

# Equacions algebraiques

ARTUR TRAVESA

Universitat de Barcelona

AUTOR

Artur **Travesa Grau**

Facultat de Matemàtiques i Informàtica

Universitat de Barcelona

CLASSIFICACIÓ AMS: Primària: 01A75, 00B50

Secundària: 01A45, 01A50, 01A55, 01A60, 01A61, 01A65, 01A72, 01A73, 01A74, 01A75,  
11-03, 30-03, 33-03, 34-03, 49-03

Universitat de Barcelona

Facultat de Matemàtiques i Informàtica

Barcelona, 2020

© 2019, 2020 Artur Travesa

# Presentació

Aquest text és fruit d'anys d'experiència en cursos destinats, essencialment, a l'estudi de les extensions algebraïques de cossos amb la finalitat principal de comprendre el problema de la resolubilitat per radicals, o no, de les equacions algebraïques en una incògnita.

Sovint succeeix en matemàtiques que quan algú troba una solució d'un problema no hi ha eines o teories suficientment potents per a poder-la explicar o difondre de manera prou senzilla. Podríem dir que costa expressar clarament les idees que hi ha darrere de la prova. És en aquest estadi que es creen les teories que serveixen essencialment per a donar una explicació de la resolució que s'ha fet del problema. I algunes vegades aquestes teories permeten resoldre altres problemes, o bé explicar-ne solucions de manera més senzilla que abans de la teoria.

Un cas paradigmàtic es presenta en la teoria de Galois. De fet, l'estudi del problema de la resolubilitat per radicals de les equacions algebraïques es remunta, si no als antics babilonis, que ja “saben resoldre” per radicals (algunes) equacions quadràtiques, als matemàtics del Renaixement. Poc a poc es van produïnt avenços, i aconseguïen resoldre per radicals algunes equacions cúbiques i algunes equacions quàrtiques (del Ferro, Tartaglia, Cardano, Ferrari). Però les quintiques es resisteixen.

Després d'uns tímids avenços d'Euler, i que els estudis de la primera part del segle XVIII no aconseguïen fer avançar (gaire) en una solució del problema, els matemàtics de la Il·lustració (per exemple, Lagrange o Legendre) posen les bases perquè, en el primer terç del segle XIX, i després de l'aparició cabdal de les *Disquisitiones Arithmeticae*, on Gauss, entre moltes altres coses, ensenya la resolució d'equacions ciclotòmiques, matemàtics molt joves com Ruffini, Abel o Galois donin un impuls definitiu a una solució del problema. En efecte, Ruffini i, independentment, Abel aconseguïen provar la irresolubilitat (per radicals) de la quintica (general), i Galois caracteritza quines equacions es poden resoldre per radicals i quines no.

Un cop resolt el problema, però, cal explicar-lo i fer-lo entenedor a la comunitat matemàtica. Només cal que pensem que la teoria de conjunts (tot i que sembla clar que, per exemple, Gauss ja la té al cap, com també hi té una certa idea de teoria de grups) no *s'inventa* fins a final del segle XIX, a partir de treballs de Dedekind o de Cantor, de manera que per a explicar la teoria de Galois en aquells moments calia fer autèntiques filigranes. És a partir de Kronecker i de Weber, a final del segle XIX i començament del segle XX, i encara més a partir d'Artin, al final del primer terç del segle XX, quan la teoria de Galois adopta una forma en què es pot explicar de manera raonablement còmoda.

Efectivament, per a l'estudi d'aquest problema, una eina que s'ha demostrat útil, i que, de fet, ha estat creada per a poder-ne presentar de manera raonablement senzilla una

explicació d'una solució, és la teoria anomenada de Galois per a extensions algebraiques finites de cossos.

Així, aquest text és una presentació d'aquesta teoria, amb l'èmfasi posat en les extensions resolubles, que són les associades de manera natural a les equacions resolubles per radicals. És per això que comencem per les equacions del tipus  $X^n = 1$  (arrels de la unitat, Gauss); més endavant estudiem les equacions del tipus  $X^n = a$  (radicals, formulació precisa del problema); i, finalment, presentem un estudi de la resolubilitat per radicals. En particular, donem una caracterització de les equacions resolubles per radicals (Galois). I també establim el resultat, no sempre prou conegut o ben comprès, de la no-existència de fórmules per a resoldre per radicals les equacions generals de grau més gran o igual que 5, que no són resolubles per radicals (Abel).

D'altra banda, la teoria que desenvolupem també permet donar resposta de manera senzilla a alguns problemes clàssics d'impossibilitat de certes construccions geomètriques que se cercaven a l'antiguitat, com a mínim, des de la Grècia clàssica: impossibilitat de duplicar un cub, o de trisecar un angle arbitrari, o de quadrar un cercle (Lindemann), només amb regla i compàs. I també permet caracteritzar de manera senzilla quines seccions del cercle es poden construir només amb regla i compàs (Gauss). Plantegem l'enunciat precís d'aquests problemes i en donem una solució com a conseqüència de la teoria explicada en el curs.

Un fet que, a parer de qui escriu aquestes notes, desvirtua l'enfocament del problema de la resolubilitat per radicals, és plantejar-se com a objectiu important el càlcul del reticle de **totes** les subextensions d'una certa extensió algebraica; per a l'autor, l'objectiu no és aquest. És cert que sovint convé calcular **alguns** dels cossos d'aquest reticle; però gairebé mai cal calcular-los tots: sol ser suficient el càlcul de només una part del reticle. Però no avancem continguts. Potser el lector podrà trobar resposta a algunes qüestions que es plantegen de manera natural en aquest context. Tampoc no les trobarà totes; i així tindrà una porta oberta a un estudi posterior del tema, si vol.

Barcelona, curs 2019-2020

Artur Travesa

# Contingut

<b>Presentació</b>	<b>iii</b>
<b>Contingut</b>	<b>v</b>
<b>Introducció</b>	<b>1</b>
0.1 Equacions de grau 1 . . . . .	1
0.2 Teorema fonamental de l'Àlgebra (enunciat) . . . . .	2
0.3 Equacions de grau 2 . . . . .	4
0.4 Equacions de grau 3 . . . . .	5
0.5 Exercicis . . . . .	7
<b>1 Equacions algebraiques</b>	<b>9</b>
1.1 Polinomis i equacions algebraiques . . . . .	9
1.2 Divisió de polinomis . . . . .	12
1.3 Divisibilitat i arrels múltiples . . . . .	14
1.4 Factorització única a $k[X]$ . . . . .	17
1.5 Factorització única a $A[X]$ . . . . .	20
1.6 Criteris d'irreductibilitat de polinomis . . . . .	23
1.7 Un mètode de factorització en $\mathbb{Z}[X]$ . . . . .	25
1.8 Exercicis . . . . .	29
<b>2 Teorema fonamental de l'Àlgebra</b>	<b>31</b>
2.1 Polinomis simètrics . . . . .	31
2.2 Fórmules de Viète . . . . .	33
2.3 Teorema de Waring . . . . .	35
2.4 Discriminant d'un polinomi . . . . .	38
2.5 Prova del teorema fonamental de l'Àlgebra . . . . .	39
2.6 Exercicis . . . . .	41
<b>3 Arrels de la unitat</b>	<b>45</b>

