Universitat de Barcelona

Facultat de Matemàtiques i Enginyeria Informàtica

Apunts

Grau en Matemàtiques

Curs 2023-2024 | *Setè Semestre*

Equacions Algebraiques (EQAL)

Autor:
Mario Vilar

Professor/a:
Dr. Xavier Guitart

Presentació de l'assignatura

L'objectiu d'aquesta matèria és oferir una introducció als fonaments de la Teoria de Galois i la seva aplicació a problemes relacionats amb la resolubilitat d'equacions mitjançant radicals. Aquest curs explora els fonaments de la teoria de cossos, amb un enfocament en extensions algebraiques, cossos de Galois i cossos ciclotòmics. També estudiarem arrels de la unitat i resolubilitat per radicals de diferents tipus d'equacions algebraiques. Basat en les notes [Gui22]. **Revisats**.

Universitat de Barcelona

Classificació AMS (2020): 00-01, 01A75, 00B50, 01A45, 01A50, 01A55, 01A60, 01A61, 01A65, 01A72, 01A73, 01A74, 01A75, 11-03, 30-03, 33-03, 34-03, 49-03.

Índex

Introducció

Tuvimos, hombre, tiempo para que nuestra sed fuera saciándose, el ancestral deseo de enumerar las cosas y sumarlas, de reducirlas hasta hacerlas polvo, arenales de números. Fuimos empapelando el mundo con números y nombres, pero las cosas existían, se fugaban del número, enloquecían en sus cantidades, se evaporaban dejando su olor o su recuerdo y quedaban los números vacíos.

Pablo NERUDA, *Oda a los números*

Primer de tot, trobareu que hi ha un índex, on hi distingim els diferents apartats ordenats seguint el meu propi criteri i, de tant en tant, seguint l'ordre cronològic del curs. Hi ha capítols, seccions, subseccions (i fins i tot subsubseccions). Us faig cinc cèntims de com he organitzat els encapçalaments de cada pàgina:

1. el número de l'últim capítol/secció/subsecció, depèn de la profunditat que hi hagi definida en aquell moment, figurarà en cada cantonada superior de pàgina parella (per exemple, *1.2*);
2. el nom del capítol es trobarà a la part dreta de la capçalera de les pàgines parelles (per exemple, «Divisibilitat i nombres primers»);
3. el nom de l'última secció/subsecció de la pàgina, a la cantonada dreta superior de les pàgines parelles (per exemple, «Polinomis: algorisme d'Euclides»);
4. el número de l'últim teorema, definició... de la pàgina en qüestió es trobarà a les pàgines senars, a la cantonada superior dreta, *destacat en el color de la seva capçalera corresponent* (per exemple, **1.2.3**).

A més, hi ha una taula, la taula de continguts. En aquest sentit, tal com acabem de dir, es veu fàcilment que s'ha seguit una mena de *sorting-by-color* per poder treballar de manera més eficient amb els diferents tipus d'enunciats matemàtics. D'aquesta manera, si busqueu una definició, un teorema... podreu distingir que estan destacats amb colors diferents (ara els introduïm) i trobar-los molt ràpidament:

1. Teoremes, proposicions, lemes, corol·laris, propietats, conjectures, processos i exercicis tindran aquest format (capçalera destacada amb color gris fosc):

   Teorema. *Compte! L'enunciat del teorema també serà en cursiva! Jove xef, porti whisky amb quinze glaçons d'hidrogen, coi!*

2. Les definicions i notacions tindran aquest format (capçalera de color gris clar):

   Definició. Aqueix betzol, Jan, comprava whisky de figa.

3. Les remarques i exemples tindran aquest format:

Observació. Zel de grum: quetxup, whisky, cafè, bon vi; ja!

Després de molts anys fent-ho malament, ara sol quedaran numerades aquelles equacions a les quals em referiré més endavant. És la *filosofia dominant* en la majoria de textos matemàtics (té nom i tot, es diu la *regla d'Occam*).

Per últim, m'estalviaré de comentar l'índex terminològic perquè el seu propòsit és clar i, en efecte, paral·lel al de l'organització d'aquest document: poder facilitar-vos al màxim la feina per localitzar qualsevol concepte que desitgeu. Espero que us serveixin d'alguna cosa aquests apunts, els he fet amb tot l'amor del món. Sort!

Mario Vilar
Sitges, Barcelona
22 de gener de 2024

Taula de continguts

Preliminars

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: grups i 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.

El propòsit principal d'aquest curs, doncs, és dunar una resposta satisfactòria a les qüestions proposades en l'enunciat següent. Enunciats i qüestions que, per la seva natura intuïtiva, cal precisar matemàticament més endavant.

> Donada una equació polinòmica $a_0 + a_1X + \cdots + a_nX^n = 0$ o bé donat un polinomi $a_0 + a_1X + \cdots + a_nX^n$:

equació	polinomi
té solucions?	té arrels?
quantes solucions?	quantes arrels?
on té les solucions?	on té les arrels?
com són les solucions?	com són les arrels?
solucions calculables?	arrels calculables?
com?	com?

Per a l'equació de grau 2:

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

Tenim la fórmula:

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

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 del polinomi com a expressions radicals dels coeficients. Sí que és cert que hi ha algunes equacions de graus ≥ 5 en les quals sí que podem expressar les arrels per radicals (per exemple $x^5 - 1 = 0$), però també n'hi ha d'altres (per exemple, $x^5 - 16x + 2$) 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 $\mathbb{K}_f$: és el cos més petit que conté les arrels de f. Per exemple, al polinomi $x^2 + 1$ li associem el cos:

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

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 $\mathbb{K}_f$ un grup finit, que s'anomena el grup de Galois de $\mathbb{K}_f$ i es denota per $\mathrm{Gal}\,(\mathbb{K}_f/\mathbb{Q})$, i tradueix els problemes sobre el cos $\mathbb{K}_f$ a problemes sobre el grup $\mathrm{Gal}\,(\mathbb{K}_f/\mathbb{Q})$. 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* $\mathrm{Gal}\,(\mathbb{K}_f/\mathbb{Q})$ *és resoluble.*

Més en general, podem començar amb un polinomi $f \in \mathbb{F}[x]$ amb coeficients en un cos $\mathbb{F}$ qualsevol. Aleshores el cos $\mathbb{K}_f$ que se li associa és un cos que conté $\mathbb{F}$ i novament conté totes les arrels de f. Es diu que $\mathbb{K}_f$ és una *extensió* de $\mathbb{F}$ (essencialment, vol dir que $\mathbb{K}_f$ conté $\mathbb{F}$). 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 jugar 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 destacat en la matemàtica actual amb aplicacions (d'ella o de generalitzacions seves) a teoria de nombres, teoria d'anells, geometria algebraica, teoria de grups, topologia algebraica, criptografia, etc.

I

Fonaments de la teoria de cossos

1.1 Definicions i primeres propietats

Definició 1.1.1 (Cos). Un cos $\mathbb{F}$ és un anell commutatiu unitari on tot element no nul és invertible pel producte i $1_F \neq 0_F$[1].

Definició 1.1.2 (Grup multiplicatiu). En particular, $\mathbb{F}^\times = \mathbb{F} \setminus \{0_F\}$ (li traiem l'únic element de $\mathbb{F}$ que no té invers) és un grup abelià amb el producte, que s'anomena *grup dels invertibles de* $\mathbb{F}$ o *grup multiplicatiu de* $\mathbb{F}$.

Exemple 1.1.3.

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 (i també que si un cos té un nombre finit d'elements aleshores el seu cardinal és p^r per algun primer p i algun $r \geq 1$).
2. Sigui R un domini d'integritat. Aleshores el seu cos de fraccions $\mathrm{Fr}(R)$ és un cos. Recordem que el cos de fraccions és

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

on la relació $\sim$ és $\frac{a}{b} \sim \frac{c}{d}$ si $ad - bc = 0$. Per exemple, podem construir els racionals a partir dels enters: $\mathrm{Fr}(\mathbb{Z}) = \mathbb{Q}$. Si $\mathbb{F}$ és un cos, l'anell $\mathbb{F}[x]$ de polinomis amb coeficients a $\mathbb{F}$ és un domini d'integritat, i definim $\mathbb{F}(x) := \mathrm{Fr}(\mathbb{F}[x])$; s'anomena el *cos de funcions racionals*[2] *en* x *amb coeficients a* $\mathbb{F}$.

Definició 1.1.4 (Morfisme de cossos). Un morfisme de cossos $\sigma : \mathbb{F} \longrightarrow \mathbb{K}$ és un morfisme d'anells; és a dir: $\sigma(a+b) = \sigma(a) + \sigma(b), \sigma(ab) = \sigma(a)\sigma(b)$ per a tot $a, b \in \mathbb{F}$, que a més compleix $\sigma(1_\mathbb{F}) = 1_\mathbb{K}$.

- $\sigma(a^{-1}) = \sigma(a)^{-1}$ i $a^{-1} \cdot a = 1_\mathbb{F}$
- Per tant, $\sigma(a^{-1} \cdot a) = \sigma(1_F) = 1_\mathbb{K}$ i $\sigma(a^{-1})\sigma(a) = 1_\mathbb{K}$.

Proposició 1.1.5. *Un morfisme de cossos bijectiu és un isomorfisme. Per tant,* σ^{-1} *és un morfisme de cossos tal que* $\sigma \circ \sigma^{-1} = Id_\mathbb{K}$ *i* $\sigma^{-1} \circ \sigma = Id_\mathbb{F}$.

[1] Prenem que 1_F és el neutre pel producte i 0_F és el neutre per la suma. $1_F \neq 0_F$ s'agafa com a requisit per a evitar tautologies.

[2] Les funcions racionals són aquelles que són divisions de polinomis que tenen coeficient en el cos corresponent.

Proposició 1.1.6.

1. *Els únics ideals d'un cos $\mathbb{F}$ són l'ideal 0 i l'ideal total $\mathbb{F}$.*
2. *Tot morfisme de cossos $\sigma : \mathbb{F} \longrightarrow \mathbb{K}$ és injectiu.*

Demostració.

1. Sigui $I \subseteq \mathbb{F}$ un ideal. Si $I \neq 0$ aleshores existeix un element no nul $a \in I$. Com que $\mathbb{F}$ 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 $I = \mathbb{F}$[3].
2. Sabem que el nucli $\ker(\sigma)$ és un ideal de $\mathbb{F}$ ($\mathrm{im}(\sigma)$ és subcòs de $\mathbb{K}$). Tenim dues opcions: o bé $\ker(\sigma) = (0)$ o bé $\ker(\sigma) = \mathbb{F}$. Com que $\sigma(1) = 1$[4], el nucli no és tot $\mathbb{F}$ i per tant ha de ser 0, amb la qual cosa σ és injectiu. ■

Definició 1.1.7 (Característica d'un cos)**.** Si $\mathbb{F}$ és un cos i $n \in \mathbb{Z}_{>0}$, definim $n \cdot 1_F := 1_F + 1_F + \overset{n}{\cdots} + 1_F$. Tenim un morfisme d'anells $f : \mathbb{Z} \longrightarrow \mathbb{F}$ definit com

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

El nucli $\ker(f)$ és doncs un ideal de $\mathbb{Z}$ i $\mathbb{Z}/\ker(f) \simeq \mathrm{im}(f)$. Com que $\mathrm{im}(f)$ 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 $\mathbb{F}$ 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 $\mathbb{F}$ és de característica p. Denotem per $\mathrm{car}(\mathbb{F})$ la característica de $\mathbb{F}$ que és 0 o un nombre primer p.

1. Si $\mathrm{car}(\mathbb{F}) = 0$, aleshores f és injectiu i $\mathbb{F}$ conté un subanell isomorf a $\mathbb{Z}$. Com que $\mathbb{F}$ és un cos, també conté doncs un subcòs isomorf al cos de fraccions de $\mathbb{Z}$, és a dir, a $\mathbb{Q}$.
2. Si $\mathrm{car}(\mathbb{F}) = p$, 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 a dir, $\ker(f) = (p)$). Observem en aquest cas també que $\mathbb{F}$ conté un subcòs isomorf a $\mathbb{F}_p$.

Definició 1.1.8 (Cos primer)**.** Si $\mathrm{car}(\mathbb{F}) = 0$, diem que $\mathbb{Q}$ és el cos primer de $\mathbb{F}$. Si $\mathrm{car}(\mathbb{F}) = p$ diem que $\mathbb{F}_p$ és el cos primer de $\mathbb{F}$.

Exemple 1.1.9. $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Q}(x), \mathbb{R}(x), \mathbb{C}(x)$ són de característica 0; en canvi, $\mathbb{F}_p$ i $\mathbb{F}_p(x)$ són de característica p.

[3] Recordem, que si $1 \in I$, $a \cdot 1 \in I$ per a tot $a \in \mathbb{F}$, de manera que tot a queda dins I; és a dir, $\mathbb{F} = I$.
[4] Si $1 \in \ker(\sigma)$, hauria de succeir $\sigma(1) = 0_{\mathbb{K}}$, però per definició de morfisme de cossos $\sigma(1_{\mathbb{F}}) = 1_{\mathbb{K}}$.

1.2

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 en $\mathbb{C}$, que és un cos més gran. De manera natural, doncs, quan estudiem arrels de polinomis amb coeficients en un cos $\mathbb{F}$, sovint hem de considerar cossos més grans que el propi $\mathbb{F}$. Això dona lloc a la noció d'extensió de cossos, que és clau en la teoria de Galois.

Definició 1.2.1 (Extensió de cossos)**.** Una extensió de cossos $\mathbb{K}/\mathbb{F}$ és una inclusió de cossos $\mathbb{F} \subset \mathbb{K}$ (és a dir, $\mathbb{F}$ és un **subcòs** de $\mathbb{K}$). Una subextensió de $\mathbb{K}/\mathbb{F}$ és una extensió $\mathbb{L}/\mathbb{F}$ amb $\mathbb{F} \subset \mathbb{L} \subset \mathbb{K}$.

Observació 1.2.2. La notació $\mathbb{K}/\mathbb{F}$ per una extensió de cossos no s'ha de confondre amb el quocient. Sovint es dibuixa un diagrama de l'estil: per indicar que $\mathbb{K}$ és una extensió de $\mathbb{F}$.

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

Figura 1.1: Extensió de cossos.

Exemple 1.2.3. **Tot cos és extensió del seu cos primer**. Així doncs, tenim les extensions $\mathbb{R}/\mathbb{Q}$, $\mathbb{C}/\mathbb{Q}$ i $\mathbb{F}_p(x)/\mathbb{F}_p$. També sabem que $\mathbb{R}$ és un subcòs de $\mathbb{C}$, així que tenim $\mathbb{C}/\mathbb{R}$. Definim el següent subconjunt dels complexos: $\mathbb{Q}(i) := \{a+bi \mid a,b \in \mathbb{Q}\}$. És clar que $\mathbb{Q}(i)$ és un subanell de $\mathbb{C}$ (això és perquè la suma i multiplicació de dos elements de $\mathbb{Q}(i)$ cau dins de $\mathbb{Q}(i)$). Per a veure que n'és un subcòs, 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

$$(a+bi)^{-1} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i, \quad \frac{a}{a^2+b^2}, \frac{b}{a^2+b^2} \in \mathbb{Q};$$

també pertany a $\mathbb{Q}(i)$, tenim doncs que $\mathbb{Q}(i)$ és un cos. Per tant, obtenim que $\mathbb{Q}(i)/\mathbb{Q}$ és una subextensió de $\mathbb{C}/\mathbb{Q}$ i, en particular, obtenim les extensions següents: $\mathbb{Q}(i)/\mathbb{Q}$ i $\mathbb{C}/\mathbb{Q}(i)$.

Una eina molt important en l'estudi de les extensions de cossos és l'àlgebra lineal. Això és possible gràcies a la propietat següent:

Proposició 1.2.4. *Si $\mathbb{K}/\mathbb{F}$ és una extensió de cossos aleshores $\mathbb{K}$ és un espai vectorial sobre $\mathbb{F}$ (el producte per escalars de $\mathbb{F}$ es defineix com el producte a $\mathbb{K}$).*

Demostració. En efecte, qualsevol extensió $\mathbb{K}$ sobre $\mathbb{F}$ és un espai vectorial sobre $\mathbb{F}$; usant les operacions additiva i multiplicativa en $\mathbb{K}$ podem definir la multiplicació escalar en l'espai vectorial sobre $\mathbb{F}$. Totes les propietats són immediates, per ser $\mathbb{K}$ un cos, excepte $1v = v$ per a tot $v \in \mathbb{K}$: cal assegurar-nos que la identitat de $\mathbb{F}$ és la identitat de $\mathbb{K}$. Com que $\mathbb{F}$ és subcòs, conté una identitat $1_{\mathbb{F}} \neq 0$ (hem de comprovar $1_{\mathbb{F}} = 1_{\mathbb{K}}$). Tenim $1_{\mathbb{F}} \cdot 1_{\mathbb{F}} = 1_{\mathbb{F}}$ per ser la identitat en $\mathbb{F}$, de manera que és un element invertible de $\mathbb{K}$; multiplicant per $1_{\mathbb{F}}^{-1}$ obtenim:

$$1_{\mathbb{F}} \cdot 1_{\mathbb{F}} \cdot 1_{\mathbb{F}}^{-1} = 1_{\mathbb{F}} \cdot 1_{\mathbb{F}}^{-1} \iff 1_{\mathbb{F}} = 1_{\mathbb{K}}. \qquad \blacksquare$$

Definició 1.2.5 (Grau d'una extensió)**.** El grau d'una extensió $\mathbb{K}/\mathbb{F}$, denotat $[\mathbb{K} : \mathbb{F}]$, és la dimensió de $\mathbb{K}$ com a $\mathbb{F}$-espai vectorial. Diem que $\mathbb{K}/\mathbb{F}$ és finita si $[\mathbb{K} : \mathbb{F}] < \infty$ i que és infinita si $[\mathbb{K} : \mathbb{F}] = \infty$. *Això no té res a veure amb la noció que el nombre d'elements del cos sigui finit o infinit.*

Exemple 1.2.6. $[\mathbb{C} : \mathbb{R}] = 2$, ja que podem expressar tot complex $z = a + bi$ on $a, b \in \mathbb{R}$, de manera que $(1, i)$ és una base de $\mathbb{C}$ com a $\mathbb{R}$-espai vectorial. Anàlogament, $[\mathbb{Q}(i) : \mathbb{Q}] = 2$. $[\mathbb{R} : \mathbb{Q}] = \infty$ ja que $\mathbb{Q}$ és numerable, però $\mathbb{R}$ no ho és. Per últim, $[\mathbb{Q}(t) : \mathbb{Q}] = \infty$, ja que $1, t, t^2, t^3, \ldots$ són linealment independents.

Exemple 1.2.7 (Extensions obtingudes a partir de polinomis irreductibles)**.** Un exemple molt important d'extensions: *extensions obtingudes a partir de polinomis irreductibles*. Ara veurem que donat un polinomi irreductible $f \in \mathbb{F}[x]$ **sempre existeix una extensió $\mathbb{K}/\mathbb{F}$ 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 manera purament algebraica[5] i després generalitzarem aquest procés a altres cossos. La clau està en considerar l'aplicació següent, que és avaluar un polinomi en i:

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

És fàcil comprovar que ϕ és un morfisme d'anells, i que ϕ és exhaustiu. Veiem 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 $f(i) = f(-i) = 0$. Per tant $(x - i)(x + i) = x^2 + 1$ divideix f i $f \in (x^2 + 1)$. La conclusió és doncs que $\mathbb{R}[x]/(x^2 + 1) \simeq \mathbb{C}$. Per més detalls, [Vil23, p. 80].

Aquest procés es pot generalitzar per a donar resposta a aquesta pregunta: donat un cos $\mathbb{F}$ i un polinomi $f \in \mathbb{F}[x]$ no constant, existeix alguna extensió $\mathbb{K}/\mathbb{F}$ en la qual f té alguna

[5] És a dir, obtindrem un cos isomorf a $\mathbb{C}$, però no obtindrem cap de les altres propietats extres que coneixem de $\mathbb{C}$ (com, per exemple, que té una topologia). Simplement estem dient que tenen la mateixa estructura com a cos.

arrel? La resposta és que sí, i ens la dóna la proposició següent. Fixem-nos que n'hi ha prou amb considerar 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 1.2.8. *Sigui $\mathbb{F}$ un cos i $f(x) \in \mathbb{F}[x]$ un polinomi irreductible de grau ≥ 1. Existeix un cos $\mathbb{K}$ i un morfisme $\iota : \mathbb{F} \longrightarrow \mathbb{K}$, on $\iota(f)$ denota el polinomi obtingut aplicant ι als coeficients de f, tal que $\iota(f)$ té alguna arrel a $\mathbb{K}$.*

Demostració. Com que $\mathbb{F}[x]$ és un domini d'ideals principals i $f(x)$ és irreductible, sabem per *Estructures Algebraiques* que l'ideal $(f(x))$ és primer i, en particular, (com $\mathbb{F}[x]$ és DIP) és maximal. Per tant el quocient $\mathbb{K} := \mathbb{F}[x]/(f(x))$ és un cos. Sigui $\pi : \mathbb{F}[x] \longrightarrow \mathbb{F}[x]/(f(x))$ és el morfisme de pas al quocient i denotem per ι la composició de π amb la inclusió natural, i, de $\mathbb{F}$ en $\mathbb{F}[x]$, que identifica $\mathbb{F}$ amb $\iota(F)$:

$$\iota : \mathbb{F} \xrightarrow{i} \mathbb{F}[x] \xrightarrow{\pi} \mathbb{K},\ \iota = i \circ \pi.$$

Clarament ι és un morfisme de cossos i $\mathbb{K}$ conté $\iota(\mathbb{F})$ que és un subcòs isomorf a $\mathbb{F}$. Ara, posem $\alpha = \pi(x)$ la classe de x a $\mathbb{F}[x]/(f(x))$. Del fet que $\pi(f(x)) = 0$, i posant $f(x) = a_n x^n + \cdots a_1 x + a_0$, obtenim:

$$\pi(f(x)) = \pi\left(a_n x^n + \cdots a_1 x + a_0\right) = \pi\left(a_n\right)\alpha^n + \cdots + \pi\left(a_1\right)\alpha + \pi\left(a_0\right) = f(\alpha) = 0.$$

En particular,

$$\iota\left(a_n\right)\alpha^n + \cdots + \iota\left(a_1\right)\alpha + \iota\left(a_0\right) = \iota(f)(\alpha),$$

amb la qual cosa $\alpha \in \mathbb{K}$ és una arrel de $\iota(f)$ en $\mathbb{K}$. *Més informalment, podem posar que $\overline{f(x)} = 0$ implica que $f(\overline{x}) = 0$.* ∎

Observació 1.2.9. Fixem-nos que ι dóna un *isomorfisme* entre $\mathbb{F}$ i el subcòs $\iota(\mathbb{F})$ de $\mathbb{K}$. Identificant $\mathbb{F}$ amb $\iota(\mathbb{F})$ via aquest isomorfisme, 1.2.8 diu que existeix una extensió $\mathbb{K}/\mathbb{F}$ a on f hi té alguna arrel, i aquesta extensió és $\mathbb{K} = \mathbb{F}[x]/(f)$. En efecte, si volem fer més precís aquest pas d'*identificar* $\mathbb{F}$ *amb* $\iota(\mathbb{F})$ podem provar que certament existeix una extensió $\mathbb{K}'/\mathbb{F}$ tal que f té una arrel a $\mathbb{K}'$ de la manera següent: prenem K_0 un conjunt de la mateixa cardinalitat que $\mathbb{K}\setminus\iota(\mathbb{F})$ i disjunt amb $\mathbb{F}$, i prenem una bijecció qualsevol $\phi_0 : K_0 \longrightarrow \mathbb{K}\setminus\iota(\mathbb{F})$. Aleshores, definim el conjunt $\mathbb{K}' = \mathbb{F} \cup K_0$ i estenem la bijecció ϕ_0 a una bijecció $\phi : \mathbb{K}' \longrightarrow \mathbb{K}$ fent que $\phi(\beta) = \iota(\beta)$ si $\beta \in \mathbb{F}$. De moment, $\mathbb{K}'$ és només un conjunt que conté $\mathbb{F}$, però li podem donar una estructura de cos definit $\beta + \gamma = \phi^{-1}(\phi(\beta) + \phi(\gamma))$ i $\beta\gamma = \phi^{-1}(\phi(\beta)\phi(\gamma))$ per $\beta, \gamma \in \mathbb{K}'$. Aleshores, $\mathbb{K}'$ és un cos que conté $\mathbb{F}$ com a subcòs i $\phi : \mathbb{K}' \longrightarrow \mathbb{K}$ és un isomorfisme de cossos tal que $\phi|_F = \iota$. Aleshores, $\phi^{-1}(\alpha)$ és una arrel de f en $\mathbb{K}'$.

Així doncs, **donat un polinomi irreductible $f(x) \in \mathbb{F}[x]$ sabem que existeix una extensió $\mathbb{K}/\mathbb{F}$ 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 1.2.10. *Amb la notació de 1.2.8 tenim que* $[\mathbb{K}:\mathbb{F}] = n$ *on* n *és el grau de* f*. Una* $\mathbb{F}$*-base de* $\mathbb{K}$ *és* $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$.

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

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

Per la divisió de polinomis tenim que

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

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

$$\begin{aligned}\pi(b(x)) &= \pi(q(x)f(x) + r(x)) = \pi(q(x)f(x)) + \pi(r(x)) = \pi(r(x)),\ \pi(x^n) = \alpha^n;\\ &= \pi(r_{n-1})\alpha^{n-1} + \cdots + \pi(r_1)\alpha + \pi(r_0) = r_{n-1}\alpha^{n-1} + \cdots + r_1\alpha + r_0,\end{aligned}$$

amb la qual cosa veiem que $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ genera $\mathbb{K}$ com a $\mathbb{F}$-espai vectorial[6]. Veiem, doncs, 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 $g(x) = c_{n-1}x^{n-1} + \cdots + c_1 x + c_0 \in \mathbb{F}[x]$ seria un polinomi tal que $\pi(g(x)) = 0$ i per tant $g(x) \in (f(x))$. Com que $\operatorname{gr}(g) \leq n-1 < \operatorname{gr}(f) = n$ tenim que necessàriament $g = 0$ i per tant tots els c_i han de ser 0. ■

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

$$\mathbb{K} = \left\{ c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1} \;\middle|\; c_i \in \mathbb{F} \right\},$$

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

Exemple 1.2.11.

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 $\mathbb{K} = \mathbb{Q}[x]/(x^2-5)$. Tenim que $[\mathbb{K}:\mathbb{Q}] = 2$ i $\mathbb{K} = \{a + b\alpha : a, b \in \mathbb{Q}\}$ i $\alpha^2 = 5$. La suma i producte en aquest cos són:
$$\begin{aligned}(a + b\alpha) + (c + d\alpha) &= (a + c) + (b + d)\alpha\\ (a + b\alpha)(c + d\alpha) &= ac + 5bd + (ad + bc)\alpha\end{aligned}$$
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 $\mathbb{K}$ són de la forma $a + b\sqrt{5}$ amb $a, b \in \mathbb{Q}$.

[6] En la última igualtat tenim $\pi(r_i) = r_i$ per a tot i perquè r_i mòdul un polinomi irreductible és el mateix r_i un altre cop.

Notació 1.2.12. Aquí $\sqrt{5}$ no vol dir el nombre real $\sqrt{5}$, sinó només un símbol que satisfà que el seu quadrat és 5. És habitual treballar amb α solament, i se li assigna aquest «nom».

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

$$\mathbb{Q}[x]/(f) = \left\{a + b\alpha + c\alpha^2 \;\middle|\; a, b, c \in \mathbb{Q}\right\}, \tag{1.1}$$

on $\alpha^3 - 7 = 0$. Novament, podem operar en aquest cos, (1.1), amb les operacions habituals, només tenint en compte que $\alpha^3 = 7$.

4. Siguin $\mathbb{F} = \mathbb{F}_2$ (el cos finit de dos elements) 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 $\mathbb{K} = \mathbb{F}_2[x]/\left(x^2 + x + 1\right)$ és un cos que comprèn $\{a + b\alpha \mid a, b \in \mathbb{F}_2 \text{ i } \alpha^2 + \alpha + 1 = 0\}$ i amb $[\mathbb{K} : \mathbb{F}_2] = 2$. Així doncs té 2^2 elements. Com hem dit, els seus elements són de la forma $a + b\alpha$ amb $a, b \in \mathbb{F}_2$ i $\alpha^2 + \alpha + 1 = 0$. F_2 compleix que $-1 \equiv 1$; per tant, $\alpha^2 = -\alpha - 1 \equiv \alpha + 1$. Així doncs, com a exemple de com podem operar tenim que:

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

1.2.1 Grups d'automorfismes d'extensions

Definició 1.2.13 (Grup d'automorfismes d'extensions). Si $\mathbb{K}/\mathbb{F}$ i $\mathbb{L}/\mathbb{F}$ són dues extensions de $\mathbb{F}$, un $\mathbb{F}$-morfisme $\sigma : \mathbb{K} \longrightarrow \mathbb{L}$ és un morfisme de cossos tal que $\sigma_{|\mathbb{F}} = Id$; és a dir, tal que $\sigma(\alpha) = \alpha$ per a tot $\alpha \in \mathbb{F}$ (es diu que σ fixa els elements de $\mathbb{F}$). De manera semblant, un $\mathbb{F}$-automorfisme $\tau : \mathbb{K} \longrightarrow \mathbb{K}$ és un automorfisme de cossos (i.e., un morfisme de cossos bijectiu) que fixa $\mathbb{F}$. Denotem per $\mathrm{Aut}(\mathbb{K}/\mathbb{F})$ el conjunt de $\mathbb{F}$-automorfismes de $\mathbb{K}$.

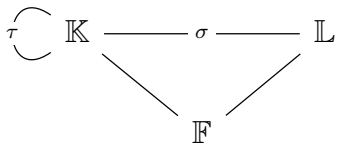


Figura 1.2: Extensions de cossos amb $\mathbb{F}$-morfismes i $\mathbb{F}$-automorfismes (de $\mathbb{K}$).

Proposició 1.2.14. *Aquest conjunt de 1.2.13 el podem dotar d'estructura de grup on l'operació és la composició.*

Demostració. En efecte, si $\sigma, \tau \in \mathrm{Aut}(\mathbb{K}/\mathbb{F})$ definim $\sigma\tau = \sigma \circ \tau$. L'operació està ben definida ja que la composició de $\mathbb{F}$-automorfismes és un $\mathbb{F}$-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 $\mathbb{F}$-automorfisme té un invers per la composició que també és un $\mathbb{F}$-automorfisme. ■

Observació 1.2.15. Com que $\mathbb{K}$ és un $\mathbb{F}$-espai vectorial, un element $\sigma \in \mathrm{Aut}(\mathbb{K}/\mathbb{F})$ queda determinat per la imatge per σ d'una $\mathbb{F}$-base de $\mathbb{K}$. Efectivament, sigui

$$\lambda_1 x_1 + \lambda_2 x_2 + \cdots + \lambda_n x_n, x_i \in \mathbb{K}, \lambda_i \in \mathbb{F}.$$

Per definició de σ, $\sigma|_{\mathbb{F}} = Id$; així doncs, $\sigma(\lambda_i) = \lambda_i$ per a tot i. Per tant:

$$\sigma(\lambda_1 x_1 + \lambda_2 x_2 + \cdots + \lambda_n x_n) = \lambda_1 \sigma(x_1) + \lambda_2 \sigma(x_2) + \cdots + \lambda_n \sigma(x_n).$$

És així com σ queda determinat pel seu valor en els elements d'una $\mathbb{F}$-base de $\mathbb{K}$. Per últim, $\sigma \in \mathrm{Aut}(\mathbb{K}/\mathbb{F})$ és un automorfisme de $\mathbb{K}$ com a $\mathbb{F}$-espai vectorial.

Exemple 1.2.16.

1. La conjugació complexa, que envia $x \longmapsto \bar{x}$, on $\bar{x}$ és la seva conjugació complexa, és un element de $\mathrm{Aut}(\mathbb{C}/\mathbb{R})$. Efectivament, per a tot $x \in \mathbb{R}$ tenim $\bar{x} = x$, però això no es compleix per a $x \in \mathbb{C} \setminus \mathbb{R}$. Si anomenem τ a aquest automorfisme de $\mathbb{C}$ en $\mathbb{C}$, tenim $\tau \in \mathrm{Aut}(\mathbb{C}/\mathbb{R})$.
2. Sigui $\mathbb{K} = \mathbb{Q}[x]/(x^2 - 5)$, amb una $\mathbb{Q}$-base $\{1, \alpha\}$ on $\alpha^2 - 5 = 0$. Si $\sigma \in \mathrm{Aut}(\mathbb{K}/\mathbb{Q})$, fixem-nos que $\sigma(\alpha^2 - 5) = \sigma(0) = 0$ i per tant $\sigma(\alpha)^2 - 5 = 0$. Es a dir, $\sigma(\alpha)$ és necessàriament una arrel de $x^2 - 5$ a $\mathbb{K}$. Les dues úniques arrels són α i $-\alpha$; per tant, $\sigma(\alpha) \in \{\alpha, -\alpha\}$. Es pot comprovar (tot i que més endavant veurem un resultat teòric que ens ho estalvia) que l'aplicació $\sigma : \mathbb{K} \longrightarrow \mathbb{K}$ tal que $\sigma(\alpha) = -\alpha$, $\sigma(1) = 1$ i

   $$\sigma(a + b\alpha) = a + b\sigma(\alpha) = a - b\alpha$$

   és un automorfisme no trivial de $\mathbb{K}$. L'altre únic automorfisme és la identitat, amb la qual cosa $\mathrm{Aut}(\mathbb{K}/\mathbb{Q}) = \{Id, \sigma\}$. Com que $\sigma^2 = Id$, tenim que $\mathrm{Aut}(\mathbb{K}/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}$.
3. Sigui $\mathbb{K}$ un cos de característica $p > 0$. L'aplicació:

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

   és un morfisme de cossos. Clarament:

   $$\mathrm{Fr}_p(\alpha\beta) = (\alpha\beta)^p \overset{7}{=} \alpha^p \beta^p = \mathrm{Fr}_p(\alpha)\,\mathrm{Fr}_p(\beta).$$

   Pel que fa a la compatibilitat respecte 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 $\mathbb{K}$ té característica p ($p = 0$ a $\mathbb{K}$), els termes del sumatori són 0.

[7] Recordem que un cos és commutatiu pel producte, així que, sí, $(xy)^p = x^p y^p$. Si tinguéssim un anell no commutatiu no podríem dir això!

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

Observació 1.2.17. A vegades el grup de $\mathbb{F}$-automorfismes de $\mathbb{K}$ també se li diu grup de Galois de $\mathbb{K}/\mathbb{F}$, i es denota per $\mathrm{Gal}(\mathbb{K}/\mathbb{F})$. 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 $\mathbb{F}$-automorfismes $\mathrm{Aut}(\mathbb{K}/\mathbb{F})$, i quan $\mathbb{K}/\mathbb{F}$ sigui de Galois aleshores a aquest grup li direm el grup de Galois i el denotarem $\mathrm{Gal}(\mathbb{K}/\mathbb{F})$.

1.2.2 Adjunció d'elements

Definició 1.2.18 (Cos d'adjunció). Sigui $\mathbb{K}/\mathbb{F}$ una extensió i $\alpha \in \mathbb{K}$. Denotem per $\mathbb{F}[\alpha]$ el menor subanell de $\mathbb{K}$ que conté $\mathbb{F}$ i α, i per $\mathbb{F}(\alpha)$ el menor subcòs de $\mathbb{K}$ que conté $\mathbb{F}$ i α. Diem que $\mathbb{F}(\alpha)$ és el cos obtingut adjuntant α a $\mathbb{F}$.

Com que $\mathbb{F}[\alpha]$ és un subanell que conté $\mathbb{F}$ i conté α, i per tant 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 $a_i \in \mathbb{F}$. Així doncs:

$$\mathbb{F}[\alpha] = \left\{a_0 + a_1\alpha + \cdots + a_n\alpha^n \;\middle|\; a_i \in \mathbb{F}, n \geq 0\right\} = \{f(\alpha) \mid f \in \mathbb{F}[x]\},$$

ja que el conjunt de la dreta és un subanell de $\mathbb{K}$ (en efecte, és la imatge del morfisme d'anells $\mathbb{F}[x] \longrightarrow \mathbb{K}$ que envia $f(x)$ a $f(\alpha)$). De manera semblant es raona que

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

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

Observació 1.2.19 (La intersecció de subcossos és un subcòs). Si $\mathbb{F} \subset \mathbb{K}_1, \mathbb{K}_2 \subset \mathbb{K}$, aleshores $\mathbb{K}_1 \cap \mathbb{K}_2$ és un subcòs que conté $\mathbb{F}$ (exercici). Tenim la inclusió

$$F(\alpha) \supseteq \bigcap_{\substack{F \subset \mathbb{K}' \subset \mathbb{K} \\ \alpha \in \mathbb{K}'}} \mathbb{K}'.$$

Ara, com sabem que la intersecció de subcossos és subcòs, tenim que el subcòs *més petit* de $\mathbb{K}$ que conté $\mathbb{F}$ i conté α està contingut en $\bigcap_{\substack{F \subset \mathbb{K}' \subset \mathbb{K} \\ \alpha \in \mathbb{K}'}} \mathbb{K}'$. Per tant, tenim la igualtat.

Definició 1.2.20 (Extensió finitament generada)**.** Una extensió $\mathbb{K}/\mathbb{F}$ és finitament generada si existeixen elements $\alpha_1, \ldots, \alpha_n$ tals que $\mathbb{K} = \mathbb{F}(\alpha_1, \ldots, \alpha_n)$. L'extensió és simple si està generada per un element, és a dir, si $\mathbb{K} = \mathbb{F}(\alpha)$ per algun $\alpha \in \mathbb{K}$.

Proposició 1.2.21 (Existència de l'extensió que conté arrels de f)**.** *Sigui $f \in \mathbb{F}[x]$ irreductible i $\mathbb{K}/\mathbb{F}$ una extensió on f té una arrel α, és a dir, $f(\alpha) = 0$. Aleshores, $\mathbb{F}(\alpha) \simeq \mathbb{F}[x]/(f)$.*

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

$$\begin{array}{rccc} \varphi_\alpha : & \mathbb{F}[x] & \longrightarrow & \mathbb{F}(\alpha) \subset \mathbb{K} \\ & p(x) & \longmapsto & p(\alpha). \end{array}$$

Com que $\varphi_\alpha(f) = f(\alpha) = 0$ tenim que $(f) \subset \ker(\varphi_\alpha)$. Per tant, φ_α indueix un morfisme $\tilde{\varphi_\alpha} : \mathbb{F}[x]/(f) \longrightarrow \mathbb{F}(\alpha)$. Com que f és irreductible, $\mathbb{F}[x]/(f)$ és un cos i, per tant, $\mathrm{im}(\tilde{\varphi_\alpha})$ és un subcòs de $\mathbb{F}(\alpha)$ que conté $\mathbb{F}$ i conté α i, per tant, conté $\mathbb{F}(\alpha)$. Això prova que $\tilde{\varphi_\alpha}$ és exhaustiu i com que tots els morfismes de cossos són injectius, veiem doncs que és un isomorfisme. ■

Observació 1.2.22. En la situació de la proposició anterior, per 1.2.10 veiem que

$$\mathbb{F}(\alpha) = \left\{ a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \;\middle|\; a_i \in \mathbb{F} \right\},$$

on $n = \mathrm{gr}(f)$. En particular en aquest cas tenim que $\mathbb{F}[\alpha] = \mathbb{F}(\alpha)$.

