q) = d(A,B)$. Fem la paral·lela a L que passa per A, traslladem amb el compàs la distància $d(A,B)$ a aquesta paral·lela, i fent paral·leles la traslladem a L. Vegeu la Figura 3

Suposem a partir d'ara que comencem amb els punts $(0,0)$ i $(1,0)$. És a dir, aquests són els punts que considerem inicialment construïts. La noció clau que ens permetrà aplicar la teoria de cossos a aquests problemes és la de nombre construïble.

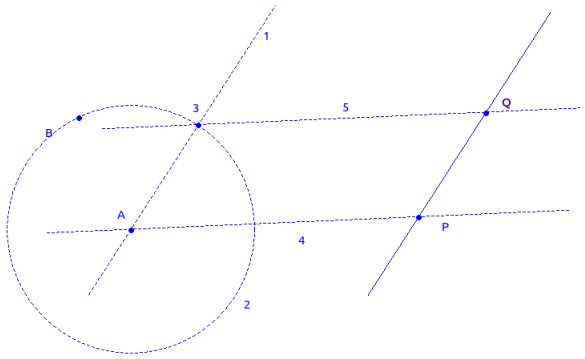


FIGURA 3. Donat $P \in L$ i dos punts A i B construïts, construcció de $Q \in L$ tal que $d(P,Q) = d(A,B)$.

Definició 4.18. Un nombre real a diem que és construïble si podem construir dos punts a distància $|a|$.

Proposició 4.19. Un punt $P = (a,b)$ és construïble si i només si ho són les seves coordenades a i b.

Demostració. Unint $(0,0)$ i $(1,0)$ podem construir l'eix de les x, i prenent la perpendicular a aquest eix que passa per $(0,0)$ construïm l'eix de les y. Ara prenem les paral·leles a cadascun dels eixos que passen per P i això ens construirà les projeccions de P als eixos, amb la qual cosa veiem que a i b són construïbles. Si partim de dos punts a distància a, per la construcció 3) podem construir el punt $(a,0)$, i partint de dos punts a distància b podem construir $(0,b)$. Prenent paral·leles als eixos que passin per aquests punts i intersecant obtenim (a,b). □

La connexió amb la teoria de cossos ens la dóna la proposició següent.

Proposició 4.20. El conjunt de nombres reals construïbles és un sucòs de $\mathbb{R}$.

Demostració. Cal veure que si a i b són construïbles, aleshores també ho són $a+b$, $a-b$, ab i a/b (si $b \neq 0$). La suma i la resta es construeixen fàcilment amb la construcció 3). Pel que fa la producte i quocient, es pot fer amb triangles semblants, com a les figures 4 i 5 □

Proposició 4.21. Si $a \in \mathbb{R}_{>0}$ és construïble, aleshores $\sqrt{a}$ també.

Demostració. Construïm un segment de longitud $1+a$, i construïm una circumferència que tingui aquest segment per diàmetre. Dibuixem, aleshores, un triangle inscrit a la circumferència com a la Figura 7a. Sabem que l'angle que veu el diàmetre és un angle recte [15]. Si tracem la perpendicular al diàmetre que passa per l'angle recte, dividim el triangle en dos triangles que són semblants (cf. Figura 7b, els dos triangles petits tenen un angle recte i un angle e). Per semblança, $\frac{a}{h} = \frac{h}{1}$ i veiem, doncs, que $h = \sqrt{a}$. □

[15] Això és un teorema de geometria bàsica, una demostració la veiem a la Figura 6. Com que el triangle està inscrit a la circumferència, els dos triangles són isòsceles (cadascun d'ells té dos costats iguals al radi de la circumferència). Del fet que $2e + 2h = 180$, obtenim que $e + h = 90$.

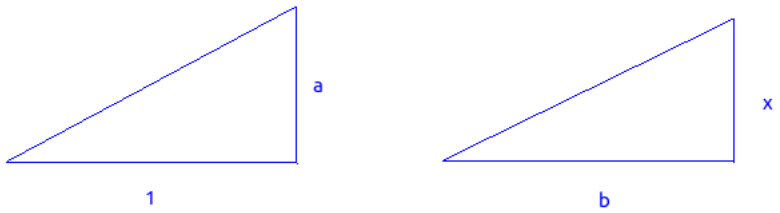


FIGURA 4. Per semblança tenim que $x = ab$

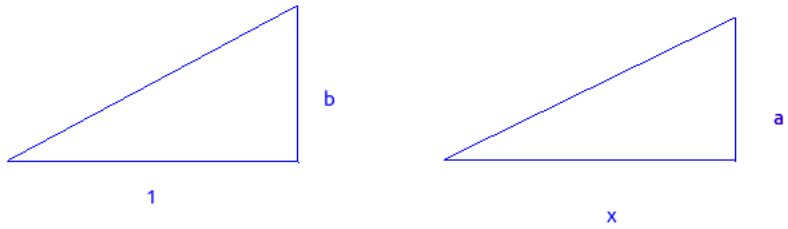


FIGURA 5. Per semblança tenim que $x = a/b$

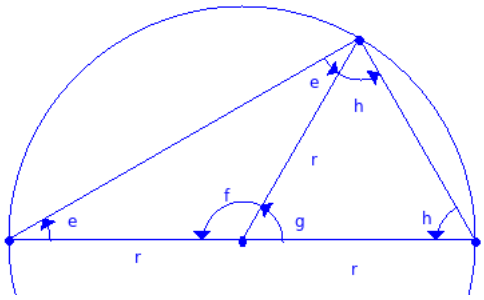


FIGURA 6

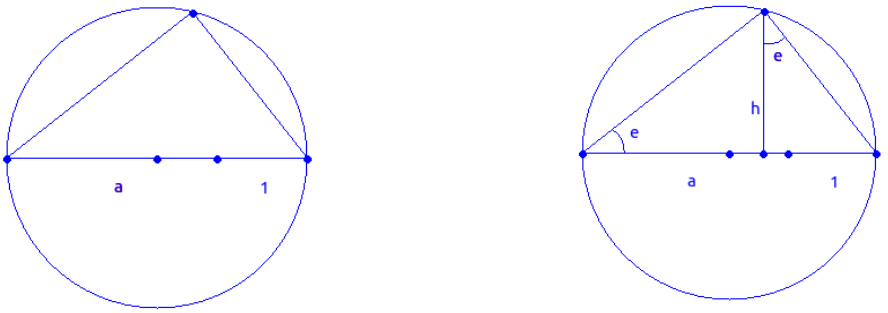
Proposició 4.22. Siguin $a_1, a_2, \ldots, a_n$ nombres construïbles i sigui $K = \mathbb{Q}(a_1, a_2, \ldots, a_n)$. Aleshores $K/\mathbb{Q}$ és finita i $[K\colon \mathbb{Q}]$ és potència de 2. De manera més precisa, existeix una cadena de subcossos

$$\mathbb{Q} = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_r = K \text{ tal que } [K_{i+1}\colon K_i] = 2. \tag{4.2}$$

Recíprocament, donada una cadena de subcossos com (4.2), tenim que tots els elements de K són construïbles.

Demostració. Els punts que construïm els obtenim només de tres maneres possibles:

(1) Intersecant dues rectes on cadascuna d'elles passa per dos punts construïts.