3.1	Arrels de la unitat . . . . .	46
3.2	Polinomis ciclotòmics . . . . .	47
3.3	Elements algebraics i elements transcendents . . . . .	51
3.4	Extensions finites de cossos . . . . .	52
3.5	Cossos ciclotòmics . . . . .	56
3.6	Cossos quadràtics . . . . .	58
3.7	Grup de Galois dels cossos ciclotòmics . . . . .	59
3.8	Grup de Galois d'una extensió algebraica . . . . .	61
3.9	Extensions normals . . . . .	63
3.10	Cossos finits . . . . .	68
3.11	Exercicis . . . . .	71
<b>4</b>	<b>Radicals</b>	<b>75</b>
4.1	L'equació $X^n = a$ . . . . .	76
4.2	Irreductibilitat de $X^{p^r} - a$ . . . . .	77
4.3	Separabilitat . . . . .	82
4.4	Extensions separables . . . . .	85
4.5	El teorema de l'element primitiu . . . . .	89
4.6	Normes i traces . . . . .	91
4.7	Separabilitat i traça . . . . .	94
4.8	El teorema 90 de Hilbert . . . . .	95
4.9	Extensions cícliques . . . . .	97
4.10	Teoria (bàsica) de Kummer . . . . .	99
4.11	Radicals en característica zero . . . . .	103
4.12	Extensions radicals . . . . .	105
4.13	Exercicis . . . . .	107
<b>5</b>	<b>Teorema fonamental i aplicacions</b>	<b>109</b>
5.1	El teorema d'Artin . . . . .	110
5.2	El teorema fonamental de la teoria de Galois . . . . .	111
5.3	Grups resolubles . . . . .	115
5.4	Resolubilitat per radicals . . . . .	118
5.5	Equacions ciclotòmiques . . . . .	121
5.6	Grups de Galois com a grups de permutacions . . . . .	122
5.7	L'equació general de grau $n$ . . . . .	125
5.8	L'equació general de grau 3 . . . . .	127
5.9	Les equacions de grau 4 . . . . .	130

5.10	Construccions amb regla i compàs . . . . .	135
5.11	Seccions construïbles del cercle . . . . .	141
5.12	La transcendència de $\pi$ . . . . .	144
5.13	Exercicis . . . . .	149
<b>A</b>	<b>Definicions i propietats bàsiques</b>	<b>151</b>
A.1	Grups . . . . .	151
A.1.1	Grups . . . . .	152
A.1.2	Morfismes de grups . . . . .	153
A.1.3	Producte de grups . . . . .	153
A.1.4	Subgrups . . . . .	154
A.1.5	Subgrups normals i grups quocient . . . . .	154
A.1.6	Accions de grups en conjunts . . . . .	156
A.2	Anells . . . . .	157
A.2.1	Anells . . . . .	157
A.2.2	Morfismes d'anell . . . . .	159
A.2.3	Subanells . . . . .	159
A.2.4	Elements invertibles. Cossos . . . . .	160
A.2.5	Divisors de zero. Dominis d'integritat . . . . .	160
A.2.6	L'anell producte . . . . .	162
A.3	Ideals i anells quocient . . . . .	162
A.3.1	Ideals . . . . .	162
A.3.2	Anells quocient . . . . .	163
A.3.3	Dominis d'ideals principals . . . . .	164
A.3.4	Ideals primers, maximals . . . . .	164
A.3.5	Característica d'un anell . . . . .	164
A.4	Mòduls i àlgebres . . . . .	165
A.4.1	Mòduls . . . . .	165
A.4.2	Àlgebres . . . . .	167
<b>B</b>	<b>El lema de Zorn</b>	<b>169</b>
<b>C</b>	<b>Solucions d'alguns exercicis</b>	<b>173</b>
C.0	Exercicis de la Introducció . . . . .	173
C.1	Exercicis del capítol 1 . . . . .	175
C.2	Exercicis del capítol 2 . . . . .	179
C.3	Exercicis del capítol 3 . . . . .	185

C.4 Exercicis del capítol 4 . . . . .	192
C.5 Exercicis del capítol 5 . . . . .	193
<b>D Cronologia</b>	<b>197</b>
<b>Referències</b>	<b>201</b>
<b>Índex de figures</b>	<b>203</b>
<b>Índex de diagrames</b>	<b>205</b>
<b>Índex terminològic</b>	<b>207</b>



# Introducció

En tota l'obra, i com és habitual, designem per  $\mathbb{Z}$ ,  $\mathbb{Q}$ ,  $\mathbb{R}$ , o  $\mathbb{C}$  els conjunts dels nombres enters, racionals, reals, o complexos, respectivament. També utilitzem lliurement les notacions usuals de la teoria de conjunts i aplicacions:  $A \subseteq B$ ,  $B \supseteq A$ ,  $\{x : \dots\}$ ,  $x \in C$ ,  $f : A \rightarrow B$ , etcètera. L'apèndix **A** conté un resum de les notacions i les propietats bàsiques que fem servir sobre grups i sobre anells. En el text principal, presentem els resultats de teoria de grups i de teoria d'anells més íntimament lligats al desenvolupament que fem de la teoria de Galois.

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

**Problema 0.** Donada una equació polinòmica  $a_0 + a_1X + \dots + a_nX^n = 0$ , o bé, equivalentment, donat un polinomi  $a_0 + a_1X + \dots + a_nX^n$ :

L'equació	El polinomi
(a) Té solucions?	(a') Té arrels?
(b) Quantes solucions té?	(b') Quantes arrels té?
(c) On té les solucions?	(c') On té les arrels?
(d) Com són les solucions?	(d') Com són les arrels?
(e) Les solucions, es poden calcular?	(e') Les arrels, es poden calcular?
(f) En cas afirmatiu, com?	(f') En cas afirmatiu, com?

Notem que parlem de *solucions* d'una equació, però, en canvi, d'*arrels* d'un polinomi (cf., més avall, **1.1.13**).

Amb la finalitat de centrar el problema, comencem amb la presentació d'alguns exemples.

## 0.1 Equacions de grau 1

Possiblement, hi hauria un consens molt ampli en què les equacions més senzilles de resoldre són les de grau 1; és a dir, les equacions de la forma  $aX + b = 0$ ,  $a \neq 0$ . En qualsevol cas, considerem aquestes en primer lloc.

**0.1.1.** És prou conegut que si  $a, b \in \mathbb{Z}$ ,  $a \neq 0$ , una condició necessària i suficient perquè l'equació  $aX + b = 0$  tingui alguna solució  $x \in \mathbb{Z}$  és que  $b$  sigui un múltiple de  $a$ . A més a més, en aquest cas, si  $c \in \mathbb{Z}$  és l'únic nombre enter tal que  $b = a \cdot c$ , llavors  $x = -c$  és l'única solució entera de l'equació.