Exemple 1.2.23.

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 $\sqrt{5}$ l'arrel quadrada positiva de 5 a $\mathbb{R}$. Aleshores, $\mathbb{Q}(\sqrt{5}) = \{a + b\sqrt{5} \mid a, b \in \mathbb{Q}\}$. Fixem-nos amb la diferència conceptual amb 1.2.11, apartat *2.*. Allà hem construït un cos on f té una arrel, mentre que aquí partíem d'un cos que ja tenim (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 1.2.21 ens diu que els cossos obtinguts en les dues construccions són isomorfs.
2. $f(x) = x^3 - 2 \in \mathbb{Q}[x]$. Posem $\sqrt[3]{2}$ l'arrel cúbica de 2 a $\mathbb{R}$. Aleshores

$$\mathbb{Q}(\sqrt[3]{2}) = \left\{ a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2 \;\middle|\; a, b, c \in \mathbb{Q} \right\} \simeq \frac{\mathbb{Q}[x]}{(x^3 - 2)}.$$

   Sabem que f té dues altres arrels a $\mathbb{C}$: $e^{\frac{2\pi}{3}}\sqrt[3]{2}$ i $e^{\frac{4\pi i}{3}}\sqrt[3]{2}$. Podem doncs considerar també per exemple el cos $\mathbb{Q}\left(e^{\frac{2\pi}{3}}\sqrt[3]{2}\right)$. Aquest cos és certament diferent de $\mathbb{Q}(\sqrt[3]{2})$ (tenen la mateixa estructura algebraica, però 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. *Tenint un isomorfisme φ entre dos cossos $\mathbb{F}$ i $\mathbb{F}'$, podem estendre'l a un isomorfisme φ' de $F(\alpha)$ a $\mathbb{F}(\alpha')$, α, α' essent les arrels de f i f', respectivament.*

Proposició 1.2.24. *Sigui $\varphi : \mathbb{F} \longrightarrow \mathbb{F}'$ un isomorfisme de cossos i sigui $f(x) \in \mathbb{F}[x]$ irreductible. Posem $f'(x) \in \mathbb{F}'[x]$ el polinomi que obtenim aplicant φ als coeficients de f. Sigui α una arrel de f en una extensió de $\mathbb{F}$, i sigui α' alguna arrel de f' en una extensió de $\mathbb{F}'$. Aleshores existeix un isomorfisme $\tilde{\varphi} : \mathbb{F}(\alpha) \xrightarrow{\cong} \mathbb{F}'(\alpha')$ tal que $\tilde{\varphi}(\alpha) = \alpha'$ i que estén φ (és a dir, $\tilde{\varphi}_{|\mathbb{F}} = \varphi$).*

Demostració. Si apliquem φ als coeficients de f ens queda:

$$\varphi(f(x)) = \varphi(a_0) + \varphi(a_1)x + \cdots + \varphi(a_n)x^n = b_0 + b_1 x + \cdots + b_n x^n \equiv f'(x).$$

El morfisme φ indueix un isomorfisme d'anells $\varphi : \mathbb{F}[x] \longrightarrow \mathbb{F}'[x]$ tal que $\varphi((f)) = (f')$. Passant al quocient tenim un isomorfisme $\mathbb{F}[x]/(f) \longrightarrow \mathbb{F}'[x]/(f')$. Per 1.2.21 el cos de l'esquerra és isomorf a $\mathbb{F}(\alpha)$ i el de la dreta a $\mathbb{F}'(\alpha')$. Composant els isomorfismes, obtenim $\tilde{\varphi}$. ■

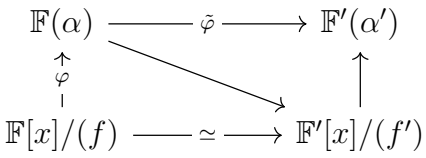


Figura 1.3: Diagrama de 1.2.24.

Observació 1.2.25 ($\sigma(\alpha)$ és arrel). Sigui f un polinomi irreductible i sigui α una arrel de f en una extensió. Considerem l'extensió $\mathbb{F}(\alpha)/\mathbb{F}$. Fixem-nos que si $\sigma \in \mathrm{Aut}(\mathbb{F}(\alpha)/\mathbb{F})$, aleshores $\sigma(\alpha)$ és necessàriament una arrel de f ja que:

$$\begin{aligned} f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n, a_i \in \mathbb{F}, \\ \sigma(f(\alpha)) = 0 \iff \sigma(a_0) + \sigma(a_1)\sigma(\alpha) + \sigma(a_2)\sigma(\alpha)^2 + \cdots + \sigma(a_n)\sigma(\alpha)^n = 0, \\ a_i \in \mathbb{F},\ \sigma(a_i) = a_i \implies a_0 + a_1\sigma(\alpha) + a_2\sigma(\alpha)^2 + \cdots + a_n\sigma(\alpha)^n = 0, \\ f(\sigma(\alpha)) = \sigma(f(\alpha)) = \sigma(0) = 0. \end{aligned}$$

Per tant, si f no té cap altra arrel a $\mathbb{F}(\alpha)$ a part de α, l'únic $\mathbb{F}$-automorfisme de $\mathbb{F}(\alpha)$ és la identitat i per tant $\mathrm{Aut}(\mathbb{F}(\alpha)/\mathbb{F}) = \{1\}$ és el grup trivial.

Proposició 1.2.26. *per a cada arrel β de f en $\mathbb{F}(\alpha)$ existeix un $\sigma \in \mathrm{Aut}(\mathbb{F}(\alpha)/\mathbb{F})$ tal que $\sigma(\alpha) = \beta$.*

Demostració. És conseqüència de 1.2.24.

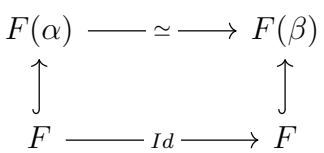


Figura 1.4: Explicació de 1.2.26.

La proposició, de fet, ens diu que hi ha un $\mathbb{F}$-morfisme $\sigma : \mathbb{F}(\alpha) \longrightarrow \mathbb{F}(\beta)$, fixem-nos que si $\beta \in \mathbb{F}(\alpha)$ aleshores $\mathbb{F}(\beta) \subset \mathbb{F}(\alpha)$ i, com que per la preposició 1.2.21 tenen la mateixa dimensió[8], tenim que $\mathbb{F}(\alpha) = \mathbb{F}(\beta)$. ■

1.3 Extensions algebraiques

Definició 1.3.1 (Element algebraic). Sigui $\mathbb{K}/\mathbb{F}$ una extensió. Un element $\alpha \in \mathbb{K} \setminus \mathbb{F}$ és algebraic sobre $\mathbb{F}$ si és arrel d'algun polinomi no nul de $\mathbb{F}[x]$, i és trascendent sobre $\mathbb{F}$ en cas contrari. L'extensió $\mathbb{K}/\mathbb{F}$ és algebraica si tot element de $\mathbb{K}$ és algebraic sobre $\mathbb{F}$, i és trascendent en cas contrari (i.e., si existeix algun element de $\mathbb{K}$ trascendent sobre $\mathbb{F}$).

Observació 1.3.2 (Transcendent i algebraic, [Tra23]). Siguin $k \subset \mathbb{K}$ cossos qualssevol i $\theta \in \mathbb{K}$ un element qualsevol de $\mathbb{K}$. Podem avaluar tots els polinomis de $k[X]$ en θ; és a dir, podem considerar l'aplicació $\psi_\theta : k[X] \longrightarrow K$ definida per $\psi_\theta(f(X)) = f(\theta)$, per a tot polinomi $f(X) \in k[X]$. Aquesta aplicació és un morfisme d'anells i, de fet, l'únic tal que $\psi_\theta(X) = \theta$ i $\psi_\theta(a) = a$ per a tot $a \in k$. $k[\theta] = \mathrm{im}(\psi_\theta)$ és el menor subanell de K que conté k i θ, o sigui, del subanell de K *generat per* k *i* θ. $\ker(\psi_\theta)$ és el conjunt de tots els polinomis $f(X) \in k[X]$ tals que $f(\theta) = 0$.

1. En particular, ψ_θ és injectiu si, i només si, θ no és arrel de cap polinomi no nul de $k[X]$; és a dir, si θ és transcendent sobre k. En aquest cas, tenim un isomorfisme $k[X]/\ker(\psi_\theta) = k[X] \simeq k[\theta]$: $k(\theta)$ és isomorf al cos de fraccions de l'anell de polinomis en una indeterminada sobre k.
2. En cas contrari, és a dir, si θ és algebraic sobre k, $\ker(\psi_\theta)$ és un ideal no nul de $k[X]$; com que $k[X]$ és un domini d'ideals principals[9]. Si $f(X)$ és un generador qualsevol de $\ker(\psi_\theta)$, obtenim que $k[X]/(f(X)) \simeq k[\theta] \subset K$. A més, com que K és un cos, $k[\theta]$ és un domini d'integritat, de manera que $(f(X))$ és un ideal primer no nul i el polinomi $f(X)$ és irreductible; així, l'ideal principal $(f(X))$ és maximal i $k[\theta]$ és un subcòs de K. Doncs, $k[\theta] = k(\theta)$.

Exemple 1.3.3.

1. $\sqrt{5}$ és algebraic sobre $\mathbb{Q}$, ja que $\sqrt{5} \neq \mathbb{Q}$ 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^2-2 a $x+a^2-5b^2 \in \mathbb{Q}[x]$.
2. A $\mathbb{Q}(x)$ l'element x és trascendent sobre $\mathbb{Q}$.
3. Els nombres reals π i e són trascendents 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 π^e és trascendent, però en canvi no se sap si e^π ho és (i tampoc si $e\pi$ o $e+\pi$ ho són).

[8] Tenim $[F(\beta) : F] = \mathrm{gr}(f)$ i $[F(\alpha) : F] = \mathrm{gr}(f)$.
[9] Com k és un cos, vam veure a *Estructures Algebraiques* que, en particular, $k[X]$ seria un domini d'ideals principals.

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 trascendents sobre $\mathbb{Q}$ (però demostrar que un nombre concret és trascendent sol ser complicat).

Observació 1.3.4. Si $\mathbb{L}/\mathbb{K}/\mathbb{F}$ és una torre d'extensions i $\alpha \in \mathbb{L}$ és algebraic sobre $\mathbb{F}$ aleshores també ho és sobre $\mathbb{K}$, ja que α és arrel d'un polinomi amb coeficients a $\mathbb{F}$ i en particular a $\mathbb{K}$.

Proposició 1.3.5. *Si $\mathbb{K}/\mathbb{F}$ és finita aleshores és algebraica.*

Demostració. Posem $n = [\mathbb{K} : \mathbb{F}]$ i prenem un element $\alpha \in \mathbb{K}\backslash\mathbb{F}$. 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 $a_i \in \mathbb{F}$ no tots nuls tals que $a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0$. Aleshores α és arrel del polinomi $a_0 + a_1x + \cdots + a_nx^n \in \mathbb{F}[x]$; és arrel d'un polinomi en $\mathbb{F}[x]$ i, per tant, $\mathbb{K}/\mathbb{F}$ és algebraica. ■

Proposició 1.3.6. *Si $\alpha \in \mathbb{K}$ és algebraic sobre $\mathbb{F}$ aleshores existeix un únic polinomi mònic $\mathrm{Irr}(\alpha, \mathbb{F})(x) \in \mathbb{F}[x]$ que és irreductible i té α com a arrel. S'anomena el polinomi irreductible de α sobre $\mathbb{F}$ i té la propietat que si $f \in \mathbb{F}[x]$ és tal que $f(\alpha) = 0$ aleshores $\mathrm{Irr}(\alpha, \mathbb{F}) \mid f$. També és el polinomi mònic de grau més petit que té α com a arrel.*

Demostració. Sigui $\varphi_\alpha : \mathbb{F}[x] \longrightarrow \mathbb{K}$ 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 $\mathbb{K}$ i, en particular, un domini d'integritat. Com que pel primer teorema d'isomorfia d'anells $\mathbb{F}[x]/\ker(\varphi_\alpha) \simeq \mathrm{im}\,(\varphi_\alpha)$ veiem que $\ker(\varphi_\alpha)$ és un ideal primer de $\mathbb{F}[x]$, que a més és no nul ja que α és algebraic. L'anell $\mathbb{F}[x]$ és un domini d'ideals principals (i, en particular, un domini de factorització única[10]) i per tant els elements primers no nuls són irreductibles. Així doncs, $\ker(\varphi_\alpha)$ és un ideal maximal i, en particular, un ideal principal generat per un polinomi irreductible; definim doncs $\mathrm{Irr}(\alpha, \mathbb{F})(x)$ com el generador mònic de $\ker(\varphi_\alpha)$, que és clar que satisfà les propietats de l'enunciat. ■

Definició 1.3.7 (Grau d'α). Si α és algebraic sobre $\mathbb{F}$, definim el seu grau sobre $\mathbb{F}$ com el grau del polinomi $\mathrm{Irr}(\alpha, \mathbb{F})(x)$.

Observació 1.3.8. Si α és algebraic sobre $\mathbb{F}$ aleshores per la proposició 1.2.21 tenim:

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

En particular, $[\mathbb{F}(\alpha) : \mathbb{F}] = \mathrm{gr}(\alpha) = \mathrm{gr}(\mathrm{Irr}(\alpha, F))$. *Aquest resultat l'utilitzem en força problemes.*

Exemple 1.3.9. Considerem l'extensió $\mathbb{Q}(\sqrt[6]{2})/\mathbb{Q}$. Tenim que $\mathrm{Irr}(\sqrt[6]{2}, \mathbb{Q})(x) = x^6 - 2$, ja que aquest és un polinomi mònic irreductible que té $\sqrt[6]{2}$ com a arrel. El grau és $[\mathbb{Q}(\sqrt[6]{2} : \mathbb{Q}] = 6$. Observem que $(\sqrt[6]{2})^3 = \sqrt{2}$, $\mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[6]{2})$ i, en particular: Però què passa amb $\mathrm{Irr}(\sqrt[6]{2}, \mathbb{Q}(\sqrt{2}))$?

[10] En un DFU, tots els ideals primers diferents del trivial, (0), són ideals maximals.

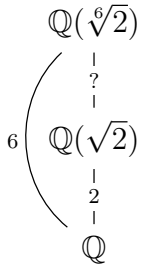


Figura 1.5: Diagrama en qüestió.

L'interrogant $[\mathbb{Q}(\sqrt[6]{2} : \mathbb{Q}(\sqrt{2})]$ serà 3 si, i només si, $x^3 - \sqrt{2} \in \mathbb{Q}(\sqrt{2})[X]$ té $\sqrt[6]{2}$ com a arrel.

Exemple 1.3.10. Considerem l'extensió $\mathbb{Q}(\sqrt[8]{3})/\mathbb{Q}$. Tenim que $\mathrm{Irr}(\sqrt[8]{3}, \mathbb{Q})(x) = x^8 - 3$ (és 3-Eisenstein), 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: $\mathbb{Q} \subset \mathbb{Q}(\sqrt{3}) \subset \mathbb{Q}(\sqrt[8]{3})$. Sovint es posa en forma de diagrama: On els nombres indiquen el grau d'extensió. Acabem de veure que $[\mathbb{Q}(\sqrt[8]{3}) : \mathbb{Q}] = 8$ i és fàcil

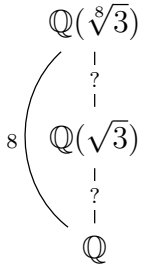


Figura 1.6: Diagrama en qüestió.

veure que $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$. El grau $[\mathbb{Q}(\sqrt[8]{3}) : \mathbb{Q}(\sqrt{3})] \leq 4$ 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 1.3.11 (Multiplicativitat dels graus)**.** *Siguin $\mathbb{F} \subset \mathbb{K} \subset \mathbb{L}$ cossos. Aleshores, $[\mathbb{L} : \mathbb{F}] = [\mathbb{L} : \mathbb{K}][\mathbb{K} : \mathbb{F}]$, on la igualtat val també en el cas en què algun dels termes és infinit.*

Demostració. Farem la demostració en cas que tots els graus involucrats siguin finits (cf. 1.3.12). Posem, doncs, $[\mathbb{L} : \mathbb{K}] = m$ i $[\mathbb{K} : \mathbb{F}] = n$. Sigui $\{\alpha_i\}_{i=1,\dots,m}$ una $\mathbb{K}$-base de $\mathbb{L}$ i $\{\beta_j\}_{j=1,\dots,n}$ una $\mathbb{F}$-base de $\mathbb{K}$. Aleshores, afirmem que $\{\alpha_i\beta_j \mid 1 \leq i \leq m, 1 \leq j \leq n\}$ és una $\mathbb{F}$-base de $\mathbb{L}$. Si veiem això ja hem acabat perquè, aleshores, $[\mathbb{L} : \mathbb{F}] = [\mathbb{L} : \mathbb{K}][\mathbb{K} : \mathbb{F}]$. Per a veure que són un sistema de generadors, prenem $\alpha \in \mathbb{L}$. Aleshores $\alpha = \sum a_i\alpha_i$ per a certs $a_i \in \mathbb{K}$. Ara cada a_i el podem escriure com $a_i = \sum b_{ij}\beta_j$ per a certs $b_{ij} \in \mathbb{F}$. Per tant, $\alpha = \sum_{i,j} b_{ij}\beta_j$. Per a veure que

són linealment independents, suposem que existeixi alguna combinació lineal:

$$\alpha = \sum_{i=1}^{m} \left(\sum_{j=1}^{n} b_{ij}\beta_j \right) \alpha_i = \sum_{i=1}^{m} \sum_{j=1}^{n} b_{ij}\alpha_i\beta_j = 0,\ b_{ij} \in \mathbb{F}.$$

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

Observació 1.3.12 (Casos infinits, 1.3.11)**.**

1. Si $[\mathbb{K} : \mathbb{F}] = \infty$ aleshores tota base de $\mathbb{K}/\mathbb{F}$ és una subcol·lecció infinita de $L/\mathbb{F}$ i linealment independent, de manera que $[\mathbb{L} : \mathbb{F}] = \infty$, també.
2. Anàlogament, si $[\mathbb{L} : \mathbb{K}] = \infty$ aleshores tota base de $\mathbb{L}/\mathbb{K}$ és un $\mathbb{K}$-linealment independent subconjunt infinit, el qual és clarament $\mathbb{F}$-linealment independent. Per tant, $[\mathbb{L} : \mathbb{F}] = \infty$ un altre cop.
3. Finalment, si $[\mathbb{L} : \mathbb{F}] = \infty$, aleshores com a mínim un dels dos factors $[\mathbb{L} : \mathbb{K}]$ o bé $[\mathbb{K} : \mathbb{F}]$ és infinit, ja que hem demostrat el cas en què tots dos són finits ens dona que $[\mathbb{L} : \mathbb{F}] < \infty$.

Corol·lari 1.3.13. *Si* $\mathbb{F} \subseteq \mathbb{K} \subseteq \mathbb{L}$ *aleshores* $[\mathbb{L} : \mathbb{K}] | [\mathbb{L} : \mathbb{F}]$ *i* $[\mathbb{K} : \mathbb{F}] | [\mathbb{L} : \mathbb{F}]$.

Demostració. Evident, per la igualtat de la multiplicativitat dels graus, $[\mathbb{L} : \mathbb{F}] = [\mathbb{L} : \mathbb{K}][\mathbb{K} : \mathbb{F}]$. ■

Observació 1.3.14. Recordem que $\mathbb{K}/\mathbb{F}$ és finitament generada si $\mathbb{K} = \mathbb{F}(\alpha_1, \ldots, \alpha_n)$ per a certs $\alpha_i \in \mathbb{K}$.

Lema 1.3.15. $\mathbb{F}(\alpha, \beta) = \mathbb{F}(\alpha)(\beta)$.

Demostració. Com que $\alpha, \beta \in \mathbb{F}(\alpha)(\beta)$ tenim que $\mathbb{F}(\alpha, \beta) \subseteq \mathbb{F}(\alpha)(\beta)$. D'altra banda $\mathbb{F}(\alpha) \subseteq \mathbb{F}(\alpha, \beta)$ i $\beta \in \mathbb{F}(\alpha, \beta)$, per tant $\mathbb{F}(\alpha)(\beta) \subseteq \mathbb{F}(\alpha, \beta)$. Provades ambdues inclusions, tenim la igualtat. ■

Observació 1.3.16. Això prova que tota extensió finitament generada $\mathbb{F}(\alpha_1, \ldots, \alpha_n)$ s'obté com una torre d'extensions:

$$\mathbb{F} \subseteq \mathbb{F}(\alpha_1) \subseteq \mathbb{F}(\alpha_1, \alpha_2) \subseteq \cdots \subseteq \mathbb{F}(\alpha_1, \ldots, \alpha_n).$$

en què cada cos és una extensió simple de l'anterior. *A cada extensió adjuntem un element.* Per exemple, si a $\mathbb{F}(\alpha_1)$ li adjuntem α_2 tindrem $\mathbb{F}(\alpha_1)(\alpha_2)$ i acabem de veure que això és igual a $\mathbb{F}(\alpha_1, \alpha_2)$.

Proposició 1.3.17. $\mathbb{K}/\mathbb{F}$ *és finita si, i només si, és algebraica i finitament generada.*

Demostració.

$\Rightarrow$ Suposem que $\mathbb{K}/\mathbb{F}$ és finita. Per 1.3.5 és algebraica. Si $\alpha_1, \ldots, \alpha_n$ és una $\mathbb{F}$-base de $\mathbb{K}$, aleshores $\mathbb{K} = \mathbb{F}(\alpha_1, \ldots, \alpha_n)$ així que també és finitament generada. Si $\alpha \in \mathbb{K} \setminus \mathbb{F}$:

$$1, \alpha, \alpha^2, \ldots, \alpha^n \in \mathbb{K} \text{ són linealment independents i n'hi ha } n+1.$$

A més, existeixen $a_i \in \mathbb{F}$ tals que $a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0$ i $\alpha \in \mathbb{K}\setminus$ és arrel d'un polinomi; en particular, $a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{F}[x]$, i l'extensió és algebraica.

$\Leftarrow$ Suposem ara que $\mathbb{K}/\mathbb{F}$ és algebraica, $\mathbb{F}(\alpha_1, \ldots, \alpha_n)$ amb α_i algebraics sobre $\mathbb{F}$, i finitament generada i volem veure que $\mathbb{F}(\alpha)/\mathbb{F}$ és finita. Per les observacions 1.3.4 i 1.3.16 tenim una torre d'extensions:

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

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 1.3.8 tenim que $[F_{i+1} : F_i] = \mathrm{gr}(\alpha_i)$[11]. Per 1.3.13 tenim que

$$[\mathbb{K} : \mathbb{F}] = [F_n : F_{n-1}][F_{n-1} : F_{n-2}] \ldots [F_1 : F_0] < \infty. \qquad \blacksquare$$

Observació 1.3.18. De fet, a la demostració hem vist que si $\alpha_1, \ldots, \alpha_n$ són algebraics sobre $\mathbb{F}$ aleshores $\mathbb{F}(\alpha_1, \ldots, \alpha_n)/\mathbb{F}$ és finita.

Proposició 1.3.19. *Si α i β són algebraics sobre $\mathbb{F}$ aleshores $\alpha+\beta, \alpha-\beta, \alpha\beta$ i α/β (si $\beta \neq 0$) són algebraics.*

Demostració. Tots aquests elements pertanyen a $\mathbb{F}(\alpha, \beta)$ que és una extensió finita de $\mathbb{F}$ i per tant algebraica i finitament generada (el conjunt de generadors són algebraics, i les seves combinacions lineals també). $\blacksquare$

Corol·lari 1.3.20. *Si $\mathbb{K}/\mathbb{F}$ és una extensió i denotem per E el conjunt d'elements de $\mathbb{K}$ que són algebraics sobre $\mathbb{F}$, aleshores E és un cos.*

Exemple 1.3.21. 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 1.3.22. *Si tenim una torre d'extensions $\mathbb{L}/\mathbb{K}/\mathbb{F}$, aleshores $\mathbb{L}/\mathbb{F}$ és algebraica si i només si $\mathbb{L}/\mathbb{K}$ i $\mathbb{K}/\mathbb{F}$ ho són.*

Demostració. Si $\mathbb{L}/\mathbb{F}$ és algebraica aleshores $\mathbb{L}/\mathbb{K}$ i $\mathbb{K}/\mathbb{F}$ també són algebraiques. Veiem la implicació contrària. Sigui $\alpha \in \mathbb{L}$ i sigui $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{K}[x]$ un polinomi tal que $f(\alpha) = 0$. Considerem el cos generat pels coeficients de f, $E = \mathbb{F}(a_0, \ldots, a_n)$. 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 $\mathbb{F}$ (ja que $\mathbb{K}/\mathbb{F}$ és algebraica) tenim que $E/\mathbb{F}$ és finita. Així doncs, $E(\alpha)/\mathbb{F}$ és finita i, en particular algebraica; per tant, α és algebraic sobre $\mathbb{F}$. $\blacksquare$

[11] Se sobreentèn que és notació per referir-se a $\mathrm{gr}(\mathrm{Irr}(\alpha_i, F_i)(X))$; el grau de l'arrel és el mateix que el de l'extensió que genera.

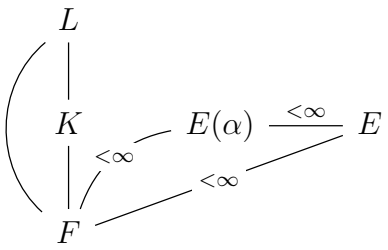


Figura 1.7: Ajuda visual a la demostració.

Proposició 1.3.23. *Si $\mathbb{K}/\mathbb{F}$ és algebraica, tot $\mathbb{F}$-morfisme $\sigma : \mathbb{K} \longrightarrow \mathbb{K}$ és un $\mathbb{F}$-automorfisme.*

Demostració. Sabem que σ és injectiva per ser morfisme de cossos. Si $\mathbb{K}/\mathbb{F}$ és finita amb $[\mathbb{K} : \mathbb{F}] = n$, aleshores σ és una aplicació lineal injectiva entre dos $\mathbb{F}$-espais vectorials de dimensió n i, per tant, és també exhaustiva (*és un resultat d'Àlgebra Lineal*). Si $\mathbb{K}/\mathbb{F}$ és infinita, donat $\alpha \in \mathbb{K}$ posem $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_r$ les arrels a $\mathbb{K}$ de $f = \mathrm{Irr}(\alpha, \mathbb{F})$. Fixem-nos que σ envia arrels de f a arrels de f (cf. 1.2.25), ja que $f(\sigma(\alpha_i)) = \sigma(f(\alpha_i)) = \sigma(0) = 0$. Per tant, si posem $\mathbb{K}' = \mathbb{F}(\alpha_1, \ldots, \alpha_r)$ tenim que $\sigma(\mathbb{K}') \subset \mathbb{K}'$. Ara, $\mathbb{K}'$ és finitament generada (ja que el nombre d'arrels que hem agafat és finit) i algebraica (ja que el conjunt de generadors és, en efecte, algebraic); per tant, és finita i $\sigma|_{\mathbb{K}'} : \mathbb{K}' \longrightarrow \mathbb{K}'$ és exhaustiva pel cas d'extensions finites. Com que $\sigma|_{\mathbb{K}'}$ és exhaustiu, α pertany a la imatge de $\sigma|_{\mathbb{K}'}$ (pel que pertany a $\mathrm{im}(\sigma)$ també) i veiem que σ és exhaustiva. ■

1.3.1 Composició de cossos

Definició 1.3.24 (Composició de cossos)**.** Sigui $\mathbb{K}$ un cos i siguin $\mathbb{L}_1/\mathbb{K}$ i $\mathbb{L}_2/\mathbb{K}$ extensions de $\mathbb{K}$ contingudes en un cos $\overline{\mathbb{K}}$. La composició de $\mathbb{L}_1$ i $\mathbb{L}_2$, denotada $\mathbb{L}_1\mathbb{L}_2$, és el subcòs de $\overline{\mathbb{K}}$ més petit que conté $\mathbb{L}_1$ i $\mathbb{L}_2$.

Exemple 1.3.25. Sigui $f(x) = x^2 - 2 \in \mathbb{Q}[x]$ descomposa com $f(x) = (x - \sqrt{2})(x + \sqrt{2})$ de manera que $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2})$. Adonem-nos que $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, de manera que no pot existir $\mathbb{Q} \subsetneq \mathbb{F} \subsetneq \mathbb{Q}(\sqrt{2})$, ja que $[\mathbb{F} : \mathbb{Q}] \mid 2$: si és 2, $\mathbb{F} = \mathbb{Q}(\sqrt{2})$; en canvi, si el grau és 1, $\mathbb{F} = \mathbb{Q}$.

Proposició 1.3.26. *L_1L_2 és la intersecció de tots els cossos $\mathbb{L}$ tals que $\mathbb{L} \subseteq \overline{\mathbb{K}}$ i $\mathbb{L}_1 \subseteq \mathbb{L}, \mathbb{L}_2 \subseteq \mathbb{L}$.*

Demostració. És directe utilitzant el fet que la intersecció de dos cossos que contenen $\mathbb{L}_1$ i $\mathbb{L}_2$ és un cos que conté $\mathbb{L}_1$ i $\mathbb{L}_2$. ■

Exemple 1.3.27. $\mathbb{Q}(\sqrt{2})\mathbb{Q}(\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. La prova és senzilla: per una banda $\sqrt{2}, \sqrt{3} \in \mathbb{Q}(\sqrt{2})\mathbb{Q}(\sqrt{3})$ i, per tant, $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2})\mathbb{Q}(\sqrt{3})$; d'altra banda, $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ 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 1.3.28. *Si $[L_1 : \mathbb{K}] < \infty$ i $[L_2 : \mathbb{K}] < \infty$ aleshores $[L_1L_2 : \mathbb{K}] \leq [L_1 : \mathbb{K}]\,[L_2 : \mathbb{K}]$.*

Hem vist que per $f \in \mathbb{F}[x]$ no constant existeix una extensió $\mathbb{K}$ de $\mathbb{F}$ que conté una arrel de f. Ara veurem que, de fet, existeix una extensió que conté totes les arrels de f.

Definició 1.3.29 (Cos de descomposició)**.** Una extensió $\mathbb{K}$ de $\mathbb{F}$ es diu que és un cos de descomposició d'un polinomi $f \in \mathbb{F}[x]$ no constant si f descompon completament (com a producte de factors de grau 1) a $\mathbb{K}$, i no ho fa en cap subextensió (subcòs) de $\mathbb{K}$. Com a conseqüència immediata, totes les arrels estan a $\mathbb{K}$[12]. De manera anàloga es defineix un cos de descomposició d'un conjunt de polinomis.

Proposició 1.3.30. *Sigui $\mathbb{F}$ un cos i $f \in \mathbb{F}[x]$ no constant. Existeix una extensió $\mathbb{K}$ de $\mathbb{F}$ on f descompon completament.*

Demostració. Farem inducció sobre $n = \operatorname{gr}(f)$. Si $n = 1$ és evident, suposem l'enunciat cert per a n i vegem-ho per a $n+1$. Sigui $\mathbb{K}_1/\mathbb{F}$ un cos on f té una arrel α (que sabem que existeix per 1.2.8). Aleshores $f(x) = (x-\alpha)g(x)$ amb $g \in \mathbb{K}_1[x]$ i $\operatorname{gr}(g) < n$[13]. Per hipòtesi d'inducció, existeix una extensió $\mathbb{K}/\mathbb{K}_1$ on g descompon completament (g hi té totes les arrels), i per tant f també descompon completament a $\mathbb{K}$. ■

Proposició 1.3.31. *Donat $f \in \mathbb{F}[x]$ no constant existeix un cos de descomposició de f.*

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

Exemple 1.3.32. $f(x) = x^4 - 2 \in \mathbb{Q}[x]$. Les arrels de f a $\mathbb{C}$ són $\sqrt[4]{2}$, $-\sqrt[4]{2}$, $i\sqrt[4]{2}$ i $-i\sqrt[4]{2}$. Per tant, un cos de descomposició de f és $\mathbb{Q}(\sqrt[4]{2}, i\sqrt[4]{2})$.

Exemple 1.3.33. $f(x) = x^n - 1 \in \mathbb{Q}[x]$. 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 1.3.34. $f(x) = x^p - 2 \in \mathbb{Q}[x]$ on p és primer; les arrels són $\sqrt[p]{2} \cdot \zeta_p^k$ amb $0 \leq k \leq p-1$. Un cos de descomposició és, doncs, $\mathbb{K} = \mathbb{Q}(\zeta_p, \sqrt[p]{2})$. Sabem alguns subcossos de $\mathbb{K}$:

[12] Però no és condició suficient, ja que a més demanem que aquestes arrels no estiguin repetides (i.e. l'extensió sigui separable, ho veurem més endavant).

[13] És una *reescriptura* que s'utilitza molt. Imaginem $f(x) = x^2 - 2$; en $\mathbb{Q}[x]$ és irreductible per ser 2-Eisenstein, però en $\mathbb{R}[x]$ es pot factoritzar com $(x-\sqrt{2})(x+\sqrt{2})$, ja que $\alpha = \sqrt{2} \in \mathbb{R}$, $x + \sqrt{2} \in \mathbb{Q}(\sqrt{2})[x]$.

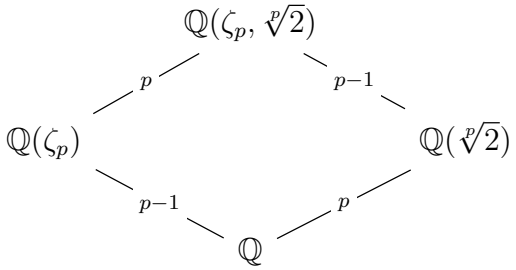


Figura 1.8: Diagrama de cossos, 1.3.34.

Els graus es justifiquen de la manera següent: $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$ ja que ζ_p és arrel de $\mathrm{Irr}(\zeta_p, \mathbb{Q}) = x^{p-1} + \cdots + x + 1$, i $\mathrm{Irr}(\sqrt[p]{2}, \mathbb{Q}) = x^p - 2$. Per tant, $[\mathbb{K} : \mathbb{Q}]$ és divisible per p i $p-1$, i com són coprimers de fet és divisible per $p(p-1)$. Ara bé, $\mathbb{K} = \mathbb{Q}(\sqrt[p]{2}) \cdot \mathbb{Q}(\zeta_p)$ (composició de subcossos) i, per tant, $[\mathbb{K} : \mathbb{Q}] \leq [\mathbb{Q}(\sqrt[p]{2}) : \mathbb{Q}][\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p(p-1)$. Això prova que $[\mathbb{K} : \mathbb{Q}] = p(p-1)$ 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.

Observació 1.3.35. En efecte, ζ_p és arrel de $f_p(x) = \frac{x^p-1}{x-1} = x^{p-1} + \cdots + x + 1$; aquest polinomi és el ciclotòmic de grau p primer; per tant, és irreductible perquè ho és

$$f_p(x+1) = x^{p-1} + \sum_{i=1}^{p-2} \binom{p}{i} x^i + p,$$

ja que és p-Eisenstein. A *Problemes* hem vist (o veurem) que $P(x)$ irreductible si, i només si, $P(x+a)$ irreductible.

Observació 1.3.36. Fixem-nos que de la demostració de les dues proposicions anteriors, 1.3.30 i 1.3.31, es dedueix que si $\mathbb{K}$ és un cos de descomposició de f sobre $\mathbb{F}$, aleshores $[\mathbb{K} : \mathbb{F}] \leq n!$, on $n = \mathrm{gr}(f)$. Si tenim igualtat, $[\mathbb{K} : \mathbb{F}] = n!$, f és irreductible.

Demostració. Suposem que f no és irreductible, diguem $f = gh$ per a certs polinomis $g, h \in \mathbb{F}[x]$ de graus ≥ 1. El conjunt d'arrels de f és la unió de les arrels de g i les arrels de h, de manera que $\mathbb{K}_f = \mathbb{K}_g \cdot \mathbb{K}_h$, on $\mathbb{K}_g$ i $\mathbb{K}_h$ denoten els cossos de descomposició de g i h, respectivament. Si posem $a = \mathrm{gr}\, g$ i $b = \mathrm{gr}\, h$ aleshores $[K_g : F] \leq a!$ i $[K_h : F] \leq b!$, de manera que $[K_f : F] \leq [K_g : F][K_h : F] \leq a!b!$. Ara bé, d'una banda tenim que

$$a!b! = (1 \cdot 2 \cdot 3 \cdots a) \cdot (1 \cdot 2 \cdot 3 \cdots b)$$

i de l'altra

$$(a+b)! = (1 \cdot 2 \cdot 3 \cdots a) \cdot ((a+1) \cdot (a+2) \cdot (a+2) \cdots (a+b)),$$

i com que $a \geq 1$ i $b \geq 1$ veiem que $a!b! < (a+b)!$. Com que $a + b = \mathrm{gr}\, f = n$, hem arribat a què $[\mathbb{K}_f : F] < n!$, que és una contradicció. ■

Proposició 1.3.37. *Sigui $\varphi : \mathbb{F} \longrightarrow \mathbb{F}'$ un isomorfisme de cossos, sigui $f \in \mathbb{F}[x]$ i $f' \in \mathbb{F}'[x]$ el polinomi obtingut aplicant φ a f. Sigui $\mathbb{K}$ un cos de descomposició de f i $\mathbb{K}'$ un de f'. Aleshores, existeix un isomorfisme $\tilde{\varphi} : \mathbb{K} \longrightarrow \mathbb{K}'$ tal que $\tilde{\varphi}|_F = \varphi$.*

Demostració. Inducció sobre $n = \mathrm{gr}(f)$. Si $n = 1$ aleshores $\mathbb{K} = \mathbb{F}$ i $\mathbb{K}' = \mathbb{F}'$ i l'enunciat és trivial. Suposem l'enunciat cert per a polinomis de grau $n-1$ i provem-ho per un f de grau n. Si tots els factors irreductibles de f tenen grau 1, aleshores $\mathbb{K} = \mathbb{F}$ i $\mathbb{K}' = \mathbb{F}'$ i l'enunciat és cert; podem suposar, doncs, que f té algun factor irreductible g de grau més gran o igual que 2. Denotem $g' = \varphi(g)$, sigui $\alpha \in \mathbb{K}$ una arrel de g i $\alpha' \in \mathbb{K}'$ una arrel de g' (que, en particular, és arrel també de f'). Per 1.2.24 sabem que existeix un isomorfisme:

$$\varphi' : \mathbb{F}(\alpha) \longrightarrow \mathbb{F}'(\alpha'), \text{ tal que } \varphi'|_F = \varphi \text{ i } \varphi'(\alpha) = \alpha'.$$

Tenim, doncs, descomposicions:

$$f(x) = (x - \alpha)f_1(x) \text{ i } f'(x) = (x - \alpha')f_1'(x),$$

amb $f_1 \in \mathbb{F}(\alpha)[x]$ i $f_1' \in \mathbb{F}'(\alpha')[x]$ 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 $\mathbb{K}/\mathbb{F}(\alpha)$ i $\mathbb{K}'/\mathbb{F}'(\alpha')$. Clarament, $\mathbb{K}$ és un cos de descomposició de $f_1(x)$ sobre $\mathbb{F}(\alpha)$ i $\mathbb{K}'$ ho és de $f_1'(x)$ sobre $\mathbb{F}'(\alpha')$. Per tant, existeix un isomorfisme $\tilde{\varphi} : \mathbb{K} \longrightarrow \mathbb{K}'$ tal que $\tilde{\varphi}|_{\mathbb{F}(\alpha)} = \varphi'$. Aleshores, $\tilde{\varphi}|_F = \varphi'|_F = \varphi$ que és el darrer que ens faltava comprovar. ■

Corol·lari 1.3.38. *Si $\mathbb{K}_1$ i $\mathbb{K}_2$ són dos cossos de descomposició de f sobre $\mathbb{F}$ aleshores $\mathbb{K}_1$ i $\mathbb{K}_2$ són $\mathbb{F}$-isomorfs.*

Demostració. Prenem $\mathbb{K} = \mathbb{K}_1, \mathbb{K}' = \mathbb{K}_2$ i $\varphi = Id$ en la proposició anterior, 1.3.37. ■

1.4 Clausures i cossos algebraicament tancats

Definició 1.4.1 (Clausura algebraica)**.** Un cos $\overline{\mathbb{F}}$ és una clausura algebraica de $\mathbb{F}$ si $\overline{\mathbb{F}}/\mathbb{F}$ és algebraica i tot polinomi de $\mathbb{F}[x]$ descompon completament a $\overline{\mathbb{F}}$.