(A) (B)

FIGURA 7. Construcció de $\sqrt{a}$

(2) Intersecant una recta que passa per dos punts construïts amb una circumferència que té centre un punt construït i passa per un punt construït.
(3) Intersecant dues circumferències, on cadascuna d'elles té centre un punt construït i passa per un punt construït.

Per a demostrar l'existència d'una cadena com (4.2) n'hi ha prou veient que en qualsevol d'aquests tres procediments, si F és un cos que conté els punts construïts inicials, aleshores els nous punts construïts viuen en una extensió quadràtica de F. Siguin, doncs, (x_j, y_j) amb $j = 0, 1, 2, 3$ punts construïts amb $x_j, y_i \in F$ per a tot j.

(1) La recta per (x_0, y_0) i (x_1, y_1) té equació
$$L\colon (x_1 - x_0)(y - y_0) - (y_1 - y_0)(x - x_0) = 0.$$
De manera anàloga, la recta per (x_2, y_2) i (x_3, y_3) té equació
$$L'\colon (x_3 - x_2)(y - y_2) - (y_3 - y_2)(x - x_2) = 0.$$
Clarament el punt d'intersecció de L i L' té coordenades a F en aquest cas.
(2) La circumferència amb centre (x_3, y_3) i que passa per (x_2, y_2) té equació
$$C\colon (x - x_3)^2 + (y - y_3)^2 = (x_2 - x_3)^2 + (y_2 - y_3)^2.$$
Per a calcular $L \cap C$, aïllem una de les variables en l'equació de la recta i substituïm a l'equació de la circumferència. Això dóna una equació quadràtica, que té solucions en una extensió quadràtica de F, l'obtinguda adjuntant l'arrel quadrada del discriminant de l'equació (si el discriminant és negatiu la recta i la circumferència no es tallen a $\mathbb{R}^2$ i, per tant, no obtenim punts).
(3) La circumferència amb centre (x_1, y_1) i que passa per (x_0, y_0) té equació
$$C'\colon (x - x_1)^2 + (y - y_1)^2 = (x_0 - x_1)^2 + (y_0 - y_1)^2.$$
Per a calcular $C \cap C'$, restem les dues equacions i obtenim:
$$\begin{aligned} &- 2xx_3 - 2yy_3 + x_3^2 + y_3^2 + 2xx_1 + 2yy_1 - x_1^2 - y_1^2 \\ &= (x_2 - x_3)^2 + (y_2 - y_3)^2 - (x_0 - x_1)^2 - (y_0 - y_1)^2, \end{aligned}$$

que és una equació lineal. Igual que en el cas anterior, aïllant una de les variables i substituint a l'equació de C, obtenim una equació quadràtica que té solució en una extensió quadràtica de F.

Que en una cadena com (4.2) tots els elements de K són construïbles surt de la Proposició 4.21 i la Proposició 4.20. □

Ja tenim les eines necessàries per a resoldre els problemes que plantejàvem a l'inici de la secció. Suposem que tenim dues rectes construïdes i que formen un angle θ. És possible construir dues rectes amb un angle $\theta/3$? La resposta és que, en general, no. Per començar, fixem-nos que si un angle θ és construïble, aleshores marcant els punts a distància 1 del vèrtex i projectant sobre un dels costats i sobre la recta perpendicular podem construir també $\cos\theta$. I al revés, si $\cos\theta$ i $\sin\theta$ són construïbles, aleshores θ és construïble.

Resulta que si prenem $\theta = 60$, aleshores θ és construïble (ja que $\cos\theta = 1/2$ i $\sin\theta = \sqrt{3}/2$), però $\cos\theta/3$ no és construïble i, per tant, $\theta/3$ tampoc. Per a veure això, partim de la identitat trigonomètrica[16]

$$\cos 3\alpha = 4\cos^3\alpha - 3\cos\alpha,$$

i fent $\alpha = \theta/3 = 20$ veiem que

$$\frac{1}{2} = 4\cos^3\alpha - 3\cos\alpha.$$

És a dir, que $\cos(\theta/3)$ és arrel del polinomi

$$4x^3 - 3x - \frac{1}{2}.$$

El polinomi $8x^3 - 6x - 1$ és primitiu i irreductible a $\mathbb{Z}[x]$ (no té cap arrel entera) i, per tant, és irreductible a $\mathbb{Q}[x]$. Així doncs, $[\mathbb{Q}(\cos(\theta/3))\colon \mathbb{Q}] = 3$, i per la Proposició 4.22 veiem que $\cos(\theta/3)$ no és construïble.

Pel que fa a l'altre problema, donat un cercle de radi 1, construir un quadrat amb la mateixa àrea és equivalent a construir π. Però $[\mathbb{Q}(\pi)\colon \mathbb{Q}] = \infty$, ja que π és transcendent sobre $\mathbb{Q}$ i novament per la Proposició 4.22 veiem que π no és construïble.

Fixem-nos que per a la resolució d'aquests problemes clàssics no hem utilitzat la teoria de Galois; només propietats bàsiques d'extensions de cossos (essencialment la multiplicativitat dels graus en torres d'extensions). Hi ha un altre problema relacionat que és: per a quins valors de n podem construir un polígon regular de n-costats amb regle i compàs? Això és equivalent a la construcció de l'angle $\frac{2\pi}{n}$, és a dir, equivalent a la construcció de $\zeta_n = e^{\frac{2\pi i}{n}}$. Ara, construir ζ_n és equivalent a construir el doble de la seva part real, que és $\zeta_n + \bar{\zeta}_n = \zeta_n + \zeta_n^{-1}$. Com que ζ_n satisfà el polinomi

$$x^2 - x(\zeta_n + \zeta_n^{-1}) + 1 \in \mathbb{Q}(\zeta_n + \zeta_n^{-1})[x]$$

veiem que $[\mathbb{Q}(\zeta_n)\colon \mathbb{Q}(\zeta_n + \zeta_n^{-1})] \leq 2$. Així doncs, si ζ_n és construïble necessàriament $[\mathbb{Q}(\zeta_n)\colon \mathbb{Q}] = 2^k$ per a algun $k \geq 0$. Recíprocament, si $[\mathbb{Q}(\zeta_n)\colon \mathbb{Q}] = 2^k$ per a algun $k \geq 0$, com que $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ és abelià, existeix una cadena de subgrups

$$1 = G_0 \leq G_1 \leq \cdots \leq G_r = \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$$

[16] Que surt del fet que $\cos 3\alpha + i\sin 3\alpha = e^{i3\alpha} = (e^{i\alpha})^3 = (\cos\alpha + i\sin\alpha)^3$.

tals que $[G_i\colon G_{i+1}] = 2$. Pel Teorema Fonamental de la teoria de Galois, la cadena de subcossos de $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ fixos pels subgrups G_i és de la forma (4.2). Tenim, doncs, el resultat següent, que fou demostrat per primer cop per Gauss.

Proposició 4.23. El polígon regular de n costats és construïble amb regle i compàs si i només si $\phi(n)$ és potència de 2. És a dir, si i només si $n = 2^r p_1 p_2 \dots p_s$ per alguns $r, s \geq 0$, on el p_i són primers senars diferents i tals que $p_i - 1$ és potència de 2.

Els primers senars tals que $p - 1$ és potència de 2 s'anomenen *primers de Fermat*. Els únics que es coneixen són $3, 5, 17, 257$ i 65537. No se sap si n'hi ha més.