**0.1.2.** També és ben conegut que si  $a, b \in \mathbb{Q}$ , o bé  $a, b \in \mathbb{R}$ , o bé  $a, b \in \mathbb{C}$ , o bé, més generalment,  $a, b$  són elements d'un cos qualsevol (cf. **A.2.28** per a la definició formal de cos),  $k$ , i  $a \neq 0$ , l'equació  $aX + b = 0$  admet una única solució en  $k$ ,  $x := -\frac{b}{a} \in k$ .

**0.1.3.** Si  $a, b$  pertanyen a altres anells, la resolució de l'equació pot ser més complicada. Per exemple, l'equació  $3X + 2 = 0$  en  $\mathbb{Z}/6\mathbb{Z}$  no té cap solució; l'equació  $4X + 2 = 0$  en  $\mathbb{Z}/6\mathbb{Z}$  té exactament les dues solucions  $x = 1$  i  $x = 4$ ; i l'equació  $5X + 2 = 0$  en  $\mathbb{Z}/6\mathbb{Z}$  té l'única solució  $x = 2$ .

**Exercici 0.1.4.** Quantes solucions té, en  $\mathbb{Z}/6\mathbb{Z}$ , l'equació  $X + 2 = 0$ ? I quantes l'equació  $2X + 2 = 0$ ?

**Observació 0.1.5.** No cal dir que podríem posar-nos en situacions en què la resposta és més complicada. Per exemple, si considerem l'anell de les funcions reals de variable

real, i definim  $a$  com la funció característica de  $\mathbb{Q}$ ,  $a(r) := \begin{cases} 1, & \text{si } r \in \mathbb{Q}, \\ 0, & \text{si } r \notin \mathbb{Q}, \end{cases}$  el cardinal

del conjunt de solucions  $x : \mathbb{R} \rightarrow \mathbb{R}$  de l'equació  $aX = 0$  és  $2^{\#\mathbb{R}}$ , un cardinal que és estrictament més gran que el cardinal del conjunt dels nombres reals.

**0.1.6.** Aquests exemples posen de manifest de manera intuïtivament clara que la resolució de l'equació de grau 1 és més senzilla en el cas que els coeficients de l'equació siguin elements d'un cos i se cerquin les solucions en aquest cos. A més a més, en aquest cas, podem resumir una solució del **Problema 0** en l'enunciat següent.

**Proposició 0.1.7.** *Siguin  $k$  un cos,  $a, b \in k$ ,  $a \neq 0$ . Existeix un únic element  $x \in k$  tal que  $ax + b = 0$ ; aquest element és  $x = -\frac{b}{a}$ .  $\square$*

**Observació 0.1.8.** Les equacions de grau 1 tenen una propietat molt especial. Suposem que  $k \subseteq K$ , on  $K$  és un cos que conté  $k$  com a subcòs, i que  $a, b \in k$ ,  $a \neq 0$ . En aquest cas,  $x = -\frac{b}{a} \in k$ ; és a dir, la solució (única) de l'equació en el cos  $K$  és la solució de l'equació en el subcòs  $k$ . Dit d'una altra manera, totes les solucions de l'equació pertanyen a qualsevol subcòs a què pertanyin els coeficients de l'equació. Presentem de seguida exemples on veiem que aquesta situació no es repeteix en general.

## 0.2 Teorema fonamental de l'Àlgebra (enunciat)

En general, el resultat de l'observació anterior (**0.1.8**), que és vàlid per a les equacions de grau 1, no s'estén a les equacions de grau més gran que 1. Per exemple, el polinomi  $X^2 + 1$  és de coeficients reals, però les seves arrels complexes,  $\sqrt{-1}$ ,  $-\sqrt{-1}$ , són nombres complexos no reals.

Amb la finalitat de centrar més el **Problema 0**, i també de situar-nos en unes hipòtesis que, d'una banda, siguin prou generals com perquè resoldre el problema tingui interès, i, de l'altra, siguin prou restrictives com perquè poguem donar-li una resposta mínimament interessant, centrem l'atenció en les equacions polinòmiques  $a_0 + a_1X + \dots + a_nX^n = 0$ , de coeficients  $a_0, a_1, \dots, a_n$  en un cert cos  $k$ ,  $a_n \neq 0$ . Així podem enunciar el problema d'una manera més precisa.

**Problema.** Siguin  $k$  un cos,  $n \geq 1$  un nombre natural, i  $a_0, a_1, \dots, a_n \in k$ , elements qualssevol, però amb  $a_n \neq 0$ . Ens interessem per les qüestions següents sobre les solucions de l'equació polinòmica  $a_0 + a_1X + \dots + a_nX^n = 0$ : en té?, quantes?, on?, com són?, es poden calcular?, de quina manera?

**Observació 0.2.1.** Notem que en els exemples previs, en què les equacions eren explícites, hem escrit els polinomis com a suma d'una successió de monomis de grau decreixent; en el cas general, però, és més còmode fer-ho com a suma d'una successió de monomis de grau creixent, com ja hem fet des de l'inici d'aquesta introducció.

Per al cas de les equacions polinòmiques de coeficients complexos, el resultat següent, anomenat *teorema fonamental de l'Àlgebra*, dóna una resposta a les tres primeres preguntes.

**Teorema 0.2.2** (fonamental de l'Àlgebra). *La suma de les multiplicitats de les arrels complexes d'un polinomi no nul de coeficients complexos coincideix amb el grau del polinomi. Equivalentment, tot polinomi no constant de coeficients complexos té alguna arrel en  $\mathbb{C}$ .*

**Observació 0.2.3.** Els conceptes de grau d'un polinomi, d'arrel d'un polinomi i de multiplicitat d'una arrel d'un polinomi són objecte d'un estudi més detallat més endavant (cf. **1.1.4**, **1.1.13**, **1.3.6**). D'altra banda, una demostració del teorema fonamental de l'Àlgebra també es presenta més endavant (cf. **2.5.1**).

Aquesta propietat de  $\mathbb{C}$  no és comuna a tots els cossos; convé donar un nom als cossos que la tenen.

**Definició 0.2.4.** Sigui  $k$  un cos. Es diu que  $k$  és un cos *algebraicament tancat* si, i només si, per a tot polinomi no nul,  $f(X)$ , de coeficients en  $k$  la suma de les multiplicitats de les arrels de  $f(X)$  en  $k$  coincideix amb el grau de  $f(X)$ . Equivalentment, si tot polinomi no constant,  $f(X)$ , de coeficients en  $k$ , té alguna arrel en  $k$ .

**Corol·lari 0.2.5.** *Sigui  $k \subseteq \mathbb{C}$  un subcòs i  $f(X)$  un polinomi no constant de coeficients en el subcòs  $k$ . La suma de les multiplicitats de les arrels de  $f(X)$  en  $\mathbb{C}$  coincideix amb el grau del polinomi.  $\square$*

**0.2.6.** En el cas, doncs, de subcossos d'un cos algebraicament tancat, tot polinomi té tantes arrels com indica el grau del polinomi, si les comptem amb llurs multiplicitats respectives; però les arrels les té en aquest cos algebraicament tancat i no necessàriament en el subcòs sobre el qual considerem el polinomi.