Definició 1.4.2 (Cos algebraicament tancat)**.** Un cos $\mathbb{K}$ és algebraicament tancat si tot polinomi no constant de $\mathbb{K}[x]$ té alguna arrel a $\mathbb{K}$.

Observació 1.4.3. Si $\mathbb{K}$ és algebraicament tancat aleshores tot $f \in \mathbb{K}[x]$ té totes les arrels a $\mathbb{K}$. En particular, no existeixen extensions algebraiques de $\mathbb{K}$ no trivials, i el propi $\mathbb{K}$ és una clausura algebraica de $\mathbb{K}$. Tot cos algebraicament tancat és cos de descomposició (cf. 1.3.29), però no tot cos de descomposició és algebraicament tancat.

Proposició 1.4.4. *Sigui $\mathbb{F}$ un cos i $\overline{\mathbb{F}}$ una clausura algebraica de $\mathbb{F}$. Aleshores $\overline{\mathbb{F}}$ és algebraicament tancat.*

Demostració. Sigui $f(x) \in \overline{\mathbb{F}}[x]$ no constant i α una arrel de f (en un cos de descomposició de f). Aleshores $\overline{\mathbb{F}}(\alpha)/\overline{\mathbb{F}}$ és algebraica. Com que $\overline{\mathbb{F}}/\mathbb{F}$ és algebraica, per 1.3.22, $\overline{\mathbb{F}}(\alpha)/\mathbb{F}$ és algebraica. Per tant α és arrel d'un polinomi amb coeficients a $\mathbb{F}$, i pertany a $\overline{\mathbb{F}}$. ■

Proposició 1.4.5. *Donat un cos $\mathbb{F}$, existeix un cos algebraicament tancat que conté $\mathbb{F}$.*

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

$$g_1 f_1(x_{f_1}) + \ldots + g_n f_n(x_{f_n}) = 1 \tag{1.2}$$

Sigui $\mathbb{K}/\mathbb{F}$ una extensió que contingui arrels α_i dels f_i. Posant $x_{f_i} = \alpha_i$ (notem doncs que $f_i(x_{f_i}) = f_i(\alpha_i) = 0$) i fent 0 les altres variables que apareguin als g_i a (1.2) 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 $K_1 = \mathbb{F}[\ldots, x_f, \ldots]/\mathcal{M}$ és un cos que conté $\mathbb{F}$ i per construcció tot $f \in \mathbb{F}[x]$ no constant té una arrel en K_1 (la classe de x_f). Ara repetim la construcció amb K_1 en lloc de $\mathbb{F}$, 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:

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

amb la propietat que tot $f \in K_i[x]$ no constant té una arrel en $K_{i+1}[x]$. Posem $\mathbb{K} = \bigcup_i K_i$, que és un cos[14]. Veiem que $\mathbb{K}$ és algebraicament tancat. Sigui $f \in \mathbb{K}[x]$. 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 $\mathbb{K}$. ■

Proposició 1.4.6. *Sigui $\mathbb{K}$ un cos algebraicament tancat que conté $\mathbb{F}$. El cos $\overline{\mathbb{F}}$ format pels elements de $\mathbb{K}$ que són algebraics sobre $\mathbb{F}$ és una clausura algebraica de $\mathbb{F}$.*

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

Exemple 1.4.7. El Teorema Fonamental de l'Àlgebra afirma que $\mathbb{C}$ és algebraicament tancat. Per tant, el cos $\overline{\mathbb{Q}}$ format pels nombres complexos que són algebraics sobre $\mathbb{Q}$ és una clausura algebraica de $\mathbb{Q}$.

[14] 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

Proposició 1.4.8 (Extensió de morfismes a un cos algebraicament tancat). *Sigui $\sigma : \mathbb{F} \longrightarrow \mathbb{K}$ un morfisme amb $\mathbb{K}$ algebraicament tancat. Si $E/\mathbb{F}$ és algebraica aleshores existeix una extensió $\tilde{\sigma} : E \longrightarrow \mathbb{K}$ de σ.*

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

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

és un morfisme que estén σ (cf. 1.2.24). El cas general és una aplicació estàndard del Lema de Zorn. Considerem:

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

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 $L' = \bigcup L_i$ i $\sigma' : L' \longrightarrow L'$ 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 $\alpha \in E \backslash M$ 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 1.4.9. *Si $\overline{\mathbb{F}}$ i $\overline{\mathbb{F}}'$ són dues clausures algebraiques de $\mathbb{F}$ aleshores són $\mathbb{F}$-isomorfes.*

Demostració. La inclusió $\sigma : \mathbb{F} \longrightarrow \overline{\mathbb{F}}$ s'estén a $\tilde{\sigma} : \overline{\mathbb{F}}' \longrightarrow \overline{\mathbb{F}}$, i la inclusió $\tau : \mathbb{F} \longrightarrow \overline{\mathbb{F}}'$ s'estén a $\tilde{\tau} : \overline{\mathbb{F}} \longrightarrow \overline{\mathbb{F}}'$. $\tilde{\sigma}, \tilde{\tau}$ són dos morfismes de cossos i per tant injectius. Com que $\overline{F}/F$ és algebraica (cf. 1.3.23), $\tilde{\sigma}$ és exhaustiva i és, doncs, un $\mathbb{F}$-isomorfisme; per tant, la composició $\tilde{\sigma} \circ \tilde{\tau} : \overline{\mathbb{F}} \longrightarrow \overline{\mathbb{F}}$ és un $\mathbb{F}$-automorfisme. ■

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

II

Extensions algebraiques de cossos

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

Ja hem vist que si $\sigma \in \mathrm{Aut}(K/F)$, aleshores $f(\sigma(\alpha)) = \sigma(f(\alpha)) = 0$, de manera que $\sigma(\alpha) \in \{\alpha_1, \ldots, \alpha_n\}$. D'altra banda, també hem vist que per a tot $i = 1, \ldots, n$ existeix $\sigma_i \in \mathrm{Aut}(K/F)$ tal que $\sigma_i(\alpha) = \alpha_i$. Com que un F-automorfisme de K queda unívocament determinat per la imatge de α, veiem que $\mathrm{Aut}(K/F) = \{\sigma_1, \ldots, \sigma_n\}$ i, en particular, $\#\ \mathrm{Aut}(K/F) = n$. Com que $n \leq d$, tenim doncs que $\#\,\mathrm{Aut}(K/F) \leq [K : F]$, i la desigualtat pot ser estricta per dos motius:

1. El polinomi $f(X) = \mathrm{Irr}(\alpha, F)(X)$ no descompon completament a K;
2. El polinomi $f(X) = \mathrm{Irr}(\alpha, F)(X)$ té arrels repetides (i.e., 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 2.1.1 (Extensió normal). Una extensió algebraica $\mathbb{K}/\mathbb{F}$ és normal si per a tot $\alpha \in \mathbb{K}$ el polinomi $\mathrm{Irr}(\alpha, \mathbb{F})$ descompon completament a $\mathbb{K}$ (totes les arrels del polinomi es troben a $\mathbb{K}$). També es diu que $\mathbb{K}$ és normal sobre $\mathbb{F}$.

Exemple 2.1.2. Per $d \in \mathbb{Q}^* \setminus (\mathbb{Q}^*)^2$ l'extensió quadràtica $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ és normal. Descompon $\mathrm{Irr}(\alpha, \mathbb{Q})$ en $\mathbb{Q}(\sqrt{d})$? 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, $\mathrm{Irr}(\alpha, \mathbb{Q}) \mid f_\alpha$ i com que f_α descompon completament a $\mathbb{Q}(\sqrt{d})$ veiem que $\mathrm{Irr}(\alpha, \mathbb{Q})$ també. En particular, $\mathrm{Irr}(\sqrt{d}, \mathbb{Q}) = x^2 - d$ té les dues arrels a $\mathbb{Q}(\sqrt{d})$, que són $\sqrt{d}$ i $-\sqrt{d}$. Fixem-nos que, per 1.2.25, hi ha un $\sigma \in \mathrm{Aut}(\mathbb{Q}(\sqrt{d}/\mathbb{Q}))$ tal que $\sigma(\sqrt{d}) = -\sqrt{d}$. De fet, aquest és l'únic automorfisme no trivial i per tant $\mathrm{Aut}(\mathbb{Q}(\sqrt{d})/\mathbb{Q}) = \{1, \sigma\}$.

Exemple 2.1.3. Més en general, si $\mathbb{F}$ és un cos qualsevol i $a \in \mathbb{F} \setminus \mathbb{F}^2$, $\mathbb{F}(\sqrt{a})$ és normal sobre $\mathbb{F}$.

Exemple 2.1.4. $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ no és normal, ja que per a $\mathrm{Irr}(\sqrt[3]{2})$ tenim $\mathbb{Q} = x^3 - 2$, amb respectives arrels: $\sqrt[3]{2} \in \mathbb{R}$, però les altres dues arrels d'aquest polinomi no viuen a $\mathbb{Q}(\sqrt[3]{2})$, que són $e^{\frac{2\pi i}{3}}\sqrt[3]{2}, e^{\frac{4\pi i}{3}}\sqrt[3]{2} \in \mathbb{C} \setminus \mathbb{R}$ (vaja, que no són reals i $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$). De nou per 1.2.25, veiem que $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2}))/\mathbb{Q} = \{1\}$.

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*, i les extensions de Galois en tenen molts.

Proposició 2.1.5. *Sigui $\mathbb{K}/\mathbb{F}$ una extensió algebraica i $\overline{\mathbb{K}}$ una clausura algebraica de $\mathbb{K}$. Les propietats següents són equivalents:*

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

Demostració.

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

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

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

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

és un $\mathbb{F}$-morfisme amb imatge $\mathbb{F}(\beta)$. Com que $\overline{\mathbb{K}}$ és algebraicament tancat i $\mathbb{K}/\mathbb{F}(\alpha)$ algebraica, per 1.4.8, σ s'estén a $\sigma : \mathbb{K} \longrightarrow \overline{\mathbb{K}}$. Com que $\tilde{\sigma}(\mathbb{K}) = \mathbb{K}$, tenim $\beta \in \tilde{\sigma}(\mathbb{K}) = \mathbb{K}$ i per *3.* sabem que $\tilde{\sigma} = \mathbb{K}$. ■

Proposició 2.1.6. *Si $\mathbb{K} = \mathbb{F}(A)$ i per a tot $\alpha \in A$ el polinomi $\mathrm{Irr}(\alpha, \mathbb{F})$ descompon completament a $\mathbb{K}$, aleshores $\mathbb{K}/\mathbb{F}$ és normal.*

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

Proposició 2.1.7. *Sigui $L/\mathbb{K}/\mathbb{F}$. Si $L/\mathbb{F}$ és normal aleshores també ho és $L/\mathbb{K}$.*

Demostració. Si L és el cos de descomposició d'un conjunt $S \subseteq \mathbb{F}[x]$, també és cos de descomposició dels mateixos polinomis pensats com a polinomis de $\mathbb{K}[x]$. *A classe hem dit que* $\mathrm{Irr}(\alpha, \mathbb{K}) \mid \mathrm{Irr}(\alpha, \mathbb{F})$. ■

Exemple 2.1.8. Posem $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$, amb el seu irreductible corresponent $\mathrm{Irr}(\sqrt[4]{2},\mathbb{Q}) = x^4 - 2$; que té arrels:

$$\sqrt[4]{2}, -\sqrt[4]{2} \in \mathbb{R} \text{ i } \sqrt[4]{-2}, -\sqrt[4]{-2} \in \mathbb{C} \setminus \mathbb{R}.$$

En altres paraules, aquestes dues últimes arrels mai no es trobaran a $\mathbb{Q}(\sqrt[4]{2})$, i l'extensió no serà normal. La torre d'extensions seria la següent:

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

on $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ és normal, $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ també ho és, però $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ no. Per tant, la clausura normal és $\mathbb{Q}(\sqrt[4]{2}, i)$.

Definició 2.1.9 (Clausura normal)**.** Donada $\mathbb{K}/\mathbb{F}$ algebraica, una clausura normal és una extensió $N/\mathbb{K}$ tal que $N/\mathbb{F}$ és normal i és minimal amb aquesta propietat (és a dir, si $\mathbb{K} \subseteq N' \subseteq N$ amb $N'/\mathbb{F}$ normal aleshores $N' = N$).

Proposició 2.1.10. *$N/\mathbb{K}$ és una clausura normal de $\mathbb{K}/\mathbb{F}$ si, i només si, N és un cos de descomposició de $\{\mathrm{Irr}(\alpha,\mathbb{F})\}_{\alpha\in\mathbb{K}}$.*

Proposició 2.1.11. *Si $\mathbb{K}/\mathbb{F}$ és finita amb $\mathbb{K} = \mathbb{F}(\alpha_1,\ldots,\alpha_n)$, aleshores una clausura normal de $\mathbb{K}$ és el cos de descomposició del polinomi $\prod_{i=1}^{n} \mathrm{Irr}(\alpha_i,\mathbb{F})$. En particular, la clausura normal de $\mathbb{K}/\mathbb{F}$ és única llevat de $\mathbb{F}$-isomorfisme.*

Proposició 2.1.12 (Extensió de morfismes en cossos normals)**.** *Sigui $\mathbb{K}/\mathbb{F}$ una extensió algebraica normal (finita) i $E/\mathbb{F}$ una subextensió (i.e. $\mathbb{F} \subseteq E \subseteq \mathbb{K}$). Tot $\mathbb{F}$-morfisme $\sigma : E \longrightarrow \mathbb{K}$ s'estén a un $\mathbb{F}$-morfisme $\tilde{\sigma} : \mathbb{K} \longrightarrow \mathbb{K}$ (en particular $\tilde{\sigma} \in \mathrm{Aut}(\mathbb{K}/\mathbb{F})$).*

Demostració. Posem $\overline{\mathbb{K}}$ una clausura algebraica de $\mathbb{K}$, és a dir, $\overline{K}$ és algebraicament tancat. Aleshores $\sigma : E \longrightarrow \mathbb{K} \subseteq \overline{\mathbb{K}}$ s'estén, per 1.4.8, a $\tilde{\sigma} : \mathbb{K} \longrightarrow \overline{\mathbb{K}}$. Com que $\mathbb{K}/\mathbb{F}$ és normal, $\tilde{\sigma}(\mathbb{K}) = \mathbb{K}$ i, per tant, tenim $\tilde{\sigma} : \mathbb{K} \longrightarrow \mathbb{K}$. Com que $\mathbb{K}/\mathbb{F}$ és algebraica, $\tilde{\sigma}$ és un automorfisme. ■

2.2 Extensions separables

Definició 2.2.1 (Polinomi separable)**.** Un polinomi $f(x) \in \mathbb{F}[x]$ es diu *separable* si totes les seves arrels en un cos de descomposició són simples (i.e., de multiplicitat 1). Es diu *inseparable* en cas contrari. Aquesta noció no depèn del cos de descomposició escollit, ja que tots ells són isomorfs.

Definició 2.2.2 (Arrel separable)**.** Sigui $\mathbb{K}/\mathbb{F}$ algebraica. Diem que $\alpha \in \mathbb{K}$ és separable sobre $\mathbb{F}$ si $\mathrm{Irr}(\alpha,\mathbb{F})$ és separable. Diem que $\mathbb{K}/\mathbb{F}$ és separable si tot $\alpha \in \mathbb{K}$ és separable sobre $\mathbb{F}$ i que $\mathbb{K}/\mathbb{F}$ és inseparable en cas contrari.

Proposició 2.2.3. *Si $\mathbb{L}/\mathbb{K}/\mathbb{F}$ i $\alpha \in \mathbb{L}$ és separable sobre $\mathbb{F}$ aleshores també ho és sobre $\mathbb{K}$.*

Demostració. Ja que $\mathrm{Irr}(\alpha, \mathbb{K}) \mid \mathrm{Irr}(\alpha, \mathbb{F})$. ■

Exemple 2.2.4.

1. $x^2 + 1 \in \mathbb{Q}[x]$ és separable: $\mathbb{Q}(i)/\mathbb{Q}$ és, doncs, separable també.
2. $x^2 + 1 \in \mathbb{F}_2[x]$ és inseparable, ja que $x^2 + 1 \equiv x^2 + 2x + 1 \equiv (x + 1)^2$. 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 $\mathbb{F} = \mathbb{F}_p(t)$ i $f(x) = x^p - t \in \mathbb{F}[x]$. 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 $\mathbb{K} = \mathbb{F}(\alpha)$ aleshores $\mathrm{Aut}(\mathbb{K}/\mathbb{F}) = \{1\}$, ja que tot $\sigma \in \mathrm{Aut}(\mathbb{K}/\mathbb{F})$ envia α a una arrel de f, però l'única arrel de f és α. El fet que $\mathbb{K}$ l'hem obtingut adjuntant α i $\mathrm{Irr}(\alpha, \mathbb{F})$ no és separable (és *inseparable*) té com a conseqüència que $\mathbb{K}/\mathbb{F}$ no té automorfismes no trivials. Això és un fet general, que anirem precisant: les extensions que no són separables, tenen «pocs automorfismes».

Definició 2.2.5 (Derivat). Donat $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{F}[x]$ definim el seu derivat com

$$f'(x) = n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \cdots + a_1.$$

Propietat 2.2.6. *Les propietats següents es comproven fàcilment a partir de la definició:*

- $(f + g)' = f' + g'$,
- $(fg)' = f'g + fg'$ *(regla de Leibniz),*
- $(af)' = af'$ *si* $a \in \mathbb{F}$.

Demostració. Exercici. ■

Lema 2.2.7. *Sigui $\mathbb{K}/\mathbb{F}$ una extensió i $f, g \in \mathbb{F}[x]$. Aleshores* $\mathrm{mcd}(f, g) = 1$ *a $\mathbb{F}[x]$ si i només si* $\mathrm{mcd}(f, g) = 1$ *a $\mathbb{K}[x]$.*

Demostració. És una conseqüència de l'algoritme d'Euclides, que calcula $\mathrm{mcd}(f, g)$ fent les operacions a $\mathbb{F}$ fins i tot si pensem f i g com a polinomis de $\mathbb{K}[x]$ (ja que $\mathbb{F}$ és tancat per producte i divisió). ■

Proposició 2.2.8. *Un polinomi f és separable si i només si* $\mathrm{mcd}\,(f, f') = 1$.

Demostració.

⇐ Ho demostrem per contrarrecíproc. Si f no és separable, aleshores $f(x) = (x-\alpha)^2 g(x)$ per a cert $\alpha \in \mathbb{K}$ i $g(x) \in \mathbb{K}[x]$. Aleshores $f'(x) = 2(x-\alpha)g(x) + (x-\alpha)^2 g(x)$ i per tant $(x-\alpha) \mid \mathrm{mcd}\,(f, f')$ (en particular, $\mathrm{mcd}(f, f') \neq 1$).

⇒ D'altra banda, si $\mathrm{mcd}(f, f') \neq 1$; és a dir, $(x-\alpha) \mid \mathrm{mcd}\,(f, f')$ aleshores prenent $\alpha \in K$ i 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 $(x-\alpha)^2 \mid f$ i f no és separable, com volíem. ■

Proposició 2.2.9. *Si* $\mathrm{car}(\mathbb{F}) = 0$ *aleshores tot* $f \in \mathbb{F}[x]$ *irreductible és separable.*

Demostració. Si $\mathrm{car}(\mathbb{F}) = 0$ tenim que $\mathrm{gr}\,(f') < \mathrm{gr}(f)$ i $f \neq 0$. Per tant $\mathrm{mcd}\,(f', f) = 1$. ■

Corol·lari 2.2.10. *Tota extensió algebraica* $\mathbb{K}/\mathbb{F}$ *algebraica d'un cos de característica 0 és separable.*

Demostració. Prenem $\alpha \in K$, $f = \mathrm{Irr}(\alpha, \mathbb{F})$ el minimal. Per definició d'f, $\mathrm{mcd}(f, f')$ és o bé 1 o bé f; com que $\mathrm{gr}(f') < \mathrm{gr}(f)$ i $f'(x) \neq 0$, tenim $\mathrm{mcd}(f, f') = 1$. Per 2.2.8, f és separable. ■

Exemple 2.2.11. Posem $\mathbb{F} = \mathbb{F}_p(t)$, amb el minimal $f(x) = x^p - t$. És evident que $f'(x) = px^{p-1}$, i t igualment serà arrel. Per tant, $\mathrm{mcd}(f, f') = \mathrm{mcd}(f, 0) = f \neq 1$.

Proposició 2.2.12. *Sigui* $\mathbb{F}$ *de característica* $p > 0$. *Un polinomi irreductible* $f \in \mathbb{F}[x]$ *és inseparable si, i només si,* $f(x) = g(x^p)$ *per a algun* $g \in \mathbb{F}[x]$.

Demostració.

⇒ Com que f és irreductible $\mathrm{mcd}(f', f)$ només pot ser 1 o f (llevat d'unitats a $\mathbb{F}[x]$). Si $f' \neq 0$, com que $\mathrm{gr}(f') < \mathrm{gr}(f)$ aleshores és 1. Per tant, si f és inseparable necessàriament $f' = 0$. Si posem:

$$f(x) = a_n x^n + \cdots + a_1 x + a_0,$$
$$f'(x) = n a_n x^{n-1} + \cdots + 2a_2 x + a_1 = 0.$$

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 algun g.

⇐ D'altra banda, és directe veure que si $f(x) = g(x^p)$ aleshores $f' = 0$ i per tant $\mathrm{mcd}(f', f) = f$. ■

El resultat següent fa precís el comentari informal de 2.2.4, apartat *3.*.

Proposició 2.2.13. *Sigui* $\mathbb{K}/\mathbb{F}$ *finita de grau* n *i* $N/\mathbb{K}$ *una extensió tal que* $N/\mathbb{F}$ *és normal. El nombre de* $\mathbb{F}$*-morfismes* $\sigma : \mathbb{K} \longrightarrow N$ *és menor o igual que* n*, amb igualtat si i només si* $\mathbb{K}/\mathbb{F}$ *és separable.*

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

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

Com que $N/\mathbb{F}$ és normal i $N/\mathbb{F}(\alpha)$ algebraica, per 2.1.12 s'estenen a $\tau_i : N \longrightarrow N$ amb $\tau_i(\alpha) = \alpha_i$. Ara considerem $N/\mathbb{F}(\alpha)$. Com que $N/\mathbb{F}(\alpha)$ és normal i $s = [\mathbb{K} : \mathbb{F}(\alpha)] < n$, per hipòtesi d'inducció existeixen $t \leq s$ $\mathbb{F}(\alpha)$-morfismes $\mathbb{K} \longrightarrow N$ amb igualtat si, i només si, $\mathbb{K}/\mathbb{F}(\alpha)$ és separable. Anomenem-los $\sigma_1, \ldots, \sigma_t$. Per $i = 1, \ldots, r$ i $j = 1, \ldots, s$ tenim un $\mathbb{F}$-morfisme $\tau_i \circ \sigma_j : \mathbb{K} \longrightarrow N$. D'aquests n'hi ha $rt \leq [\mathbb{K} : \mathbb{F}(\alpha)][\mathbb{K} : \mathbb{F}(\alpha)] = [\mathbb{K} : \mathbb{F}]$. Veiem ara que tot $\mathbb{F}$-morfisme $\sigma : \mathbb{K} \longrightarrow N$ és de la forma $\tau_i \circ \sigma_j$ per algun i i per algun j. Sabem que $\sigma(\alpha) = \alpha_i$ per algun i, i per tant $\tau_i^{-1} \circ \sigma$ fixa α. Això vol dir que $\tau_i^{-1} \circ \sigma$ és un $\mathbb{F}(\alpha)$-morfisme i per tant $\tau_i^{-1} \circ \sigma = \sigma_j$ per 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 $\mathbb{F}(\alpha)$-morfisme; si $\tau_i \circ \sigma_j = \tau_{i'} \circ \sigma_{j'}$ aleshores $\sigma_j(\alpha) = \alpha$ i $\sigma_{j'}(\alpha) = \alpha$, ambdós per ser $\mathbb{F}$-morfismes. Així, tenim la igualtat $\tau_i = \tau_{i'}$ i com que els τ' són automorfismes compleixen que $\alpha_i = \alpha_{i'}$; per tant, $i = i'$ i $\sigma_j = \sigma_{j'}$ (de manera que també $j = j'$). Finalment: si $\mathbb{K}/\mathbb{F}$ és separable aleshores val la igualtat, ja que llavors $r = [\mathbb{F}(\alpha) : \mathbb{F}]$ i $t = s$. I si $\mathbb{K}/\mathbb{F}$ no és separable aleshores no val la igualtat, ja que llavors podem prendre $\alpha \in \mathbb{K}$ inseparable sobre $\mathbb{K}$ i tenim que $r < [\mathbb{F}(\alpha) : \mathbb{F}]$ amb la qual cosa $rt < [\mathbb{K} : \mathbb{F}]$. ■

Proposició 2.2.14. *Una extensió algebraica simple $\mathbb{F}(\alpha)/\mathbb{F}$ és separable si, i només si, α és separable.*

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

Proposició 2.2.15. *Sigui $\mathbb{K}/E/\mathbb{F}$ una torre d'extensions algebraiques. Aleshores $\mathbb{K}/\mathbb{F}$ és separable si, i només si, $\mathbb{K}/E$ i $E/\mathbb{F}$ són separables.*

Demostració. Exercici, s'ha d'usar 2.2.13 (Indicació: feu primer el cas en què $\mathbb{K}/\mathbb{F}$ és finita, i veieu que el cas general es redueix a aquest). ■

[1] El grau de l'extensió coincideix amb el nombre d'arrels quan l'extensió és, en efecte, separable!

2.3

Extensions simples

Teorema 2.3.1 (Teorema de l'element primitiu)**.** *Tota extensió $\mathbb{K}/\mathbb{F}$ finita i separable és simple.*

Demostració. Si $\mathbb{F}$ és cos finit ho veurem més endavant. Suposem ara que $\mathbb{F}$ té un nombre infinit d'elements. Donats $\alpha, \beta \in \mathbb{K}$ trobarem un $\gamma \in \mathbb{K}$ tal que $\mathbb{F}(\alpha, \beta) = \mathbb{F}(\gamma)$. Si veiem això ja ho tindrem, perquè $\mathbb{K}/\mathbb{F}$ és finita i per tant $\mathbb{K} = \mathbb{F}(\delta_1, \delta_2, \ldots, \delta_n)$. Posem $f = \mathrm{Irr}(\alpha, \mathbb{F})$ i $g = \mathrm{Irr}(\beta, \mathbb{F})$. 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 ($\mathbb{K}/\mathbb{F}$ és separable i, per tant, f, g són ambdós separables). Com que $\mathbb{F}$ és infinit, existeix $\lambda \in \mathbb{F}$ tal que

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

Posem $\gamma = \alpha + \lambda\beta$, i volem veure $F(\alpha + \lambda\beta) = F(\alpha, \beta)$. Clarament $\mathbb{F}(\gamma) \subseteq \mathbb{F}(\alpha, \beta)$. Per a veure la inclusió contrària, n'hi ha prou amb veure que $\beta \in \mathbb{F}(\gamma)$ (ja que llavors $\alpha = \gamma - \lambda\beta \in \mathbb{F}(\gamma)$). Posem $h = \mathrm{Irr}(\beta, \mathbb{F}(\gamma))$, i volem veure que $\mathrm{gr}(h) = 1$ (això ens permetrà dir que $\beta \in F(\gamma)$). Aleshores $h \mid g$ i per tant les seves arrels només poden estar entre els β_i, és a dir, h és també separable. També tenim que $h \mid f(\gamma - \lambda x)$, $f(\gamma - \lambda x) \in F(\gamma)[X]$, 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 $f(\gamma - \lambda\beta_j) = 0$ ($\gamma - \lambda\beta_j$ seria arrel de f) i per tant $\gamma - \lambda\beta_j = \alpha_i$ per algun i, i $\lambda = \frac{\alpha_1 - \alpha_i}{\beta_1 - \beta_j}$, però això és una contradicció amb (2.1). La conclusió doncs és que l'única arrel de h és $\beta = \beta_1$, és a dir, h té grau 1 i $\beta \in \mathbb{F}(\gamma)$. ■

III

Teoria de Galois

3.1 Preliminars

Observació 3.1.1.

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

$$\mathrm{Aut}(\mathbb{K}/\mathbb{F}) = \{\mathbb{F}\text{-morfismes } \sigma : \mathbb{K} \longrightarrow \overline{\mathbb{K}}\},\ \sigma(\mathbb{K}) = \mathbb{K}.$$

2. Si $\mathbb{F} \subseteq E \subseteq \mathbb{K}$ aleshores $\mathrm{Aut}(\mathbb{K}/E)$ és un subgrup de $\mathrm{Aut}(\mathbb{K}/\mathbb{F})$, ja que com E està contingut en $\mathbb{K}$, tot element de E també és fix, i per tant tenim la inclusió en clau de subgrup, amb la següent notació: $\mathrm{Aut}(\mathbb{K}/E) \leq \mathrm{Aut}(\mathbb{K}/\mathbb{F})$.

Definició 3.1.2 (Cos fix). Sigui G un subgrup de $\mathrm{Aut}(\mathbb{K}/\mathbb{F})$. El cos fix de G és:

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

És fàcil veure que $\mathbb{K}^G$ és un subcòs de $\mathbb{K}$ que conté $\mathbb{F}$; és a dir, tenim la cadena $\mathbb{F} \subset \mathbb{K}^G \subset \mathbb{K}$. Tenim, doncs, una *correspondència bijectiva* i dues aplicacions, $\mathcal{G}$ i $\mathcal{F}$:

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

Proposició 3.1.3. *Les aplicacions $\mathbb{F}$ i $\mathcal{G}$ satisfan les propietats següents:*

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

Demostració. Són directes a partir de les definicions. ∎

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

3.2

Extensions de Galois

Definició 3.2.1 (Extensió finita de Galois)**.** Una extensió (algebraica) finita[1] $\mathbb{K}/\mathbb{F}$ és de Galois si és normal i separable.

Exemple 3.2.2. Hem vist a classe de problemes que l'extensió $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$ és normal i separable; com també és finita[2], és algebraica, i podríem dir que aquesta extensió finita és de Galois.

Proposició 3.2.3. *$\mathbb{K}/\mathbb{F}$ és de Galois si, i només si, $\mathbb{K}$ és cos de descomposició d'un polinomi separable de $\mathbb{F}[x]$.*

Demostració. A grans trets, la idea és la següent. $\mathbb{K}/\mathbb{F}$ és normal si, i només si, $\mathbb{K}$ és el cos de descomposició de $S \subset \mathbb{F}[x]$; per tant, ho és d'un polinomi $p \in S$ que tindrà totes les arrels a $\mathbb{K}$. D'altra banda, $\mathbb{K}/\mathbb{F}$ és separable si, i només si, per a tot $\alpha \in \mathbb{K} \setminus \mathbb{F}$ algebraic tenim $\mathrm{Irr}(\alpha,\mathbb{F})$ separable, de manera que $p \in S$ és, a més, separable. ■

Definició 3.2.4 (Grup de Galois)**.** Si $\mathbb{K}/\mathbb{F}$ és de Galois aleshores el grup $\mathrm{Aut}(\mathbb{K}/\mathbb{F})$ s'anomena grup de Galois de l'extensió i es denota $\mathrm{Gal}(\mathbb{K}/\mathbb{F})$.

Observació 3.2.5. Fixem-nos que si $\mathbb{K}/\mathbb{F}$ és Galois i $E/\mathbb{F}$ és una subextensió, aleshores $\mathbb{K}/E$ és Galois (cf. 2.1.7 i 2.2.3).

Proposició 3.2.6. *Si $\mathbb{K}/\mathbb{F}$ és de Galois aleshores $\mathbb{F} = \mathbb{K}^{\mathrm{Gal}(\mathbb{K}/\mathbb{F})}$.*

Demostració. Ja sabem que $\mathbb{F} \subseteq \mathbb{K}^{\mathrm{Gal}(\mathbb{K}/\mathbb{F})}$, provarem l'altra inclusió. Sigui ara $\alpha \in \mathbb{K}^{\mathrm{Gal}(\mathbb{K}/\mathbb{F})} \subset \mathbb{K}$; veurem que de fet $\mathbb{F}(\alpha) = \mathbb{F}$, provant que $[\mathbb{F}(\alpha):\mathbb{F}] = 1$, i això ja ens dirà que $\alpha \in \mathbb{F}$. Sigui $\sigma : \mathbb{F}(\alpha) \longrightarrow \mathbb{K}$ un $\mathbb{F}$-morfisme; com que $\mathbb{K}/\mathbb{F}$ és normal, σ estén a $\tilde{\sigma} \in \mathrm{Aut}(\mathbb{K}/\mathbb{F}) = \mathrm{Gal}(\mathbb{K}/\mathbb{F})$. Ara $\tilde{\sigma}_{|\mathbb{F}} = Id$ i $\tilde{\sigma}(\alpha) = \alpha$ (ja que $\alpha \in \mathbb{K}^{\mathrm{Gal}(\mathbb{K}/\mathbb{F})}$). Així doncs $\tilde{\sigma}_{|\mathbb{F}(\alpha)} = Id$ (ja que si fixa el generador fixarà l'extensió que genera) i, per tant, $\sigma = Id$, de manera que σ és la inclusió. Tenim, doncs que només hi ha un únic $\mathbb{F}$-morfisme $\mathbb{F}(\alpha) \longrightarrow \mathbb{K}$ i com que $\mathbb{K}/\mathbb{F}$ és normal i $\mathbb{F}(\alpha)$ separable, això vol dir que $|\{\mathbb{F}\text{-morfismes } \mathbb{F}(\alpha) \longrightarrow \mathbb{K}\}| = 1$ i $[\mathbb{F}(\alpha):\mathbb{F}] = 1$ per 2.2.13. ■

Proposició 3.2.7. *Si $\mathbb{K}/\mathbb{F}$ és de Galois aleshores $\mathcal{F} \circ \mathcal{G} = Id$.*

Demostració. Si $\mathbb{K}/\mathbb{F}$ és Galois també $\mathbb{K}/E$ és Galois per a tota subextensió $E/\mathbb{F}$. Per tant $E = \mathbb{K}^{\mathrm{Gal}(\mathbb{K}/E)}$, per la proposició anterior. I ara prenem $H = \mathrm{Gal}(\mathbb{K}/E)$, així que tenim $\mathcal{F}(H) = \mathbb{K}^H$ i $\mathcal{G}(\mathbb{K}^H) = \mathrm{Aut}(\mathbb{K}/E) = \mathrm{Gal}(\mathbb{K}/E) = H$, de manera que $\mathcal{F} \circ \mathcal{G} = Id$. ■

[1] 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.

[2] Convé no confondre el terme extensió finita amb el d'extensió finitament generada. Tota extensió finita és finitament generada, però no és cert el recíproc (per exemple, per a extensions simples transcendents).

Proposició 3.2.8. *Sigui $\mathbb{K}/\mathbb{F}$ finita. Aleshores $|\operatorname{Aut}(\mathbb{K}/\mathbb{F})| \leq [\mathbb{K}:\mathbb{F}]$ amb igualtat si i només si $\mathbb{K}/\mathbb{F}$ és Galois.*

Demostració.

$\Rightarrow$ Prenem el nombre de $\mathbb{F}$-morfismes $\sigma : \mathbb{K} \longrightarrow \overline{\mathbb{K}}$, i el denotem per $|\mathcal{M}|$, on $\mathcal{M} = \{\mathbb{F}\text{-morfismes } \sigma : \mathbb{K} \longrightarrow \overline{\mathbb{K}}\}$. A més a més, notem que $\operatorname{Aut}(\mathbb{K}/\mathbb{F}) \subset \mathcal{M}$. És $|\mathcal{M}| \leq [\mathbb{K}:\mathbb{F}]$ amb igualtat si, i només si, $\mathbb{K}/\mathbb{F}$ és separable. Si $\mathbb{K}/\mathbb{F}$ és Galois tot $\mathbb{F}$-morfisme $\sigma : \mathbb{K} \longrightarrow \overline{\mathbb{K}}$ de fet pertany a $\sigma \in \operatorname{Gal}(\mathbb{K}/\mathbb{F})$ per ser $\mathbb{K}/\mathbb{F}$ normal; per tant, $\operatorname{Aut}(\mathbb{K}/\mathbb{F}) = \mathcal{M}$. I exactament $|\mathcal{M}| = [\mathbb{K}:\mathbb{F}]$ per ser $\mathbb{K}/\mathbb{F}$ separable.