4.4. **El teorema fonamental de l'àlgebra.** Tot i que hi ha moltes demostracions diferents del Teorema Fonamental de l'Àlgebra, no se'n coneix cap que utilitzi únicament arguments algebraics sinó que es necessita algun resultat de caire analític o topològic. La demostració que presentem, basada en l'existència de cossos de descomposició de polimomis i en el Teorema Fonamental de la teoria de Galois, és d'Emil Artin i utilitza els resultats següents de caire analític.

Lema 4.24. $\mathbb{R}$ no té extensions algebraiques de grau senar no trivials.

Demostració. Això és perquè tot polinomi $f \in \mathbb{R}[x]$ de grau senar té alguna arrel real (pel Teorema de Bolzano aplicat a la funció contínua donada per f). □

Lema 4.25. $\mathbb{C}$ no té extensions quadràtiques.

Demostració. Això és perquè tot $z \in \mathbb{C}$ té arrel quadrada a $\mathbb{C}$. En efecte, si pensem z en polars, $z = re^{i\theta}$, aleshores $\sqrt{r}e^{i\theta/2}$ és una arrel quadrada. □

També utilitzarem la propietat següent dels grups finits. La seva demostració s'ha vist a Estructures Algebraiques, com a part dels teoremes de Sylow.

Proposició 4.26. Si G és un grup finit i p un primer amb $p^s \mid |G|$, aleshores existeix un sugrup $H \leq G$ de cardinal p^s.

Teorema 4.27 (Fonamental de l'Àlgebra)**.** $\mathbb{C}$ és algebraicament tancat.

Demostració. Cal veure que tot polinomi $f \in \mathbb{C}[x]$ descompon completament a $\mathbb{C}$. Denotem per $\bar{f}$ el polinomi obtingut a partir de f conjugant els coeficients. Fixem-nos que $g := f \cdot \bar{f}$ té coeficients que són fixos per la conjugació complexa i, per tant, $g \in \mathbb{R}[x]$. Si α és arrel de g, aleshores α o $\bar{\alpha}$ és arrel de f. N'hi ha prou, doncs, amb demostrar que tot polinomi $g \in \mathbb{R}[x]$ no constant té alguna arrel a $\mathbb{C}$.

Sigui, doncs, $g \in \mathbb{R}[x]$ de grau $n \geq 1$ i sigui K un cos de descomposició de g sobre $\mathbb{R}$. Aleshores, $K(i)$ és una extensió de Galois de $\mathbb{R}$. Posem $G = \mathrm{Gal}(K(i)/\mathbb{R})$ i escrivim el cardinal de G com $|G| = 2^r \cdot m$ amb m senar. Fixem-nos que $r \geq 1$, ja que $\mathbb{R} \subseteq \mathbb{C} \subseteq K(i)$ i, per tant, $[\mathbb{C}\colon \mathbb{R}] \mid |G|$.

Sigui G_2 un 2-Sylow de G (és a dir, un subgrup de G amb $|G_2| = 2^r$). Sigui $K_2 = K(i)^{G_2}$, de manera que $\mathrm{Gal}(K(i)/K_2) \simeq G_2$. Com que $[K_2\colon \mathbb{R}] = m$ és senar, tenim que $K_2 = \mathbb{R}$ pel primer lema. Així doncs veiem que $\mathrm{Gal}(K(i)/\mathbb{R})| = 2^r$ i, per tant, $|\mathrm{Gal}(K(i)/\mathbb{C})| = 2^{r-1}$. Si $r > 1$, aleshores tindríem que $2^{r-2} \mid |G|$ i, per tant, existiria un subgrup $H \leq G$ amb $|H| = 2^{r-2}$; el cos fix $K(i)^H$ tindria grau 2 sobre $\mathbb{C}$, cosa que hem vist que no pot passar. Per tant, $r = 1$, d'on veiem que $K(i) = \mathbb{C}$ i, en particular, $K \subseteq \mathbb{C}$. Això prova que totes les arrels de g viuen a $\mathbb{C}$, com volíem veure. □

5. Resolubilitat per radicals de les equacions algebraiques

En tot aquest capítol assumirem, per simplicitat, que tots els cossos involucrats són de característica 0. En particular, totes les extensions són separables.

5.1. **Polinomis resolubles, extensions radicals i Teorema de Galois.** L'objectiu és donar una caracterització dels polinomis $f(x) \in F[x]$ per als quals les arrels es poden expressar en termes dels coeficients mitjançant les operacions de cos i l'operació d'extreure arrels. Primer cal formalitzar aquesta noció en el llenguatge de cossos.

Definició 5.1. Una extensió K/F és radical si existeix una cadena de subsossos

$$F = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_{r-1} \subseteq K_r = K$$

amb[17] $K_{i+1} = K_i(\sqrt[n_i]{a_i})$ per a certs $a_i \in K_i$ i certs $n_i \geq 1$.

Definició 5.2. Un element α algebraic sobre F es pot expressar per radicals si pertany a alguna extensió radical K de F.

Aquesta definició formalitza el concepte que un nombre es pugui escriure a partir d'elements del cos base, fent operacions aritmètiques (suma, resta, producte i divisió) i extracció d'arrels. Per exemple, $\alpha = \sqrt[5]{2+\sqrt{3}} + \sqrt[3]{-5}$ es pot expressar per radicals en el sentit de la definició, ja que viu al cos K amb una cadena de subcossos següent:

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{-5}) = K_1 \subseteq K_1(\sqrt{3}) = K_2 \subseteq K_2\left(\sqrt[5]{2+\sqrt{3}}\right) = K.$$

Definició 5.3. Diem que un polinomi $f \in F[x]$ és resoluble per radicals si totes les seves arrels es poden expressar per radicals.

Per tant, un polinomi $f \in F[x]$ és resoluble per radicals si i només si cadascuna de les seves arrels pertany a alguna extensió radical.

Remarca 5.4. Aquí cal anar amb compte, perquè es podria pensar que f és resoluble per radicals si i només si el cos $F(\alpha)$ generat per cadascuna de les seves arrels és radical sobre F. Però això no és cert: pot passar que $F(\alpha)$ no sigui radical i que estigui contingut en un cos L que sí que sigui radical. Per exemple, el polinomi $f(x) = x^3 - 3x + 1$ és irreductible; si denotem per α una arrel de f tenim que $[\mathbb{Q}(\alpha)\colon \mathbb{Q}] = 3$, i resulta que $\mathbb{Q}(\alpha)$ és el cos de descomposició de f ja que es pot comporovar que

$$x^3 - 3x + 1 = (x - \alpha)(x - (\alpha^2 - 2))(x - (2 - \alpha - \alpha^2)).$$

Com que $\mathbb{Q}(\alpha)$ no té cap subcòs no trivial, l'única manera que podria ser radical és que $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt[n]{a})$ per a algun $n \geq 2$ i algun $a \in \mathbb{Q}$. Però si això fos cert, tindríem que $\mathbb{Q}(\zeta_n) \subseteq \mathbb{Q}(\alpha)$ i mirant graus això només és possible per a $n = 2$, cosa que no pot ser perquè $\mathbb{Q}(\alpha)/\mathbb{Q}$ no és quadràtica. En canvi, f és resoluble per radicals (sabem que tot polinomi de grau 3 ho és) i, per tant, $\mathbb{Q}(\alpha)$ està contingut en una extensió radical.