**Observació 0.2.7.** Encara que ho pugui semblar, aquest resultat no és gaire restrictiu. En efecte, se satisfà el teorema següent, una demostració del qual usa l'axioma de l'elecció en la forma del lema de Zorn (cf. **B.0.28** i **B.0.30**).

**Teorema 0.2.8.** *Tot cos és subcòs d'un cos algebraicament tancat.  $\square$*

Aquests preliminars ens permeten donar una resposta a les tres primeres qüestions plantejades.

*Si  $k$  és un cos i  $\bar{k}$  és un cos algebraicament tancat que conté  $k$ , tot polinomi no nul de coeficients en  $k$  té tantes arrels en  $\bar{k}$  com indica el seu grau, si comptem cadascuna amb la seva multiplicitat.*

Però encara resten pendents de resposta les altres qüestions. En particular, per a un cos qualsevol,  $k$ , i un polinomi no nul  $f(X)$  de coeficients en  $k$ , resta dir *com són* les arrels del polinomi  $f(X)$ , si es *poden calcular* i, en cas afirmatiu, *com es poden calcular*. I, d'altra banda, convé precisar més *on són les arrels*. Continuem amb més exemples.

### 0.3 Equacions de grau 2

A part de les equacions lineals (o sigui, les de grau 1), les equacions la resolució de les quals és més senzilla són les equacions quadràtiques (o sigui, les de grau 2). A continuació en donem una solució. Convé distingir els casos en què  $2 \neq 0$  en  $k$  o bé  $2 = 0$  en  $k$ ; comencem pel primer.

**Proposició 0.3.1.** *Siguin  $k$  un subcòs d'un cos algebraicament tancat,  $\bar{k}$ , tal que  $2 \neq 0$  en  $k$ , i  $a, b, c \in k$ ,  $a \neq 0$ , elements qualssevol.*

- (a) *L'equació  $aX^2 + bX + c = 0$  té les seves solucions en  $k$  si, i només si,  $b^2 - 4ac$  és el quadrat d'algun element de  $k$ .*
- (b) *Sigui  $\alpha \in \bar{k}$  tal que  $\alpha^2 = b^2 - 4ac$ ; és a dir, sigui  $\alpha$  una arrel en  $\bar{k}$  del polinomi  $X^2 - (b^2 - 4ac)$  (existeix perquè  $\bar{k}$  és algebraicament tancat). Les solucions en  $\bar{k}$  de l'equació  $aX^2 + bX + c = 0$  són  $x_1 := \frac{-b + \alpha}{2a}$ ,  $x_2 := \frac{-b - \alpha}{2a}$ . En particular,  $x_1 \in k$  si, i només si,  $\alpha \in k$ , si, i només si,  $x_2 \in k$ .*
- (c) *A l'anell de polinomis en la indeterminada  $X$  i de coeficients en  $\bar{k}$ , se satisfà la igualtat  $aX^2 + bX + c = a(X - x_1)(X - x_2)$ .*

DEMOSTRACIÓ: En primer lloc, observem que per a tot  $x \in \bar{k}$  se satisfà que  $ax^2 + bx + c = 0$  si, i només si,  $4a(ax^2 + bx + c) = 0$ , ja que  $4a \neq 0$ . Ara bé,  $4a(ax^2 + bx + c) = (2ax + b)^2 - (b^2 - 4ac)$ , de manera que  $ax^2 + bx + c = 0$  si, i només si,  $(2ax + b)^2 = b^2 - 4ac$ .

Així, si  $x \in \bar{k}$  és una solució de  $aX^2 + bX + c = 0$ , per a  $\alpha := 2ax + b \in \bar{k}$  és  $\alpha^2 = b^2 - 4ac$ . Recíprocament, si  $\alpha \in \bar{k}$  és tal que  $\alpha^2 = b^2 - 4ac$ , per a  $x := \frac{-b + \alpha}{2a}$ , i per a  $x := \frac{-b - \alpha}{2a}$ , és  $ax^2 + bx + c = 0$ . A més a més, la relació entre  $\alpha$  i les solucions de l'equació ens ensenya que  $\alpha \in k$  si, i només si, qualsevol de les solucions de l'equació  $aX^2 + bX + c = 0$  pertany a  $k$ .

Finalment,  $a(X - x_1)(X - x_2) = a(X^2 - (x_1 + x_2)X + x_1x_2)$ ; però, com que  $\alpha^2 = b^2 - 4ac$ , resulta que

$$x_1 + x_2 = \frac{-b + \alpha}{2a} + \frac{-b - \alpha}{2a} = \frac{-b}{a}, \quad x_1x_2 = \frac{-b + \alpha}{2a} \frac{-b - \alpha}{2a} = \frac{b^2 - \alpha^2}{4a^2} = \frac{c}{a}.$$

Per tant,  $a(X - x_1)(X - x_2) = aX^2 + bX + c$ .  $\square$

**Observació 0.3.2.** Notem que hem evitat fer ús del símbol d'arrel quadrada,  $\sqrt{b^2 - 4ac}$ , i que, en canvi, hem escrit  $\alpha$  per a designar una qualsevol de les dues arrels quadrades; llavors, l'altra és  $-\alpha$ ; en el text, ho fem sovint.

**Proposició 0.3.3.** *Siguin  $k$  un subcòs d'un cos algebraicament tancat,  $\bar{k}$ , per al qual és  $2 = 0$  en  $k$ , i  $a, b, c \in k$ ,  $a \neq 0$ , elements qualssevol. Si  $x_1 \in \bar{k}$  és una solució de l'equació  $aX^2 + bX + c = 0$ , l'altra és  $x_2 := x_1 + \frac{b}{a}$ . En particular, se satisfà que  $x_1 \in k$  si, i només si,  $x_2 \in k$ . A més a més,  $a(X - x_1)(X - x_2) = aX^2 + bX + c$ .*

DEMOSTRACIÓ: Clarament, si posem  $x_2 := x_1 + \frac{b}{a}$  i tenim en compte que  $2 = 0$ , se satisfà que

$$ax_2^2 + bx_2 + c = a\left(x_1^2 + \frac{b^2}{a^2}\right) + bx_1 + \frac{b^2}{a} + c = ax_1^2 + bx_1 + c = 0;$$

per tant, si  $x_1$  és solució de  $aX^2 + bX + c = 0$ ,  $x_2$  també ho és. D'altra banda,

$$x_1 + x_2 = \frac{b}{a} = -\frac{b}{a}, \quad x_1x_2 = x_1\left(x_1 + \frac{b}{a}\right) = x_1^2 + \frac{b}{a}x_1 = -\frac{c}{a} = \frac{c}{a},$$

de manera que  $a(X - x_1)(X - x_2) = a(X^2 - (x_1 + x_2)X + x_1x_2) = aX^2 + bX + c$ . Per tant, les úniques possibles solucions de  $aX^2 + bX + c = 0$  són  $x_1$  i  $x_2$ .  $\square$

Notem que, en aquest cas, no donem cap manera explícita d'expressió, ni molt menys de càlcul, de les solucions; només diem que si una és  $x_1$ , l'altra és  $x_2 := x_1 + \frac{b}{a}$ . En particular, també és  $x_1 = x_2 + \frac{b}{a}$ .