$\Leftarrow$ D'altra banda, tot $\sigma \in \operatorname{Aut}(\mathbb{K}/\mathbb{F})$ dona lloc a un $\mathbb{F}$-morfisme $\mathbb{K} \longrightarrow \overline{\mathbb{K}}$. Si $\mathbb{K}/\mathbb{F}$ no és separable d'aquests $\mathbb{F}$-morfismes n'hi ha menys que $[\mathbb{K}:\mathbb{F}]$; és a dir $|\mathcal{M}| < |\mathbb{K}:\mathbb{F}|$. Si $\mathbb{K}/\mathbb{F}$ no és normal existeix un $\mathbb{F}$-morfisme $\sigma : \mathbb{K} \longrightarrow \overline{\mathbb{K}}$ tal que $\sigma(\mathbb{K}) \neq \mathbb{K}$, i, per tant, $\sigma \notin \operatorname{Aut}(\mathbb{K}/\mathbb{F})$; és a dir, $\operatorname{Aut}(\mathbb{K}/\mathbb{F}) \subsetneq \mathcal{M}$. ■

Teorema 3.2.9 (d'Artin). *Sigui $\mathbb{K}/\mathbb{F}$ una extensió finita i $G \leq \operatorname{Aut}(\mathbb{K}/\mathbb{F})$. Posem $E = \mathbb{K}^G$. Aleshores $\mathbb{K}/E$ és de Galois i $\operatorname{Gal}(\mathbb{K}/E) = G$.*

Demostració. Com que $\mathbb{K}/\mathbb{F}$ és finita $\mathbb{K}/E$ també ho és i, en particular, és algebraica. Veiem ara que $\mathbb{K}/E$ és normal i separable. Posem $G = \{\sigma_1, \ldots, \sigma_n\}$, prenem $\alpha \in \mathbb{K}$ i posem $\{\alpha_1, \ldots, \alpha_r\} = \{\sigma_1(\alpha), \ldots, \sigma_n(\alpha)\}$, $r \leq n$ (si $\mathbb{K}/\mathbb{F}$ finita, $|\operatorname{Aut}(\mathbb{K}/\mathbb{F})| < \infty$). Fixem-nos que, com que G és un grup, per a tot $\sigma \in G$ tenim que

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

Definim el polinomi:

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

Així,

$$\sigma(p(x)) = (x-\sigma(\alpha_1))\cdots(x-\sigma(\alpha_r)) = (x-\alpha_1)\cdots(x-\alpha_r) = p(x). \tag{3.3}$$

La igualtat de conjunts (3.2) implica que $\sigma(p) = p$ per a tot $\sigma \in G$, com hem vist a (3.3) i, per tant, els $a_i \in E$, i $p(x) \in E[x]$. Veiem doncs que α és arrel d'un polinomi separable $p(x) \in E[x]$ que descompon completament (és a dir, que té totes les arrels a K) i per tant $\mathbb{K}/E$ és normal i separable; és de Galois.

Ara volem veure $G = \operatorname{Gal}(\mathbb{K}/E)$. Tenim que $G \leq \operatorname{Gal}(\mathbb{K}/E)$ i com que $\mathbb{K}/E$ és Galois $|\operatorname{Gal}(\mathbb{K}/E)| = [\mathbb{K}:E]$; cal veure doncs que $|G| = [\mathbb{K}:E]$. Com que $G \subseteq \operatorname{Gal}(\mathbb{K}/E)$ tenim que $|G| \leq |\operatorname{Gal}(\mathbb{K}/E)| = [\mathbb{K}:E]$. Per a l'altra desigualtat, sigui $\alpha \in \mathbb{K}$. Aleshores $[E(\alpha):E] \leq |G|$, ja que hem vist abans que α és arrel d'un polinomi amb coeficients a E de grau $\leq |G|$. Prenem $\alpha \in \mathbb{K}$ de grau màxim sobre E. Afirmem que $\mathbb{K} = E(\alpha)$. En efecte, si $\beta \in \mathbb{K}$ aleshores pel Teorema de l'Element Primitiu, 2.3.1, $E(\alpha,\beta) = E(\gamma)$, però $[E(\gamma):E] = [E(\alpha):E]$ per la maximalitat del grau i això dona $E(\gamma) \subset E(\alpha)$; com que $E(\alpha) \subseteq E(\gamma)$ (perquè $E(\alpha), E(\beta) \subset E(\alpha,\beta) = E(\gamma)$), veiem que $E(\alpha) = E(\gamma)$ i $\beta \in E(\alpha)$. Així doncs $[\mathbb{K}:E] = [E(\alpha):E] \leq G$. ■

Observació 3.2.10. El Teorema d'Artin de fet és cert en una versió una mica més general, que diu que si $\mathbb{K}$ és un cos, G un subgrup finit dels automorfismes de $\mathbb{K}$ i $E = \mathbb{K}^G$, aleshores $\mathbb{K}/E$ és Galois i $\mathrm{Gal}(\mathbb{K}/E) = G$. L'únic que ens ha faltat provar d'aquest resultat més general és que $\mathbb{K}/E$ és finita.

Corol·lari 3.2.11. *Si $\mathbb{K}/\mathbb{F}$ és de Galois, aleshores $\mathcal{G} \circ \mathcal{F} = Id$.*

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

Lema 3.2.12. *Sigui $\mathbb{K}/\mathbb{F}$ de Galois i E un cos intermedi. Per a tot $\sigma \in \mathrm{Gal}(\mathbb{K}/\mathbb{F})$ tenim que $\sigma(E)$ és un altre cos intermedi i $\mathrm{Gal}(\mathbb{K}/\sigma(E)) = \sigma\,\mathrm{Gal}(\mathbb{K}/E)\sigma^{-1}$.*

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

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

Proposició 3.2.13. *Si $\mathbb{K}/\mathbb{F}$ és Galois i $E/\mathbb{F}$ és una subextensió, aleshores $E/\mathbb{F}$ és Galois si, i només si, $\mathrm{Gal}(\mathbb{K}/E) \trianglelefteq \mathrm{Gal}(\mathbb{K}/\mathbb{F})$.*

Demostració. $E/\mathbb{F}$ és separable (cf. 2.2.15) i per tant $E/\mathbb{F}$ és Galois si, i només si, $E/\mathbb{F}$ és normal. Com que $\mathbb{K}/\mathbb{F}$ és Galois, tot $\mathbb{F}$-morfisme $\sigma_0 : E \longrightarrow \mathbb{K}$ s'aixeca a $\sigma \in \mathrm{Gal}(\mathbb{K}/\mathbb{F})$. Per tant, $E/\mathbb{F}$ és normal si i només si $\sigma(E) = E$ per a tot $\sigma \in \mathrm{Gal}(\mathbb{K}/\mathbb{F})$. Per la injectivitat de $\mathcal{G}$, això és si i només si $\mathrm{Gal}(\mathbb{K}/E) = \mathrm{Gal}(\mathbb{K}/\sigma(E))$ per a tot $\sigma \in \mathrm{Gal}(\mathbb{K}/\mathbb{F})$. Per 3.2.12 això és si, i només si, $\mathrm{Gal}(\mathbb{K}/E) = \sigma\,\mathrm{Gal}(\mathbb{K}/E)\sigma^{-1}$ per a tot $\sigma \in \mathrm{Gal}(\mathbb{K}/\mathbb{F})$, és a dir, si i només si $\mathrm{Gal}(\mathbb{K}/E)$ és normal. ■

Observació 3.2.14. Si $E/\mathbb{F}$ és una subextensió de Galois de $\mathbb{K}/\mathbb{F}$ aleshores l'aplicació

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

és un morfisme de grups exhaustiu (cf. 2.1.12) amb nucli $\mathrm{Gal}(\mathbb{K}/E)$. Així

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

3.3 Teorema Fonamental

Teorema 3.3.1 (Teorema Fonamental de la Teoria de Galois)**.** *Si $\mathbb{K}/\mathbb{F}$ és de Galois finita aleshores les aplicacions $\mathcal{F}$ i $\mathcal{G}$ de* (3.1) *són bijeccions i inverses una de l'altra, és a dir:*

1. $\mathbb{K}^{\mathrm{Gal}(\mathbb{K}/E)} = E$,
2. $\mathrm{Gal}(\mathbb{K}/\mathbb{K}^H) = H$.

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 $[\mathbb{K} : E] = |H|$ i $[E : \mathbb{F}] = [\mathrm{Gal}(\mathbb{K}/\mathbb{F}) : H]$.*
3. *Si H es correspon amb $E, \mathbb{K}/E$ és de Galois amb $\mathrm{Gal}(\mathbb{K}/E) = H$.*
4. *E és de Galois sobre $\mathbb{F}$ si i només si $\mathrm{Gal}(\mathbb{K}/E) \trianglelefteq \mathrm{Gal}(\mathbb{K}/\mathbb{F})$ i aleshores:*
$$\mathrm{Gal}(E/\mathbb{F}) \simeq \mathrm{Gal}(\mathbb{K}/\mathbb{F})/\mathrm{Gal}(\mathbb{K}/E).$$
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, el cos més petit que conté 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 de 2.1.12 i el Teorema d'Artin, 3.2.9. 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 3.3.2. La propietat *5.* ens diu que el reticle de subcossos de $\mathbb{K}/\mathbb{F}$ i el reticle de subgrups de $\mathrm{Gal}(\mathbb{K}/\mathbb{F})$ són duals (un diagrama és igual que l'altre girat cap per avall).

Exemple 3.3.3. Considerem $\mathbb{K} = \mathbb{Q}(\sqrt{2}, \sqrt{3})$; és el cos de descomposició de $(x^2-2)(x^2-3)$ sobre $\mathbb{Q}$ i per tant $\mathbb{K}/\mathbb{Q}$ és Galois ($\mathbb{K}/\mathbb{Q}$ és normal per ser $\mathbb{K}$ és cos de descomposició i, a més, és separable perquè, per exemple, $\mathbb{Q}$ té característica 0). Tenim que $[\mathbb{K} : \mathbb{Q}] = 4$. Per a veure-ho, fixem-nos que
$$[\mathbb{K} : \mathbb{Q}] = [\mathbb{K} : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}];$$
clarament $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ i $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] \leq 2$ (ja que $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ i $\sqrt{3}$ satisfà el polinomi $x^2 - 3 \in \mathbb{Q}(\sqrt{2})[x]$). Posem a partir d'ara $\mathbb{K} = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Si $[\mathbb{K} : \mathbb{Q}(\sqrt{2})]$ fos 1 tindríem que $\mathbb{K} = \mathbb{Q}(\sqrt{2})$ i, en particular, que $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$ cosa que ràpidament es veu que no pot ser. Per tant $[\mathbb{K} : \mathbb{Q}(\sqrt{2})] = 2$ i $[\mathbb{K} : \mathbb{Q}] = 4$. Una $\mathbb{Q}$-base de $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ és $\{1, \sqrt{2}, \sqrt{3}, \sqrt{2} \cdot \sqrt{3}\}$. D'aquí, veiem que $|\mathrm{Gal}(\mathbb{K}/\mathbb{Q})| = 4$. Tot $s \in \mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ satisfà que $s(\sqrt{2}) = \pm\sqrt{2}$ i $s(\sqrt{3}) = \pm\sqrt{3}$[3]. Aquestes quatre aplicacions indueixen quatre $\mathbb{Q}$-automorfismes de $\mathbb{K}$, que podem definir en funció dels generadors[4]:
$$\begin{array}{rcccc} Id: & \sqrt{2} & \longmapsto & \sqrt{2} & \qquad \sigma: \quad \sqrt{2} \longmapsto -\sqrt{2} \\ & \sqrt{3} & \longmapsto & \sqrt{3} & \qquad\quad \sqrt{3} \longmapsto \sqrt{3} \\ \tau: & \sqrt{2} & \longmapsto & \sqrt{2} & \qquad \rho: \quad \sqrt{2} \longmapsto -\sqrt{2} \\ & \sqrt{3} & \longmapsto & -\sqrt{3} & \qquad\quad \sqrt{3} \longmapsto -\sqrt{3} \end{array}$$

[3] No podem tenir $s(\sqrt{2}) = \pm\sqrt{3}$, ja que s envia arrels de l'irreductible a arrels del *mateix* irreductible. És fàcil veure que $\sqrt{2}$ i $\sqrt{3}$ no comparteixen el mateix irreductible.

[4] Fixem-nos, per exemple, en σ. Sigui $\alpha = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$ un element genèric de $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. Aleshores, $\sigma(\alpha) = a - b\sqrt{2} + c\sqrt{3} - d\sqrt{6}$, que està completament determinat per $\sqrt{2}$ i $\sqrt{3}$.

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

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

és a dir que $\mathrm{Gal}(\mathbb{K}/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (no hi ha cap element d'ordre 4, així que $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ no pot ser isomorf a $\mathbb{Z}/4\mathbb{Z}$). El reticle de subgrups de $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ és:

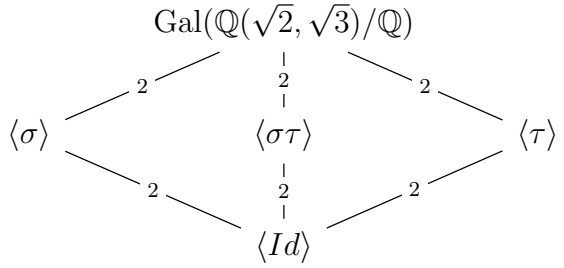


Figura 3.1: Reticle de subgrups de $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$.

Pel teorema fonamental això ens dona el diagrama de subcossos de $\mathbb{K}$, fixos pels diferents $\mathbb{K}$-automorfismes:

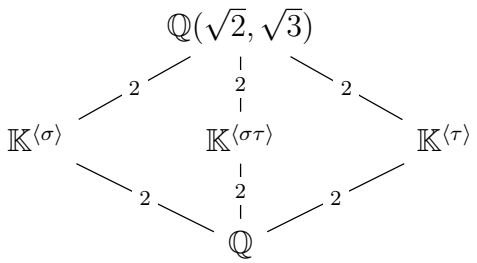


Figura 3.2: Diagrama de subcossos de $\mathbb{K}$.

Aquí per raonar que $\mathbb{K}^{\langle\sigma\rangle} = \mathbb{Q}(\sqrt{3})$, fixem-nos que clarament $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$, i $\mathbb{Q}(\sqrt{3}) \subset \mathbb{K}^{\langle\sigma\rangle}$; ara, pel teorema fonamental, 3.3.1, $[\mathbb{K}^{\langle\sigma\rangle} : \mathbb{Q}] = [\mathrm{Gal}(\mathbb{K}/\mathbb{Q}) : \langle\sigma\rangle] = 2$. Com $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = [\mathbb{K}^{\langle\sigma\rangle} : \mathbb{Q}]$ obtenim la igualtat desitjada: si tenim la mateixa dimensió com a $\mathbb{K}$-espais vectorials sobre $\mathbb{Q}$ i una de les inclusions, tenim igualtat. La resta de cossos s'obtenen igual.

Exemple 3.3.4. Sigui $\mathbb{K}$ 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[5]. Veiem, doncs, que:

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

[5] Bé, ja com a comentari, una arrel de la unitat no té per què ser arrel primitiva de la unitat; per exemple, l'arrel sisena de la unitat no és primitiva ja que no genera el conjunt d'arrels sisenes de la unitat.

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

$$\sigma: \begin{array}{ccc} \sqrt[3]{2} & \longmapsto & \rho\sqrt[3]{2} \\ \sqrt{-3} & \longmapsto & \sqrt{-3} \end{array} \qquad \tau: \begin{array}{ccc} \sqrt[3]{2} & \longmapsto & \sqrt[3]{2} \\ \sqrt{-3} & \longmapsto & -\sqrt{-3} \end{array}$$

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:

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

on hem usat que $\sigma^2(\sqrt[3]{2}) = \sigma(\rho)\sigma(\sqrt[3]{2}) = \rho^2\sqrt[3]{2}$. Del que acabem de fer veiem que $\sigma^3 = Id$, ja que σ^3 fixa els dos generadors. De manera semblant, podem calcular que $\sigma^2 = Id$ i $\sigma\tau = \tau\sigma^2$. Per tant,

$$\mathrm{Gal}(\mathbb{K}/\mathbb{F}) = \langle \sigma, \tau \;\big|\; \sigma^3 = 1, \tau^2 = 1, \sigma\tau = \tau\sigma^2 \rangle \simeq D_6 \simeq S_3.$$

L'únic grup de 6 elements que no és commutatiu. El diagrama de subgrups és el següent:

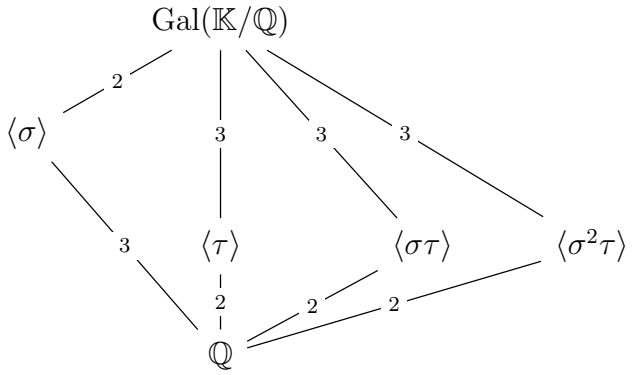


Figura 3.3: Diagrama de subgrups.

Pel teorema fonamental això ens dona el diagrama de subcossos de $\mathbb{K}$:

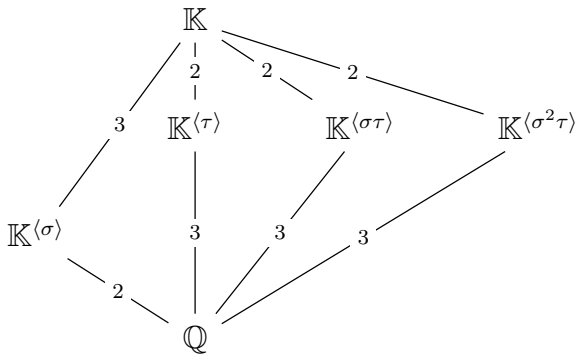


Figura 3.4: Diagrama de subcossos de $\mathbb{K}$. Cal tenir en compte que $\mathbb{K}^{\langle\tau\rangle} = \mathbb{Q}(\sqrt[3]{2})$, $\mathbb{K}^{\langle\sigma\tau\rangle} = \mathbb{Q}(\rho\sqrt[3]{2})$, $\mathbb{K}^{\langle\sigma^2\tau\rangle} = \mathbb{Q}(\rho^2\sqrt[3]{2})$ i $\mathbb{K}^{\langle\sigma\rangle} = \mathbb{Q}(\sqrt{-3})$.

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

Observació 3.3.5. Donat $f \in \mathbb{F}[x]$, volem identificar $\mathrm{Gal}(\mathbb{K}_f/\mathbb{F})$ com a grup. Observem que $\mathbb{K}_f$ és el cos de descomposició de manera que el podem posar com a $\mathbb{K}_f = \mathbb{F}(\alpha_1, \ldots, \alpha_n)$, on $\alpha = \{\alpha_1, \ldots, \alpha_n\}$ són les diferents arrels de f. Sigui σ un automorfisme de $\mathrm{Gal}(\mathbb{K}_f/\mathbb{F})$, tal que per a tot i existeix un j tal que $\sigma(\alpha_i) = \alpha_j$. Podem definir:

$$\begin{array}{ccc} \mathrm{Gal}(\mathbb{K}_f/\mathbb{F}) & \longrightarrow & S_n \\ \sigma & \longmapsto & \tilde{\sigma} \end{array} \qquad \text{on } \sigma(\alpha_i) = \alpha_{\tilde{\sigma}(i)}$$

és a dir, permutem els índexs de les arrels. Es pot veure fàcilment que és un morfisme de cossos injectiu. Per tant, el que fem és **identificar** $\mathrm{Gal}(\mathbb{K}_f/\mathbb{F})$ **com a subgrup de** S_n, llevat de conjugació.

Exemple 3.3.6.

1. Per a $\tilde{\sigma} = (1,2)$ i $\tilde{\tau} = (3,4)$, tenim $\mathrm{Gal}(\mathbb{K}_f/\mathbb{F}) = \langle(1,2)(3,4) \subset S_4$.
2. Per a $\tilde{\sigma} = (1,2,3)$ i $\tilde{\tau} = (2,3)$, tenim $\mathrm{Gal}(\mathbb{K}_f/\mathbb{F}) \simeq \langle(1,2,3)(2,3)\rangle = S_3$.

IV

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 4.1.1 (Cos finit)**.** 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 $\mathbb{F}_p$.

Observació 4.1.2. Si E és un espai vectorial sobre $\mathbb{F}$ de dimensió n, aleshores $E \simeq \mathbb{F}^n$ i podem posar un isomorfisme tal que $x \longmapsto (\lambda_1, \ldots, \lambda_n)$, on $(v_1, \ldots, v_n)$ és base de E. Per a tot $x \in E$, $x = \lambda_1 v_1 + \cdots + \lambda_n v_n$ tal que $\lambda_i \in E$ per a tot i.

Proposició 4.1.3. *Si $\mathbb{K}$ és un cos finit aleshores $|\mathbb{K}| = p^r$ per algun primer p i algun $r \in \mathbb{Z}_{\geq 1}$.*

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

$$\mathbb{K} = \left\{ a_1\alpha_1 + \cdots + a_r\alpha_r \;\middle|\; a_i \in \mathbb{F}_p \right\}$$

i per tant $|\mathbb{K}| = p^r$. ∎

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

Exemple 4.1.4. Sigui $x^2 + x + 1 \in \mathbb{F}_2[x]$ un irreductible, i posem $\mathbb{K} = \mathbb{F}_2[x]/(x^2 + x + 1)$ un cos[1] i, clarament, $[\mathbb{K} : \mathbb{F}_2] = 2$. Sigui α una arrel de $p(x)$; és a dir, $\alpha^2 + \alpha + 1 = 0$. Podem veure, per 1.2.16, que $\alpha(\alpha + 1) = \alpha^2 + \alpha$ que, en $\mathbb{F}_2$, és $\alpha + 1 + \alpha \equiv 1$. Per tant, una $\mathbb{F}_2$-base de $\mathbb{K}$ és $\{0, 1, \alpha, \alpha + 1\}$, però $K \not\simeq \mathbb{Z}/4\mathbb{Z}$ perquè no tenim cap element d'ordre 4, i $K \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. El cardinal $\#K$ és $4 = 2^2$.

Proposició 4.1.5. *Sigui p un nombre primer, $r \geq 1$. Posem $q = p^r$. Aleshores, existeix un cos de cardinal q. Tots els cossos de cardinal q són isomorfs.*

[1] Com $\mathbb{F}_2$ és DIP i $p(x) = x^2 + x + 1$ és irreductible, $(x^2 + x + 1)$ és ideal maximal i, per tant, $\mathbb{K}$ és un cos.

Demostració. Considerem $f = x^q - x \in \mathbb{F}_p[x]$. Com que $f' = qx^{q-1} - 1 = p^r x^{q-1} - 1 = -1$ tenim que $\mathrm{mcd}(f, f') = 1$; aleshores, f és separable i té q arrels diferents en un cos de descomposició. Sigui $\mathbb{K}$ un cos de descomposició de f. Aleshores $\mathbb{K}$ conté les q arrels de f, i de fet el conjunt d'aquestes arrels és un cos (volem veure, de fet, que $\mathbb{K} \subset \{\text{conjunt d'arrels de } f\}$). Per a veure-ho, hem de provar que si α, β són arrels de f aleshores $\alpha\beta, \frac{\alpha}{\beta}$ amb $\beta \neq 0, \alpha + \beta$ i $\alpha - \beta$ també ho són.

- Clarament si $\alpha^q = \alpha$ i $\beta^q = \beta$ tenim que $\alpha^q\beta^q$ i, com tenim commutativitat, $(\alpha\beta)^q = \alpha\beta$; és a dir, $\alpha\beta$ és arrel de f. De manera semblant es veu que α/β també n'és arrel: si $\beta \neq 0$, $\left(\frac{\alpha}{\beta}\right)^q = \frac{\alpha^q}{\beta^q} = \frac{\alpha}{\beta}$.
- Per a $\alpha + \beta$, com que $\mathbb{K}$ és de característica p per 1.2.16, apartat *2.*. Així doncs,

$$\begin{aligned}(\alpha+\beta)^p &= \alpha^p + \beta^p \\ (\alpha+\beta)^{p^2} &= \alpha^{p^2} + \beta^{p^2} \\ &\vdots \\ (\alpha+\beta)^q &= \alpha^q + \beta^q = \alpha + \beta\end{aligned}$$

  i, per tant, $\alpha + \beta$ també és arrel de f; de manera similar es veu $\alpha - \beta$:

$$(\alpha - \beta)^q = \alpha^q - \beta^q = \alpha - \beta.$$

Així doncs, $\mathbb{K}$ és el conjunt d'arrels de f i per tant $|\mathbb{K}| = q$.

D'altra banda, si $\mathbb{K}'$ és un altre cos de cardinal q, el grup multiplicatiu de $\mathbb{K}'$ té cardinal $q-1$ i tot $\alpha \in \mathbb{K}' \setminus \{0\}$ 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 $\mathbb{K}'$ són arrels de f i $\mathbb{K}'$ és doncs un cos de descomposició de f. Per tant, $\mathbb{K}' \simeq \mathbb{K}$ 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 4.1.6. *$\mathbb{F}_q/\mathbb{F}_p$ 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 (tota extensió de $\mathbb{F}_p$ és separable). ■

Proposició 4.1.7. *Tot subgrup finit G del grup multiplicatiu $\mathbb{F}^\times$ d'un cos $\mathbb{F}$ 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 $n_i > 1$ per tot i, i $n_1 \mid n_2 \mid \cdots \mid n_k$. Si prenem $g \in \mathbb{Z}/n_1\mathbb{Z}$ tenim que $\text{ord}(g) \mid n_1 \mid \cdots n_k$; si $g \in \mathbb{Z}/n_2\mathbb{Z}$, $\text{ord}(g) \mid n_2 \mid \cdots \mid n_k$ i així successivament. En efecte, tot element de g té doncs ordre dividint n_k, i per tant és arrel del polinomi $x^{n_k} - 1$; és a dir, $g^{n_k} = 1$. El polinomi $x^{n_k} - 1$ té $n_1 \cdots n_k$ arrels a $\mathbb{F}$; si $k > 1$, llavors com $n_i > 1$ per a tot i, i evidentment $n_1 \cdots n_k > n_k$, cosa que no pot ser. Per tant $k = 1$ i G és isomorf a $\mathbb{Z}/n_1\mathbb{Z}$, és cíclic. ■

Corol·lari 4.1.8. *$\mathbb{F}_q^\times$ és cíclic.*

Demostració. Si p és primer, $(\mathbb{Z}/p\mathbb{Z})^\times = \mathbb{F}_p^\times$ és cíclic. De fet, $\mathbb{F}_p^\times = \langle g \rangle$ per a algun $g \in \mathbb{F}_p$. Com $\mathbb{F}_q$ és $\mathbb{F}_{p^r}$, i p^r és finit, $\mathbb{F}_q$ també ho serà, i G serà finit i, en particular, cíclic per 4.1.7. ■

Exemple 4.1.9. Tenim que $\mathbb{F}_7^\times = \langle \overline{3} \rangle$. En efecte, fent les respectives potències de 3 obtenim cadascuna de les $p - 1 = 6$ classes d'equivalència que generen el grup multiplicatiu:

$$\mathbb{F}_7^\times = \{\overline{3}^0, \overline{3}^1, \overline{3}^2, \overline{3}^3, \overline{3}^4, \overline{3}^5\} = \{\overline{1}, \overline{3}, \overline{2}, \overline{6}, \overline{4}, \overline{5}\}.$$

Corol·lari 4.1.10. *$\mathbb{F}_q$ és simple. En particular, existeix un polinomi irreductible de grau r amb coeficients a $\mathbb{F}_p$. O, en altres paraules, $[\mathbb{F}_q : \mathbb{F}_p] = r$.*

Demostració. Si $\alpha \in \mathbb{F}_q$ és tal que $\mathbb{F}_q^\times = \{1, \alpha, \ldots, \alpha^{q-2}\}$ tenim que $\mathbb{F}_q = \mathbb{F}_p(\alpha)$, i $\text{Irr}(\alpha, \mathbb{F}_p)$; $\text{gr}(Irr(\alpha, \mathbb{F}_p)) = [\mathbb{F}_p(\alpha) : \mathbb{F}_p] = r$ i $\text{Irr}(\alpha, \mathbb{F}_p)$ és irreductible de grau r. ■

Definició 4.1.11 (automorfisme de Fröbenius)**.** L'automorfisme de Fröbenius (cf. l'exemple 1.2.16, apartat *3.*) és el següent:

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

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

Proposició 4.1.12. *$\text{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ és cíclic d'ordre r generat per Fr_p.*

Demostració. Com que $\mathbb{F}_q/\mathbb{F}_p$ és de Galois i i $[\mathbb{F}_q : \mathbb{F}_p] = r$ sabem que $|\text{Gal}(\mathbb{F}_q/\mathbb{F}_p)| = r$. Clarament $\text{Fr}_p^i(\alpha) = \alpha^{p^i}$ per a tot $i \geq 1$; en particular, $\text{Fr}_p^r(\alpha) = \alpha^{p^r} = \alpha^q = \alpha$ i per tant $\text{Fr}_p^r = Id$. 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 $\mathbb{F}_q$, contradicció. Per tant, Fr_p té ordre r i $\text{Gal}(\mathbb{F}_q/\mathbb{F}_r) = \langle \text{Fr}_p \rangle$. ■

Corol·lari 4.1.13. *$\mathbb{F}_q = \mathbb{F}_{p^r}$ conté $\mathbb{F}_{p^d}$ si, i només si, $d \mid r$.*

Demostració.

$\Rightarrow$ Pel teorema fonamental de la teoria de Galois els subcossos de $\mathbb{F}_q$ es corresponen amb els subgrups de $\text{Gal}(\mathbb{F}_q/\mathbb{F}_p) \simeq \mathbb{Z}/r\mathbb{Z}$, i la dimensió del subcòs sobre $\mathbb{F}_p$ coincideix amb l'índex del subgrup. Així doncs, $[\mathbb{F}_{p^d} : \mathbb{F}_p] = d \mid r = [\mathbb{F}_{p^r} : \mathbb{F}_p]$.

$\Leftarrow$ 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. ■

Exemple 4.1.14. Tenim que $\mathbb{F}_4 \subset \mathbb{F}_{16}$, ja que $2^2, 2^4$ compleixen $2 \mid 4$. No és el cas de $\mathbb{F}_8$ i $\mathbb{F}_{16}$, ja que per a $2^3, 2^4$ tenim $3 \nmid 4$ i, per tant, $\mathbb{F}_8 \not\subseteq \mathbb{F}_{16}$.

Proposició 4.1.15. *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 $x^{p^d} - x \in \mathbb{F}_p[x]$. Com que $\mathbb{F}_{p^d}$ és un cos de descomposició de $x^{p^d} - x$, conté totes les arrels de f i, en particular, una arrel α de f. Aleshores $\mathbb{F}_p(\alpha)$ és un subcòs de $\mathbb{F}_q$ de grau d i per 4.1.13 tenim que $[\mathbb{F}_p(\alpha) : \mathbb{F}_p] = d \mid r = [\mathbb{F}_q : \mathbb{F}_p]$. 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 $[\mathbb{F}_p(\alpha) : \mathbb{F}_p] = d$ tenim $\mathbb{F}_p(\alpha) \simeq \mathbb{F}_{p^d}$ i $\mathbb{F}_p(\alpha)$ és el cos de descomposició de $x^{p^d} - x$ (el conjunt d'arrels de $x^{p^d} - x$) i, per tant, α és arrel de $x^{p^d} - x$, amb la qual cosa veiem que $f \mid x^{p^d} - x$. Utilitzant que si $d \mid r$ el polinomi $x^{p^d} - x$ divideix $x^q - x$,[2] 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. ■

Lema 4.1.16. *$x^a - 1$ divideix $x^b - 1$ si, i només si, $a \mid b$.*

Demostració.

$\Rightarrow$ Suposem que $x^a - 1$ divideix $x^b - 1$. Volem veure que si posem $b = ac + r$ (per a certs c, r, tals que $r < a$), o bé $b - r = ac$ de manera equivalent, necessàriament $r = 0$. En efecte, si sumem i restem x^r tenim:

$$\begin{aligned} x^b - x^r + x^r - 1 = x^r(x^{b-r} - 1) + x^r - 1 = x^r((x^a)^c - 1) + x^r - 1 \\ = x^r(x^a - 1)((x^a)^{c-1} + \cdots + x^a + 1) + x^r - 1. \end{aligned} \tag{4.1}$$

En aquest moment, a grans trets, hem trobat que $(x^b - 1) = (x^a - 1)u + v$; però com $x^a - 1 \mid x^b - 1$, necessàriament $x^a - 1 \mid v = x^r - 1$. Per l'elecció d'a, és $r = 0$, com volíem veure.

$\Leftarrow$ Si $a \mid b$, aleshores $b = ca$, $c \geq 1$; per tant, podem aplicar un raonament semblant a (4.1) i, naturalment:

$$x^b - 1 = (x^a)^c - 1^c = (x^a - 1)((x^a)^{c-1} + \cdots + x^a + 1) \implies x^a - 1 \mid x^b - 1. \qquad ■$$

[2] Ambdós termes són divisibles per x, de manera que $x^{p^d} - x \mid x^{p^r} - x$ si, i només si, $x^{p^d-1} - 1 \mid x^{p^r-1} - 1$. Com que $x^n - 1 \mid x^m - 1 \iff n \mid m$ (cf. 4.1.16), tenim la següent cadena d'equivalències: $x^{p^d-1} - 1 \mid x^{p^r-1} - 1 \iff p^d - 1 \mid p^r - 1 \iff d \mid r$.

Exemple 4.1.17. Sigui $\mathbb{F}_i$ el cos de descomposició de $x^i - x$, prendrem els valors $i = 4, 8, 16$. Si descomposem aquests polinomis trobem el següent:

$$p(X) = X^4 - X = X(X-1)(X^2+X+1)$$
$$q(X) = X^8 - X = X(X-1)(X^3+X+1)(X^3+X^2+1)$$
$$r(X) = X^{16} - X = X(X-1)(X^2+X+1)(X^4+X^3+X^2+X+1)(X^4+X^3+1)(X^4+X+1)$$
$$= p(X)\cdot(X^4+X^3+X^2+X+1)(X^4+X^3+1)(X^4+X+1).$$

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 $\bigcup_{n\geq 1} \mathbb{F}_{p^n}$ és un cos que conté totes les extensions finites de $\mathbb{F}_p$.

Proposició 4.1.18. $\overline{\mathbb{F}}_p = \bigcup_{n\geq 1} \mathbb{F}_{p^n}$.

4.2 Cossos ciclotòmics

Definició 4.2.1 (Cos ciclotòmic)**.** El subcòs dels nombres complexos generat sobre $\mathbb{Q}$ per $\zeta_n = e^{\frac{2\pi i}{n}}$ (arrel n-èsima primitiva de 1, arrel de $x^n - 1$ d'ordre n) s'anomena cos ciclotòmic. 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-èsimes de la unitat, és a dir les arrels de $x^n - 1$. Sabem que:

$$\mu_n = \{\zeta_n^a : 0 \leq a \leq n-1\} \subset \mathbb{C}$$

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:

$$\chi : \begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} & \longrightarrow & \mu_n \\ a & \longmapsto & \zeta_n^a \end{array} \qquad \chi(\overline{a+b}) = \chi_n^{a+b} = \chi_n^a \chi_n^b = \chi(\overline{a})\chi(\overline{b})$$

Per tant, $\mu^n \leq \mathbb{C}^\times$ i μ_n és cíclic. 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-èsima de la unitat, i que és primitiva si, i només si, $(a, n) = 1$.

Definició 4.2.2 (Polinomi ciclotòmic)**.** El polinomi ciclotòmic n-èsim és el polinomi que té per arrels les arrels n-èsimes primitives de la unitat:

$$\Phi_n(x) = \prod_{\substack{1\leq a<n \\ (a,n)=1}} (x - \zeta_n^a)\,. \tag{4.2}$$

Proposició 4.2.3.

$$x^n - 1 = \prod_{d|n} \Phi_d(x). \tag{4.3}$$

Demostració. Com que les arrels de $x^n - 1$ són les arrels n-èsimes de la unitat i tota arrel n-èsima és primitiva d'ordre d per algun $d \mid n$ tenim (4.3). ■

Observació 4.2.4. Comparant graus, això ens dóna la identitat $n = \sum_{d|n} \varphi(d)$.

La fórmula (4.3) ens permet calcular alguns polinomis ciclotòmics de manera recurrent. També, per $n = p$ primer obtenim que $x^p - 1 = \Phi_1(x)\Phi_p(x) = (x-1)\Phi_p(x)$; en particular,

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

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.

Exemple 4.2.5. Prenem $\Phi_6(x)$. Aleshores, $x^6 - 1 = \Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_6(x) = (x-1)(x+1)(x^2+x+1)$. Per tant:

$$\Phi_6(x) = \frac{x^6 - 1}{(x-1)(x+1)(x^2+x+1)} = \frac{(x-1)(x^2+x+1)(x^3+1)}{(x-1)(x+1)(x^2+x+1)} = x^2 - x + 1.$$

Proposició 4.2.6. *$\Phi_n(x)$ 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 (4.3) tenim que $x^n - 1 = \Phi_n(x) \cdot f(x)$, on $f(x)$ és un polinomi mònic amb coeficients enters; de fet, és $\prod_{m|n} \Phi_m$. 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 4.2.7. *$\Phi_n(x)$ és irreductible a $\mathbb{Q}[x]$. En particular, $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$.*

Demostració. Pel Lema de Gauss n'hi ha prou veient que és irreductible a $\mathbb{Z}[x]$[3]. En particular, si no ho fos hi hauria una factorització:

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

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-èsima primitiva que sigui arrel de f, i sigui p un primer que no divideix n. Aleshores ζ^p també és una arrel n-èsima primitiva i per tant és arrel de $f(x)$ o de $g(x)$. Veiem que no pot ser arrel de $g(x)$.

[3] Tinguem en compte que $\Phi_n(x)$ és mònic i, per tant, té contingut 1: és primitiu; si és irreductible sobre $\mathbb{Z}[x]$, ho serà, doncs, sobre $\mathbb{Q}[x]$ i ja haurem acabat.