La caracterització de quan un polinomi és resoluble per radicals serà en termes del grup de Galois d'un cos de descomposició del polinomi. A aquest grup de Galois se l'anomena *el grup de Galois del polinomi.*

[17] Recordem que $K_{i+1} = K_i(\sqrt[n_i]{a_i})$ és una notació per denotar que $K_{i+1} = K_i(\alpha)$ amb α una arrel del polinomi $x^{n_i} - a_i$.

Definició 5.5. Sigui $f \in F[x]$ i sigui K un cos de descomposició de f. El grup de Galois de f és el grup de Galois de l'extensió K/F.

Observació 5.6. Fixem-nos que K/F és una extensió de Galois: és normal per ser el cos de descomposició d'un polinomi, i és separable perquè estem assumint que F és perfecte.

Teorema 5.7 (Teorema de Galois)**.** El polinomi $f(x)$ és resoluble per radicals si i només si el seu grup de Galois és resoluble.

Recordem que un grup G és resoluble si existeix una cadena se subgrups, cadascun normal en l'anterior

$$1 \trianglelefteq G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_{r-1} \trianglelefteq G_r = G \tag{5.1}$$

tal que G_{i+1}/G_i és abelià. Si G és finit, una definició equivalent de resoluble és que existeixi una cadena (5.1) tal que cada quocient G_{i+1}/G_i sigui cíclic[18]. Per això, i de cara a fer la demostració del Teorema 5.7 (que farem a la Secció 5.6), primer haurem d'estudiar a la Secció 5.5 les extensions amb grup de Galois cíclic.

Abans, però, veurem algunes aplicacions del Teorema 5.7. Recordem alguns exemples de grups resolubles i grups no resolubles:

- Tot grup abelià és resoluble.
- El grup diedral D_{2n} és resoluble.
- S_3 i S_4 són resolubles, mentre que S_n i A_n per $n \geq 5$ no són resolubles.

En particular, si un polinomi té grup de Galois isomorf a S_n amb $n \geq 5$, aleshores no és resoluble. Tot seguit, veurem que el grup de Galois d'un polinomi de grau n és un subgrup de S_n.

5.2. **Grup de Galois com a subgrups del grup simètric.** Si K/F és una extensió de Galois finita, aleshores $K = F(\alpha_1, \ldots, \alpha_n)$, on els α_i són les arrels d'un polinomi separable $f \in F[x]$. Fixem-nos que tot $\sigma \in \mathrm{Gal}(K/F)$ envia arrels de f a arrels de f. És a dir, cada $\sigma \in \mathrm{Gal}(K/F)$ dóna lloc a una permutació dels α_i, i σ està completament determinat per la seva acció en els α_i. Això dóna un morfisme injectiu de grups

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

que ens permet identificar $\mathrm{Gal}(K/F)$ com un subgrup del grup simètric S_n. Aquesta identificació depèn dels α_i escollits i de la seva ordenació.

Un subgrup G de S_n es diu *transitiu* si per a tot $i \neq j$ en $\{1, 2, \ldots, n\}$ existeix un element de G que envia i a j. Si el polinomi f és irreductible, sempre existeix $\sigma \in \mathrm{Gal}(K/F)$ tal que $\sigma(\alpha_i) = \alpha_j$ i, per tant, $\mathrm{Gal}(K/F)$ vist com a subgrup de S_n és transitiu.

5.3. **El polinomi general de grau n.** Siguin $x_1, x_2, \ldots, x_n$ indeterminades, i considerem el cos de funcions racionals $F(x_1, \ldots, x_n)$.

Definició 5.8. El polinomi general de grau n és el polinomi

$$(x - x_1)(x - x_2) \cdots (x - x_n) \in F(x_1, \ldots, x_n)[x].$$

És a dir, és el polinomi mònic que té per arrels $x_1, \ldots, x_n$.

[18] Això és perquè tot grup abelià finit és isomorf a un producte de grups cíclics i, per tant, podem refinar la cadena amb quocients abelians a una cadena amb quocients cíclics.

Sabem que aquest polinomi és igual a

$$x^n - s_1 x^{n-1} + s_2 x^{n-2} + \cdots + (-1)^n s_n, \tag{5.2}$$

on els s_i són els polinomis simètrics elementals:

$$s_i = \sum_{1 \leq j_1 < \cdots < j_i \leq n} x_{j_1} \dots x_{j_i}.$$

Fixem-nos que tenim una inclusió de cossos $F(s_1, \dots, s_n) \subseteq F(x_1, \dots, x_n)$, i que de fet l'extensió $F(x_1, \dots, x_n)/F(s_1, \dots, s_n)$ és de Galois, ja que $F(x_1, \dots, x_n)$ és el cos de descomposició del polinomi (5.2). Tot $\sigma \in \mathrm{S}_n$ dóna lloc a un automorfisme de $F(x_1, \dots, x_n)$ (l'acció és permutant les variables), i $F(s_1, \dots, s_n)$ és fix per aquesta acció. Tenim, doncs, un morfisme injectiu

$$\mathrm{S}_n \hookrightarrow \mathrm{Gal}(F(x_1, \dots, x_n)/F(s_1, \dots, s_n)).$$

D'aquí veiem que, en particular,

$$[F(x_1, \dots, x_n) \colon F(s_1, \dots, s_n)] \geq n!.$$

D'altra banda, per l'Observació 1.58, sabem que

$$[F(x_1, \dots, x_n) \colon F(s_1, \dots, s_n)] \leq n!,$$

d'on veiem que el grau de fet és $n!$ i, per tant,

$$\mathrm{Gal}(F(x_1, \dots, x_n)/F(s_1, \dots, s_n)) \simeq \mathrm{S}_n.$$

En particular, d'aquí deduïm que $F(x_1, \dots, x_n)^{\mathrm{S}_n} = F(s_1, \dots, s_n)$. És a dir, tota funció racional simètrica és una funció racional en els simètrics elementals. De fet, a la classe de problemes hem vist una propietat més forta: tot polinomi simètric és un polinomi en els simètrics elementals. No només això, sinó que també hem vist que els polinomis simètrics són algebraicament independents, és a dir, no hi ha cap combinació polinòmica en els s_i que s'anul·li. És a dir, el cos $F(s_1, \dots, s_n)$ és isomorf al cos de funcions racionals en n variables. Per tant, podem partir d'indeterminades $s_1, \dots, s_n$ i considerar el polinomi general

$$x^n - s_1 x^{n-1} + s_2 x^{n-2} + \cdots + (-1)^n s_n.$$

Si anomenem $x_1, \dots, x_n$ les arrels d'aquest polinomi (en un cos de descomposició), sabem que justament els s_i són els polinomis simètrics elementals en els x_i, amb la qual cosa hem demostrat el resultat següent.

Proposició 5.9. Siguin $s_1, \dots, s_n$ indeterminades. El polinomi general de grau n sobre el cos $F(s_1, \dots, s_n)$

$$x^n - s_1 x^{n-1} + s_2 x^{n-2} + \cdots + (-1)^n s_n$$

té grup de Galois isomorf a S_n.

Les fórmules per a les solucions generals de les equacions de graus 2, 3 i 4 són expressions per radicals de les arrels dels polinomis generals en termes dels coeficients. Com a corol·lari de la Proposició 5.9, del Teorema 5.7 i del fet que S_n no és resoluble per $n \geq 5$, obtenim que tal fórmula no existeix per a graus ≥ 5.