**Exemple 0.3.4.** En un cos algebraicament tancat que contingui  $\mathbb{Z}/2\mathbb{Z}$ , l'equació  $X^2 + X + 1 = 0$  té dues solucions diferents; i, si una és  $x_1$ , l'altra és  $x_2 := x_1 + 1$ . A més a més, per a totes dues se satisfà l'equació  $X^3 + 1 = 0$ , de manera que són les dues arrels cúbiques de 1 diferents de 1. Notem que cadascuna de les dues és el quadrat de l'altra (i, ahora, la seva "arrel quadrada"). Succeeix alguna cosa estranya?

Deixem pendent, de moment, donar una resposta a aquesta darrera qüestió, que tracem més endavant en estudiar les arrels de la unitat.

## 0.4 Equacions de grau 3

A continuació, i per a acabar els exemples preliminars, donem les solucions de les equacions cúbiques (o sigui, les de grau 3). Però, per a simplificar, només ho fem en el cas en què  $2 \neq 0$  i  $3 \neq 0$  en el cos.

Per a les equacions de coeficients reals i solucions reals, els matemàtics italians del Renaixement ja havien après a resoldre casos particulars de l'equació. Essencialment, escrivien les equacions en diferents formes  $p(X) = q(X)$ , on  $p(X)$  és un polinomi de grau 3 i coeficients positius, i  $q(x)$  és un polinomi de coeficients positius i grau menor que 3 que només conté monomis que no conté el polinomi  $p(X)$  (per exemple,  $X^3 + X = X^2 + 1$ , o bé  $X^3 + X^2 = X + 1$ ); i explicaven com obtenir-ne solucions, que en aquell moment de la història només podien ser positives. Així, per exemple, les dues equacions anteriors només tenien la solució  $X = 1$  (tot i que la segona també admet la solució real  $X = -1$ , amb multiplicitat 2, i la primera, les solucions complexes, no reals,  $X = \sqrt{-1}$ ,  $X = -\sqrt{-1}$ ). Les fórmules que expressen les solucions de les equacions cúbiques s'anomenen sovint fórmules de Cardano.

**Proposició 0.4.1.** *Sigui  $k$  un subcòs d'un cos algebraicament tancat  $\bar{k}$  en el qual  $2 \neq 0$  i  $3 \neq 0$ . Donats  $a, b, c, d \in k$ ,  $a \neq 0$ , posem*

$$p := \frac{c}{a} - \frac{b^2}{3a^2}, \quad q := \frac{d}{a} + \frac{2b^3}{27a^3} - \frac{bc}{3a^2}, \quad \Delta := -4p^3 - 27q^2.$$

*Siguin  $\alpha, \beta, \gamma \in \bar{k}$  elements tals que  $\alpha^2 = \Delta$ ,  $\beta^2 = -3$ ,  $\gamma^3 = \frac{-27q + 3\alpha\beta}{54}$ , i posem  $\omega := \frac{-1 + \beta}{2}$ . Amb aquestes notacions, les solucions  $x_1, x_2, x_3 \in \bar{k}$  de l'equació  $aX^3 + bX^2 + cX + d = 0$  s'expressen per les fórmules següents: si  $p \neq 0$ ,*

$$x_1 = \gamma - \frac{p}{3\gamma} - \frac{b}{3a}, \quad x_2 = \omega\gamma - \frac{p\omega^2}{3\gamma} - \frac{b}{3a}, \quad x_3 = \omega^2\gamma - \frac{p\omega}{3\gamma} - \frac{b}{3a}.$$

*Però si, en canvi, és  $p = 0$ , considerem un element  $\theta \in \bar{k}$  tal que  $\theta^3 = -q$ ; llavors, les solucions són*

$$x_1 = \theta - \frac{b}{3a}, \quad x_2 = \omega\theta - \frac{b}{3a}, \quad x_3 = \omega^2\theta - \frac{b}{3a}.$$

*En tots els casos és  $a(X - x_1)(X - x_2)(X - x_3) = aX^3 + bX^2 + cX + d$ .*

**DEMOSTRACIÓ:** Les solucions de l'equació  $aX^3 + bX^2 + cX + d = 0$  són les mateixes, evidentment, que les de l'equació  $X^3 + BX^2 + CX + D = 0$ , on  $B := \frac{b}{a}$ ,  $C := \frac{c}{a}$ , i  $D := \frac{d}{a}$ ; i si fem  $x := X + \frac{B}{3}$ , obtenim que, per a  $X \in \bar{k}$ ,  $X^3 + BX^2 + CX + D = 0$  si, i només si,  $x^3 + px + q = 0$ , on  $p := C - \frac{B^2}{3}$  i  $q := D + \frac{2B^3}{27} - \frac{BC}{3}$ . Això explica el canvi dels coeficients  $a, b, c, d$  als  $p, q$  en l'enunciat.

D'aquesta manera, només cal aprendre a calcular les solucions de l'equació  $x^3 + px + q = 0$  i aplicar-les-hi el canvi de variables. Això és, cal veure que les arrels d'aquesta darrera equació són les  $x_1 + \frac{b}{3a}$ ,  $x_2 + \frac{b}{3a}$ ,  $x_3 + \frac{b}{3a}$ , per als valors  $x_1, x_2, x_3$  donats a l'enunciat. Ara, per a veure això, observem els fets següents.

En primer lloc,  $\omega^2 = \frac{-1 - \beta}{2}$ ,  $\omega^3 = 1$ , i  $1 + \omega + \omega^2 = 0$ . D'altra banda, per a  $Y, y_1, y_2, y_3$  qualssevol, és

$$(Y - y_1)(Y - y_2)(Y - y_3) = Y^3 - (y_1 + y_2 + y_3)Y^2 + (y_1y_2 + y_1y_3 + y_2y_3)Y - y_1y_2y_3.$$

Finalment, si  $p \neq 0$ , llavors  $\gamma \neq 0$ . En efecte,  $\gamma = 0$  si, i només si,  $27q = 3\alpha\beta$ , i aquesta igualtat implica que  $81q^2 = \alpha^2\beta^2 = -3\Delta = 12p^3 + 81q^2$ ; o sigui, que  $12p^3 = 0$ , d'on  $p = 0$ , perquè  $2 \neq 0$  i  $3 \neq 0$  en  $k$ .