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:

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

com que $\overline{g}(x^p) = (\overline{g}(x))^p$ veiem que necessàriament $\overline{f}$ i $\overline{g}$ tenen un factor en comú, alguna arrel comuna, en $\overline{\mathbb{F}_p}$. Per tant, $\overline{\Phi}_n(x) = \overline{f}(x)\overline{g}(x)$ 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. Per tant, $\overline{\Phi}_n(x) \mid x^n - 1$; $x^n - 1$ és separable a $\mathbb{F}_p$ si $p \nmid n$ ($(\text{mcd}(nx^{n-1}, x^n - 1) = 1)$ 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 altres primers veiem que ζ^a és arrel de $f(x)$ per a tot $a = p_1 \cdots p_n$ amb $p_i \nmid n$. És a dir, per a tot a coprimer amb n, i per tant (cf. (4.2)) $f(x) = \Phi_n(x)$. ■

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-èsima 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, 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 4.2.8. *L'aplicació:*

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

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 sortida i 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 $\sigma_a\sigma_b(\zeta_n) = \sigma_a\left(\zeta_n^b\right) = \zeta_n^{ab}$. ■

Observació 4.2.9. Ho podríem haver fet amb la inversa, és a dir:

$$\begin{array}{rccc} \lambda: & \operatorname{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) & \longrightarrow & (\mathbb{Z}/n\mathbb{Z})^\times \\ & \sigma & \longmapsto & \lambda(\sigma) = \overline{a_\sigma} \end{array}$$

És un morfisme de grups si, i només si, $\lambda(\sigma_1\sigma_2) = \lambda(\sigma_1)\lambda(\sigma_2)$ i, en efecte,

$$\lambda(\sigma_1\sigma_2) = \overline{a_{\sigma_1\sigma_2}} = \overline{a_{\sigma_1}} \cdot \overline{a_{\sigma_2}} = \lambda(\sigma_1)\lambda(\sigma_2) \implies \sigma_1\sigma_2(\zeta_n) = \zeta_n^{\overline{a_{\sigma_1\sigma_2}}} = \sigma_1(\zeta_n^{\overline{a_{\sigma_2}}}) = \zeta_n^{\overline{a_{\sigma_1}a_{\sigma_2}}}.$$

A més, és injectiu, ja que si $\overline{a_{\sigma_1}} = \overline{a_{\sigma_2}}$ aleshores $\zeta_n^{\overline{a_{\sigma_1}}} = \zeta_n^{\overline{a_{\sigma_2}}}$. Com que $\zeta_n^{\overline{a_{\sigma_1}}} = \sigma_1(\zeta_n)$ i $\zeta_n^{\overline{a_{\sigma_2}}} = \sigma_2(\zeta_n)$ tenim $\sigma_1 = \sigma_2$, com volíem provar. Per últim, com que la cardinalitat del grup de Galois $\operatorname{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) = \varphi(n)$, que és la mateixa que la de $(\mathbb{Z}/n\mathbb{Z})^\times$, tenim un morfisme λ injectiu amb dos espais de la mateixa dimensió, λ és, efectivament, un isomorfisme.

Observació 4.2.10. Una extensió de Galois $\mathbb{K}/\mathbb{F}$ es diu abeliana si $\mathrm{Gal}(\mathbb{K}/\mathbb{F})$ és un grup abelià. Amb aquesta terminologia, $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ és doncs una extensió abeliana (ja que $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$ i $(\mathbb{Z}/n\mathbb{Z})^\times$ ho és).

Observació 4.2.11 (Conclusions)**.**

1. Hem vist que tot grup de la forma $(\mathbb{Z}/n\mathbb{Z})^\times$ és el grup de Galois d'una extensió $\mathbb{K}/\mathbb{Q}$.
2. El mateix és cert per a tot grup finit abelià: si G és un grup finit abelià, aleshores existeix una extensió de Galois $\mathbb{K}/\mathbb{Q}$ tal que $\mathrm{Gal}(\mathbb{K}/\mathbb{Q}) \simeq G$[4].
3. No se sap si el resultat és cert per a un grup finit qualsevol, és a dir, *que no sigui abelià.* Aquest és un problema obert i molt important, que s'anomena el Problema Invers de la Teoria de Galois[5].

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 4.2.12 (Teorema de Kronecker-Weber)**.** *Si $\mathbb{K}/\mathbb{Q}$ és una extensió abeliana aleshores $\mathbb{K}$ 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 $\mathbb{F}$ amb $[\mathbb{F} : \mathbb{Q}] < \infty$.

Observació 4.2.13 (Teorema xinès del residu, [Tra23])**.** De la definició de la funció φ d'Euler es dedueix immediatament que $\varphi(n)$ és l'ordre del grup dels elements invertibles de l'anell $\mathbb{Z}/n\mathbb{Z}$. El teorema xinès del residu ens diu que, si m, n, són dos nombres naturals tals que $\mathrm{mcd}(m, n) = 1$, el morfisme d'anells $\mathbb{Z} \longrightarrow (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$, donat per la reducció mòdul m en la primera coordenada i la reducció mòdul n en la segona, és exhaustiu i té nucli l'ideal $mn\mathbb{Z}$; per tant, obtenim un isomorfisme d'anells $\mathbb{Z}/mn\mathbb{Z} \simeq (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$. Aquest isomorfisme d'anells indueix un isomorfisme entre els grups dels elements invertibles dels dos anells; és a dir, un isomorfisme $(\mathbb{Z}/mn\mathbb{Z})^* \simeq ((\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z}))^*$; per tant, obtenim una igualtat entre els ordres d'aquests grups. Així doncs, $((\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z}))^* = (\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*$.

Proposició 4.2.14. *Siguin $m, n \geq 1$ nombres naturals primers entre si. Llavors, el producte $\zeta_m\zeta_n$ és una arrel primitiva mn-èsima de la unitat i se satisfan les igualtats $\mathbb{Q}(\zeta_m, \zeta_n) = \mathbb{Q}(\zeta_m\zeta_n) = \mathbb{Q}(\zeta_{mn})$ i $\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}$.*

[4] 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.

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

4.3

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 l'existència de cossos de descomposició de polimomis i en el Teorema Fonamental de la Teoria de Galois, 3.3.1, és d'Emil Artin, i utilitza els resultat següents de caire analític.

Lema 4.3.1. $\mathbb{R}$ *no té extensions algebraiques de grau senar no trivials.*

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

Lema 4.3.2. $\mathbb{C}$ *no té extensions quadràtiques.*

Demostració. Si $\mathbb{K}/\mathbb{C}$ amb $[\mathbb{K} : \mathbb{C}] = 2$, aleshores existeix $a \in \mathbb{C}$ tal que $\mathbb{K} = \mathbb{C}(\sqrt{a})$, però resulta que tot $a \in \mathbb{C}$ 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 i $\mathbb{K} = \mathbb{C}(\sqrt{a}) = \mathbb{C}$. ■

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

Teorema 4.3.4 (Teorema 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 $\overline{f}$ el polinomi obtingut a partir de f conjugant els coeficients. Fixem-nos que $g := f \cdot \overline{f}$ 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 $\overline{\alpha}$ 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 $\mathbb{K}$ un cos de descomposició de g sobre $\mathbb{R}$. Aleshores $\mathbb{K}(i)$ és una extensió de Galois de $\mathbb{R}$ (això és perquè és cos de descomposició de $g(x)(x^2+1)$). Posem $G = \mathrm{Gal}(\mathbb{K}(i)/\mathbb{R})$ i escrivim el cardinal de G com $|G| = 2^r \cdot m$ amb m senar (és a dir, $2 \nmid m$). Fixem-nos que $r \geq 1$ ja que $\mathbb{R} \subseteq \mathbb{C} \subseteq \mathbb{K}(i)$ i per tant $[\mathbb{C} : \mathbb{R}] \mid |G|$.

Sigui G_2 un 2-Sylow de G (és a dir, un 2-subgrup de G amb $|G_2| = 2^r$, l'existència del qual està garantida pel primer teorema de Sylow). Sigui $\mathbb{K}_2 = \mathbb{K}(i)^{G_2}$, de manera que $\mathrm{Gal}(\mathbb{K}(i)/\mathbb{K}_2) \simeq G_2$ per 3.2.6. Com que $[\mathbb{K}_2 : \mathbb{R}]$ és:

$$|G| = |\operatorname{Gal}(\mathbb{K}(i)/\mathbb{R})| = [\mathbb{K}(i) : \mathbb{R}] = 2^r \cdot m \implies \frac{|G|}{|G_2|} = m \implies \operatorname{Gal}(\mathbb{K}_2/\mathbb{R}) \simeq G/G_2$$

i m és senar, tenim que $\mathbb{K}_2 = \mathbb{R}$ per 4.3.1 ($\mathbb{R}$ no té extensions de grau senar m, $m > 1$, de manera que forçosament $[\mathbb{K}_2 : \mathbb{R}] = 1$). Així doncs veiem que $\mathrm{Gal}(\mathbb{K}(i)/\mathbb{R}) = 2^r$ i per tant $|\operatorname{Gal}(\mathbb{K}(i)/\mathbb{C})| = \frac{2^r}{2} = 2^{r-1}$. Si $r > 1$, aleshores tindríem que $|\operatorname{Gal}(\mathbb{K}(i)/\mathbb{C})| \geq 2$, $2^{r-2} \mid |G|$ i, per tant, existiria un subgrup $H \leq G$ amb $|H| = 2^{r-2}$; el cos fix $\mathbb{K}(i)^H$ tindria grau 2 sobre $\mathbb{C}$, cosa que per 4.3.2 no pot passar. Per tant $r = 1$, d'on veiem que $\mathbb{K}(i) = \mathbb{C}$ i en particular $\mathbb{K} \subseteq \mathbb{C}$. Això prova que totes les arrels de g viuen a $\mathbb{C}$, com volíem veure. ■

V

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, extensions i Teorema de Galois

L'objectiu és donar una caracterització dels polinomis $f(x) \in \mathbb{F}[x]$ 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 5.1.1 (Extensió radical)**.** Una extensió $\mathbb{K}/\mathbb{F}$ és radical si existeix una cadena de subcossos:

$$\mathbb{F} = \mathbb{K}_0 \subseteq \mathbb{K}_1 \subseteq \cdots \subseteq \mathbb{K}_{r-1} \subseteq \mathbb{K}_r = \mathbb{K}$$

amb $\mathbb{K}_{i+1} = \mathbb{K}_i\left(\sqrt[n_i]{a_i}\right)$ per a certs $a_i \in K_i$ i certs $n_i \geq 1$[1]. En aquest cas, diem que els elements de $\mathbb{K}$ es poden expressar per radicals.

Aquesta definició formalitza el concepte que un nombre es pugui escriure a partir d'elements del cos base realitzant operacions aritmètiques (suma, resta, producte i divisió) i extracció d'arrels.

Notació 5.1.2. Posarem $\mathbb{K}_{i+1} = \mathbb{K}_i(\alpha)$, on α és una arrel de $x^{n_i} - a_i$.

Exemple 5.1.3. 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 $\mathbb{K}$ amb una cadena de subcossos següent:

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{-5}) = K_1 \subseteq \mathbb{K}_1(\sqrt{3}) = \mathbb{K}_2 \subseteq \mathbb{K}_2\left(\sqrt[5]{2+\sqrt{3}}\right) = \mathbb{K}.$$

Definició 5.1.4 (Polinomi resoluble per radicals)**.** Diem que un polinomi $f \in \mathbb{F}[x]$ és resoluble per radicals si totes les seves arrels es poden expressar per radicals. Per tant, un polinomi $f \in \mathbb{F}[x]$ és resoluble per radicals si i només si existeix alguna extensió radical $L/\mathbb{F}$ on f descompongui completament.

Observació 5.1.5. Aquí cal anar en compte, perquè es podria pensar que f és resoluble per radicals si i només si el cos de descomposició $\mathbb{K}$ de f és radical sobre $\mathbb{F}$, però això no és cert: pot passar que $\mathbb{K}$ **no** sigui radical i que estigui contingut en un cos L que **sí** sigui radical.

[1] Recordem que $\mathbb{K}_{i+1} = \mathbb{K}_i\left(\sqrt[n_i]{a_i}\right)$ és una notació per denotar que $\mathbb{K}_{i+1} = \mathbb{K}_i(\alpha)$ amb α una arrel del polinomi $x^{n_i} - a_i$

Exemple 5.1.6. Per exemple, el polinomi $f(x) = x^3 - 3x + 1$ és irreductible; si denotem per α una arrel de f tenim que $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$, i resulta que $\mathbb{Q}(\alpha)$ és el cos de descomposició de f ja que es pot comprovar 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 algun $n \geq 2$ i algun $a \in \mathbb{Q}$. Però si això fos cert, tindríem que $\mathbb{Q}(\zeta_n) \subseteq \mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt[n]{a})$ i mirant graus això només és possible per $n = 2$, 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*.

Definició 5.1.7 (Grup de Galois, d'un polinomi)**.** Sigui $f \in \mathbb{F}[x]$ i sigui $\mathbb{K}$ un cos de descomposició de f. El grup de Galois d'un polinomi f és el grup de Galois de l'extensió $\mathbb{K}/\mathbb{F}$.

Observació 5.1.8. Fixem-nos que $\mathbb{K}/\mathbb{F}$ és una extensió de Galois: és normal per ser el cos de descomposició d'un polinomi, i és separable perquè estem assumint que $\mathbb{F}$ és perfecte.

Teorema 5.1.9 (de Galois)**.** *El polinomi $f(x)$ és resoluble per radicals si, i només si, el seu grup de Galois és resoluble.*

Observació 5.1.10.

- Recordem que un grup G és resoluble si existeix una cadena de 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[2]. Per això, i de cara a fer la demostració de 5.1.9 (que farem a la secció 5.3), primer haurem d'estudiar a la secció 5.2 les extensions amb grup de Galois cíclic.
- Abans, però, veurem algunes aplicacions del Teorema de Galois, 5.1.9. Recordem alguns exemples de grups resolubles i grups no resolubles:
  1. Tot grup abelià és resoluble.
  2. El grup diedral D_{2n} és resoluble.
  3. 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. Per a tot polinomi de grau n, el seu grup de Galois és un subgrup de S_n.

[2] 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.

5.1.1 Grup de Galois com a subgrups del grup simètric

Si $\mathbb{K}/\mathbb{F}$ és una extensió de Galois finita, aleshores $\mathbb{K} = \mathbb{F}(\alpha_1, \ldots, \alpha_n)$ on els α_i són les arrels d'un polinomi separable $f \in \mathbb{F}[x]$. Fixem-nos que tot $\sigma \in \mathrm{Gal}(\mathbb{K}/\mathbb{F})$ envia arrels de f a arrels de f. És a dir, cada $\sigma \in \mathrm{Gal}(\mathbb{K}/\mathbb{F})$ 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 $\mathrm{Gal}(\mathbb{K}/\mathbb{F}) \hookrightarrow S_n$, que ens permet identificar $\mathrm{Gal}(\mathbb{K}/\mathbb{F})$ com un subgrup del grup simètric S_n (permutacions de $\{\alpha_1, \ldots, \alpha_n\}$). 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 $\sigma \in \mathrm{Gal}(\mathbb{K}/\mathbb{F})$ tal que $\sigma(\alpha_i) = \alpha_j$, i per tant $\mathrm{Gal}(\mathbb{K}/\mathbb{F})$ vist com a subgrup de S_n és transitiu.

Definició 5.1.11 (Polinomi general de grau n). Siguin $x_1, x_2, \ldots, x_n$ indeterminades, i considerem el cos $\mathbb{F}(x_1, \ldots, x_n)$. El polinomi general de grau n és el polinomi:

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

És a dir, és el polinomi mònic que té per arrels $x_1, \ldots, x_n$. 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* (ho hem vist a Problemes):

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

Observació 5.1.12. $s_1, \ldots, s_n$ són polinòmicament independents; és a dir, no existeix $p(t_1, \ldots, t_n) \neq 0$ tal que $p(s_1, \ldots, s_n) = 0$.

Proposició 5.1.13. *Siguin $s_1, \ldots, s_n$ indeterminades. El polinomi general de grau n sobre el cos $\mathbb{F}(s_1, \ldots, s_n)$*

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

té grup de Galois isomorf a S_n.

Demostració. Fixem-nos que tenim una inclusió de cossos $\mathbb{F}(s_1, \ldots, s_n) \subseteq \mathbb{F}(x_1, \ldots, x_n)$, i que de fet l'extensió $\mathbb{F}(x_1, \ldots, x_n)/\mathbb{F}(s_1, \ldots, s_n)$ és de Galois ja que $\mathbb{F}(x_1, \ldots, x_n)$ és el cos de descomposició del polinomi (5.2). Tot $\sigma \in S_n$ dóna lloc a un automorfisme de $\mathbb{F}(x_1, \ldots, x_n)$ (l'acció és permutant les variables), i $\mathbb{F}(s_1, \ldots, s_n)$ és fixe per aquesta acció; és a dir, $\sigma(f) = f(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$ i, per a s_i, tenim $\sigma(s_i) = s_i$. Tenim, doncs, un morfisme injectiu:

$$S_n \hookrightarrow \mathrm{Gal}\left(\mathbb{F}(x_1, \ldots, x_n)/\mathbb{F}(s_1, \ldots, s_n)\right).$$

D'aquí veiem que, en particular:

$$[\mathbb{F}(x_1,\dots,x_n):\mathbb{F}(s_1,\dots,s_n)]\geq n!$$

D'altra banda, per 1.3.36 sabem que

$$[\mathbb{F}(x_1,\dots,x_n):\mathbb{F}(s_1,\dots,s_n)]\leq n!,$$

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

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

En particular, d'aquí en deduïm que $\mathbb{F}\left(x_1,\dots,x_n\right)^{S_n}=\mathbb{F}\left(s_1,\dots,s_n\right)$. És a dir, tota funció racional simètrica és una funció racional en els simètrics elementals.

A Problemes hem vist una propietat més forta: *tot polinomi simètric és un polinomi simètric en els simètrics elementals*[3]. 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. Per tant, podem partir d'indeterminades $s_1,\dots,s_n$ i considerar el polinomi general:

$$x^n-s_1x^{n-1}+s_2x^{n-2}+\cdots+(-1)^ns_n.$$

Si anomenem $x_1,\dots,x_n$ les arrels d'aquest polinomi (en un cos de descomposició), $(x-x_1)\cdots(x-x_n)$. Sabem que els $x_1,\dots,x_n$ són polinòmicament independents (cf. 5.1.12), de manera que $\prod_{\sigma\in S_n}p(t_{\sigma(1)},\dots,t_{\sigma(n)})$ un polinomi simètric diferent de zero que anul·la $x_1,\dots,x_n$; és a dir, són justament els s_i, els polinomis simètrics elementals en els x_i, amb la qual cosa hem demostrat el resultat que volíem. ■

Proposició 5.1.14. *Si $n\geq 5$ l'equació general de grau n no és resoluble per radicals.*

Demostració. 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 5.1.13, de 5.1.9 i del fet que S_n no és resoluble per $n\geq 5$, obtenim que tal fórmula no existeix per a graus ≥ 5. ■

5.1.2 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 $f\in\mathbb{F}[x]$ de grau ≥ 5 tals que les seves arrels es puguin expressar per radicals. Per exemple, les arrels del x^n-a clarament es poden expressar per radicals. El Teorema de Galois, 5.1.9, ens dóna un criteri per decidir quan això és possible i quan no. En canvi, hi ha polinomis amb grup de Galois no resoluble, i aquests no són resolubles per radicals.

[3] Vam veure que $F[s_1,\dots,s_n]^{S_n}=F[s_1,\dots,s_n]$, i això implica $F(s_1,\dots,s_n)^{S_n}=F(s_1,\dots,s_n)$, ja que una funció racional no és sinó un quocient de polinomis. A l'inrevés no tindríem per què; és a dir, partint d'una igualtat de funcions racionals, hauríem d'arribar a demostrar que aquesta es dona quan aquestes funcions racionals són exactament polinomis.

Lema 5.1.15. *Si σ és un cicle de longitud 5 a S_5 i τ és una transposició, aleshores $\langle \sigma, \tau \rangle = S_5$.*

Proposició 5.1.16. *Sigui $f(x) \in \mathbb{Q}[x]$ un polinomi irreductible de grau 5 amb tres arrels reals i dues arrels complexes no reals. El grup de Galois de f és S_5.*

Demostració. Posem $\mathbb{K} = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5) \subseteq \mathbb{C}$ el cos de descomposició de f, amb $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{R}$ i $\alpha_4, \alpha_5 \in \mathbb{C}\backslash\mathbb{R}$. Sabem que $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ és un subgrup de S_5 de cardinal divisible per 5. En particular, existeix algun element de S_5 d'ordre 5, que, de fet, és un cicle de longitud 5 (perquè, per exemple $\mathrm{Gal}(\mathbb{K}/\mathbb{Q}) \subset S_5$). Sigui $\tau \in \mathrm{Aut}(\mathbb{C}/\mathbb{Q})$ la conjugació complexa. La restricció $\tau_{|\mathbb{K}}$ de τ a $\mathbb{K}$ és un element de $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ 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[4]. ■

Exercici 5.1.17. *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 $f(1) = -13$), i 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 $f\left(\frac{-2}{\sqrt[4]{5}}\right) > 0$ i $f\left(\frac{2}{\sqrt[4]{5}}\right) < 0$. ■

5.2 Extensions cícliques

Definició 5.2.1 (Extensió cíclica)**.** Una extensió $\mathbb{K}/\mathbb{F}$ és cíclica si és de Galois i el seu grup de Galois és cíclic.

Notació 5.2.2. En aquesta secció n denota un nombre natural coprimer amb la característica de $\mathbb{F}$ (en particular, n pot ser qualsevol si $\mathbb{F}$ és de característica 0). Denotem per μ_n el conjunt de les arrels n-èsimes de la unitat (i.e. les arrels de $x^n - 1$) en una clausura algebraica $\overline{\mathbb{F}}$ de $\mathbb{F}$. Com que μ_n és un subgrup finit de $\overline{\mathbb{F}}^\times$ és cíclic, i als seus generadors els anomenem arrels n-èsimes primitives de la unitat. Si $a \in \mathbb{F}^\times$, denotem per $\sqrt[n]{a}$ una arrel qualsevol del polinomi $x^n - a$.

Proposició 5.2.3. *Si $\mathbb{F}$ conté les arrels n-èsimes de la unitat aleshores $\mathbb{F}(\sqrt[n]{a})/\mathbb{F}$ és cíclica de grau dividint n.*

Demostració. Les arrels de $x^n - a$ són de la forma $\{\zeta_n^k \sqrt[n]{a} \mid k = 0, \ldots, n\}$. Com que n és coprimer amb la característica de $\mathbb{F}$ ($\mathrm{car}(F) \nmid n$), el polinomi $x^n - a$ és separable i hi ha n arrels de la unitat. Sigui ζ_n una arrel n-èsima primitiva de la unitat. Aleshores els elements $\zeta_n^k \sqrt[n]{a}$ amb

[4] Hem d'usar 5.1.15. 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. I com que les transposicions generen el grup simètric, això ens dóna el resultat.

$k = 0, 1, \ldots, n-1$ són n arrels diferents de $x^n - a$ i per tant són totes. Això prova que $\mathbb{F}(\sqrt[n]{a})$ conté totes les arrels de $x^n - a$ i per tant és de Galois sobre $\mathbb{F}$ (o, en altres paraules, el cos de descomposició de $x^n - a$ sobre $\mathbb{F}$ és $\mathbb{F}(\sqrt[n]{a})$).

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

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

Com que:

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

l'aplicació $\sigma \longmapsto k_\sigma$ és un morfisme de grups i, clarament, és injectiu[5]. Podem dir, doncs, que realitza $\mathrm{Gal}(\mathbb{F}(\sqrt[n]{a})/\mathbb{F})$ com un subgrup de $\mathbb{Z}/n\mathbb{Z}$. En més detall, $\mathrm{Gal}(\mathbb{F}(\sqrt[n]{a})/\mathbb{F})$ és isomorf a un subgrup de $\mathbb{Z}/n\mathbb{Z}$ i tots els subgrups de $\mathbb{Z}/n\mathbb{Z}$ són cíclics de cardinal dividint n. ■

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 juga un paper important en algunes demostracions de la correspondència de Galois diferents de la que hem vist aquí).

Definició 5.2.4 (Caràcter d'un grup). Si G és un grup i $\mathbb{F}$ és un cos, un caràcter de G en $\mathbb{F}$ és un morfisme de grups $\chi : G \longrightarrow \mathbb{F}^\times$.

Exemple 5.2.5.

1. Posem $G = \mathbb{Z}/n\mathbb{Z}$ i $\mathbb{F} = \mathbb{Q}(\zeta_n)$, tal que $\chi : G \longrightarrow \mathbb{F}^\times$ i $a \longmapsto \zeta_n^a$; de manera que $\chi(a+b) = \zeta_n^{a+b} = \zeta_n^a \zeta_n^b = \chi(a)\chi(b)$.
2. Posem $\mathbb{K}/\mathbb{F}$ Galois i $\sigma \in \mathrm{Gal}(\mathbb{K}/\mathbb{F})$, de manera que $\sigma : \mathbb{K}^\times \longrightarrow \mathbb{K}^\times$ és un morfisme de grups i σ és un caràcter de $G := \mathbb{K}^\times$ en $\mathbb{K}$. Sigui $A_p = (G, \mathbb{F}) := \{\text{aplicacions de } G \text{ en } F\}$; podem comprovar que, de fet, A_p és un $\mathbb{F}$-espai vectorial. En efecte, si tenim $\varphi_1, \varphi_2 : G \longrightarrow \mathbb{F}$, aleshores $(\varphi_1 + \varphi_2)(g) := \varphi_1(g) + \varphi_2(g)$ (és la suma a $\mathbb{F}$) i $(\lambda\varphi)(g) := \lambda\varphi(g)$ (és el producte a $\mathbb{F}$). El caràcter és un χ tal que $\chi \in A_p(G, F)$.

Teorema 5.2.6 (Independència lineal de caràcters). *Sigui G un grup i siguin $\chi_1, \ldots, \chi_n : G \longrightarrow \mathbb{F}^\times$ caràcters de G. Si els χ_i són diferents entre ells, aleshores són $\mathbb{F}$-linealment independents.*

Demostració. Volem veure que si $\alpha_1, \ldots, \alpha_n \in \mathbb{F}$ 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 $g' \in G$

[5] Per si no s'acaba de veure, si $k_\sigma = 0$, aleshores $\sigma(\sqrt[n]{a}) = \sqrt[n]{a}$ i σ és la identitat, com volíem.

tal que $\chi_1(g') \neq \chi_n(g')$. Ara multipliquem (5.3) per $\chi_n(g')$:

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

Escrivim (5.3) per gg' i utilitzant que $\chi_i(gg') = \chi_i(g)\chi_i(g')$ tenim:

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

Restant (5.5) i (5.4) tenim que

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

Això és una relació de dependència lineal de $\chi_1, \ldots, \chi_{n-1}$ i per inducció tots els coeficients han de ser 0. En particular, aplicant la hipòtesi d'inducció tenim $\alpha_1(\chi_1(g') - \chi_n(g')) = 0$ 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 5.2.7 (Norma)**.** Si $\mathbb{K}/\mathbb{F}$ és una extensió de Galois definim la norma d'un element $\alpha \in \mathbb{K}$ com:

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

Proposició 5.2.8. *$N_{\mathbb{K}/\mathbb{F}}(\alpha)$ pertany a $\mathbb{F}$ i l'aplicació $N_{\mathbb{K}/\mathbb{F}} : \mathbb{K}^\times \longrightarrow \mathbb{F}^\times$ és un morfisme de grups. Si $\beta \in \mathbb{K}^*$ i $\sigma \in \mathrm{Gal}(\mathbb{K}/\mathbb{F})$, aleshores $N_{\mathbb{K}/\mathbb{F}}(\frac{\beta}{\sigma(\beta)}) = 1$.*

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

Teorema 5.2.9 (Teorema 90 de Hilbert)**.** *Sigui $\mathbb{K}/\mathbb{F}$ una extensió cíclica amb $\mathrm{Gal}(\mathbb{K}/\mathbb{F}) = \langle\sigma\rangle$. Un element $\alpha \in \mathbb{K}^\times$ té norma 1 si, i només si, existeix $\beta \in \mathbb{K}^\times$ tal que $\alpha = \beta/\sigma(\beta)$.*

Demostració. És fàcil veure que si $\alpha = \beta/\sigma(\beta)$ aleshores $N_{\mathbb{K}/\mathbb{F}}(\alpha) = 1$. Sigui ara $\alpha \in \mathbb{K}$ (a classe hem dit, de fet, que $\alpha \in \mathbb{K}^*$) de norma 1, és a dir, tal que:

$$\alpha \cdot \sigma(\alpha) \cdot \sigma^2(\alpha) \cdots \sigma^{n-1}(\alpha) = 1, \tag{5.6}$$

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

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

és una aplicació $\chi : \mathbb{K} \longrightarrow \mathbb{K}$ no nul·la. Aleshores, existeix un $\gamma \in \mathbb{K}$ 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 (5.6) es comprova que $\alpha \cdot \sigma(\beta) = \beta$,

$$\begin{aligned}
\beta &= \gamma + \alpha\sigma(\gamma) + \alpha\sigma(\alpha)\sigma^2(\gamma) + \cdots + \alpha\sigma(\alpha)\cdots\sigma^{n-2}(\alpha)\sigma^{n-1}(\gamma).\\
\sigma(\beta) &= \sigma(\gamma) + \sigma(\alpha)\sigma^2(\gamma) + \sigma(\alpha)\sigma^2(\alpha)\sigma^3(\gamma) + \cdots + \sigma(\alpha)\sigma^2(\alpha)\cdots\sigma^{n-1}(\alpha)\underbrace{\sigma^n(\gamma)}_{\gamma}.\\
\alpha\sigma(\beta) &= \alpha\sigma(\gamma) + \alpha\sigma(\alpha)\sigma^2(\gamma) + \alpha\sigma(\alpha)\sigma^2(\alpha)\sigma^3(\gamma) + \cdots + \underbrace{\alpha\sigma(\alpha)\sigma^2(\alpha)\cdots\sigma^{n-1}(\alpha)\gamma}_{1}.\\
&= \gamma + \alpha\sigma(\gamma) + \alpha\sigma(\alpha)\sigma^2(\gamma) + \cdots + \underbrace{\alpha\sigma(\alpha)\cdots\sigma^{n-2}(\alpha)\sigma^{n-1}(\gamma)}_{\beta}.
\end{aligned}$$

De manera que $\alpha = \frac{\beta}{\sigma(\beta)}$ com volíem provar. ■

Corol·lari 5.2.10. *Si $\mathbb{K}/\mathbb{F}$ és cíclica de grau n i $\mu_n \subseteq \mathbb{F}$ aleshores $\mathbb{K} = \mathbb{F}(\sqrt[n]{a})$ per algun $a \in \mathbb{F}$.*

Demostració. Sigui σ un generador del grup de Galois, $\mathrm{Gal}(\mathbb{K}/\mathbb{F}) = \langle\sigma\rangle$, i sigui $\zeta_n \in \mathbb{F}$ una arrel n-èsima primitiva de la unitat. Com que ζ_n té norma 1, ja que $N_{\mathbb{K}/\mathbb{F}}(\zeta_n) = \zeta_n^n = 1$ (i $\sigma(\zeta_n) = \zeta_n$, per a tot $\sigma \in \mathrm{Gal}(\mathbb{K}/\mathbb{F})$), pel Teorema 90 de Hilbert, 5.2.9, tenim que existeix $\beta \in \mathbb{K}$ amb $\zeta_n = \frac{\beta}{\sigma(\beta)} \iff 1 = \frac{\beta^n}{(\sigma(\beta))^n}$. Ara el nostre objectiu és provar que $\mathbb{K} = \mathbb{F}(\sqrt[n]{a})$. Com que

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

veiem que $\beta^n \in \mathbb{K}^{\langle\sigma\rangle} = \mathbb{F}$, ja que $\sigma(\beta^n) = \beta^n$. Posem $a = \beta^n \in \mathbb{F}$, de manera que $\sqrt[n]{a} = \beta$. Com que $\sigma(\beta) = \beta\zeta_n^{-1}$, $\sigma^2(\sqrt[n]{a}) = \sigma(\beta)\sigma(\zeta_n^{-1}) = \beta\zeta_n^{-2}$, i σ fixa ζ_n, veiem que:

$$\sigma^i(\sqrt[n]{a}) = \sqrt[n]{a}\zeta_n^{-i} \iff \sigma(\sqrt[n]{a}) \neq \sqrt[n]{a},\ \forall i = 1, \ldots, n-1.$$

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

Exemple 5.2.11 (Ternes pitagòriques)**.** Posem $X^2+Y^2 = Z^2$, per a valors $X, Y, Z \in \mathbb{Z}$. Exemples d'aquestes ternes són $(3,4,5), (7,24,25)$, i n'hi ha infinites. (X,Y,Z) és una solució de $X^2+Y^2+Z^2$ amb $X,Y,Z \in \mathbb{Z}$. Si passem Z^2 dividint, tenim que $(\frac{X}{Z})^2 + (\frac{Y}{Z})^2 = 1$ i $(\frac{X}{Z}, \frac{Y}{Z})$ és una solució racional de $X^2+Y^2 = 1$. Si $a, b \in \mathbb{Q}$, tal que $a^2+b^2 = 1$, tenim que $a = \frac{X}{Z}$ i $b = \frac{Y}{Z}$, $X, Y, Z \in \mathbb{Z}$, de manera que $(\frac{X}{Z})^2 + (\frac{Y}{Z})^2 = 1$ i, equivalentment, $X^2+Y^2 = Z^2$. D'aquesta manera, (X,Y,Z) tal com hem definit és una terna pitagòrica.

Proposició 5.2.12. *Si $a, b \in \mathbb{Q}$ amb $a^2+b^2 = 1$, aleshores existeixen $c, d \in \mathbb{Z}$ tals que:*

$$(a,b) = \left(\frac{c^2-d^2}{c^2+d^2}, \frac{2cd}{c^2+d^2}\right).$$

Demostració. $\mathbb{Q}(i)\mathbb{Q}$ és cíclica, $\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q}) = \langle\sigma\rangle$, de manera que σ envia $a+bi$ al seu conjugat, $a-bi$, i la norma d'un element $N(a+bi) = (a+bi)(a-bi) = a^2+b^2 = 1$ i, pel teorema 90 de

Hilbert 5.2.9, existeixen $c, d \in \mathbb{Z}$ tals que:

$$a + bi = \frac{c+di}{c-di} = \underbrace{\frac{c^2-d^2}{c^2+d^2}}_{a} + i\,\underbrace{\frac{2cd}{c^2+d^2}}_{b},$$

és a dir, totes les solucions de $X^2+Y^2 = Z^2$ amb $X, Y, Z \in \mathbb{Z}$ són de la forma $(c^2-d^2, 2cd, c^2+d^2)$, però així no les tenim totes (són úniques llevat de multiplicació per escalar), de manera que, ara sí, $(kc^2 - kd^2, 2kcd, kc^2 + kd^2)$ amb $k, c, d \in \mathbb{Z}$ són totes les solucions de l'equació. ■

5.3 Extensions radicals

Lema 5.3.1. *La composició d'extensions radicals és radical. És a dir, si tenim $\mathbb{K}/\mathbb{F}$ i $\mathbb{K}'/\mathbb{F}$ dues extensions radicals, aleshores $\mathbb{K}\cdot\mathbb{K}'/\mathbb{F}$ és radical.*

Demostració. Suposem que $\mathbb{K}/\mathbb{F}$ i $\mathbb{K}'/\mathbb{F}$ són radicals. Si

$$\mathbb{F} = \mathbb{K}_0 \subseteq \mathbb{K}_1 \subseteq \cdots \subseteq \mathbb{K}_{r-1} \subseteq \mathbb{K}_r = \mathbb{K},\ \mathbb{K}_{i+1} = \mathbb{K}_i(\sqrt[n_i]{a_i})$$
$$\mathbb{F} = \mathbb{K}'_0 \subseteq \mathbb{K}'_1 \subseteq \cdots \subseteq \mathbb{K}'_{r-1} \subseteq \mathbb{K}'_r = \mathbb{K}',\ \mathbb{K}'_{i+1} = \mathbb{K}'_i(\sqrt[n_i]{a_i}).$$

és una torre d'extensions radicals simples per $\mathbb{K}$ (resp., per $\mathbb{K}'$):

$$\mathbb{K}' = \mathbb{K}'\mathbb{K}_0 \subseteq \mathbb{K}'\mathbb{K}_1 \subseteq \cdots \subseteq \mathbb{K}'\mathbb{K}_{r-1} \subseteq \mathbb{K}'\mathbb{K}_r = \mathbb{K}'\mathbb{K},\ \mathbb{K}_{i+1}\mathbb{K}' = \mathbb{K}_i\mathbb{K}'(\sqrt[n_i]{a_i}).$$

és una torre d'extensions radicals simples per $\mathbb{K}'\mathbb{K}/\mathbb{K}'$. Ajuntant-la amb una torre d'extensions radicals simples per $\mathbb{K}'/\mathbb{K}$ obtenim el resultat. ■

Demostració de 5.1.9.

⇒ Posem $\mathbb{K}$ el cos de descomposició de f. Siguin $\alpha_1, \ldots, \alpha_n$ les arrels de f en $\mathbb{K}$, de manera que $\mathbb{K} = \mathbb{F}(\alpha_1, \ldots, \alpha_n)$, i $\mathbb{K}/\mathbb{F}$ és Galois.
Suposem en primer lloc que $f(x)$ és resoluble per radicals. Aleshores $\mathbb{K}$ està contingut en un cos $\tilde{\mathbb{L}}$ amb la propietat que $\tilde{\mathbb{L}}/\mathbb{F}$ és radical (però, a priori, no té per què ser Galois). Sigui $\mathbb{L}$ la clausura normal de $\tilde{\mathbb{L}}$ sobre $\mathbb{F}$, de manera que $\mathbb{L}/\mathbb{F}$ és Galois. Volem veure que $\mathbb{L}/\mathbb{F}$ és, també, radical.

1. Tenim que $\mathbb{L}$ és la composició dels cossos $\sigma(\tilde{\mathbb{L}})$ amb $\sigma \in \mathrm{Gal}(\mathbb{L}/\mathbb{F})$, és a dir:

$$\mathbb{L} = \prod_{\sigma\in\mathrm{Gal}(\mathbb{K}/\mathbb{F})} \sigma(\tilde{\mathbb{L}}).$$

⊇ Com que $\mathbb{L} \supset \tilde{\mathbb{L}}$, aleshores $\mathbb{L} = \sigma(\mathbb{L}) \supset \sigma(\tilde{\mathbb{L}})$.

$\subseteq$ D'altra banda, posant $\mathbb{L}' = \prod_{\sigma\in\mathrm{Gal}(\mathbb{K}/\mathbb{F})} \sigma(\tilde{L})$, aleshores $\mathbb{L}' \subset \mathbb{L}$ i $\mathbb{L}'/\mathbb{F}$ és normal i definim $\tau : \mathbb{L}' \longrightarrow \mathbb{L}'$. Es dona que $\tau \in \mathrm{Gal}(\mathbb{L}/\mathbb{F})$, i podem arribar a la següent cadena d'igualtats:

$$\mathbb{L}' = \tau(\mathbb{L}') = \tau\left(\prod_{\sigma\in\mathrm{Gal}(\mathbb{K}/\mathbb{F})} \sigma(\tilde{\mathbb{L}})\right) = \prod_{\sigma\in\mathrm{Gal}(\mathbb{L}/\mathbb{F})} \tau\sigma(\tilde{\mathbb{L}}) = \mathbb{L}'.$$

I és fàcil veure que si $\tilde{\mathbb{L}}/\mathbb{F}$ és radical aleshores $\sigma(\tilde{\mathbb{L}})/\mathbb{F}$ també és radical: si

$$\mathbb{F} = \tilde{\mathbb{L}}_0 \subseteq \tilde{\mathbb{L}}_1 \subseteq \cdots \subseteq \tilde{\mathbb{L}}_{r-1} \subseteq \tilde{\mathbb{L}}_r = \tilde{\mathbb{L}},$$

amb $\tilde{\mathbb{L}}_{i+1} = \tilde{\mathbb{L}}_i\left(\sqrt[n_i]{a_i}\right)$, aleshores

$$\mathbb{F} = \sigma(\tilde{\mathbb{L}}_0) \subseteq \sigma(\tilde{\mathbb{L}}_1) \subseteq \cdots \subseteq \sigma(\tilde{\mathbb{L}}_{r-1}) \subseteq \sigma(\tilde{\mathbb{L}}_r) = \sigma(\tilde{\mathbb{L}}) = \mathbb{L},$$

amb $\sigma(\tilde{\mathbb{L}}_{i+1}) = \sigma(\tilde{\mathbb{L}}_i)(\sqrt[n_i]{\sigma(a_i)})$.