Proposició 5.10. Si $n \geq 5$, l'equació general de grau n no és resoluble per radicals.

5.4. **Polinomis no resolubles per radicals.** Que l'equació general de grau $n \geq 5$ no sigui resoluble per radicals no vol dir que no existeixin polinomis $f \in F[x]$ de grau ≥ 5 tals que les seves arrels es puguin expressar per radicals. Per exemple, les arrels de $x^n - a$ clarament es poden expressar per radicals. El Teorema 5.7 ens dóna un criteri per decidir quan això és possible i quan no. El resultat següent ens mostra que hi ha polinomis amb grup de Galois no resoluble, i aquests no són resolubles per radicals.

Proposició 5.11. Sigui $f(x) \in \mathbb{Q}[x]$ un polinomi irreductible amb tres arrels reals i dues arrels complexes no reals. El grup de Galois de f és S_5.

Demostració. Posem $K = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5) \subseteq \mathbb{C}$ el cos de descomposició de f, amb $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{R}$ i $\alpha_4, \alpha_5 \in \mathbb{C} \setminus \mathbb{R}$. Sabem que $\mathrm{Gal}(K/\mathbb{Q})$ és un subgrup de S_5 de cardinal divisible per 5. En particular, existeix algun element de $\mathrm{Gal}(K/\mathbb{Q})$ d'ordre 5 que, de fet, és un cicle de longitud 5. Sigui $\tau \in \mathrm{Aut}(\mathbb{C}/\mathbb{Q})$ la conjugació complexa. La restricció $\tau_{|K}$ de τ a K és un element de $\mathrm{Gal}(K/\mathbb{Q})$ que fixa $\alpha_1, \alpha_2, \alpha_3$ i intercanvia α_4 i α_5. Per tant, és una transposició. El subgrup generat per un cicle de longitud 5 i una transposició és tot S_5[19]. □

Proposició 5.12. El polinomi $f(x) = x^5 - 16x + 2$ té grup de Galois S_5.

Demostració. El polinomi és irreductible perquè és 2-Eisenstein. Té almenys una arrel positiva ($f(0) = 2$ i $f(1) = -13$). Per la regla dels signes de Descartes té, doncs, dues arrels positives i una de negativa.

Alternativament, f' només té dues arrels reals: $\frac{\pm 2}{\sqrt[4]{5}}$, i $f(\frac{-2}{\sqrt[4]{5}}) > 0$ i $f(\frac{2}{\sqrt[4]{5}}) < 0$. □

5.5. **Extensions cícliques.**

Definició 5.13. Una extensió K/F és cíclica si és de Galois i el seu grup de Galois és cíclic.

En aquesta secció n denota un nombre natural tal que $\mathrm{char}(F) \nmid n$ (en particular, n pot ser qualsevol si F és de característica 0). Denotem per μ_n el conjunt de les arrels n-èssimes de la unitat (és a dir, les arrels de $x^n - 1$) en una clausura algebraica $\overline{F}$ de F. Com que μ_n és un subgrup finit de $\overline{F}^\times$, és cíclic; als seus generadors els anomenem *arrels n-èssimes primitives de la unitat*. Si $a \in F^\times$, denotem per $\sqrt[n]{a}$ una arrel qualsevol del polinomi $x^n - a$.

Proposició 5.14. Si F conté les arrels n-èssimes de la unitat, aleshores $F(\sqrt[n]{a})/F$ és cíclica de grau dividint n.

Demostració. Com que n és coprimer amb la característica de F, el polinomi $x^n - 1$ és separable i hi ha n-arrels de la unitat. Sigui ζ_n una arrel n-èssima primitiva de la unitat. Aleshores, els elements $\zeta_n^k \sqrt[n]{a}$ amb $k = 0, 1, \ldots, n-1$ són n arrels diferents de $x^n - a$ i, per tant, són totes. Això prova que $F(\sqrt[n]{a})$ conté totes les arrels de $x^n - a$ i, per tant, és de Galois sobre F.

Si $\sigma \in \mathrm{Gal}(F(\sqrt[n]{a})/F)$, aleshores $\sigma(\sqrt[n]{a}) = \zeta_n^{k_\sigma} \sqrt[n]{a}$ per a algun $k_\sigma \in \mathbb{Z}$, ben determinat mòdul n. Tenim, doncs, una aplicació

$$\begin{array}{ccc} \mathrm{Gal}(F(\sqrt[n]{a})/F) & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \\ \sigma & \longmapsto & k_\sigma. \end{array}$$

[19] En efecte, reetiquetant podem suposar que $\sigma = (1\ 2\ 3\ 4\ 5)$. Tornant a reetiquetar si cal, també podem suposar que $\tau = (1\ i)$. Canviant σ per σ^{i-1} i reetiquetant, podem suposar que $\tau = (1\ 2)$. Ara $\sigma\tau\sigma^{-1} = (2\ 3)$, $\sigma^2\tau\sigma^{-2} = (3\ 4)$, $\sigma^3\tau\sigma^{-3} = (4\ 5)$. És fàcil veure que ara podem construir totes les transposicions que falten, per exemple: $(2\ 3)(1\ 2)(2\ 3) = (1\ 3)$, i de manera semblant amb la resta. Com que les transposicions generen el grup simètric, això ens dóna el resultat.

Com que

$$\sigma\tau(\sqrt[n]{a}) = \sigma(\zeta_n^{k_\tau}\sqrt[n]{a}) = \zeta_n^{k_\tau}\sigma(\sqrt[n]{a}) = \zeta_n^{k_\tau}\zeta_n^{k_\sigma}\sqrt[n]{a} = \zeta_n^{k_\sigma+k_\tau}\sqrt[n]{a},$$

l'aplicació $\sigma \mapsto k_\sigma$ és un morfisme de grups; com que clarament és injectiu, realitza $\mathrm{Gal}(F(\sqrt[n]{a})/F)$ com un subgrup de $\mathbb{Z}/n\mathbb{Z}$. □

Veurem que el recíproc d'aquesta proposició també és cert. Per a fer-ho, necessitem provar abans un parell de resultats que són importants també en si mateixos (per exemple, el resultat següent té un paper important en algunes demostracions de la correspondència de Galois diferents de la que hem vist aquí).

Teorema 5.15 (Independència lineal de caràcters)**.** Sigui G un grup i siguin $\chi_1, \dots, \chi_n \colon G \to F^\times$ morfismes de grups[20]. Si els χ_i són diferents entre ells, aleshores són F-linealment independents.