Estudiem primerament el cas  $p \neq 0$ . Per a  $Y := x$ ,  $y_i := x_i + \frac{b}{3a}$ ,  $1 \leq i \leq 3$ , i tenint en compte els valors anteriors de  $\omega^3$  i  $\omega + \omega^2$ , obtenim que

$$y_1 + y_2 + y_3 = 0, \quad y_1y_2 + y_1y_3 + y_2y_3 = -p(\omega + \omega^2) = p,$$

i, per al darrer terme,

$$\begin{aligned}
 y_1 y_2 y_3 &= \gamma^3 - \frac{p^3}{27\gamma^3} \\
 &= \frac{-27q + 3\alpha\beta}{54} - \frac{2p^3}{-27q + 3\alpha\beta} = \frac{(-27q + 3\alpha\beta)^2 - 4 \cdot 27p^3}{54(-27q + 3\alpha\beta)} \\
 &= \frac{27^2 q^2 - 6 \cdot 27q\alpha\beta + 9\alpha^2\beta^2 - 4 \cdot 27p^3}{54(-27q + 3\alpha\beta)} \\
 &= \frac{27^2 q^2 - 6 \cdot 27q\alpha\beta - 27\Delta - 4 \cdot 27p^3}{54(-27q + 3\alpha\beta)} \\
 &= \frac{54q^2 - 6q\alpha\beta}{2(-27q + 3\alpha\beta)} = -q.
 \end{aligned}$$

Per tant,  $(x - y_1)(x - y_2)(x - y_3) = x^3 + px + q$ ; o sigui,

$$a(X - x_1)(X - x_2)(X - x_3) = aX^3 + bX^2 + cX + d.$$

El cas  $p = 0$  es fa de manera semblant. En aquest cas, l'equació és  $x^3 + q = 0$ ; però, per a  $y_1 := \theta$ ,  $y_2 := \omega\theta$ ,  $y_3 := \omega^2\theta$ , és  $y_1 + y_2 + y_3 = \theta(1 + \omega + \omega^2) = 0$ ,  $y_1 y_2 + y_1 y_3 + y_2 y_3 = \theta^2(\omega + \omega^2 + \omega^3) = 0$ , i  $y_1 y_2 y_3 = \theta^3 = -q$ ; per tant,  $(x - \theta)(x - \omega\theta)(x - \omega^2\theta) = x^3 + q$ . La prova s'acaba desfent el canvi de variables  $x = X + \frac{b}{3a}$ .  $\square$

**Observació 0.4.2.** Per al cas en què  $2 = 0$ , la resolució de la cúbica comporta la resolució d'una equació quadràtica similar a la de l'exemple **0.3.4**; i en el cas  $3 = 0$ , la resolució comporta considerar també equacions cúbiques similars a la de l'exemple **0.3.4**; per exemple, l'equació  $X^3 + X + 1 = 0$ . Cal notar, d'altra banda, que en el cas  $3 = 0$  no podem fer, en general, un canvi lineal de variables de manera que l'equació sigui de la forma  $AX^3 + CX + D = 0$ , o bé  $AX^3 + BX^2 + D = 0$ . No ens entretenim en els detalls de la resolució de les equacions cúbiques en els casos  $2 = 0$  o  $3 = 0$ .

**Observació 0.4.3.** Igual que en el cas de les equacions quadràtiques, ara tampoc no hem utilitzat el símbol d'arrel cúbica,  $\sqrt[3]{\frac{-27q + 3\alpha\beta}{54}}$ , i hem considerat  $\gamma$  una qualsevol de les tres arrels cúbiques.

## 0.5 Exercicis

En el primer dels exercicis següents es proposa recobrar les fórmules de Cardano per a la resolució de les equacions cúbiques sobre cossos en què  $2 \neq 0$  i  $3 \neq 0$  (cf. **0.4.1**), però fet-ho de manera algorítmica. En el segon, es tracta d'aplicar aquest algoritme per a calcular les solucions d'algunes equacions cúbiques concretes i de comparar les expressions que s'obtenen així amb altres expressions que es poden obtenir a partir, majoritàriament, de la descomposició dels polinomis en factors irreductibles (cf. el capítol següent).

**Exercici 0.5.1** (Fórmules de Cardano). Siguin  $k$  un cos en què  $2 \neq 0$  i  $3 \neq 0$ , i  $f(X) = aX^3 + bX^2 + cX + d$  un polinomi de grau 3 i coeficients  $a, b, c, d \in k$ , amb  $a \neq 0$ .

- (a) Es demana demostrar que existeix un element  $m \in k$  tal que el polinomi  $g(X) := \frac{1}{a}f(X - m)$  és de la forma  $g(X) = X^3 + pX + q \in k[X]$ , amb  $p, q \in k$ ; expressar

els coeficients  $p, q$  en funció de  $a, b, c, d$  (cf. **0.4.1**), i determinar la relació entre les arrels de  $f(X)$  i les de  $g(X)$ .

- (b) També es demana demostrar que, si se substitueix  $X$  per  $U+V$  en l'equació  $g(X) = 0$ , s'obté l'equació  $(U^3+V^3)+(3UV+p)(U+V)+q = 0$ ; observar que si ara se substitueix  $V$  per  $-p/(3U)$  s'obté una equació que només conté  $U^3$  com a incògnita; i comprovar que per a  $Z := U^3$  se satisfà l'equació auxiliar, de segon grau,  $Z^2 + qZ - p^3/27 = 0$ .
- (c) Siguin  $z_1$  i  $z_2$  les solucions de l'equació anterior, fixem una arrel cúbica  $u$  de  $z_1$ , i posem  $v = -p/3u$ . Es demana comprovar que  $v$  és una arrel cúbica de  $z_2$  i que  $u^3 + v^3 = -q$ , i demostrar que  $u + v$  és una solució de l'equació  $X^3 + pX + q = 0$ .
- (d) Finalment, es demana comprovar que  $\omega := \frac{-1 + \sqrt{-3}}{2}$  és una arrel cúbica de la unitat i deduir que les solucions de l'equació  $X^3 + pX + q = 0$  són (cf. **0.4.1**):

$$\omega^k \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{27q^2 + 4p^3}{108}}} + \omega^{-k} \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{27q^2 + 4p^3}{108}}}, \quad k = 0, 1, 2,$$

on cal prendre la segona arrel cúbica de manera que el producte de les dues arrels cúbiques sigui  $-p/3$ .

**Exercici 0.5.2.** Es demana aplicar les fórmules de Cardano per a calcular les arrels dels polinomis

$$X^3 - 6X - 6, \quad X^3 - 6X - 4, \quad X^3 - 2X + 1, \quad X^3 - \sqrt{3}X^2 - 2X + 2\sqrt{3}.$$

A continuació, es pregunta de quins d'aquests polinomis se saben trobar fàcilment les arrels sense utilitzar les fórmules de Cardano? I, finalment, per a cadascun d'aquests, es demana comparar els resultats obtinguts mitjançant els diferents procediments.



# Capítol 1

## Equacions algebraiques

Els conceptes intuïtius de polinomi, de funció polinòmica i d'equació polinòmica s'adquireixen a l'ensenyament secundari; però en aquella etapa no se sol fer cap construcció formal dels polinomis. El capítol comença, doncs, amb aquesta construcció formal.