2. Com que la composició d'extensions radicals és radical, veiem que $\mathbb{L}/\mathbb{F}$ és radical. És a dir que existeix:

$$\mathbb{F} = \mathbb{L}_0 \subseteq \mathbb{L}_1 \subseteq \cdots \subseteq \mathbb{L}_{r-1} \subseteq \mathbb{L}_r = \mathbb{L} \tag{5.7}$$

amb $\mathbb{L}_{i+1} = L_i\left(\sqrt[n_i]{a_i}\right)$ per a certs $a_i \in \mathbb{L}_i$ i certs $n_i \geq 1$.

Posem $m = n_0 \cdot n_1 \cdots n_{r-1}$ i considerem $\mathbb{L}(\zeta_m)/\mathbb{F}(\zeta_m)$ que també és de Galois. Fixem-nos que adjuntant ζ_m als subcossos de (5.7) obtenim:

$$\mathbb{F}(\zeta_m) = \mathbb{L}_0(\zeta_m) \subseteq \mathbb{L}_1(m) \subseteq \cdots \subseteq \mathbb{L}_{r-1}(\zeta_m) \subseteq \mathbb{L}_r(m) = \mathbb{L}(\zeta_m).$$

Per 5.2.3 cada extensió $\mathbb{L}_{i+1}(\zeta_m)/\mathbb{L}_i(\zeta_m)$ és cíclica de grau dividint n_i. Posem G_i com $\mathrm{Gal}(\mathbb{L}(\zeta_m)/\mathbb{L}_i(\zeta_m))$, de manera que tenim:

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

Fixem-nos que tenim una aplicació exhaustiva

$$\begin{array}{ccc} G_i = \mathrm{Gal}\left(\mathbb{L}(\zeta_m)/\mathbb{L}_i(\zeta_m)\right) & \longrightarrow & \mathrm{Gal}\left(\mathbb{L}_{i+1}(\zeta_m)/\mathbb{L}_i(\zeta_m)\right) \\ \sigma & \longmapsto & \sigma_{|\mathbb{L}_{i+1}(\zeta_m)} \end{array}$$

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

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

amb nucli $\mathrm{Gal}\left(\mathbb{L}(\zeta_m)/\mathbb{F}(\zeta_m)\right)$. Acabem de veure que $\mathrm{Gal}\left(\mathbb{L}(\zeta_m)/\mathbb{F}(\zeta_m)\right)$ és resoluble, i $\mathrm{Gal}\left(\mathbb{F}(\zeta_m)/\mathbb{F}\right)$ és abelià (hi ha un morfisme de grups injectiu $\mathrm{Gal}\left(\mathbb{F}(\zeta_m)/\mathbb{F}\right) \longrightarrow (\mathbb{Z}/m\mathbb{Z})^\times$ donat per $\sigma \longmapsto \sigma_k$ 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 $\mathrm{Gal}\,(\mathbb{L}(\zeta_m)/\mathbb{F})$ és resoluble. Finalment, tenim un morfisme exhaustiu:

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

que mostra que $\mathrm{Gal}(\mathbb{K}/\mathbb{F})$ 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 $\mathrm{Gal}(\mathbb{K}/\mathbb{F})$ és resoluble.

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

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

amb G_i/G_{i+1} cíclic. Posant $\mathbb{K}_i = \mathbb{K}^{G_i}$, $m = n_0 \cdots n_r$, tenim una torre de subcossos:

$$\mathbb{F} = \mathbb{K}_0 \subseteq \mathbb{K}_1 \subseteq \cdots \subseteq \mathbb{K}_{r-1} \subseteq \mathbb{K}_r = \mathbb{K},$$

on $\mathrm{Gal}(\mathbb{K}_{i+1}/\mathbb{K}_i) \simeq G_i/G_{i+1}$ és cíclica d'ordre n_i. Sigui $\mathbb{F}'$ el cos obtingut adjuntant totes les arrels de la unitat d'ordre n_i; és a dir, $\mathbb{F}' = \mathbb{F}(\zeta_m)$, i considerem:

$$\mathbb{F} \subseteq \mathbb{F}' = \mathbb{F}'\mathbb{K}_0 \subseteq \mathbb{F}'\mathbb{K}_1 \subseteq \cdots \subseteq \mathbb{F}'\mathbb{K}_{r-1} \subseteq \mathbb{F}'\mathbb{K}_r = \mathbb{F}'\mathbb{K}.$$

La restricció dóna lloc a un morfisme de grups, on $\mathrm{Gal}\,(K_{i+1}/K_i)$ és cíclic:

$$\mathrm{Gal}\,(\mathbb{F}'K_{i+1}/\mathbb{F}'K_i) \longrightarrow \mathrm{Gal}\,(\mathbb{K}_{i+1}/\mathbb{K}_i)$$

que és injectiu: en efecte, si σ és del nucli aleshores fixa $\mathbb{F}'$ i K_{i+1} i, per tant, fixa $\mathbb{F}'K_{i+1}$. Així doncs $\mathrm{Gal}\,(\mathbb{F}'K_{i+1}/\mathbb{F}'K_i)$ és cíclic d'ordre dividint n_i i per 5.2.3 és radical simple, és a dir, $\mathbb{F}'\mathbb{K}_{i+1} = \mathbb{F}'\mathbb{K}_i(\sqrt[n_i]{a_i})$. Com que $\mathbb{F}'/\mathbb{F}$ també és radical tenim que $\mathbb{F}'\mathbb{K}/\mathbb{F}$ és radical. Com que totes les arrels de f viuen a $\mathbb{F}'\mathbb{K} \supseteq \mathbb{K}_f$, aleshores f és resoluble per radicals. ■

A

Més aplicacions de la Teoria de Galois

A.1 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.

Exemple A.1.1.

- Trisecció d'angles: És possible trisecar un angle qualsevol només amb regle i compàs?[1].
- 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:

1. Si dos punts estan construïts, podem traçar la recta que els uneix. Aquesta recta la considerarem construïda.
2. 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.
3. Els punts d'intersecció de rectes i cercles construïts també els considerarem construïts.

A partir d'aquestes construccions bàsiques, en podem fer d'altres. 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 A.1 si $P \in L$ és el de la figura A.2.

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.
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.

[1] 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.

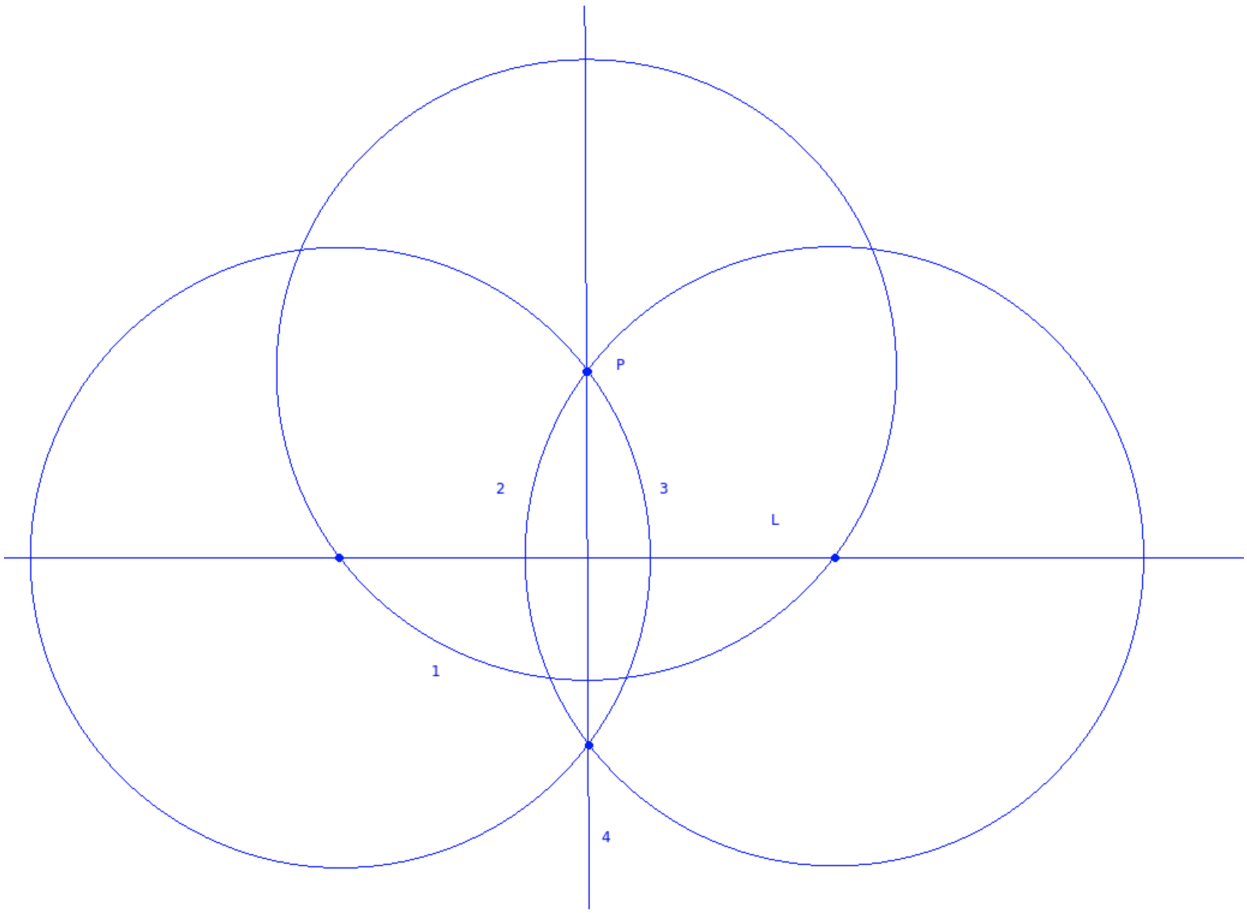


Figura A.1: Recta perpendicular a L que passa per P quan $P \notin L$. Els nombres indiquen l'ordre amb què cal construir cada element.

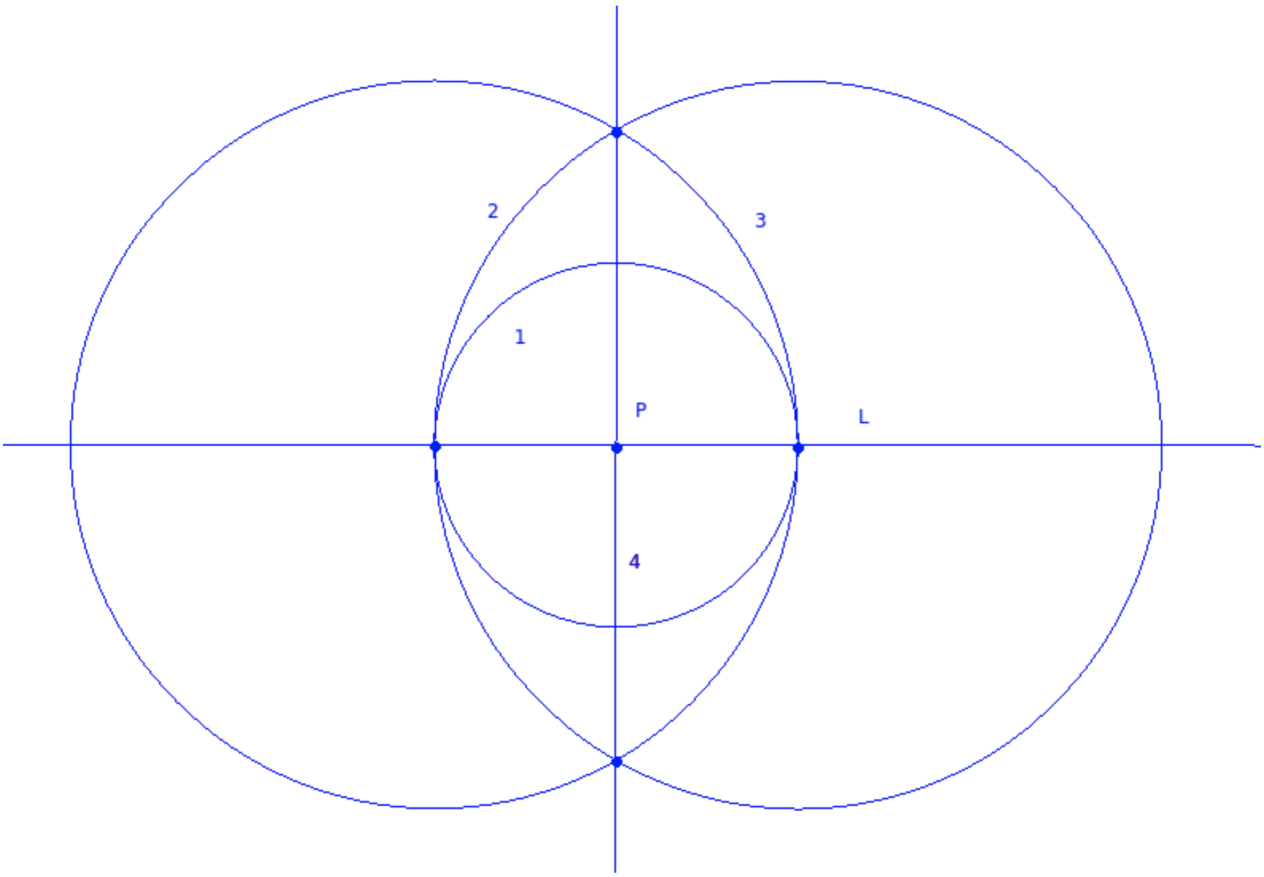


Figura A.2: Recta perpendicular a L que passa per p quan $P \in L$.

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 A.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.

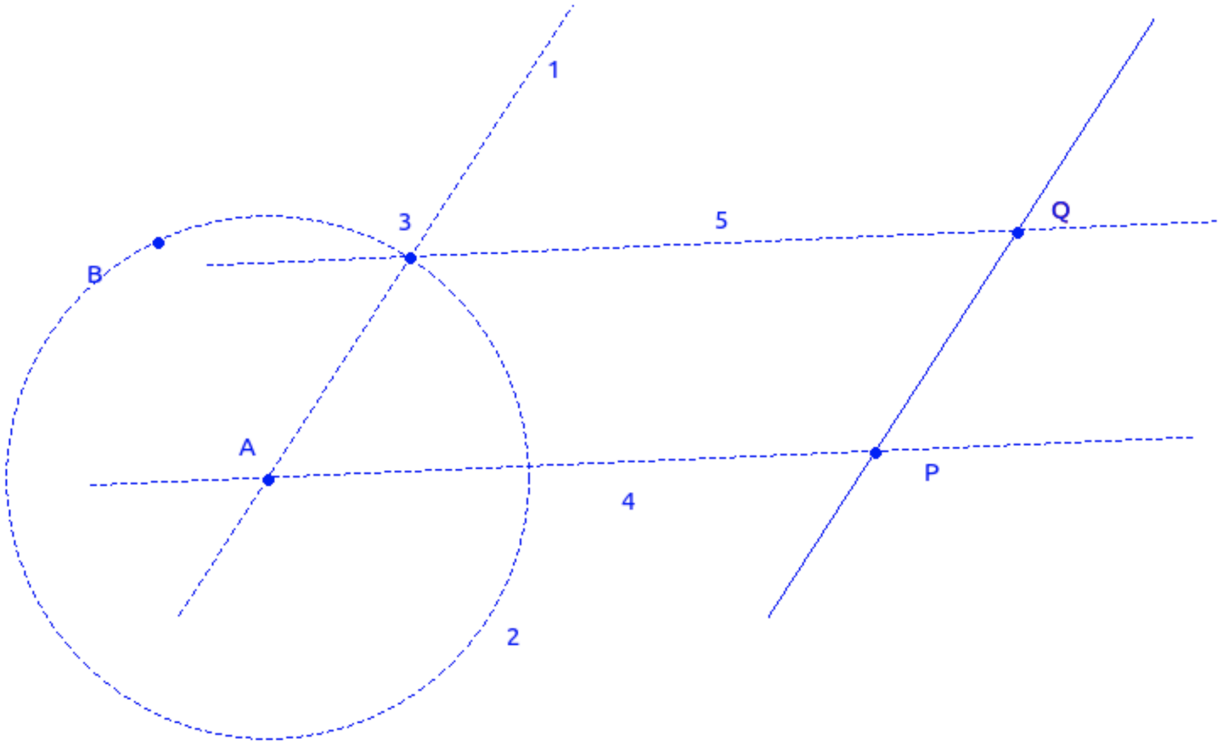


Figura A.3: Donat $P \in L$ i dos punts A i B construïts, construcció de $Q \in L$ tal que $d(P,Q) = d(A,B)$.

Definició A.1.2 (Nombre real construïble)**.** Un nombre real a diem que és construïble si podem construir dos punts a distància $|a|$.

Proposició A.1.3. *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 A.1.4. *El conjunt de nombres reals construïbles és un subcòs de $\mathbb{R}$.*

Demostració. Cal veure que si a i b són construïbles, aleshores també ho són $a+b, a-b, ab$ i $\frac{a}{b}$ (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 A.4 i A.5. ■

Proposició A.1.5. *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 A.7a. Sabem que l'angle que veu el diàmetre és un angle recte[2]. Si tracem la perpendicular al diàmetre que passa per l'angle recte dividim el triangle en dos triangles que són semblants (cf. figura A.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 $h = \sqrt{a}$. ■

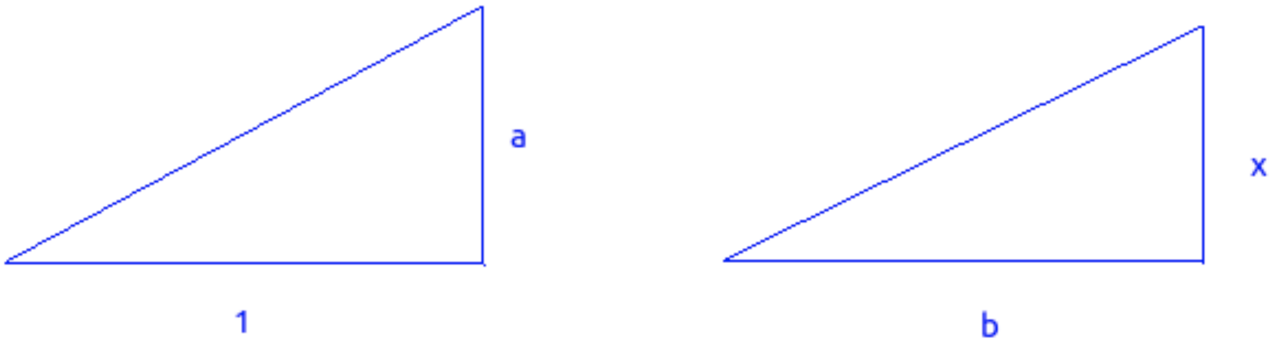


Figura A.4: Per semblança, tenim que $x = ab$.

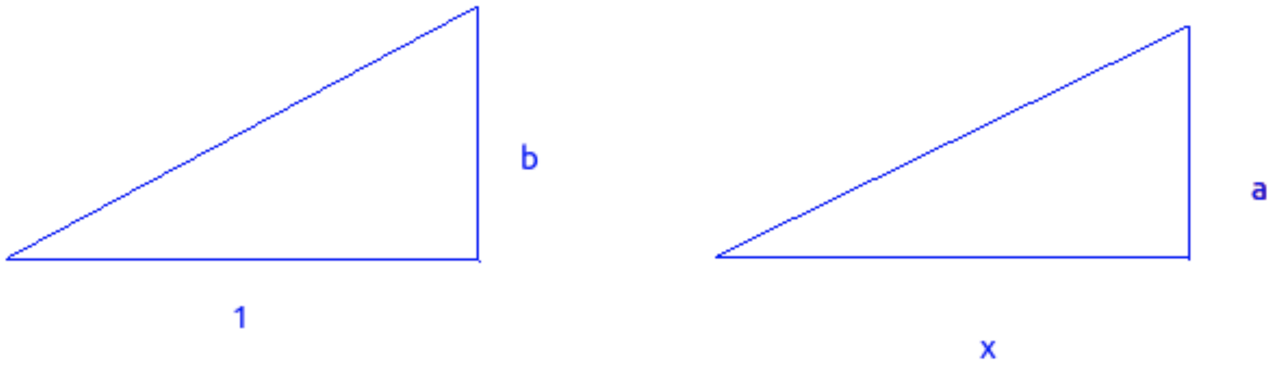


Figura A.5: Per semblança, tenim que $x = a/b$.

[2] Això és un teorema de geometria bàsica, una demostració la veiem a la figura A.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 $e + h = 90°$.

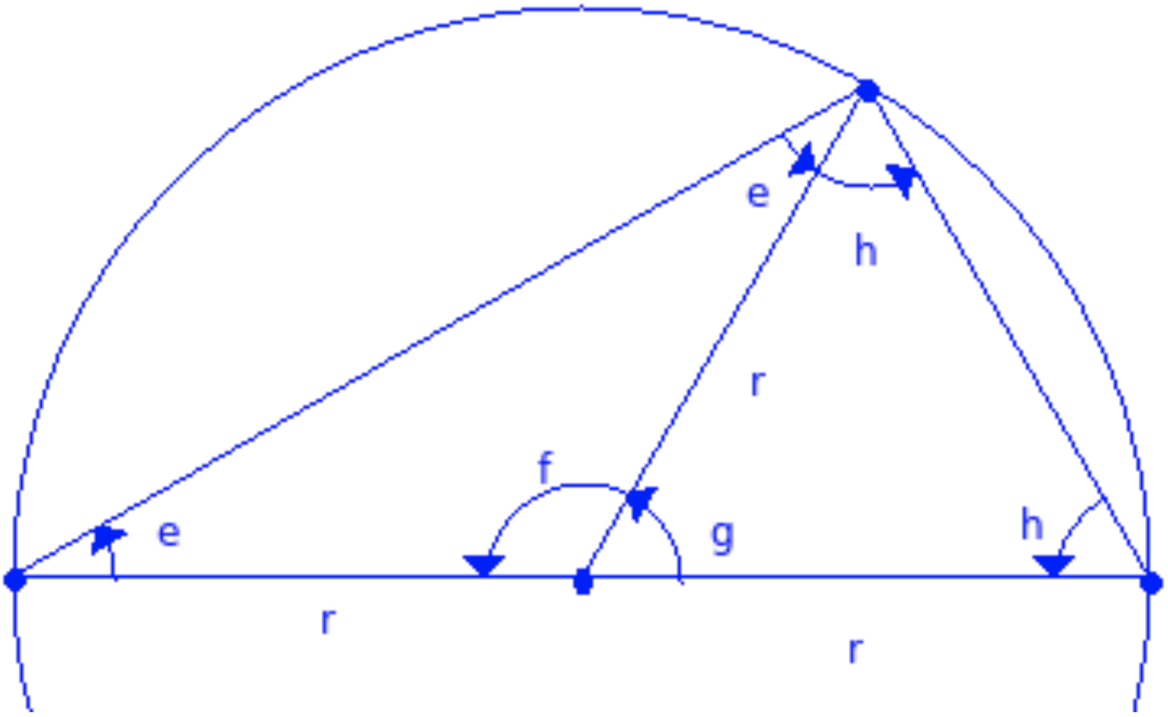


Figura A.6: Representació gràfica.

Proposició A.1.6. *Siguin $a_1, a_2, \ldots, a_n$ nombres construïbles i sigui $\mathbb{K} = \mathbb{Q}(a_1, a_2, \ldots, a_n)$. Aleshores $\mathbb{K}/\mathbb{Q}$ és finita i $[\mathbb{K} : \mathbb{Q}]$ és potència de 2. De manera més precisa, existeix una cadena de subcossos:*

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

Recíprocament, donada una cadena de subcossos com (A.1) *tenim que tots els elements de $\mathbb{K}$ són construïbles.*

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

1. Intersectant dues rectes on cadascuna d'elles passa per dos punts construïts.

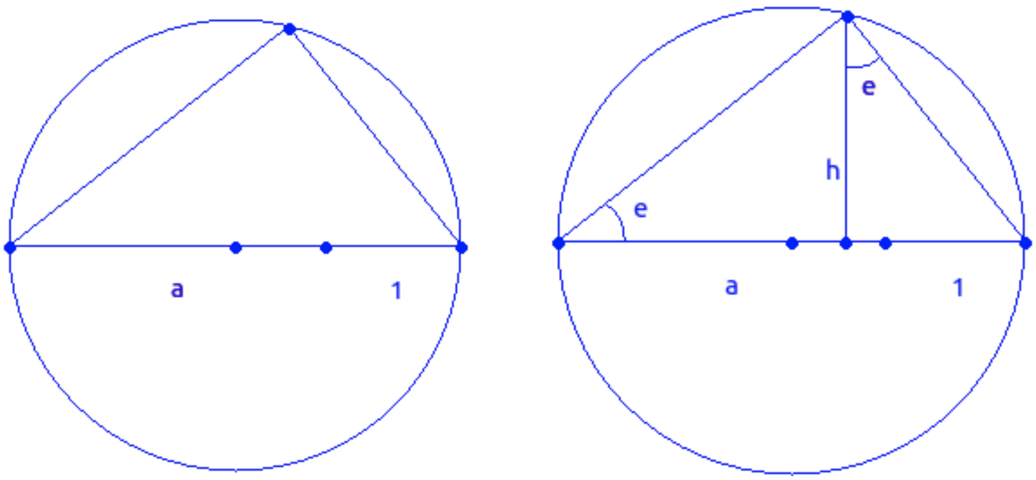


Figura A.7: Construcció d'$\sqrt{a}$.

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

1. La recta per (x_0, y_0) i (x_1, y_1) té equació:

$$L : (x_1 - x_0)(y - y_0) - (y_1 - y_0)(x - x_0) = 0.$$

   De manera anàloga, la recta per (x_2, y_2) i (x_3, y_3) té equació:

$$L' : (x_3 - x_2)(y - y_2) - (y_3 - y_2)(x - x_2) = 0.$$

   Clarament el punt d'intersecció de L i L' té coordenades a $\mathbb{F}$ en aquest cas.
2. La circumferència amb centre (x_3, y_3) i que passa per (x_2, y_2) té equació:

$$C : (x - x_3)^2 + (y - y_3)^2 = (x_2 - x_3)^2 + (y_2 - y_3)^2.$$

   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 $\mathbb{F}$, 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:

$$C' : (x - x_1)^2 + (y - y_1)^2 = (x_0 - x_1)^2 + (y_0 - y_1)^2.$$

   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 $\mathbb{F}$ (de grau exactament el de l'equació).

Que en una cadena com (A.1) tots els elements de $\mathbb{K}$ són construïbles surt de A.1.5 i A.1.4. ■

Ja tenim les eines necessàries per a resoldre els problemes que plantejàvem a l'inici de la secció.

Exercici A.1.7. *Suposem que tenim dues rectes construïdes i que formen un angle θ. És possible construir dues rectes amb un angle $\frac{\theta}{3}$?*

Demostració. 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 $\cos\theta = \frac{1}{2}$ i $\sin\theta = \frac{\sqrt{3}}{2}$), però $\cos\frac{\theta}{3}$ no és construïble i per tant $\frac{\theta}{3}$ tampoc. Per a veure això, partim de la identitat trigonomètrica[3]:

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

i fent $\alpha = \frac{\theta}{3} = 20°$ veiem que

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

És a dir, que $\cos(\frac{\theta}{3})$ 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 $[\mathbb{Q}(\cos(\theta/3)) : \mathbb{Q}] = 3$, i per A.1.6 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 $[\mathbb{Q}(\pi) : \mathbb{Q}] = \infty$ ja que π és transcendent sobre $\mathbb{Q}$ i novament per A.1.6 veiem que π no és construïble; d'aquesta manera, demostraríem que la quadratura del cercle no és possible (tant $[\mathbb{Q}(\pi) : \mathbb{Q}] = \infty$ com $[\mathbb{Q}(\sqrt{\pi}) : \mathbb{Q}] = \infty$).

Proposició A.1.8. *Doblar el cub no és possible.*

Demostració. En efecte, si passem d'un cub d'aresta 1 a aresta $\sqrt[3]{2}$, tenim $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$. ■

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).

Teorema A.1.9 (de Gauss)**.** *Per a quins valors de n podem construir un polígon regular de n-costats amb regle i compàs? En particular, el polígon regular de n costats és construïble amb regle i compàs si i només si $\phi(n) = [\mathbb{Q}(\zeta_n) : \mathbb{Q}]$ 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.*

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

Demostració. 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 $\zeta_n + \overline{\zeta}_n = \zeta_n + \zeta_n^{-1}$ i, recordem, que $\zeta_n + \zeta_n^{-1}$ és $2\cos(\frac{2\pi}{n})$; ara, és evident que $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$ serà $\mathbb{Q}(\cos(\frac{2\pi}{n}))$. També, 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 $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_n + \zeta_n^{-1})] \leq 2$. Així doncs, si ζ_n és construïble necessàriament $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = 2^k$ per algun $k \geq 0$. També tenim que $\mathbb{Q}(\zeta_n + \zeta_n^{-1})/\mathbb{Q}$ és Galois i té grau potència de 2. Recíprocament, si $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = 2^k$ per algun $k \geq 0$, com que $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ és abelià (i té cardinal potència de 2) existeix una cadena de subgrups:

$$1 = G_0 \leq G_1 \leq \cdots \leq G_r = \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$$
$$\mathbb{Q} = \mathbb{K}_r \subset \mathbb{K}_{r-1} \subset \cdots \subset \mathbb{K}_0 = \mathbb{Q}(\zeta_n + \zeta_n^{-1}).$$

tals que $[G_i : G_{i+1}] = 2$ i $\mathbb{K}_i = \mathbb{Q}(\zeta_n + \zeta_n^{-1})^{G_i}$, $[\mathbb{K}_i : \mathbb{K}_{i+1}] = 2$. 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 que acabem de veure, i també tenim a (A.1). Tenim doncs el resultat següent, que fou demostrat per primer cop per Gauss. ■

Observació A.1.10. Si posem $n = p_0^{r_0} p_1^{r_1} \cdots p_s^{r_s}$, tenim que $\varphi(n) = (p_0 - 1)p_0^{r_0 - 1} \cdots (p_s - 1)p_s^{r_s - 1}$.

Exemple A.1.11 (Primers de Fermat)**.** 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.

A.2 Teoria de codis

Sigui p un nombre primer, $q := p^r$ i $f(x) = \mathbb{F}_p[x]$ un polinomi irreductible de grau r. El cos que resulta del quocient $\mathbb{F}_p[x]/(f)$, $\mathbb{F}_q$, és un cos de q elements.

Exemple A.2.1. $\mathbb{F}_{16} = \mathbb{F}_2[x]/(x^4 + x + 1)$, posem $\alpha = \overline{x}$, de manera que $\alpha^4 + \alpha + 1 = 0$. Així doncs:

$$\mathbb{F}_{16} = \{0, 1, \alpha, \alpha + 1, \alpha^2, \alpha^2 + 1, \alpha^2 + \alpha, \alpha^2 + \alpha + 1, \alpha^3, \alpha^3 + 1, \alpha^3 + \alpha, \alpha^3 + \alpha + 1, \alpha^3 + \alpha^2,$$
$$\alpha^3 + \alpha^2 + 1, \alpha^3 + \alpha^2 + \alpha, \alpha^3 + \alpha^2 + \alpha + 1\}.$$

Al seu torn, $(\alpha^2 + \alpha)(\alpha^3 + \alpha + 1) = \alpha^5 + \alpha^4 + \alpha^3 + \alpha = \alpha^3 + \cdots + \alpha + 1$.

Introduïts al segle XIX com a objectes d'interès purament matemàtic, van trobar aplicacions inesperades al segle XX.

Definició A.2.2 (Codi de Hamming $(7,4,3)$)**.**

1. Les 16 paraules binàries de longitud 4 es codifiquen amb 7 bits: 0000000, 0001011, 0010101, 0011110, 0100110, 0101101 0110011, 0111000, 1000111, 1001100, 1010010, 1011001 1100001, 1101010, 1110100, 1111111.
2. Propietat: dues paraules codi difereixen com a mínim en tres bits.
3. 0000 es codifica com 0000000, 0001 es codifica com 0001011, etc.
4. Si es produeix un error, per exemple 0001111, resulta que hi ha una única paraula del codi a distància 1 d'aquesta: 0001011, totes les altres estan a distància més gran o igual a 2.

Aquest és el naixement de la teoria de codis correctors d'errors. Missatges: paraules de $\mathbb{F}_2^4$. Paraules codi: $\mathbb{F}_2^7$. En general: missatges $\mathbb{F}_q^k$, codi: $\mathbb{F}_q^n$.

Definició A.2.3 (Distància de Hamming)**.** $u = (u_1, \ldots, u_n), v = (v_1, ..., v_n) \in F_q^n, d_h(u,v) = \#\{i \mid u_i \neq v_i\}$. És una distància ja que $d(u,v) \leq d(u,w) + d(w,v)$.

Definició A.2.4 (Codi de bloc)**.** Un codi de bloc q-ari de longitud n és un subconjunt $C \subset \mathbb{F}_q^n$. Distància mínima: $d_C = \min_{\substack{u,v \in C \\ u \neq v}} d_h(u,v)$. Pot corregir $t_C = \lfloor \frac{d_C - 1}{2} \rfloor$ errors.

Conjectura A.2.5 (Problema fonamental de la teoria de codis)**.** *Donats n, d, es pot trobar C de longitud n i distància d amb $\#C$ màxim.*

Definició A.2.6 (Codis lineals)**.** Un codi lineal és un subespai vectorial $C \subset \mathbb{F}_q^n$.

1. Si C té dimensió k i distància d, és un codi (n,k,d).
2. Conjunt de missatges: $\mathbb{F}_q^k$, les paraules codi són de $\mathbb{F}_q^n$, taxa $\frac{k}{n}$.
3. C està completament determinat per una base.
4. Matriu generadora del codi: té per files una base de C.
5. $C = \{vG \mid v \in \mathbb{F}_q^k\}$.

Exemple A.2.7. El Hamming $(7,4,3)$ té:

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}, \; C = \{(v_1, \ldots, v_4)G \mid v_i \in \mathbb{F}_2\}.$$

Definició A.2.8 (Codis de Reed-Solomon (1960))**.** Prenem $n \in [1, 2, ..., q]$ i $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{F}_q$ elements diferents. Sigui $k \leq n$ i $\mathbb{F}_q[x]_k = \{\text{polinomis de grau més petit que } k\} \simeq \mathbb{F}_q^k$. L'aplicació avaluació en $\alpha = (\alpha_1, \ldots, \alpha_n)$ és injectiva:

$$\begin{array}{rccc} \varepsilon: & \mathbb{F}_q[x]_k \simeq \mathbb{F}_q^k & \longrightarrow & \mathbb{F}_q^n \\ & f(x) & \longmapsto & (f(\alpha_1), \ldots, f(\alpha_n)) \end{array}$$

ja que un polinomi té com a màxim $k-1$ zeros i $n > k-1$. De fet, $RS_\alpha(k) = \varepsilon(F_q[x]_k)$. Dos polinomis diferents poden prendre el mateix valor en com a màxim $k-1$ dels α_i distància del codi més gran o igual que $n-(k-1)$. La Matriu generadora resulta ésser: $V_k(\alpha_1, \ldots, \alpha_n)$. Bons algoritmes de decodificació (basats en algoritme d'Euclides).

Definició A.2.9 (Empaquetament d'esferes a $\mathbb{R}^n$)**.** Sigui $S \subset \mathbb{R}^n$ una esfera oberta n-dimensional, $c_1, c_2, \ldots$ una seqüència infinita de punts a $\mathbb{R}^n$.

1. Empaquetament: si els traslladats $c_1 + S, c_2 + S, \ldots$ són disjunts.
2. Densitat d'empaquetament: fracció de $\mathbb{R}^n$ coberta per les esferes.

Conjectura A.2.10. *Es poden seleccionar els centres per tal de maximitzar la densitat.*

State of the art.

1. En dimensió 1 el problema és trivial: la densitat màxima és 1.
2. En dimensió 2 és fàcil trobar l'empaquetament òptim, $\delta = \frac{\pi}{12} \approx 0.906$, i és òptim (Thue, 1892).
3. En $n = 3$ trobem l'empaquetament òptim a partir del de $n = 2$. Té $\delta = \frac{\pi}{3} \approx 0.74$, però és difícil provar aquest δ és òptim. Conjecturat per Kepler el 1611 i provat per Thomas Hales el 2005: prova molt complicada i que fa servir càlculs fets amb ordinador, però ha estat verificada formalment el 2017.
4. En dimensió superior a 3 els empaquetaments òptims en dimensió inferior no ajuden. Fins fa poc, no se sabia el δ òptim per cap $n > 3$. ■

Ara anem a veure la relació entre empaquetaments i codis: prenem un morfisme de reducció mòdul p, $\pi : \mathbb{Z}^n \longrightarrow \mathbb{F}_p^n$. Si $C \subset \mathbb{F}_p^n$ és un codi, considerem $\Lambda_C := \pi^{-1}(C)$, que és una col·lecció de centres amb bones propietats d'empaquetament.

Observació A.2.11. Dimensions 8 i 24: hi ha dos empaquetaments, E_8 i Λ_{24} molt especials que s'obtenen d'aquesta construcció per a certs codis.

- Per $n = 8$ és el codi de Hamming estès $(8, 4, 4)$ (bit extra de paritat).
- Per $n = 24$ el codi de Golay binari estès $(24, 12, 8)$.

En els dos casos $\pi^{-1}(C)$ té «forats» molt grans que es poden omplir. Omplint-los convenientment s'obtenen el reticle E_8 i el reticle de Leech Λ_{24}.

Recordem l'isomorfisme d'espais vectorials $\mathbb{F}_q^n \simeq \mathbb{F}_q[x]/(x^n - 1)$. Aquest espai de la dreta té una estructura d'anell.

Definició A.2.12 (Codi cíclic)**.** El subespai donat per un ideal de $\mathbb{F}_q[x]/(x^n - 1)$.

Observació A.2.13. Si $(a_0, a_1, \ldots, a_{n-1}) \in C$ es correspon amb $a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}$ aleshores $x(a_0 + a_1 x + \cdots + a_{n-1}x^{n-1})$ és del codi i, per tant, $(a_{n-1}, a_0, \ldots, a_{n-2}) \in C$.

Tot codi cíclic és generat per un polinomi $f | x^n - 1$.

Exemple A.2.14 (Codi de Golay binari)**.** A $\mathbb{F}_2[x]$ el polinomi $x^{23} - 1$ factoritza com:

$$(x + 1) \cdot (x^{11} + x^9 + x^7 + x^6 + x^5 + x + 1)(x^{11} + x^{10} + x^6 + x^5 + x^4 + x^2 + 1).$$

És el generat per un dels factors de grau 11, és un codi $(23, 12, 7)$. El codi estès $(24, 12, 8)$ s'obté afegint un bit de paritat.