Demostració. Volem veure que si $\alpha_1, \dots, \alpha_n \in F$ són tals que

$$\alpha_1\chi_1(g) + \cdots + \alpha_n\chi_n(g) = 0 \quad \text{per a tot } g \in G, \tag{5.3}$$

aleshores $\alpha_i = 0$ per a tot i. Farem inducció sobre n. El cas $n = 1$ és evident; suposem-ho cert per a tot conjunt de $n-1$ caràcters i suposem que tenim (5.3). Com que $\chi_1 \neq \chi_n$, existeix $g' \in G$ tal que $\chi_1(g') \neq \chi_n(g')$. Escrivint (5.3) per gg' i utilitzant que $\chi_i(gg') = \chi_i(g)\chi_i(g')$ tenim

$$\alpha_1\chi_1(g)\chi_1(g') + \cdots + \alpha_n\chi_n(g)\chi_n(g') = 0 \quad \text{per a tot } g \in G. \tag{5.4}$$

Ara multipliquem (5.3) per $\chi_n(g')$:

$$\alpha_1\chi_1(g)\chi_n(g') + \cdots + \alpha_n\chi_n(g)\chi_n(g') = 0 \quad \text{per a tot } g \in G. \tag{5.5}$$

Restant (5.4) i (5.5) tenim que

$$\alpha_1(\chi_1(g') - \chi_n(g'))\chi_1(g) + \cdots + \alpha_{n-1}(\chi_{n-1}(g') - \chi_n(g'))\chi_{n-1}(g) = 0 \quad \text{per a tot } g \in G. \tag{5.6}$$

Això és una relació de dependència lineal de $\chi_1, \dots, \chi_{n-1}$ i, per inducció, tots els coeficients han de ser 0. En particular, $\alpha_1(\chi_1(g') - \chi_n(g')) = 0$ i, com que $\chi_1(g') \neq \chi_n(g')$, tenim que $\alpha_1 = 0$. La relació (5.3) amb $\alpha_1 = 0$ és una relació de dependència lineal que involucra $n-1$ caràcters i, per tant, $\alpha_2 = \cdots = \alpha_n = 0$. □

Definició 5.16. Si K/F és una extensió de Galois, definim la norma d'un element $\alpha \in K$ com a

$$\mathrm{N}_{K/F}(\alpha) = \prod_{\sigma \in \mathrm{Gal}(K/F)} \sigma(\alpha).$$

Proposició 5.17. $\mathrm{N}_{K/F}(\alpha)$ pertany a F i l'aplicació $\mathrm{N}_{K/F} \colon K^\times \to F^\times$ és un morfisme de grups.

Demostració. La primera afirmació és perquè $\sigma\left(\mathrm{N}_{K/F}(\alpha)\right) = \mathrm{N}_{K/F}(\alpha)$ per a tot $\sigma \in \mathrm{Gal}(K/F)$, la segona surt directa de la definició de norma. □

Teorema 5.18 (Teorema 90 de Hilbert)**.** Sigui K/F una extensió cíclica amb $\mathrm{Gal}(K/F) = \langle\sigma\rangle$. Un element $\alpha \in K^\times$ té norma 1 si, i només si, existeix $\beta \in K^\times$ tal que $\alpha = \beta/\sigma(\beta)$.

Demostració. És fàcil veure que si $\alpha = \beta/\sigma(\beta)$, aleshores $\mathrm{N}_{K/F}(\alpha) = 1$. Sigui ara $\alpha \in K$ de norma 1, és a dir, tal que

$$\alpha \cdot \sigma(\alpha) \cdot \sigma^2(\alpha) \cdots \sigma^{n-1}(\alpha) = 1, \tag{5.7}$$

[20] Els morfismes d'un grup en el grup multiplicatiu d'un cos s'anomenen *caràcters del grup*.

on n és l'ordre de σ. Pensem els σ^i com a caràcters $K^\times \to K^\times$; com que són diferents, són linealment independents sobre K. Per tant, la combinació lineal

$$\chi = \mathrm{id} + \alpha\cdot\sigma + \alpha\cdot\sigma(\alpha)\cdot\sigma^2 + \cdots + \alpha\cdot\sigma(\alpha)\cdot\sigma^2(\alpha)\cdots\sigma^{n-2}(\alpha)\cdot\sigma^{n-1}$$

és una aplicació $\chi\colon K \to K$ no nul·la. Sigui $\gamma \in K$ tal que $\beta = \chi(\gamma) \neq 0$. Tenim, doncs, que

$$\beta = \gamma + \alpha\cdot\sigma(\gamma) + \alpha\cdot\sigma(\alpha)\cdot\sigma^2(\gamma) + \cdots + \alpha\cdot\sigma(\alpha)\cdot\sigma^2(\alpha)\cdots\sigma^{n-2}(\alpha)\cdot\sigma^{n-1}(\gamma).$$

Utilitzant (5.7) es comprova que $\alpha\cdot\sigma(\beta) = \beta$, de manera que $\alpha = \beta/\sigma(\beta)$ com volíem provar. □

Corol·lari 5.19. Si K/F és cíclica de grau n i $\mu_n \subseteq F$ aleshores $K = F(\sqrt[n]{a})$ per a algun $a \in F$.

Demostració. Sigui σ un generador del grup de Galois, i sigui $\zeta_n \in F$ una arrel n-èssima primitiva de la unitat. Com que ζ_n té norma 1, pel Teorema 90 tenim que existeix $\beta \in K$ amb $\zeta_n = \beta/\sigma(\beta)$. Com que

$$\frac{\beta^n}{\sigma(\beta^n)} = \frac{\beta^n}{\sigma(\beta)^n} = \zeta_n^n = 1,$$

veiem que $\beta^n \in K^{\langle\sigma\rangle} = F$. Posem $a = \beta^n \in F$, de manera que $\sqrt[n]{a} = \beta$. Com que $\sigma(\beta) = \beta\zeta_n^{-1}$ i σ fixa ζ_n, veiem que

$$\sigma^i(\sqrt[n]{a}) = \sqrt[n]{a}\zeta_n^{-i}.$$

Per tant, $\sqrt[n]{a}$ no pertany al cos fix per cap subgrup del $\mathrm{Gal}(K/F)$ així que no pertany a cap subextensió pròpia de K/F, amb la qual cosa $K = F(\sqrt[n]{a})$. □

5.6. **Extensions radicals.**

Lema 5.20. La composició d'extensions radicals és radical.

Demostració. Suposem que K/F i K'/F són radicals. Si

$$F = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_{r-1} \subseteq K_r = K$$

és una torre d'extensions radicals simples per K

$$K' = K'K_0 \subseteq K'K_1 \subseteq \cdots \subseteq K'K_{r-1} \subseteq K'K_r = K'K$$

és una torre d'extensions radicals simples per $K'K/K'$. Ajuntant-la amb una torre d'extensions radicals simples per K'/K obtenim el resultat. □

5.7. **Demostració del Teorema 5.7.** Posem K el cos de descomposició de f. Siguin $\alpha_1, \ldots, \alpha_n$ les arrels de f en K, de manera que $K = F(\alpha_1, \ldots, \alpha_n)$.