Després d'aquesta introducció, i tot i que el càlcul bàsic amb polinomis se sol fer en cursos d'àlgebra lineal, i el problema de la factorització se sol tractar en l'estudi de les estructures algebraiques bàsiques, a la secció segona, es repassa la divisió entera de polinomis i, com a conseqüència, s'obté que l'anell de polinomis de coeficients en un cos qualsevol té la propietat, que també té l'anell dels nombres enters, que tots els seus ideals són principals; i es dedica la secció tercera a l'estudi de la multiplicitat de les arrels dels polinomis i a la prova del fet que, en un cos, la suma de les multiplicitats de les arrels d'un polinomi no nul de coeficients en aquest cos no pot superar el grau del polinomi.

Es dediquen les seccions quarta i cinquena a l'estudi de l'existència de descomposició dels polinomis com a producte de factors irreductibles; per a polinomis en una indeterminada i coeficients en un cos, la secció quarta, i per a polinomis en més d'una indeterminada i coeficients en un cos, o més generalment, en un domini de factorització única, la cinquena.

Finalment, a la secció sisena es fa l'estudi d'alguns criteris d'irreductibilitat de polinomis i, a la setena, el d'un algoritme bàsic per a la factorització de polinomis de coeficients enters. Tot i que l'algoritme que es presenta no és, ni de bon tros, eficient, pot ser útil en determinades ocasions per a alguns casos no trivials. Es deixa per al capítol següent l'estudi d'altres propietats de polinomis en més d'una indeterminada que es necessiten, o són útils, més endavant; especialment, les relacionades amb els polinomis simètrics o les relacions entre les arrels i els coeficients dels polinomis.

### 1.1 Polinomis i equacions algebraiques

Tot i que podríem definir de manera senzilla els polinomis en una indeterminada i coeficients en un anell no necessàriament commutatiu, ens limitem al cas commutatiu. Això no exclou que l'avaluació de polinomis en una indeterminada es pot fer, i de fet es fa sovint, en àlgebres no necessàriament commutatives sobre l'anell de coeficients. Per exemple, en l'estudi de l'àlgebra lineal, se solen avaluar els polinomis en un endomorfisme d'un espai vectorial de dimensió finita i a partir d'aquí s'obté, en particular, el polinomi mínim

de l'endomorfisme o el teorema de Cayley-Hamilton. Utilitzem, més endavant, aquesta tècnica; per exemple, per a tractar el polinomi minimal d'un element algebraic en parlar de traces i de normes (cf. la secció 4.6).

**Definició 1.1.1.** Sigui  $A$  un anell commutatiu (cf. A.2.1). Podem considerar el conjunt  $P(A)$  de totes les successions  $(a_0, a_1, \dots, a_n, 0, \dots)$  d'elements de  $A$  que, a partir d'un lloc, només contenen l'element 0; s'anomenen *polinomis* de coeficients en  $A$ . Els components de la successió s'anomenen els *coeficients* del polinomi i els polinomis dels quals només un coeficient és diferent de zero s'anomenen *monomis*. Donats polinomis

$$\alpha = (a_0, a_1, \dots, a_n, 0, \dots) \quad \text{i} \quad \beta = (b_0, b_1, \dots, b_m, 0, \dots),$$

es defineix la seva suma

$$\alpha + \beta := (a_0 + b_0, a_1 + b_1, \dots, a_t + b_t, 0, \dots)$$

i el seu producte

$$\alpha\beta := (c_0, c_1, \dots, c_t, 0, \dots),$$

on

$$c_r := \sum_{i+j=r} a_i b_j, \quad r \geq 0.$$

Notem que per a  $t > \max\{m, n\}$  és  $a_t + b_t = 0$  i que per a  $r > n + m$  és  $c_r = 0$ , de manera que tant la suma com el producte de polinomis estan definits com a operacions binàries en el conjunt  $P(A)$ . En efecte, si  $i + j = r > n + m$ , llavors  $i > n$  o bé  $j > m$  (o bé les dues propietats), de manera que  $a_i = 0$  o bé  $b_j = 0$  i, per tant,  $a_i b_j = 0$ , i la suma,  $c_r = 0$ .

**1.1.2.** El conjunt  $P(A)$ , amb la suma i el producte que acabem de definir, és un anell, que és commutatiu perquè  $A$  és commutatiu; els elements neutres de la suma i del producte són, respectivament, els polinomis

$$0 = (0, 0, \dots, 0, \dots) \quad \text{i} \quad 1 = (1, 0, \dots, 0, \dots).$$

Cal notar la gran diferència entre aquest anell i l'anell producte d'una quantitat numerable de còpies de l'anell  $A$  (cf. A.2.40). A més a més que com a conjunts són diferents, i tot i que la suma es defineix de manera semblant, component a component, no succeeix així amb el producte. I, a més a més, l'element neutre del producte és diferent en els dos casos; de fet, el de l'anell producte ni tan sols pertany a l'anell de polinomis.

**1.1.3.** L'aplicació  $A \rightarrow P(A)$  definida per  $a \mapsto (a, 0, \dots, 0, \dots)$  és un morfisme injectiu d'anells (cf. A.2.8), de manera que permet identificar  $A$  com un subanell (cf. A.2.17) de  $P(A)$ . Els elements de  $A$ , pensats com a polinomis, s'anomenen els *polinomis constants*.

**Definició 1.1.4.** Llevat del polinomi 0, tot altre polinomi,  $\alpha$ , té algun coeficient diferent de 0; i com que tots els coeficients d'un lloc endavant són 0, podem considerar el màxim dels índexs  $n$  tals que  $a_n \neq 0$ ; aquest nombre natural  $n$  s'anomena el *grau* del polinomi i s'escriu  $\text{gr}(\alpha) := n$ , i el coeficient  $n$ -èsim s'anomena el *coeficient dominant* o *coeficient principal* del polinomi. Convé definir el grau del polinomi 0 com  $-\infty$ . I, com és habitual, per a tot nombre natural  $n$  es defineix  $-\infty < n$ ,  $-\infty + n = n + (-\infty) = -\infty$ , i  $-\infty + (-\infty) = -\infty$ .

**1.1.5.** De la definició de polinomi es dedueix de seguida que el grau d'una suma és menor o igual que el màxim dels graus dels sumands i que el grau d'un producte és menor o igual que la suma dels graus dels factors. En general, cap de les dues desigualtats no és una igualtat. D'altra banda, els polinomis constants són el polinomi 0 i els polinomis de grau 0. Un polinomi s'anomena *mònic* si el seu coeficient principal, és a dir, el coeficient del seu monomi no nul de grau màxim, és 1 o bé, més generalment, un element invertible  $a \in A^*$  (cf. **A.2.27**). Sovint és còmode utilitzar el concepte més restrictiu (coeficient principal igual a 1) de polinomi mònic.