Definició A.2.15 (Reticle de Leech)**.** El 1967 John Leech es va adonar que l'aixecament del codi de Golay binari a $\mathbb{Z}^{24}$ té forats, i que omplint-los s'obté un reticle Λ_{24} amb el doble de densitat. El 1968 va calcular el grup d'automorfismes de Λ_{24}, que té cardinal $2^{22}\cdot 3^9\cdot 5^4\cdot 7^2\cdot 11\cdot 13\cdot 23$. Entre els seus subgrups hi va descobrir tres grups simples esporàdics nous.

El reticle E_8 té densitat $\frac{\pi^2}{384}$, i el de Leech Λ_{24} en té $\frac{\pi^{12}}{12!}$. No és gens evident que aquests reticles donin la densitat òptima.

Maryna Viazovska (Ucraïna, 1984) va provar que E_8 dóna la densitat òptima (2017). Poc després, conjuntament amb H. Cohn, A. Kumar, S. D. Miller i D. Radchenko van provar que Λ_{24} dóna la densitat òptima. Va rebre la Medalla Fields el 2022. Elkies i Cohn havien provat que si existeix una funció $f : \mathbb{R}^n \longrightarrow \mathbb{R}$ que ella i la seva transformada de Fourier satisfan certes propietats, aleshores E_8 i Λ_{24} són òptims. Viazovska va trobar aquesta funció *màgica* fent servir la teoria de formes modulars.

B

Grups

B.1 Grups i subgrups

Definició B.1.1 (Grup)**.** És un conjunt G no buit dotat d'una operació interna associativa, amb element neutre i tal que tot element té simètric. Si, a més, l'operació és commutativa, diem que el grup és *abelià*:

1. per a tots $x, y, z \in G$, $(x \circledcirc y) \circledcirc z = x \circledcirc (y \circledcirc z)$, la propietat associativa;
2. existeix $e \in G$ tal que $e \circledcirc x = x \circledcirc e = x$, per a tot $x \in G$ (e és l'element neutre de G).
3. per a tot $x \in G$, existeix $x' \in G$ tal que $x' \circledcirc x = x \circledcirc x' = e$ (x' és l'element simètric de x);

Definició B.1.2 (Subgrup)**.** Un subgrup d'un grup G és un subconjunt no buit H de G tal que:

1. $x, y \in H \implies xy \in H$ (H és tancat respecte de l'operació de G).
2. H és grup amb l'operació de G.

Proposició B.1.3. *Siguin G un grup i $H \subset G$ un subconjunt no buit. Els tres enunciats següents són equivalents:*

1. *H és subgrup de G.*
2. *H satisfà les següents propietats:*
   2.1. *$e \in H$,*
   2.2. *per a tot $x \in H$ es compleix $x^{-1} \in H$,*
   2.3. *per a tot $x, y \in H$ es compleix $xy \in H$.*
3. *Per a tot $x, y \in H$ es compleix $xy^{-1} \in H$.*

Definició B.1.4 (Grup simètric)**.** Posem S_n el conjunt de les permutacions de n elements amb el producte de permutacions. És un grup que es diu *grup simètric*. A S_n tenim $n!$ permutacions.

B.2 Morfismes de grups

Definició B.2.1 (Morfisme)**.** Si G, G' són grups, una aplicació $f : G \longrightarrow G'$ és un morfisme de grups si $f(xy) = f(x)f(y)$, per a tot $x, y \in G$.

Definició B.2.2 (Tipus de morfismes)**.** Suposem dos grups G, G' i f una aplicació $f : G \longrightarrow G'$.

1. Un *monomorfisme* de grups és un morfisme de grups injectiu, és a dir, $\ker(f) = \{e\}$.
2. Un *epimorfisme* de grups és un morfisme de grups exhaustiu, és a dir, $\text{im}(f) = G'$.
3. Un *isomorfisme* de grups és un morfisme de grups bijectiu. Diem que dos grups G, G' són isomorfs i posem $G \cong G'$ si existeix un isomorfisme de grups $f : G \longrightarrow G'$. Clarament, la relació de ser isomorfs és una relació d'equivalència.
4. Un *endomorfisme* d'un grup G és un morfisme de grups de G en G.
5. Un *automorfisme* de G és un endomorfisme de G bijectiu.

Definició B.2.3 (Nucli i imatge d'un grup)**.** Siguin G, G' grups. Per a un morfisme de grups $f : G \longrightarrow G'$ definim el nucli de f com $\ker(f) = \{x \in G \mid f(x) = e'\}$ (els elements del conjunt inicial que s'envien per f al neutre del conjunt d'arribada) i definim la imatge de f com $\text{im}(f) = \{f(x) \mid x \in G\}$ (el conjunt d'imatges per f).

Proposició B.2.4. *Si $f : G \longrightarrow G'$ és morfisme de grups, $\ker(f)$ és subgrup de G i $\text{im}(f)$ és subgrup de G'.*

Proposició B.2.5. *Sigui $f : G \longrightarrow G'$ un morfisme de grups:*

1. *Si H és un subgrup de G, $f(H) = \{f(H) \mid x \in H\}$ és subgrup de G'.*
2. *Si H' és subgrup de G', $f^{-1}(H') = \{x \in G \mid f(x) \in H'\}$ és subgrup de G.*

Proposició B.2.6. *Sigui $f : G \longrightarrow G'$ un morfisme de grups. f és un morfisme injectiu si, i només si, $\ker(f) = \{e\}$.*

Demostració.

$\Rightarrow$ Suposem f injectiu i sigui $x \in \ker(f)$. Tenim $f(x) = e' = f(e) \implies x = e$, a causa de la definició d'injectivitat. Per tant, $\ker(f) = \{e\}$.

$\Leftarrow$ Suposem ara $\ker(f) = \{e\}$ i siguin $x, y \in G$ tals que $f(x) = f(y)$. Tenim $f(x) = f(y) \implies e' = f(x)f(y)^{-1} = f(x)f(y^{-1}) = f(xy^{-1})$. Per tant, $xy^{-1} \in \ker(f)$. Notem que totes les implicacions que hem fet resulten ser equivalències. Així, fem servir la hipòtesi que $\ker(f) = \{e\}$. Aleshores, $xy^{-1} = e$; equivalentment, $x = y$.

■

B.3 Lagrange

Definició B.3.1 (Ordre d'un grup)**.** Donat un grup G, diem que G és finit si el conjunt G és finit i, en aquest cas, diem ordre de G i indiquem per $|G|$ el cardinal del conjunt G.

Definició B.3.2 (Índex de grup)**.** Donats un grup G i un subgrup H de G, posem $[G : H]$ i diem índex de G en H el cardinal de G/D (que hem vist és igual al de G/E). En altres paraules, és el nombre de classes d'equivalència que existeix, tant per la dreta com per l'esquerra.

Teorema B.3.3 (Teorema de Lagrange)**.** *Donats un grup G i un subgrup H de G, el grup G és finit si, o només si, H i $[G : H]$ són finits. En aquest cas,*

$$|G| = |H| \cdot [G : H].$$

En particular, $|H|$ i $[G : H]$ són divisors de $|G|$.

Demostració.

$\Rightarrow$ Suposem G finit. Com que H és subgrup (i, en particular, subconjunt) de G, H és finit i com les classes d'equivalència per D formen una partició de G, és a dir, G és reunió disjunta de les classes d'equivalència, $[G : H]$ és finit.

$\Leftarrow$ Suposem ara H i $[G : H]$ finits. Com G és reunió disjunta de les classes d'equivalència per D, hi ha $[G : H]$, i a cada classe d'equivalència, hi ha tants elements com a H, tenim $|G| = |H| \cdot [G : H]$.

■

B.4 Grups normals i quocients

Proposició B.4.1. *Sigui G un grup, H un subgrup de G, D i E les relacions definides a partir d'H. Els enunciats següents són equivalents:*

- *$xH = Hx$, per a tot $x \in G$;*
- *$xHx^{-1} = \{xhx^{-1} \mid h \in H\} = H$, per a tot $x \in G$;*
- *$xHx^{-1} \subset H$, per a tot $x \in G$;*
- *D és compatible amb l'operació de G;*
- *E és compatible amb l'operació de G.*

Demostració.

$1 \Rightarrow 2$ Suposat $xH = Hx$ per a tot $x \in G$ volem provar que $xHx^{-1} = H$, per a tot $x \in G$ un altre cop. Siguin $x \in G$ i $h \in H$. Posem $xh \in xH = Hx$. Per tant, existeix un $h' \in H$ tal que $xh = h'x$.

$$(xh)x^{-1} = (h'x)x^{-1} = h'(xx^{-1}) = h' \in H.$$

Hem vist que $xHx^{-1} \subset H$ per a tot $x \in G$. $x^{-1}Hx \subset H \iff H \subset xHx^{-1}$ i, per tant, $x^{-1}hx = h' \iff xh'x^{-1} = h$.

$2 \Rightarrow 3$ Una igualtat és una doble inclusió. Simplement cal usar la inclusió cap a la dreta.

$2 \Rightarrow 1$ Ara prenem com a hipòtesi $xHx^{-1} = H$ per a tot $x \in G$. En particular, tenim que $xHx^{-1} \subset H$ per a tot $x \in G$; per tant, $xH = Hx$ per a tot $x \in G$. Existeix $h' \in H$ tal que $xhx^{-1} = h'$ i això implica que $xh = h'x \in Hx$, és a dir, $xH \subset Hx$. Podem obtenir la inclusió contrària anàlogament, $x^{-1}Hx \subset H$ per a tot $x \in G$; per tant, existeix $h' \in H$ tal que $x^{-1}hx = h'$ i això implica que $xh = h'x \in xH$.

$1 \Rightarrow 4$ D resulta ser compatible amb el producte de G.

$$\left.\begin{matrix} x' = xh \\ y' = yh' \end{matrix}\right\} \implies x'y' = x(hy)h' = x(yh'')h' = xy(h''h') \implies \left.\begin{matrix} xDx' \\ yDy' \end{matrix}\right\} \implies xyDx'y'.$$

$3 \Leftarrow 4$ Ara suposem que D és compatible. Volem demostrar que $xHx^{-1} \subset H$, per a tot $x \in G$. Volem veure $x \in G$ i $h \in H$ implica que $xhx^{-1} \in H$.

$$\left.\begin{matrix} xhDx \\ x^{-1}Dx^{-1} \end{matrix}\right\} \implies xhx^{-1}Dxx^{-1} = e \implies xhx^{-1} \in H.$$

$1 \Rightarrow 5$ Ara volem provar que si $xH = Hx$ per a tot $x \in G$, E és compatible amb el producte de G. Posem $x' = hx$ i $y' = h'y$. Aleshores, $x'y' = h(xh')y = (hh'')xy$, on a la segona igualtat hem usat que $xh' = h''x$ per a algun $h'' \in H$. Per tant, $(x'y')E(xy)$ i ja hem acabat.

$3 \Leftarrow 5$ Suposant que E és compatible, volem trobar que $xHx^{-1} \subset H$ per a tot $x \in G$. Prenem $x \in G$ i $h \in H$. Per hipòtesi, xEx i $hx^{-1}Ex^{-1}$; així, $xhx^{-1}Exx^{-1} = e \implies xhx^{-1} \in H$.

■

Definició B.4.2 (Morfisme de pas al quocient)**.** El definim per $\pi : G \longrightarrow G/H$ i envia cada element de G a la seva classe en G/H. És epimorfisme de grups amb nucli H.

Definició B.4.3 (Grup normal)**.** Un subgrup H de G es diu normal si es compleix alguna (i, per conseqüència, totes) de les condicions de B.4.1. En aquest cas, $G/D = G/E$ i l'escrivim G/H o $H \lhd G$. En particular, anomenem $x \longmapsto [x]$ com morfisme de pas al quocient.

Definició B.4.4 (Grup quocient)**.** Sigui H un subgrup de G. Si H és normal, G/H té estructura de grup. En efecte, $[x][y] = [xy]$ i es diu grup quocient de G en H.

Proposició B.4.5. *Si $f : G \longrightarrow G'$ és un morfisme de grups,* $\ker(f)$ *és subgrup normal de G.*

Proposició B.4.6. *Sigui $f : G \longrightarrow G'$ un morfisme de grups.*

1. *Si H és un subgrup de G, aleshores $f(H)$ és subgrup de G'.*
2. *Si H' és subgrup de G', aleshores $f^{-1}(H')$ és subgrup de G. A més, si H' és subgrup normal de G', aleshores $f^{-1}(H')$ és subgrup normal de G.*

Proposició B.4.7. *Si G és abelià, aleshores cada subgrup H de G és normal. Si $[G : H] = 2$, aleshores H és normal en G.*

B.5 Teoremes d'isomorfia

Definició B.5.1 (f factoritza a través de G/H)**.** Siguin G, G' grups i sigui $f : G \longrightarrow G'$ un morfisme de grups i sigui H un subgrup normal de G. Diem que f factoritza a través de G/H

si existeix un morfisme de grups $\overline{f} : G/H \longrightarrow G'$ tal que $f = \overline{f} \circ \pi$, on $\pi : G \longrightarrow G/H$ és el morfisme de pas a quocient, és a dir, si existeix un morfisme de grups $\overline{f} : G/H \longrightarrow G'$ que faci commutatiu el diagrama:

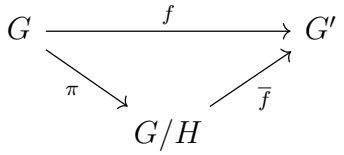


Figura B.1: El diagrama commuta si, i només si, $f = \overline{f} \circ \pi$.

Proposició B.5.2. *Siguin G, G' grups i sigui $f : G \longrightarrow G'$ un morfisme de grups i sigui H un subgrup normal de G. Aleshores, f factoritza a través de G/H si, i només si, $H \subset \ker(f)$.*

Demostració.

⇒ Si f factoritza a través de G/H i $h \in H$, tenint en compte la definició de π i que $\overline{f}$ és morfisme, obtenim $f(h) = \overline{f}(\pi(h)) = \overline{f}([h]) = \overline{f}(\overline{e}) = e'$, on en la tercera igualtat $[h] = \overline{e}$ per la sel·lecció d'h. $\overline{e}$ indica l'element neutre de G/H i e' el del de G'. Per tant, $H \subset \ker(f)$.

⇐ Si $H \subset \ker(f)$, definim $\overline{f} : G/H \longrightarrow G'$ per $\overline{f}([x]) = f(x)$, on $[x]$ indica la classe a G/H d'un element x de G. Hem de veure que la definició no depèn del representant de la classe, és a dir, que $[x] = [y] \implies f(x) = f(y)$. Si $y \in [x]$ tenim que $y = xh$, amb $h \in H$. Per tant,

$$f(y) = f(xh) = f(x)f(h) = f(x)e' = f(x),$$

ja que $h \in H \subset \ker(f)$. Ara, cal veure si $\overline{f}$ és morfisme de grups. Si $x, y \in G$, tenim:

$$\overline{f}([x][y]) = \overline{f}([xy]) = f(xy) = f(x)f(y) = \overline{f}([x])\overline{f}([y]),$$

per la definició d'operació al grup quocient G/H (el producte de classes), el fet que f és morfisme de grups i la definició de $\overline{f}$. Finalment, és clar que $f = \overline{f} \circ \pi$ (així doncs, f factoritza a través de G/H per definició).

■

Teorema B.5.3 (Primer teorema d'isomorfia)**.** *Si G, G' són grups i $f : G \longrightarrow G'$ és un morfisme de grups, aleshores f factoritza a través de $G/\ker(f)$ i tenim $f = i \circ \tilde{f} \circ \pi$, amb $\tilde{f}$ isomorfisme de grups $G/\ker(f)$ en $\mathrm{im}(f)$, on $\pi : G \longrightarrow G/\ker(f)$ és el morfisme de pas al quocient i $i : \mathrm{im}(f) \longrightarrow G'$ la inclusió. Tenim, doncs, un diagrama commutatiu:*

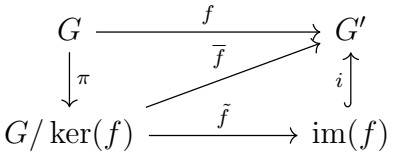


Figura B.2: Primer teorema d'isomorfia.

Demostració. Per B.5.2, existeix un morfisme $\overline{f} : G/\ker(f) \longrightarrow G'$, que envia $[x] \longmapsto f(x)$, tal que $f = \overline{f} \circ \pi$. Clarament, $\overline{f}$ és injectiu i $\overline{f} = i \circ \tilde{f}$, amb $\tilde{f}$ isomorfisme de $G/\ker(f)$ en $\mathrm{im}(\overline{f})$. Com $\mathrm{im}(\overline{f}) = \mathrm{im}(f)$, per la definició de $\overline{f}$ obtenim el resultat desitjat.

$$\overline{f} = i \circ \tilde{f}, \quad \begin{array}{rccc} \tilde{f}: & G/\ker(f) & \longrightarrow & \mathrm{im}(\overline{f}) \\ & [x] & \longmapsto & f(x) \end{array} \quad f = i \circ \tilde{f} \circ \pi, \ \tilde{f} \text{ és injectiva.}$$

$\tilde{f}$ és injectiva ja que, donada una classe $[x] \in G/\ker(f)$, $\tilde{f}([x]) = f(x) = e'$, de manera que $x \in \ker(f)$ i, per tant, $[x] = [e]$; de fet, $\ker(\tilde{f}) = \{[e]\}$ i, en efecte, $\tilde{f}$ és injectiva. Com que $\overline{f}$ és un morfisme, $\tilde{f}$ és un morfisme també. ■

Teorema B.5.4 (Segon teorema d'isomorfia). *Sigui $\varphi : G \longrightarrow G'$ un epimorfisme de grups. Sigui H' un subgrup normal de G' i $H = \varphi^{-1}(H')$. Aleshores, φ indueix un isomorfisme de G/H en $G'H'$.*

Corol·lari B.5.5. *Si G és un grup i F i H són subgrups normals de G amb $F \subset H$, aleshores H/F és subgrup normal de G/F i el morfisme de pas al quocient $G \longrightarrow G/F$ indueix un isomorfisme de G/H en $(G/F)/(H/F)$.*

Teorema B.5.6 (Tercer teorema d'isomorfia). *Sigui G un grup, H i F subgrups de G, amb H normal en G. Posem $HF := \{hf \mid h \in H, f \in F\}$. Aleshores, HF és un subgrup de G, $F \cap H$ és un subgrup normal de F i H és un subgrup normal d'HF. A més, la inclusió d'F en HF indueix un isomorfisme de $F/(F \cap H)$ en HF/H.*

B.6 Grups cíclics

Definició B.6.1 (Ordre d'un element). El subgrup $\langle x \rangle$ és el conjunt dels elements de G que són iguals a x^n per a algun $n \in \mathbb{Z}$. En particular, $\ker(f_x) = m\mathbb{Z}$ és subgrup de $\mathbb{Z}$. Tenim $\langle x \rangle \cong \mathbb{Z}/m\mathbb{Z}$. Si $m > 0$, diem que m és l'ordre de x i posem $\mathrm{ord}(x)$. En cas que $m = 0$, diem que x té ordre infinit. L'ordre de l'element és l'ordre del subgrup que genera. En particular, l'ordre de x divideix l'ordre de G, $|G|$.

Definició B.6.2 (Grup cíclic). Un grup G es diu cíclic si existeix $x \in G$ tal que $G = \langle x \rangle$ (és a dir, que està generat per un únic element). Diem que G està generat per x. Denotem per C_n el grup cíclic d'ordre n i aquest és isomorf a $\mathbb{Z}/n\mathbb{Z}$.

Proposició B.6.3. *Tot grup cíclic és isomorf a $\mathbb{Z}$ o bé a $\mathbb{Z}/m\mathbb{Z}$, per a un enter $m > 0$. Per tant, dos grups cíclics del mateix ordre són isomorfs entre ells.*

Lema B.6.4. *Sigui $G = \langle x \rangle$ un grup cíclic d'ordre n per a tot enter $k > 0$, es compleix:*

$$\operatorname{ord}(x^k) = \frac{n}{\operatorname{mcd}(n,k)}.$$

Corol·lari B.6.5. *Sigui $G = \langle x \rangle$ un grup cíclic d'ordre n. Aleshores, x^k genera G si, i només si,* $\operatorname{mcd}(n,k) = 1$.

Proposició B.6.6. *Tot subgrup d'un grup cíclic és cíclic.*

Demostració. Si $G = \langle x \rangle$ i H és el subgrup trivial, el resultat és trivial: $H = \{e\} = \langle e \rangle$. Si H és subgrup no trivial de G, sigui m l'enter estrictament positiu més petit tal que $x^m \in H$. Volem veure $H = \langle x^m \rangle$. Clarament, $\langle x^m \rangle \subset H$ (tota potència d'$x \in H$ es troba en H perquè l'operació és tancada). Sigui ara $x^\ell \in H$; hem de veure que $x^\ell \in \langle x^m \rangle$, per demostrar l'inclusió. Fem la divisió entera $x^\ell = x^{mq+r} = (x^m)^q + x^r$ que implica $x^r = x^l (x^m)^{-q} \in H$. Per l'elecció de m (l'element *més petit* tal que $x^m \in H$), ha de ser $r = 0$ i, per tant:

$$x^\ell = (x^m)^q \in \langle x^m \rangle.$$

Hem obtingut, doncs, $H = \langle x^m \rangle$; en particular, que H és cíclic. ■

Proposició B.6.7. *Si G és un grup cíclic d'ordre n, per a cada divisor d de n existeix un únic subgrup de G d'ordre d.*

Demostració. Sigui $G = \langle x \rangle$ un grup cíclic d'ordre n ($|G| = n$) i d un divisor de n. Un subgrup d'un grup cíclic G és cíclic, B.6.6, i és d'ordre d si està generat per un element d'ordre d. Per B.6.4, $x^{\frac{n}{d}}$ té ordre d i $\langle x^{\frac{n}{d}} \rangle$ és subgrup de G d'ordre d. De nou per B.6.4, els elements de G que tenen ordre d són els x^k amb $\frac{n}{\operatorname{mcd}(n,k)} = d$, és a dir, són els x^k amb k múltiple d'$\frac{n}{d}$ ($k = \ell \frac{n}{d}$ per algun ℓ). Per tant,

$$x^k = (x^{\frac{n}{k}})^\ell \in \langle x^{\frac{n}{d}} \rangle.$$

Com hem vist, tots aquests elements estan continguts en el subgrup $\langle x^{\frac{n}{d}} \rangle$. Per tant, aquest subgrup és l'únic d'ordre d. ■

B.7 Subgrup generat per un conjunt

Definició B.7.1 (Subgrup generat per S)**.** Sigui G un grup, S un subconjunt de G. Definim el subgrup de G generat per S, que indicarem per $\langle S \rangle$, com la intersecció de tots els subgrups de G que contenen S. Si H és subgrup de G i $H = \langle S \rangle$, direm que S és un conjunt (o sistema) de generadors de H. Clarament $\langle \emptyset \rangle = \{e\}$.

Proposició B.7.2. *El subgrup de G generat per un subconjunt no buit S de G és el conjunt de tots els elements de la forma*

$$x_1^{n_1} \dots x_r^{n_r},$$

on r és un enter positiu, $x_1, \dots, x_r$ són elements de S i $n_1, \dots, n_r \in \mathbb{Z}$.

B.8

Producte directe de grups

Definició B.8.1 (Producte directe de $G_1 \times \cdots \times G_r$)**.** Generalitzant, si $G_1, \dots, G_r$ grups en el producte cartesià $G_1 \times \cdots \times G_r$ definim la operació binària interna per $(x_1, \dots, x_r)(y_1, \dots, y_r) = (x_1y_1, \dots, x_ry_r)$. $G_1 \times \cdots \times G_r$ és grup:

1. l'element neutre és $(e_1, \dots, e_r)$ (on e_i és l'element neutre de G_i, $1 \leq i \leq r$),
2. existeix l'element invers $(x_1, \dots, x_r)^{-1}$ definit per $(x_1^{-1}, \dots, x_r^{-1})$.

Diem que $G_1 \times \cdots \times G_r$ és el producte directe de $G_1, \dots, G_r$.

Proposició B.8.2. *Siguin G_1 i G_2 grups cíclics d'ordres n_1 i n_2, respectivament. El producte directe $G_1 \times G_2$ és cíclic si i només si n_1 i n_2 són primers entre ells. En aquest cas, si x_1 és un generador de G_1 i x_2 és un generador de G_2, $\langle (x_1, x_2) \rangle$ és un generador de $G_1 \times G_2$.*

Demostració. Per a $(x_1, x_2) \in G_1 \times G_2$, es compleix

$$\operatorname{ord}(x_1, x_2) = \operatorname{mcm}(\operatorname{ord} x_1, \operatorname{ord} x_2),$$

ja que, per a un enter natural n, $(x_1, x_2)^n = (x_1^n, x_2^n) = (e_1, e_2) \iff x_1^n = e_1$ i $x_2^n = e_2 \implies \operatorname{ord} x_1 \mid n$ i $\operatorname{ord} x_2 \mid n$.

$$(x_1, x_2)^{\operatorname{mcm}(\operatorname{ord}(x_1), \operatorname{ord}(x_2))} = (e_1, e_2).$$

Definim $n_1 = \operatorname{ord}(x_1)$ i $n_2 = \operatorname{ord}(x_2)$. Per tant, si $\operatorname{mcd}(n_1, n_2) = 1$ i $G_1 = \langle x_1 \rangle, G_2 = \langle x_2 \rangle$, aleshores (x_1, x_2) és un element de $G_1 \times G_2$ que té ordre $n_1n_2 = |G_1 \times G_2|$ i $G_1 \times G_2$ és cíclic. En aquest cas, $G_1 \times G_2 = \langle (x_1, x_2) \rangle$. Si $\operatorname{mcd}(n_1, n_2) \neq 1, G_1 \times G_2$ no pot tenir cap element d'ordre igual a n_1n_2. ■

Definició B.8.3 (Producte directe intern)**.** Si f està definida com

$$\begin{array}{rccc} f: & H_1 \times H_2 & \longrightarrow & G \\ & (h_1, h_2) & \longmapsto & h_1h_2 \end{array}$$

i és isomorfisme, diem que G és producte directe intern de $H_1 \cap H_2$. Equivalentment, si es compleixen les tres condicions següents:

1. $G = H_1H_2$ (és morfisme exhaustiu);
2. per a tot $h_1 \in H_1$ i tot $h_2 \in H_2$ es compleix que $h_1h_2 = h_2h_1$ (és morfisme);

3. $H_1 \cap H_2 = \{e\}$ (és morfisme injectiu).

Si G és producte directe intern dels subgrups H_1 i H_2, aleshores H_1 i H_2:

$$\begin{array}{l} H_1 \cong \{(h_1, e_2) \mid h_1 \in H_1\} \text{ subgrup normal d'} H_1 \times H_2, \\ H_2 \cong \{(e_1, h_2) \mid h_2 \in H_2\} \text{ subgrup normal d'} H_1 \times H_2; \end{array}$$

B.9

Grups definits per generadors i relacions

Definició B.9.1 (Relació entre elements)**.** Sigui G un grup generat per un conjunt finit $S = \{x_1, \ldots, x_n\}$, és a dir, $G = \langle x_1, \ldots, x_n \rangle$. Una relació entre els elements de S és una igualtat del tipus

$$x_1^{k_1} \ldots x_n^{k_n} = e, \text{ on } k_1, \ldots, k_n \in \mathbb{Z}.$$

Definició B.9.2 (Grup definit pels generadors)**.** Si G és un grup finit definit pel conjunt de generadors S i el conjunt de relacions R a partir de R i S podem escriure els elements de G i la taula del producte de G.

B.10

Grups resolubles

Definició B.10.1 (Grup resoluble)**.** Un grup G és resoluble si existeix una cadena finita de subgrups de G de la següent forma: comença amb el trivial i cadascun està inclòs en el següent i cadascun d'ells compleix que cadascun és normal amb el següent i els quocients són abelians:

$$\{e\} = G_0 \subset G_1 \subset \cdots \subset G_n = G,\ i = 0 \div n - 1.$$

1. G_i és normal en G_{i+1},
2. G_{i+1}/G_i és abelià.

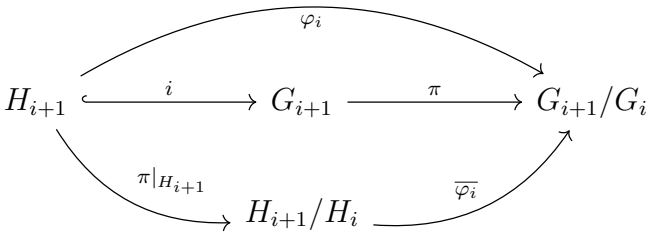
Una successió de grups es diu que és una *torre normal* si compleix la primera propietat i és una *torre abeliana* si compleix la segona propietat. És *resoluble* si és una torre abeliana l'últim subgrup de la qual és el neutre (és a dir, que $G_0 = \{e\}$, el subgrup trivial de G).

Proposició B.10.2.

1. *Tot subgrup d'un grup resoluble és resoluble.*
2. *Tot quocient d'un grup resoluble per un subgrup normal és resoluble.*
3. *Si G és grup i H subgrup normal de G tal que H i G/H són grups resolubles, aleshores G és resoluble.*

Demostració.

1. Si G és resoluble, per definició $\exists G_0 = \{e\} \subset G_1 \subset \cdots \subset G_n = G$ amb G_i normal a G_{i+1} i G_{i+1}/G_i, aleshores sigui H subgrup de G. Posem $H_i = G_i \cap H$, amb $H_i \subset H_{i+1}$. Considerem el següent diagrama:



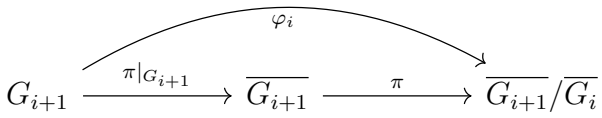
$$\ker(\varphi_i) = H_{i+1} \cap G_i = (H \cap G_{i+1}) \cap G_i = H \cap G_i = H_i \implies H_i \lhd H_{i+1}$$
$$\varphi_i \text{ factoritza a través de } H_{i+1}/H_i \text{ i } \overline{\varphi_2} : H_{i+1}/H_i \longrightarrow G_i/G_{i+1}.$$

- Per B.4.5, $\ker(\varphi_i) \lhd H_{i+1}$; així doncs, $H_i \lhd H_{i+1}$.
- $\overline{\varphi_i}$ és injectiu pel teorema d'isomorfia: sigui $[x] \in H_{i+1}/H_i$ tal que, en concret, $[x] \in \ker(\overline{\varphi_i})$. Aleshores, $\overline{\varphi_i}([x]) = \varphi_i(x) = \overline{e}$, on $\overline{e}$ és el neutre en G_{i+1}/G_i. Prenent $x \in \ker(\varphi_i) = H_i$, $[x]$ és la classe del neutre en H_{i+1}/H_i: $\overline{\varphi_i}([x]) = \varphi_i(x) = \overline{e}$.
- Així, H_{i+1}/H_i és isomorf a $\mathrm{im}(\overline{\varphi_i}) \subset G_{i+1}/G_i$ abelià (ja que G és resoluble per hipòtesi), de manera que H_{i+1}/H_i és també abelià.

2. Sigui $\overline{G}$ el quocient de G per un subgrup normal, $\pi : G \longrightarrow \overline{G}$ és un morfisme de pas al quocient. $\overline{G_i} = \pi(G_i)$, amb $\overline{G_i} \subset \overline{G_{i+1}}$ i $\overline{G_n} = \overline{G}$.

$$\overline{G_i} \lhd \overline{G_{i+1}} \;\Big|\; \forall x \in G_i, \forall y \in G_{i+1}, G_i \lhd G_{i+1}, yxy^{-1} \in G_i \implies \overline{y}\,\overline{x}\,\overline{y}^{-1} \in \overline{G_i}$$

Per tant, considerem el següent diagrama un altre cop:



Per tant, $G_i \subset \ker(\varphi_i)$; en particular, $G_{i+1}/\ker(\varphi_i)$ és isomorf a $\overline{G_{i+1}}/\overline{G_i}$. Així doncs, $G_i \subset \ker(\varphi_i) \subset G_{i+1}$ implica, per B.5.5:

$$G_{i+1}/\ker(\varphi_i) \cong \frac{G_{i+1}/G_i}{\ker(\varphi_i)/G_i} \text{ és abelià } (G_{i+1}/G_i \text{ abelià, } G \text{ és resoluble})$$
$$\implies G_{i+1}/\ker(\varphi_i) \text{ abelià} \implies \overline{G_{i+1}}/\overline{G_i} \text{ abelià.}$$

3. Sigui G un grup, H un subgrup normal de G tal que H i G/H són resolubles. Posem $\overline{G} = G/H$. Sigui

$$\{e\} = H_0 \subset H_1 \subset \cdots \subset H_r = H$$

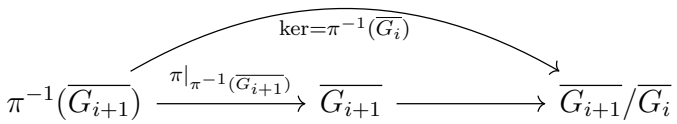
una torre abeliana de H i

$$\{\overline{e}\} = \overline{G}_0 \subset \overline{G}_1 \subset \cdots \subset \overline{G}_n = \overline{G}$$

una torre abeliana de $\overline{G}$. Sigui $\pi : G \longrightarrow \overline{G}$ el morfisme de pas al quocient. Considerem la torre de G. Sabem que $G_i = \pi^{-1}(\overline{G_i})$ és subgrup de G, $G_{i+1} = \pi^{-1}(\overline{G_{i+1}})$ és subgrup de G_{i+1}, $\pi^{-1}(\overline{G_0}) = \pi^{-1}(\overline{e}) = \ker(\pi) = H$ i $\pi^{-1}(\overline{G}) = G$:

$$\{e\} = H_0 \subset H_1 \subset \cdots \subset H_r = H = \pi^{-1}\left(\overline{G}_0\right) \subset \pi^{-1}\left(\overline{G}_1\right) \subset \cdots \subset \pi^{-1}\left(\overline{G}_n\right) = G.$$

Tenim $\overline{G}_i \lhd \overline{G}_{i+1}$ implica $\pi^{-1}\left(\overline{G}_i\right) \lhd \pi^{-1}\left(\overline{G}_{i+1}\right)$ i $\pi^{-1}\left(\overline{G}_i\right)$ és el nucli de la composició de $\pi : \pi^{-1}\left(\overline{G}_{i+1}\right) \longrightarrow \overline{G}_{i+1}$ amb el morfisme de pas al quocient $\overline{G}_{i+1} \longrightarrow \overline{G}_{i+1}/\overline{G}_i$.



Per tant pel primer teorema d'isomorfia, $\pi^{-1}\left(\overline{G}_{i+1}\right)/\pi^{-1}\left(\overline{G}_i\right) \cong \overline{G}_{i+1}/\overline{G}_i$ és abelià. Hem provat doncs que $\overline{G_{i+1}}/\overline{G_i}$ és una torre abeliana de G i per tant G és resoluble. ■

B.11 Grups simples

Definició B.11.1 (Grup simple)**.** Un grup G es diu simple si no té subgrups normals propis no trivials, és a dir, diferents de $\{e\}$ i G. Els grups S_3, A_4, S_4, D_{2n} no són simples.

Proposició B.11.2. *Un grup no trivial és simple i resoluble si, i només si, és cíclic d'ordre primer.*

B.12 Grups diedrals

Definició B.12.1 (Grup diedral D_{2n})**.** D_{2n} és el grup generat per ρ i σ amb relacions $\rho^n = Id$, $\sigma^2 = Id$ i $\sigma\rho\sigma = \rho^{-1}$. Posem

$$D_{2n} = \left\langle \rho, \sigma \mid \rho^n = Id, \sigma^2 = Id, \sigma\rho\sigma = \rho^{-1} \right\rangle.$$

B.13 Accions i òrbites

Definició B.13.1 (Acció per l'esquerra d'un grup)**.** Sigui S un conjunt i G un grup. Una acció de G sobre S és una aplicació:

$$\begin{array}{ccc} G \times S & \longrightarrow & S \\ (g, s) & \longmapsto & g \cdot s \end{array}$$

Complint:

1. $g, h \in G$ tal que $(gh)s = g(hs)$, per a tot $g, h \in G$ i $s \in S$.
2. $eg = g$, per a tot $g \in G$.

Definició B.13.2 (Òrbita d'una acció)**.** Si $G \times S \longrightarrow S$ és una acció, $s \in S$, diem òrbita de S el conjunt $\{gs \mid g \in G\} = O_s$. L'estabilitzador de s és $E(s) = \{g \in G \mid gs = s\}$.

Definició B.13.3 (Fix per l'acció)**.** Diem que $s \in S$ és fix per l'acció de G si $gs = s$, per a tot $g \in G$. Equivalentment, $O(s) = \{s\}$ o $E(s) = G$.

Proposició B.13.4. *Donada una acció p de G sobre S, amb $s \in S$, l'aplicació:*

$$\begin{array}{ccc} G & \longrightarrow & S \\ g & \longmapsto & gs \end{array}$$

dona una bijecció del conjunt de classes per la dreta de G mòdul $E(s)$ en $O(s)$. Si G és finit, $|O(s)| \cdot |E(s)| = |G|$.

Definició B.13.5 (Acció per conjugació)**.** L'acció per conjugació d'un grup sobre ell mateix és:

$$\begin{array}{ccc} G \times G & \longrightarrow & G \\ (g, h) & \longmapsto & ghg^{-1} \end{array}$$

El nucli és $\{g \in G \mid ghg^{-1} = h, \forall h \in G\} \iff \{g \in G \mid gh = hg, \forall h \in G\}$. Es diu centre de G, es denota per $Z(G)$ i $Z(G) \lhd G$.

$$E(h) = \{g \in G \mid ghg^{-1} = h\} = Z_G(h), \text{ centralitzada d'} h \text{ en } G.$$
$$O(h) = \{ghg^{-1} \mid g \in G\}, \text{ és la classe de conjugació d'} h.$$

Definició B.13.6 (Acció per conjugació d'un grup sobre el conjunt dels seus subgrups)**.** Sigui H subgrup de G. Sigui $g \in G$. El conjugat d'H per g és un subgrup de G tal que $gHg^{-1} = \{ghg^{-1} \mid h \in H\}$. L'acció per conjugació d'un grup sobre el conjunt dels seus subgrups és

$$(gh_1g^{-1})(gh_2g^{-1}) = g(h_1h_2)g^{-1} \in gHg^{-1}.$$
$$(ghg^{-1})^{-1} = gh^{-1}g^{-1} \in gHg^{-1}.$$

En particular, gHg^{-1} és el conjugat d'H per G. Prenem $\mathscr{H} = \{H \mid H \text{ és subgrup de } G\}$.

$$\begin{array}{ccc} G \times \mathscr{H} & \longrightarrow & \mathscr{H} \\ (g, H) & \longmapsto & gHg^{-1} \end{array}$$

L'òrbita d'un subgrup H de G per aquesta acció és el conjunt dels seus conjugats. Els punts fixos per aquesta acció són els subgrups normals de G. $E(H) = \{g \in G \mid gHg^{-1} = H\}$ és el normalitzador d'H en G i el denotem per N_GH (evidentment, $H \lhd N_GH$, i $H \lhd N_GH \iff \forall g \in N_GH, gHg^{-1} = H$). És el subgrup més gran de G que conté H com a subgrup normal.