Suposem, en primer lloc, que $f(x)$ és resoluble per radicals. Com que K és la composició dels cossos $F(\alpha_i)$ i cada $F(\alpha_i)$ està contingut en una extensió radical, pel Lemma 5.20 tenim que K està contingut en un cos $\tilde{L}$ tal que $\tilde{L}/F$ és radical. Sigui L la clausura normal de $\tilde{L}$ sobre F, de manera que L/F és Galois. Tenim que L és la composició dels cossos $\sigma(\tilde{L})$ amb $\sigma \in \mathrm{Gal}(L/F)$, i és fàcil veure que si $\tilde{L}/F$ és radical, aleshores $\sigma(\tilde{L})/F$ també és radical (si $\tilde{L}_{i+1} = \tilde{L}_i(\sqrt[n_i]{a_i})$, aleshores $\sigma(\tilde{L}_{i+1}) = \sigma(\tilde{L}_i)(\sqrt[n_i]{\sigma(a_i)})$). Com que la composició d'extensions radicals és radical, veiem que L/F és radical. És a dir, que existeix

$$F = L_0 \subseteq L_1 \subseteq \cdots \subseteq L_{r-1} \subseteq L_r = L \tag{5.8}$$

amb $L_{i+1} = L_i(\sqrt[n_i]{a_i})$ per a certs $a_i \in L_i$ i certs $n_i \geq 1$. Posem $m = n_0 \cdot n_1 \cdots n_{r-1}$ i considerem $L(\zeta_m)/F(\zeta_m)$, que també és de Galois. Fixem-nos que adjuntant ζ_m als subcossos de (5.8) obtenim:

$$F(\zeta_m) = L_0(\zeta_m) \subseteq L_1(\zeta_m) \subseteq \cdots \subseteq L_{r-1}(\zeta_m) \subseteq L_r(\zeta_m) = L(\zeta_m).$$

Per la Proposició 5.14 cada extensió $L_{i+1}(\zeta_m)/L_i(\zeta_m)$ és cíclica de grau dividint n_i. Posem $G_i = \mathrm{Gal}(L(\zeta_m)/L_i(\zeta_m))$, de manera que tenim

$$\{1\} = G_r \leq G_{r-1} \leq \cdots \leq G_2 \leq G_1 \leq G_0 = \mathrm{Gal}(L(\zeta_m)/F(\zeta_m))$$

Fixem-nos que tenim una aplicació exhaustiva

$$\begin{array}{ccc} G_i = \mathrm{Gal}(L(\zeta_m)/L_i(\zeta_m)) & \longrightarrow & \mathrm{Gal}(L_{i+1}(\zeta_m)/L_i(\zeta_m)) \\ \sigma & \longmapsto & \sigma_{|L_{i+1}(\zeta_m)} \end{array}$$

amb nucli G_{i+1}. Així doncs, $G_i/G_{i+1} \simeq \mathrm{Gal}(L_{i+1}(\zeta_m)/L_i(\zeta_m))$, que és cíclic i, per tant, $\mathrm{Gal}(L(\zeta_m)/F(\zeta_m))$ és resoluble. La restricció d'automorfismes dóna lloc a un morfisme de grups exhaustiu

$$\mathrm{Gal}(L(\zeta_m)/F) \longrightarrow \mathrm{Gal}(F(\zeta_m)/F)$$

amb nucli $\mathrm{Gal}(L(\zeta_m)/F(\zeta_m))$. Acabem de veure que $\mathrm{Gal}(L(\zeta_m)/F(\zeta_m))$ és resoluble, i $\mathrm{Gal}(F(\zeta_m)/F)$ és abelià (hi ha un morfisme de grups injectiu $\mathrm{Gal}(F(\zeta_m)/F) \to (\mathbb{Z}/m\mathbb{Z})^\times$ donat per $\sigma \mapsto \sigma_k$, on k és tal que $\sigma(\zeta_m) = \zeta_m^k$), i, per tant, també resoluble. Sabem de teoria de grups que si $N \trianglelefteq G$, aleshores G és resoluble si i només si N i G/N ho són, d'on deduïm que $\mathrm{Gal}(L(\zeta_m)/F)$ és resoluble. Finalment, tenim un morfisme exhaustiu

$$\mathrm{Gal}(L(\zeta_m)/F) \longrightarrow \mathrm{Gal}(K/F),$$

que mostra que $\mathrm{Gal}(K/F)$ és un quocient d'un grup resoluble. Novament, sabem de teoria de grups que els quocients de grups resolubles són resolubles, amb la qual cosa $\mathrm{Gal}(K/F)$ és resoluble.

Suposem ara que $G_0 = \mathrm{Gal}(K/F)$ és resoluble. Per tant, existeix una cadena de subgrups

$$\{1\} = G_r \leq G_{r-1} \leq \cdots \leq G_2 \leq G_1 \leq G_0 = \mathrm{Gal}(K/F)$$

amb G_i/G_{i+1} cíclic. Posant $K_i = K^{G_i}$, tenim una torre de subcossos

$$F = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_{r-1} \subseteq K_r = K, \tag{5.9}$$

on K_i/K_{i+1} és cíclica d'ordre n_i. Sigui F' el cos obtingut adjuntant totes les arrels de la unitat d'ordre n_i, i considerem

$$F \subseteq F' = F'K_0 \subseteq F'K_1 \subseteq \cdots \subseteq F'K_{r-1} \subseteq F'K_r = F'K. \tag{5.10}$$

La restricció dóna lloc a un morfisme de grups

$$\mathrm{Gal}(F'K_{i+1}/F'K_i) \longrightarrow \mathrm{Gal}(K_{i+1}/K_i)$$

que és injectiu (si σ és del nucli aleshores fixa F' i K_{i+1}; per tant fixa $F'K_{i+1}$). Així doncs, $\mathrm{Gal}(F'K_{i+1}/F'K_i)$ és cíclic d'ordre dividint n_i i pel Corol·lari 5.19 és radical simple. Com que F'/F també és radical tenim que $F'K/F$ és radical. Com que totes les arrels de f viuen a $F'K$, f és resoluble per radicals.

Apèndix A. Repàs de la teoria d'anells

Tot seguit recordem breument algunes definicions i resultats que s'utilitzen al llarg del text. Tot això es veu a Estructures Algebraiques, o sigui que aquí ens limitem a presentar els resultats de manera molt concisa i ometem les demostracions.

Definició A.1. Un anell és un conjunt R amb dues operacions $+$ i $\cdot$ (suma i producte) tals que:

- $(R, +)$ és un grup commutatiu (en particular, té un element neutre 0_R),
- El producte $\cdot$ és associatiu, commutatiu i té element neutre 1_R,
- Es compleix la propietat distributiva: $a \cdot (b + c) = a \cdot b + a \cdot c$ per a tot $a, b, c \in R$.

Observació A.2. Hi ha textos on a la definició d'anell no es demana que el producte sigui commutatiu ni que sigui unitari (és a dir, que tingui neutre pel producte). Com que els anells que ens trobem en aquest curs sempre són commutatius i unitaris, adoptem la terminologia que inclou aquests axiomes en la definició. Un abús de notació habitual és ometre el producte; així doncs, escrivim ab en comptes de $a \cdot b$. També escriurem 1 i 0 per denotar els elements neutres pel producte i la suma quan l'anell a què pertanyen sigui clar pel context.

Un element $r \in R$ és una *unitat* (o un *invertible*) si té invers pel producte. El conjunt $R^\times$ de les unitats de R és un grup amb el producte. Un cos és un anell on tot element no nul és invertible i $1 \neq 0$.

Dos exemples importants d'anells a tenir presents són l'anell dels nombres enters $\mathbb{Z}$ i l'anell $F[x]$ de polinomis en una variable i coeficients en un cos F (per exemple, $\mathbb{Q}[x]$).

Definició A.3. Un morfisme (o homomorfisme) d'anells és una aplicació $\phi\colon R \to S$ tal que

- $\phi(a + b) = \phi(a) + \phi(b)$ per a tot $a, b \in R$,
- $\phi(ab) = \phi(a)\phi(b)$ per a tot $a, b \in R$,
- $\phi(1) = 1$.