Definició B.13.7 (Acció per translació)**.** Si H és un subgrup d'un grup G, podem considerar l'acció de H en G per translació a l'esquerra

$$\begin{array}{ccc} H \times G & \longrightarrow & G \\ (h, g) & \longmapsto & hg. \end{array}$$

Si F és qualsevol subgrup de G, podem considerar l'acció per translació a l'esquerra de H sobre el conjunt quocient G/D_F de classes per la dreta de G mòdul F:

$$\begin{array}{rccc} \rho: & H \times G/D_F & \longrightarrow & G/D_F \\ & (h, gF) & \longmapsto & (hg)F. \end{array}$$

L'acció de G sobre G/D_F per translació a l'esquerra és transitiva. L'acció de H sobre G per translació a l'esquerra és fidel. Per a l'acció de H sobre G/D_F, el nucli és

$$H \cap \left(\bigcap_{g \in G} gFg^{-1} \right).$$

I $E(gF) = H \cap gFg^{-1}$.

Proposició B.13.8 (Equació de les classes)**.** *Si G és un grup finit, es compleix*

$$|G| = |Z(G)| + \sum_{i=1}^{r} [G : Z_G(x_i)]$$

on $\{x_1, \ldots, x_r\}$ és un conjunt de representants de les classes de conjugació amb més d'un element.

Demostració. Considerem l'acció de G sobre ell mateix per conjugació. Aleshores $Z(G)$ és el conjunt de punts fixos, $Z_G(x_i)$ és l'estabilitzador de x_i i

$$|S| = |S_0| + \sum_{i=1}^{r} [G : E(x_i)],$$

dona la fórmula de l'enunciat. ■

Definició B.13.9 (p-grup)**.** Si p és un nombre primer, un grup finit G s'anomena p-grup si $|G| = p^r$, per a algun r enter natural > 0.

Proposició B.13.10 (Congruència dels punts fixos)**.** *Si G és un p-grup que opera sobre un conjunt finit S, aleshores*

$$|S| \equiv |S_0| \pmod{p}$$

Demostració. Si $x_i \in O_i$ de manera que O_i són òrbites amb més d'un element, és a dir, no és punt fix, $[G : E(x_i)]$ divideix $|G|$ i és > 1. Per tant, $[G : E(x_i)]$ és divisible per p. Ja sabem que $|S| - |S_0| = \sum_{i=1}^{r} [G : E(x_i)]$. Com que l'ordre de G és una potència de p per ser un p-grup, $[G : E(x_i)]$ és divisible per p. ■

Corol·lari B.13.11. *Si G és un p-grup, el seu centre $Z(G)$ és no trivial.*

Corol·lari B.13.12 (Congruència del normalitzador)**.** *Sigui H un p-subgrup d'un grup finit G. Aleshores*

$$[N_G(H) : H] \equiv [G : H] \pmod{p}.$$

B.14

Cauchy i Sylow

Teorema B.14.1 (Teorema de Cauchy)**.** *Sigui G un grup finit d'ordre n i p un nombre primer que divideix n. Aleshores G té un element (i per tant un subgrup) d'ordre p.*

Demostració. Sigui $S = \{(g_1, \ldots, g_p) \in G \times \overset{p}{\cdots} \times G \mid g_1 \cdots g_p = e\}$. Podem definir una acció de $S \times \mathbb{Z}/p\mathbb{Z}$ sobre S que corre els índexs k posicions:

$$(k, (g_1, \cdots, g_p)) \longmapsto (g_{k+1}, \ldots, g_{k+p}),$$

per a $k \in \mathbb{Z}/p\mathbb{Z}, (g_1, \ldots, g_p) \in S$, on la suma en els subíndexs es fa mòdul p. Com $\mathbb{Z}/p\mathbb{Z}$ és un p-grup i $|S| = n^{p-1}$ (g_p queda determinat per $g_1, \ldots, g_{p-1}$) és divisible per p, tenim que el cardinal del conjunt S_0 de punts fixos és divisible per p.

$$|S_0| \equiv |S| \pmod{p} \implies p \mid |S_0|.$$

El conjunt en qüestió és el següent:

$$S_0 = \{(x, \ldots, x) \mid x \in G, x^p = e\}.$$

Com $(e, \ldots, e) \in S_0$ i $p \mid |S_0|$, el conjunt S_0 ha de contenir algun $(x, \ldots, x) \in S_0$ amb $x \neq e, x \in G$. En particular, x és, doncs, element d'ordre p. ∎

Definició B.14.2 (p-subgrup de Sylow)**.** Els p-subgrups de G amb ordre la màxima potència de p dividint $|G|$ es diuen p-subgrups de Sylow de G. En particular, si G és grup d'ordre n i p primer amb $p \mid n$, diem p-subgrup de Sylow de G un subgrup de G d'ordre p^r amb $p^r \mid n$ i $p^{r+1} \nmid n$.

Teorema B.14.3 (Primer teorema de Sylow)**.** *Sigui G un grup finit, p un nombre primer i $r > 0$ un nombre enter tals que p^r divideix $|G|$. Aleshores existeixen subgrups $H_1, \cdots, H_r$ de G tals que $|H_i| = p^i, 1 \leq i \leq r$, i $H_i \lhd H_{i+1}, 1 \leq i \leq r-1$. En particular, H_r és subgrup de Sylow.*

Demostració. Raonem per inducció. Si $r = 1$, és conseqüència directa del teorema de Cauchy B.14.1. Seguim la inducció sobre r. Suposem que $r \geq 2$ i que existeixen subgrups $H_1, \ldots, H_{r-1}$ de G tals que $|H_i| = p^i$ i $H_i \lhd H_{i+1}$. Com $p \mid [G : H_{r-1}]$, per la congruència del normalitzador B.13.12, tenim $p \mid [N_G(H_{r-1}) : H_{r-1}]$. Pel teorema de Lagrange, el grup quocient $N_G(H_{r-1})/H_{r-1}$ (on $H_{r-1} \lhd N_G(H_{r-1})$) té un subgrup divisible per p i, per B.14.1 un altre cop, aquest és precisament p. La seva antiimatge per la projecció

$$\pi : N_G(H_{r-1}) \longrightarrow N_G(H_{r-1})/H_{r-1}$$

és un subgrup H_r de $N_G(H_{r-1})$ d'ordre p^r (ja que $[H_r : H_{r-1}] = p$) i tal que $H_{r-1} \lhd H_r$ (ja que $H_r \subset N_G(H_{r-1})$). ∎

Corol·lari B.14.4. *Si G es un grup finit i p un nombre primer dividint $|G|$, aleshores existeixen p-subgrups de Sylow de G. Tot p-grup és resoluble.*

Teorema B.14.5 (Segon teorema de Sylow)**.** *Siguin G un grup finit, H un p-subgrup de G i S un p-subgrup de Sylow de G, amb p primer. Aleshores existeix $x \in G$ tal que $H \subset xSx^{-1}$. En particular dos p-subgrups de Sylow de G són conjugats.*

Demostració. Considerem l'acció de H en G/D_S per translació a l'esquerra:

$$\begin{array}{ccc} H \times G/D_S & \longrightarrow & G/D_S \\ (h, gS) & \longrightarrow & hgS \end{array}$$

Per a tot element $gS \in G/D_S, g \in G$, l'estabilitzador de gS és el subgrup conjugat gSg^{-1}. Aleshores, mirem el conjunt de punts fixos per aquesta acció: si existeix algun punt fix, ja hem acabat. Donada una classe xS, tenim que xS queda fixa $\iff hxS = xS$:

$$\begin{aligned} gS \text{ punt fix} &\iff hgS = gS \iff g^{-1}hgS = S \iff g^{-1}hg \in S \\ &\iff h \in gSg^{-1} \iff H \subset gSg^{-1}, \forall h \in H. \end{aligned}$$

Per tant, el conjunt de punts fixos és $X_0 = \{xS \in G/D_S \mid H \subset xSx^{-1}\}$. Com que H és p-grup i $|G/D_S| = [G : S]$, la congruència de punts fixos B.13.10 dona $|X_0| \equiv [G : S] \pmod{p}$. Com $p \nmid [G : S]$ (G/S és p-subgrup de Sylow), tenim $p \nmid |X_0|$ i, per tant, $|X_0|$ no és buit. ■

Corol·lari B.14.6. *El grup G té un únic p-subgrup de Sylow S si, i només si, G té un p-subgrup de Sylow que és un subgrup normal.*

Teorema B.14.7 (Tercer teorema de Sylow)**.** *Sigui G un grup finit i n_p el nombre de p-subgrups de Sylow de G. Aleshores es compleix*

1. *$n_p = [G : N_G(S_p)]$, per a tot p-subgrup de Sylow S_p de G;*
2. *$n_p \mid [G : S_p]$, per a tot p-subgrup de Sylow S_p de G;*
3. *$n_p \equiv 1 \pmod{p}$.*

Demostració.

1. Pel segon teorema de Sylow B.14.5, n_p és el cardinal de l'òrbita d'un p-subgrup de Sylow S_p per l'acció de G per conjugació sobre el conjunt dels subgrups de G. L'estabilitzador de S_p per a aquesta acció és $N_G(S_p)$, de manera que $n_p = [G : N_G(S_p)]$.
2. Ara $[G : S_p] = [G : N_G(S_p)]\,[N_G(S_p) : S_p]$, per tant, n_p divideix $[G : S_p]$, ja que $S_p \subset N_G \subset G$.
$$[G : S_p] = [G : N_G(S_p)]\,[N_G(S_p) : S_p] \iff \frac{|G|}{|S_p|} = \frac{|G|}{|N_G(S_p)|} \cdot \frac{|N_G(S_p)|}{|S_p|}.$$
D'aquesta manera, $n_p \mid [G : S_p]$.

3. Sigui ara X el conjunt de p-subgrups de Sylow de G. Considerem l'acció de S_p en X per conjugació. Aleshores el conjunt de punts fixos és $X_0 = \{T \in X \mid xTx^{-1} = T, \forall x \in S_p\} = \{T \in X \mid S_p \subset N_G(T)\}$. Volem veure $X_0 = \{S_p\}$. En efecte, si $T \in X_0$, aleshores S_p i T són p-subgrups de Sylow de $N_G(T)$ i T és normal en $N_G(T)$. Com que $T \lhd N_G(T)$ implica que $N_G(T)$ té exactament un p-subgrup de Sylow, apliquem B.14.6 i ens queda $T = S_p$ i $X_0 = \{S_p\}$. Com $|X| = n_p$ i $|X_0| = 1$, per la congruència dels punts fixos, B.13.10, tenim $n_p \equiv 1 \pmod{p}$.

Amb tot, havent provat els tres apartats, ja hem acabat. ■

C

Anells

C.1 Anells

Definició C.1.1 (Anell)**.** És un conjunt A no buit dotat de dues operacions internes, la suma i el producte, tals que:

- la suma és associativa, commutativa, amb element neutre 0 i oposat (és grup abelià amb la suma),
- el producte és associatiu ($(ab)c = a(bc)$) i distributiu ($a(b+c) = ab+ac$ i $(b+ca) = ba+ca$) respecte de la suma.

Definició C.1.2 (Element invertible)**.** Un element a d'un anell amb unitat A es diu invertible si té invers a A. Si a és element invertible de l'anell A es compleix $ab = 0 \implies b = 0$, ja que $ab = 0 \implies a^{-1}(ab) = a^{-1} \cdot 0 = 0$, i d'altra banda, $a^{-1}(ab) = (a^{-1}a)b = 1 \cdot b = b$.

$$A^* = \{a \in A \mid a \text{ és invertible}\},\ A^* \text{ és grup amb el producte d'} A.$$

Es diu que A^* és grup multiplicatiu de l'anell A.

Definició C.1.3 (Subanell)**.** Sigui A un anell. Un subanell d'A és un subconjunt no buit B d'A tal que:

- $(B, +)$ és subgrup d'$(A, +)$.
- B és tancat respecte del producte d'A: $b, b' \in B \implies bb' \in B$.

A partir d'ara, anell ≡ anell commutatiu i unitari

Definició C.1.4 (Divisor de zero)**.** Un element a d'un anell A, $a \neq 0$, es diu divisor de zero si existeix $b \in A, b \neq 0$ tal que $ab = 0$.

Definició C.1.5 (Domini d'integritat)**.** Sigui A un anell. Diem que A és un domini d'integritat si no té divisors de zero. Si A és domini d'integritat i prenem $a, b \in A$ tals que $ab = 0$, aleshores $a = 0$ o bé $b = 0$ (o, per contrarrecíproc, $a \neq 0, b \neq 0 \implies ab \neq 0$).

Proposició C.1.6. *Si A és domini d'integritat, aleshores $A[X]$ és domini d'integritat.*

Definició C.1.7 (Ideal)**.** Donat un anell A, un ideal d'A és un subconjunt I d'A tal que

1. $(I, +)$ és subgrup d'$(A, +)$.
2. $\forall a \in A, \forall x \in I$, aleshores $ax \in I$.

Definició C.1.8 (Domini d'ideals principals)**.** Si A és domini d'integritat i tots els ideals d'A són principals, diem que A és un domini d'ideals principals (DIP).

Proposició C.1.9. *Si $\mathbb{K}$ és cos, l'anell $\mathbb{K}[X]$ és domini d'ideals principals.*

Definició C.1.10 (Divisor)**.** Si A és un anell, amb $a, b \in A$, diem que a divideix b si existeix $c \in A$ tal que $b = ac$. Ho denotem per $a \mid b$. Clarament, $a \mid b \iff b \in (a)$.

Definició C.1.11 (Ideal suma)**.** Donats dos ideals I, J de l'anell A, posem $I + J$ el conjunt dels elements de l'anell A que són suma d'un element d'I i un element de J. Clarament, $I + J$ és un ideal d'A i és l'ideal d'A generat pel conjunt $I \cup J$. Anomenem $I + J$ *l'ideal suma* de I i J. Més generalment, si $\{I_j\}_{j\in\mathcal{J}}$ és una família d'ideals d'A:

$$\text{L'ideal suma } \sum_{j\in\mathcal{J}} I_j \text{ és l'ideal generat per } \bigcup_{j\in\mathcal{J}} I_j.$$

Definició C.1.12 (Ideal producte)**.** Donats dos ideals I, J de l'anell A, posem IJ el conjunt dels elements de l'anell A que són producte d'un element d'I i un element de J.

$$IJ = \{a_1b_1 + \cdots + a_kb_k \mid k \in \mathbb{N}; a_i \in I, b_i \in J; 1 \leq i \leq k\}.$$

Anomenem IJ *l'ideal producte* de I i J. Més generalment, si $I_1, \ldots, I_k$ són ideals d'A, posem $I_1 \cdots I_k$ l'ideal generat pel conjunt dels elements de l'anell A que són producte d'un element d'I_1, un element de I_2, i així fins un element d'I_k. Diem que $I_1 \cdots I_k$ és l'ideal producte dels ideals $I_1, \ldots, I_k$.

Està format pels elements de l'anell A que són sumes finites d'elements de la forma $a_1 \cdots a_k$, amb $a_i \in I$ i $1 \leq i \leq k$. Clarament, $I_1 \cdots I_k \subset I_1 \cap \cdots \cap I_k$. Si I és un ideal, posarem I^k per denotar el producte de l'ideal I amb ell mateix k vegades.

Proposició C.1.13 (Anell quocient)**.** *Sigui A un anell i I un ideal d'aquest anell A. Aleshores, A/I és anell. En particular, direm que A/I és l'anell quocient d'A per I.*

Proposició C.1.14.

1. *Si A és un anell de característica k, existeix un únic morfisme de $\mathbb{Z}/(k)$ en A i aquest morfisme és un monomorfisme.*
2. *Si A és un anell i k un enter, $k > 0$, es compleix $\operatorname{car} A = k \iff k$ és el menor enter positiu tal que $ka = 0$, per a tot $a \in A$.*
3. *Si A és domini d'integritat, la característica de A és o bé 0 o bé un nombre primer.*

C.2

Morfismes d'anells

Definició C.2.1 (Morfisme d'anells)**.** Si A, A' són anells, una aplicació $f : A \longrightarrow A'$ és morfisme d'anells si compleix:

$$f(a+b) = f(a) + f(b) \text{ i } f(ab) = f(a)f(b),$$

per a tot parell d'elements a, b d'A, i $f(1_A) = 1_{A'}$. Notem que si $f : A \longrightarrow A'$ és morfisme d'anells, aleshores f és morfisme de grups d'$(A, +)$ en $(A', +)$.

Definició C.2.2 (Morfisme injectiu)**.** Si $f : A \longrightarrow A'$ és morfisme d'anells, el nucli de f és $\ker(f) = \{a \in A \mid f(a) = 0_{A'}\}$; és a dir, el nucli de f com a morfisme de grups. Tenim, doncs, que f és un morfisme injectiu si, i només si, $\ker(f) = \{0_A\}$.

Proposició C.2.3. *Si $f : A \longrightarrow A'$ és morfisme d'anells, $\ker(f)$ és ideal d'A i $\mathrm{im}(f)$ és subanell d'A'.*

C.3

Teorema d'isomorfia

Definició C.3.1 (f factoritza a través d'un anell quocient)**.** Siguin A, A' anells, $f : A \longrightarrow A'$ un morfisme d'anells, I un ideal d'A i $\pi : A \longrightarrow A/I$ si existeix un morfisme d'anells $\overline{f} : A/I \longrightarrow A'$ tal que $f = \overline{f} \circ \pi$, és a dir, que faci commutatiu el diagrama:

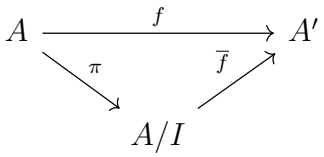


Figura C.1: Diagrama de factorització a través del quocient

Proposició C.3.2. *Siguin A, A' anells, $f : A \longrightarrow A'$ un morfisme d'anells, I un ideal propi d'A i $\pi : A \longrightarrow A/I$ el morfisme de pas al quocient. Aleshores, f factoritza a través d'A/I si, i només si, $I \subset \ker(f)$.*

Teorema C.3.3 (Primer teorema d'isomorfia per a anells)**.** *Si A, A' són anells i $f : A \longrightarrow A'$ és un morfisme d'anells, aleshores f factoritza a través d'$A/\ker(f)$ i tenim $f = i \circ \tilde{f} \circ \pi$, amb $\tilde{f}$ isomorfisme d'anells d'$A/\ker(f)$ en $\mathrm{im}(f)$, i la inclusió d'$\mathrm{im}(f)$ en A', $\pi : A \longrightarrow A/\ker(f)$ el morfisme de pas al quocient. Tenim, doncs, un diagrama commutatiu:*

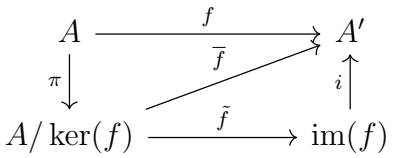


Figura C.2: Diagrama commutatiu del primer teorema d'isomorfis per a anells

C.4

Ideals primers i maximals

Definició C.4.1 (Ideal primer)**.** Sigui A un anell, un ideal I d'A es diu ideal primer si és ideal propi ($I \neq A$) i es compleix el següent per a tot $a, b \in A$: $ab \in I \implies a \in I$ o bé $b \in I$.

Proposició C.4.2. *Sigui I un ideal de l'anell A. Aleshores, I és primer si, i només si, A/I és domini d'integritat.*

Definició C.4.3 (Ideal maximal)**.** Un ideal I d'un anell A es diu maximal si és ideal propi i no existeix cap ideal J d'A tal que $I \subsetneq J \subsetneq A$. En altres paraules:

$$\left.\begin{array}{r} I \subsetneq J \implies J = A \\ I \subset J \subsetneq A \implies J = I \end{array}\right\} \iff I \text{ és maximal.}$$

Proposició C.4.4. *Sigui I un ideal d'un anell A. Aleshores, I és maximal si, i només si, A/I és un cos. En particular, tot ideal maximal és primer.*

Lema C.4.5 (Lema de Zorn)**.** *Sigui S un conjunt no buit ordenat inductivament. Aleshores, existeix un element maximal a S.*

Proposició C.4.6. *Sigui A un anell i $\mathfrak{a}$ un ideal propi d'A, és a dir, un ideal d'A diferent d'A. Aleshores, existeix un ideal maximal d'A que conté $\mathfrak{a}$.*

Corol·lari C.4.7. *Tot anell té al menys un ideal maximal.*

C.5

Cos de fraccions d'un domini

Sigui A un domini d'integritat. En el conjunt $A \times (A \setminus \{0\})$, definim $(a, b) \sim (a', b') \iff ab' = a'b$, on $\sim$ és una relació d'equivalència. La prova que és, en efecte, d'equivalència, és prou senzilla. Solament indicarem la transitivitat:

$$\left.\begin{array}{r} (a,b) \sim (a',b') \iff ab' = a'b \\ (a',b') \sim (a'',b'') \iff a'b'' = a''b' \end{array}\right\} \implies (ab'')b' = a'bb'' = a''b'b = (a''b)b'$$
$$\implies ab'' = a''b \iff (a,b) \sim (a'',b'').$$

en l'última implicació hem hagut d'usar que A és un domini d'integritat, ja que hem aplicat la propietat cancel·lativa.

Definició C.5.1 (Cos de fraccions d'A). Sigui $\mathbb{K}(A)$ el conjunt quocient de $A \times (A \setminus \{0\})$ per la relació d'equivalència $\sim$. Posem $\frac{a}{b}$ la classe d'(a, b) de manera que:

$$\frac{a}{b} = \frac{a'}{b'} \iff ab' = a'b.$$

Volem definir a $\mathbb{K}(A)$ una suma i un producte. Definim la suma per:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}.$$

Volem veure que no depèn del representant. Si $\frac{a}{b} = \frac{a'}{b'}$ i $\frac{c}{d} = \frac{c'}{d'}$, tenim que $ab' = a'b$ i $cd' = c'd$; per tant, $(ad + bc)b'd' = (a'd' + c'b')bd$ i

$$a'd'bd + c'b'bd = adb'd' + bb'cd' \implies \frac{ad + bc}{bd} = \frac{a'd' + b'c'}{b'd'}.$$

Per a la suma tenim que el neutre és $\frac{0}{b}$ i l'oposat, $-\frac{a}{b} = \frac{-a}{b}$. Per tant, la suma no depèn del representant i està ben definida. Pel que fa al producte, el definim per:

$$\frac{a}{b}\frac{c}{d} = \frac{ac}{bd}.$$

Hem de veure que no depèn del representant. En efecte, si $\frac{a}{b} = \frac{a'}{b'}$ i $\frac{c}{d} = \frac{c'}{d'}$, tenim $ab' = a'b$ o $cd' = c'd$ i, per tant:

$$(ac)(b'd') = (ab')(cd') = (a'b)(c'd) = (a'c')(bd) \implies \frac{ac}{bd} = \frac{a'c'}{b'd'}.$$

Clarament, $\frac{1}{1}$ és el neutre pel producte. Per tant, $\mathbb{K}(A)$ és anell amb aquestes suma i producte. Tot element no nul de $\mathbb{K}(A)$ té inversa, ja que per a $\frac{a}{b} \neq 0_{\mathbb{K}_A}$ tenim que $a \neq 0$ i $\frac{b}{a}\frac{a}{b} = \frac{ab}{ab} = 1_{\mathbb{K}(A)}$. Per tant, $\mathbb{K}(A)$ és un cos que anomenem *cos de fraccions d'A*.

Proposició C.5.2. *Siguin A un domini d'integritat, L un cos i $g : A \longrightarrow L$ un monomorfisme d'anells. Aleshores, existeix un únic monomorfisme de cossos $h : \mathbb{K}(A) \longrightarrow L$ tal que $g = h \circ i$; és a dir, tal que el diagrama:*

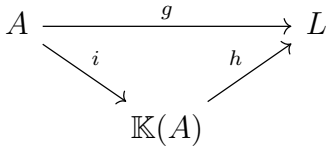


Figura C.3: Diagrama de C.5.2

commuta.

C.6

Divisibilitat

Definició C.6.1 (Elements associats)**.** Dos elements a, b d'un anell A es diuen associats si existeix una unitat $u \in A$ (element invertible) tal que $b = ua$. Posem $a \sim b$ per indicar que a i b són associats. Clarament, la relació $\sim$ és d'equivalència.

Proposició C.6.2. *Sigui A un anell, $a, b \in A$. Si més no un dels dos elements a, b és no divisor de zero, es compleix:*

$$a \mid b \ i \ b \mid a \iff a \sim b.$$

En particular, si A és domini d'integritat, aleshores es compleix l'equivalència per a tot parell d'elements $a, b \in A$.

Definició C.6.3 (Divisors propis)**.** Si a és un element no nul d'un anell A, les unitats d'A i els elements associats d'a divideixen a. Direm divisors propis d'a els divisors d'a diferents d'aquests.

Definició C.6.4 (Element irreductible)**.** Un element a no nul d'un domini d'integritat d'A s'anomena *irreductible* si no és una unitat i no té divisors propis. Un element a no nul i no unitat s'anomena compost si té divisors propis.

Definició C.6.5 (Màxim comú divisor)**.** Siguin A un anell, $a, b, d \in A$. Diem que d és un màxim comú divisor d'a i b si se satisfan les dues propietats següents:

1. $d \mid a$, $d \mid b$ i
2. si $c \in A$ satisfà que $c \mid a$ i $c \mid b$, aleshores $c \mid d$.

El màxim comú divisor queda determinat tret d'associats.

Definició C.6.6 (Mínim comú múltiple)**.** Siguin A un anell i $a, b, m \in A$. Diem que m és un màxim comú múltiple d'a i b si se satisfan les dues propietats següents:

1. $a \mid m$, $b \mid m$ i
2. si $n \in A$ satisfà que $a \mid n$ i $b \mid n$, aleshores $m \mid n$.

El mínim comú múltiple queda determinat tret d'associats.

C.7

Dominis euclidians

Definició C.7.1 (Domini euclidià)**.** Sigui A un domini d'integritat. Direm que A és un domini euclidià si existeix una aplicació $\delta : A \setminus \{0\} \longrightarrow \mathbb{N}$ tal que:

1. Si $a, b \in A \setminus \{0\}$ i $a \mid b$, aleshores $\delta(a) \leq \delta(b)$.
2. *Divisió entera respecte de δ*: Donats $a, b \in A$, amb $b \neq 0$, existeixen $q, r \in A$ tals que $a = bq + r$ i $\delta(r) < \delta(b)$, sempre que $r \neq 0$ (si $r = 0$, $a = bq$).

Si A és un domini euclidià i $\delta : A \setminus \{0\} \longrightarrow \mathbb{N}$ és una aplicació que compleix ambdues propietats, direm que (A, δ) és un domini euclidià.

Proposició C.7.2. *Tot domini euclidià és domini d'ideals principals.*

Definició C.7.3 (Norma euclidiana)**.** Sigui A un anell. Una norma d'A és una aplicació $N : A \longrightarrow \mathbb{Z}$ tal que compleix les següents propietats:

1. Si $a \in A$, $N(a) = 0$ si, i només si, $a = 0$;
2. $N(ab) = N(a)N(b)$ per a qualssevol elements a, b d'A.

Proposició C.7.4. *Sigui A un anell que té una norma N; aleshores:*

1. *A és domini d'integritat.*
2. *$\delta : A \setminus \{0\} \longrightarrow \mathbb{N}$ definida per $\delta(a) = |N(a)|$ compleix la primera propietat del domini euclidià.*
3. $N(1) = 1$.
4. $u \in A^* \implies N(u) = \pm 1$.

C.8

Factorialitat en dominis d'ideals principals

Definició C.8.1 (Element primer)**.** Un element p d'un domini d'integritat A es diu primer si p és no nul i no unitat, i per a $a, b \in A$ es compleix:

$$p \mid ab \implies p \mid a \text{ o bé } p \mid b.$$

Proposició C.8.2. *En un domini d'integritat A, un element p no nul és primer si, i només si, l'ideal (p) és primer.*

Proposició C.8.3. *En un domini d'integritat, tot element primer és irreductible. En un domini d'ideals principals, tot element irreductible és primer.*

C.9

Dominis de factorització única

Definició C.9.1 (Domini de factorització única)**.** Un domini d'integritat A es diu *domini de factorització única* si es compleixen les dues propietats següents:

1. Per a tot element a no nul i no unitat d'A, existeixen elements irreductibles $p_1, \ldots, p_r$ d'A tals que $a = p_1 \cdots p_r$.
2. Si $p, p_1, \ldots, p_r$ són elements irreductibles d'A i $p \mid p_1 \cdots p_r$, aleshores p és associat amb algun p_i.

Definició C.9.2 (Domini de factorització)**.** Si A és un domini d'integritat que compleix la primera propietat de la factorització única, direm simplement que és un *domini de factorització*.

Observació C.9.3. Tenim que tot domini euclidià és un domini d'ideals principals. Al seu torn, tot domini d'ideals principals és domini de factorització única. Es dona, doncs, aquesta cadena d'implicacions.

Proposició C.9.4. *Sigui A un domini de factorització. Aleshores, A és domini de factorització única si, i només si, tot element irreductible d'A és primer.*

Proposició C.9.5. *Per a un nombre enter d lliure de quadrats, l'anell $\mathbb{Z}[\sqrt{d}]$ és domini de factorització.*

C.10

Factorialitat en un anell de polinomis

Proposició C.10.1. *Sigui A un domini d'integritat. Les propietats següents són equivalents:*

1. *A és un cos.*
2. *$A[X]$ és un domini euclidià.*
3. *$A[X]$ és un domini d'ideals principals.*

Definició C.10.2 (Contingut d'un polinomi)**.** Sigui $f(X) = a_n X^n + \cdots + a_1 X + a_0 \in A[X]$ un polinomi amb coeficients en un domini de factorització única A. Anomenarem *contingut* de f un màxim comú divisor dels coeficients d'f. Denotem per $c(f)$ el contingut de f. Tenim, doncs:

$$c(f) = \operatorname{mcd}(a_0, a_1, \ldots, a_n).$$

Clarament, el contingut d'un polinomi d'$A[X]$ queda determinat tret d'un factor d'A^*.

Definició C.10.3 (Primitiu)**.** Direm que f és primitiu si el seu contingut $c(f)$ és una unitat.

Definició C.10.4 (Polinomi primitiu corresponent a f)**.** Donat $f \in A[X]$, existeix clarament un polinomi primitiu f^* tal que $f = c(f)f^*$. El polinomi f^* és únic en el sentit següent: si $f = c\tilde{f}$, amb $c \in A$ i $\tilde{f}$ primitiu, aleshores $c \sim c(f)$ i $\tilde{f} \sim f^*$. Direm que f^* és un polinomi primitiu corresponent a f.

Proposició C.10.5 (Lema de Gauss)**.** *Sigui A un domini de factorització única. Aleshores, en $A[X]$ el producte de polinomis primitius és primitiu. Més generalment, si $f, g \in A[X]$, $c(fg) \sim c(f)c(g)$.*

Corol·lari C.10.6. *Sigui A un domini de factorització única, $\mathbb{K}$ el cos de fraccions d'A i $f \in A[X]$ mònic. Si $f = gh$, amb $g, h \in \mathbb{K}[X]$ mònics, aleshores $g, h \in A[X]$.*

Corol·lari C.10.7 (Lema de Gauss, versió 2)**.** *Siguin A un domini de factorització única, $\mathbb{K}$ el seu cos de fraccions, $f(X) \in A[X]$ un polinomi no nul i $g(X), h(X) \in K[X]$ polinomis tals que $f(X) = g(X)h(X)$. Existeixen elements $c_g, c_h \in K$ i polinomis $g'(X), h'(X) \in A[X]$ de contingut 1 tals que $g(X) = c_g \cdot g'(X)$ i $h(X) = c_h \cdot h'(X)$, el producte $c_g c_h \in A$ i $f(X) = (c_g c_h)g'(X)h'(X)$. És a dir, una descomposició de $f(X)$ en $K[X]$ dona lloc a una descomposició de $f(X)$ en $A[X]$.*

Definició C.10.8 (Element irreductible, anell de polinomis)**.** Sigui A un domini de factorització única. Un element d'A és element irreductible d'$A[X]$ si, i només si, és element irreductible d'A (un element d'$A[X]$ de grau positiu no pot dividir un element d'A).

Proposició C.10.9. *Sigui A un domini de factorització única i sigui $f(X) \in A[X]$. Les condicions següents són equivalents:*

1. *$f(X)$ té grau positiu i és irreductible a $A[X]$.*
2. *$c(f) \sim 1$ (f és primitiu) i $f(X)$ és irreductible a $\mathbb{K}[X]$.*

Demostració. Provarem la implicació cap a baix, $\Rightarrow$, i cap a dalt, $\Leftarrow$.

$\boxed{\Rightarrow}$ Suposem que $f(X)$ té grau positiu i és irreductible a $A[X]$. Tot element irreductible d'A és irreductible a $A[X]$. La factorització $f = c(f)f^*$, amb f^* primitiu, és no trivial (sempre que $c(f)$ no sigui una unitat). Com que f és irreductible, deduïm que $c(f)$ és una unitat; és a dir, $c(f) \sim 1$. Per veure que $f(X)$ és irreductible a $\mathbb{K}[X]$, posem $f = gh$, amb $g, h \in \mathbb{K}[X]$ i $\mathrm{gr}(h) > 0$. *Volem veure que g ha de tenir grau zero i, per tant, ha de ser una unitat de $\mathbb{K}[X]$.* Si a és denominador comú dels coeficients de $g(X)$ i b dels de $h(X)$, tenim que ag i bh són elements d'$A[X]$ i $abf = (ag)(bh)$ és una factorització d'abf en $A[X]$. Siguin g^*, h^* els polinomis primitius corresponents a ag i bh: $ag = c(ag)g^*$ i $bh = c(bh)h^*$. Aleshores:

$$ab \sim c(abf) = c((ag)(bh)) \sim c(ag)c(bh),$$

pel lema de Gauss i, per tant, $f = ug^*h^*$, amb $u \in A^*$. Com f és irreductible a $A[X]$ i h^* té grau positiu, g^* és una unitat d'$A[X]$ i, per tant, $g^* \in (A[X])^* = A^*$. En conseqüència, g^* és de grau 0 i g és constant.

$\boxed{\Leftarrow}$ Sigui $f \in A[X]$ amb $c(f) \sim 1$, i suposem que f és irreductible a $\mathbb{K}[X]$. Posem $f = gh$, amb $g, h \in A[X]$, h de grau positiu. Com $A[X] \subset \mathbb{K}[X]$, g ha de tenir grau 0 i, així, $g \in \mathbb{K} \cap A[X] = A$. Ara, la relació $1 \sim c(f) \sim c(g)c(h) \sim g \cdot c(h)$ dona que $g \in A^*$. Per tant, f és irreductible a $A[X]$.

■

Lema C.10.10. *Si $p \in A$ és un primer en A, aleshores p també és un primer en $A[X]$.*

Corol·lari C.10.11. *Per a tot cos $\mathbb{K}$ i tot $n \geq 1$, l'anell de polinomis $\mathbb{K}[X_1, \ldots, X_n]$ és un domini de factorització única.*

Teorema C.10.12. *Si A és un domini de factorització única, aleshores $A[X]$ és un domini de factorització única.*

Proposició C.10.13 (Criteris d'irreductibilitat)**.**

1. *Sigui $f(X) \in A[X], f(X) = a_0 + a_1X + \cdots + a_nX^n$. Si $\frac{c}{d}$ és una arrel de f a $\mathbb{K}$, amb $\mathrm{mcd}(c,d) = 1$, aleshores $c \mid a_0$ i $d \mid a_n$.*
2. *Sigui $f(X) \in A[X]$ un polinomi primitiu de grau 2 o 3. Aleshores, $f(X)$ és irreductible si, i només si, no té cap arrel a $\mathbb{K}$.*

Proposició C.10.14 (Criteri modular)**.** *Sigui $f(X) = a_0+a_1X+\cdots+a_nX^n \in A[X]$, primitiu, i suposem que existeix $p \in A$, irreductible, tal que $p \nmid a_n$ i que el polinomi $\overline{f}(X) = \overline{a_0} + \overline{a_1}X + \cdots + \overline{a_n}X^n \in (A/(p))[X]$ és irreductible (on $\overline{a}$ indica la classe d'$a \in A$ en el quocient $A/(p)$ pel morfisme de pas al quocient $\pi : A \longrightarrow A/(p)$). Aleshores, f és irreductible en $A[X]$.*

Proposició C.10.15 (Criteri d'Eisenstein)**.** *Sigui $f(X) = a_0 + a_1X + \cdots + a_nX^n \in A[X]$ primitiu i sigui $p \in A$, irreductible en A. Suposem que $p \mid a_0, p \mid a_1, \ldots, p \mid a_{n-1}, p \mid a_n$ i $p^2 \nmid a_0$. Aleshores, $f(X)$ és irreductible.*

Bibliografia

[Lan02] Serge Lang. *Algebra*. eng. 3rd ed. 2002. Graduate Texts in Mathematics, 211. New York, NY: Springer New York, 2002. ISBN: 1-4613-0041-X.

This book is intended as a basic text for a one-year course in Algebra at the graduate level, or as a useful reference for mathematicians and professionals who use higher-level algebra. It successfully addresses the basic concepts of algebra. For the revised third edition, the author has added exercises and made numerous corrections to the text.

[Lav20] Olga Lavila Vidal. *Equacions algebraiques : 274 exercicis resolts*. cat. Textos docents ; 423. Barcelona: Edicions de la Universitat de Barcelona, 2020. ISBN: 9788491683919.

[Cre22] Teresa Crespo. *Estructures Algebraiques*. 1a ed. Vol. 1. Barcelona, BCN: Universitat de Barcelona, 2022.

Apunts de l'assignatura Estructures Algebraiques, impartida per Teresa Crespo durant el semestre de tardor del curs 2022-2023.

[Gui22] Xavier Guitart. *Equacions Algebraiques*. 1a ed. Vol. 1. Barcelona, BCN: Universitat de Barcelona, 2022.

Apunts de l'assignatura Equacions Algebraiques, impartida per Xavier Guitart durant el semestre de tardor del curs 2023-2024.

[Vil23] Mario Vilar. *Estructures Algebraiques*. Barcelona, BCN, 2023. URL: `https://mariovilar.github.io/matematiques-enginyeria-informatica/3/cinque-semestre/EA/apunts-estructures.pdf`.

Apunts de l'assignatura Estructures Algebraiques, impartida per Teresa Crespo durant el semestre de tardor del curs 2022/2023.

[Tra23] Artur Travesa. *Equacions Algebraiques*. 1a ed. Vol. 1. Barcelona, BCN: Universitat de Barcelona, 2020/2023. URL: `https://travesa.cat/fitxers/notes/EquacionsAlgebraiques.pdf`.

Apunts de l'assignatura Equacions Algebraiques, impartida per Artur Travesa.