El *nucli* de ϕ és

$$\ker(\phi) := \{r \in R\colon \phi(r) = 0\},$$

i la *imatge* de ϕ és

$$\mathrm{im}(\phi) := \{\phi(r)\colon r \in R\}.$$

El morfisme ϕ és injectiu si i només si $\ker(\phi) = 0$. Si ϕ és bijectiu, aleshores l'aplicació inversa $\phi^{-1}\colon S \to R$ és també un morfisme d'anells; en aquest cas diem que ϕ és un isomorfisme. Dos anells R i S es diu que són isomorfs, denotat $R \simeq S$, si existeix algun isomorfisme entre ells.

Un *ideal* de R és un subconjunt $I \subseteq R$ tal que:

- I és un grup amb la suma.
- Si $i \in I$ i $r \in R$, aleshores $ri \in I$.

En particular, $\{0\}$ i R sempre són ideals de R, i $I = R$ si i només si I conté alguna unitat. El nucli d'un morfisme d'anells és un ideal (de l'anell de sortida). La imatge d'un morfisme d'anells és un subanell (de l'anell d'arribada).

Si $r \in R$, denotem per $r + I$ la classe

$$r + I := \{r + i\colon i \in I\},$$

i denotem per R/I el conjunt de classes:

$$R/I := \{r + I\colon r \in R\}.$$

Al conjunt R/I se l'anomena *el conjunt quocient de R per I*. Dues classes $r+I$ i $r'+I$ són iguals si i només si $r-r' \in I$. El conjunt quocient es pot dotar d'estructura d'anell amb les operacions de classes

$$(r+I)+(r'+I) := r+r'+I,$$
$$(r+I)(r'+I) := rr'+I.$$

És fàcil comprovar que aquestes operacions no depenen dels representants r i r' i que R/I satisfà els axiomes d'anell amb aquestes operacions. Per tant, parlem de l'anell quocient R/I. Una notació alternativa per a la classe $r+I$ és $\bar{r}$, quan I ja se sobreentén pel context. L'aplicació

$$\pi\colon R \longrightarrow R/I$$

que a cada element r li fa correspondre la seva classe $\bar{r}$ és un morfisme d'anells exhaustiu amb nucli I.

Si $\phi\colon R \to S$ és un morfismes d'anells i J és un ideal de S, aleshores $\phi^{-1}(J)$ (l'antiimatge de J per ϕ) és un ideal de R. En particular, $\ker(\phi)$ és un ideal de R, ja que $\ker(\phi) = \phi^{-1}(\{0\})$. També com a cas particular, si I és un ideal de R i considerem el morfisme de pas al quocient $\pi\colon R \to R/I$, per a tot ideal J de R/I tenim que $\pi^{-1}(J)$ és un ideal de R que conté I. Això estableix una bijecció entre els ideals de R/I i els ideals de R que contenen I.

Tot morfisme d'anells $\phi\colon R \to S$ indueix un morfisme d'anells

$$\bar{\phi}\colon R/\ker\phi \longrightarrow S$$

donat per $\bar{\phi}(\bar{r}) = \phi(r)$, que és un isomorfisme amb la imatge. Tenim, doncs, que

$$R/\ker\phi \simeq \mathrm{im}(\phi).$$

Un ideal $I \neq R$ és *primer* si té la propietat que sempre que $ab \in I$, aleshores $a \in I$ o $b \in I$. Un ideal I és *maximal* si $I \neq R$ i I no està contingut en cap altre ideal propi de R (és a dir, si J és un ideal i $I \subseteq J$, aleshores $J = I$ o $J = R$). Per a tot ideal propi I de R, existeix algun ideal maximal M de R tal que $I \subseteq M$. La demostració d'aquesta darrera propietat utilitza el Lema de Zorn[21], que és equivalent a l'Axioma de l'Elecció.

Si $a \in R$, l'ideal principal generat per a és

$$(a) := aR = \{ar\colon r \in R\}.$$

Més en general, l'ideal generat per una col·lecció d'elements $a_1, \ldots, a_n \in R$ és

$$(a_1, \ldots, a_n) := \{r_1a_1 + \cdots + r_na_n\colon r_1, \ldots, r_n \in R\}.$$

Un element $p \in R$ és primer si l'ideal principal (p) és primer i diferent de (0). Equivalentment, p és primer si no és 0 ni una unitat, i satisfà que sempre que p divideix un producte ab, aleshores necessàriament divideix a o b.

Un anell R és un domini d'integritat (o simplement domini) si és no nul i no té divisors de zero no nuls, és a dir, si sempre que $ab = 0$ es té que $a = 0$ o $b = 0$. Exemples de dominis són $\mathbb{Z}$, $F[x]$ o qualsevol cos. Un ideal I de R és primer si i només si R/I és un domini, i és maximal si i només si R/I és un cos. En particular, tot ideal maximal és primer (però el recíproc no és cert en general).

[21] Lema de Zorn: Sigui S un conjunt parcialment ordenat tal que tota cadena (és a dir, tot subconjunt totalment ordenat) C de S té una fita superior en S (és a dir, un element $f \in S$ tal que $c \leq f$ per a tot $c \in C$). Aleshores S conté almenys un element maximal m (és a dir, m té la propietat que no existeix cap element $s \in S$ amb $s \neq m$ i $m \leq s$).

Un domini R és un *domini d'ideals principals (DIP)* si tot ideal de R és principal. En un DIP tot ideal primer no nul és maximal.

En un domini d'integritat, diem que un element no nul $r \in R$ és *irreductible* si no és una unitat i sempre que es pugui escriure com a producte de dos elements $r = st$, aleshores s o t són unitats de R. Tot element primer és irreductible (però el recíproc no és cert en general).

Si $r = ut$ i u és una unitat, diem que r i t són associats. Diem que un domini R és un domini de factorització única (DFU) si tot element no nul de R es pot escriure com a producte d'irreductibles i aquesta expressió és única llevat de l'ordre i d'associats. En un DFU, tot element irreductible és primer. Si R és un DFU, aleshores $R[x]$, l'anell de polinomis en una variable i coeficients en R, també és un DFU. Inductivament, $R[x_1, \ldots, x_n]$ també és un DFU.

Un domini R és *Euclidià* si existeix una funció norma $N\colon R \to \mathbb{N}$ tal que per a tots $a, b \in R$ amb $b \neq 0$ existeixen $q, r \in R$ tals que $a = bq + r$ i $r = 0$ o $N(r) < N(b)$. Tot domini Euclidi és un DIP, i tot DIP és un DFU.

Tenim que $\mathbb{Z}$ és un domini Euclidià (la norma és el valor absolut) i $F[x]$ amb F un cos també és un domini Euclidià (la norma és el grau). El cas que en interessa més és el cas de $F[x]$. Tot ideal de $F[x]$ és principal. Els ideals primers de $F[x]$ són el (0) i els ideals de la forma (f) amb f un polinomi irreductible. Els ideals maximals són els de la forma (f) amb f un polinomi irreductible. Així doncs, si f és irreductible, el quocient $F[x]/(f)$ és un cos.

Referències

[Art91] Michael Artin. *Algebra*. Prentice Hall, Inc., Englewood Cliffs, NJ, 1991.

[DF04] David S. Dummit and Richard M. Foote. *Abstract algebra*. John Wiley & Sons, Inc., Hoboken, NJ, third edition, 2004.

[DFX93] F. Delgado, M. Fuertes, and S. Xambo. *Introducción al álgebra II*. 1993.

[Que] Jordi Quer. *Apunts d'àlgebra abstracta*.