**Definició 1.1.6.** S'acostuma a donar un nom al polinomi  $(0, 1, 0, \dots, 0, \dots)$ ; si s'anomena  $X := (0, 1, 0, \dots, 0, \dots)$ , llavors s'escriu  $A[X]$  en lloc de  $P(A)$  i es diu que  $A[X]$  és l'anell de polinomis en la *indeterminada*  $X$  i de coeficients en  $A$ . Així, doncs, la *indeterminada* no és res més que el polinomi  $X$ .

**1.1.7.** Sigui  $A$  un domini d'integritat (cf. **A.2.33**). Llavors, l'anell de polinomis  $A[X]$  és un domini d'integritat; i si  $f(X), g(X) \in A[X]$  són polinomis diferents de zero, se satisfà que  $\text{gr}(f(X) \cdot g(X)) = \text{gr}(f(X)) + \text{gr}(g(X))$ .

**1.1.8.** Per a qualsevol anell  $A$ , en  $A[X]$  se satisfà la igualtat

$$(a_0, a_1, \dots, a_n, 0, \dots) = a_0 + a_1X + \dots + a_nX^n;$$

per tant, tot polinomi s'escriu de manera única en la forma

$$a_0 + a_1X + \dots + a_nX^n, \quad a_0, \dots, a_n \in A.$$

Dit d'una altra manera, l'anell de polinomis  $A[X]$ , pensat com a  $A$ -mòdul, és lliure de base el conjunt  $\{1, X, X^2, \dots, X^n, \dots\}$ .

**Observació 1.1.9.** Notem que, encara que considerem el cas en què l'anell  $A$  no és commutatiu, el polinomi  $X$  pertany al centre (cf. **A.2.22**) de l'anell de polinomis  $A[X]$ ; més generalment, si d'un polinomi  $f(X) = a_0 + a_1X + \dots + a_nX^n \in A[X]$ ,  $a_0, \dots, a_n \in A$ , tots els coeficients  $a_i$  pertanyen al centre de l'anell  $A$ , llavors  $f(X)$  pertany al centre de  $A[X]$ . Aquesta observació és tautològica si  $A$  és commutatiu, però és útil en algun altre cas.

**1.1.10.** Siguin  $A$  i  $B$  anells i  $f : A \rightarrow B$  un morfisme d'anells. Existeix un únic morfisme d'anells  $g : A[X] \rightarrow B[X]$  tal que  $g(X) = X$  i per a tot  $a \in A$  és  $g(a) = f(a)$ . Aquest morfisme  $g$  s'anomena *el morfisme extensió* de  $f$  de  $A[X]$  en  $B[X]$ .

**Definició 1.1.11.** Donat un anell commutatiu  $A$ , definim per inducció l'anell de polinomis en les indeterminades  $X_1, \dots, X_n$  com

$$A[X_1, \dots, X_n] := A[X_1, \dots, X_{n-1}][X_n];$$

és a dir,  $A[X_1, \dots, X_n]$  és l'anell de polinomis en la indeterminada  $X_n$  i de coeficients en l'anell  $A[X_1, \dots, X_{n-1}]$ .

**1.1.12.** Tot polinomi en les indeterminades  $X_1, \dots, X_n$  s'escriu de manera única en la forma

$$\sum_{i_1, \dots, i_n} a_{i_1, \dots, i_n} X_1^{i_1} X_2^{i_2} \dots X_n^{i_n}, \quad a_{i_1, \dots, i_n} \in A,$$

en la qual tots els elements  $a_{i_1, \dots, i_n}$  llevat, potser, d'una quantitat finita, són 0. Els elements  $a_{i_1, \dots, i_n}$  s'anomenen els *coeficients* del polinomi.

**Definició 1.1.13.** Donats un anell  $A$  i un polinomi

$$f(X_1, \dots, X_n) := \sum_{i_1, \dots, i_n} a_{i_1, \dots, i_n} X_1^{i_1} X_2^{i_2} \cdots X_n^{i_n} \in A[X_1, \dots, X_n], \quad a_{i_1, \dots, i_n} \in A,$$

l'aplicació (entre conjunts)  $A^n \rightarrow A$  definida per

$$(x_1, \dots, x_n) \mapsto f(x_1, \dots, x_n) := \sum_{i_1, \dots, i_n} a_{i_1, \dots, i_n} x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n},$$

s'anomena *l'aplicació polinòmica* definida per  $f(X_1, \dots, X_n)$  o també *funció polinòmica* definida per  $f(x_1, \dots, x_n)$ . Els elements  $(x_1, \dots, x_n) \in A^n$  tals que  $f(x_1, \dots, x_n) = 0$  s'anomenen les *arrels* en  $A$  del polinomi  $f(X_1, \dots, X_n)$  o els *zeros* de la funció polinòmica associada, o les *solucions* en  $A$  de *l'equació algebraica*  $f(X_1, \dots, X_n) = 0$ , o els punts  $A$ -racionals de la varietat afí definida per  $f(X_1, \dots, X_n)$ .

**1.1.14.** Ens interessen les equacions algebraiques en una *incògnita*; és a dir, les equacions polinòmiques definides per un polinomi en una *indeterminada*. El grau del polinomi s'anomena el *grau de l'equació*. Les equacions de grau 1 també s'anomenen *lineals*; les de grau 2, *quadràtiques*; les de grau 3, *cúbiques*; etcètera.

**1.1.15.** En general, el nombre d'arrels d'alguns polinomis (en una indeterminada) pot ésser més gran que el seu grau. A més a més de l'exemple donat en **0.1.3**, podem observar que, en  $\mathbb{Z}/8\mathbb{Z}$ , el polinomi  $X^2 - 1$ , de grau 2, té les quatre arrels  $x = 1$ ,  $x = 3$ ,  $x = 5$  i  $x = 7$ . Fins i tot, un polinomi pot tenir una quantitat no finita d'arrels (cf. els dos exercicis següents, **1.1.16** i **1.1.17**). Aquest fet no succeeix si l'anell sobre el qual es consideren el polinomi i les arrels és un domini d'integritat. Veiem aquest fet al final de la secció tercera.

**Exercici 1.1.16.** Es demana calcular les arrels en  $\mathbf{M}(2, \mathbb{Q})$  del polinomi  $X^2 - 1$ ; és a dir, es demana calcular les matrius  $M \in \mathbf{M}(2, \mathbb{Q})$  tals que  $M^2 = 1_2$ , on  $1_2$  és la matriu identitat, o sigui, l'element unitat de l'anell de matrius. (Aquest exercici es pot considerar, de fet, com un exercici d'àlgebra lineal.)

**Exercici 1.1.17.** Considerem  $A := \prod_{n \in \mathbb{N}} \mathbb{Z}$ , l'anell producte d'una infinitat numerable de còpies de l'anell  $\mathbb{Z}$  dels nombres enters. Llavors,  $A$  és un anell *commutatiu* i el conjunt de les arrels en  $A$  del polinomi  $X^2 - 1$  és infinit no numerable.

**1.1.18.** L'estudi de les arrels dels polinomis en més d'una indeterminada té un caràcter més geomètric. Per exemple, les arrels en el pla  $\mathbb{R}^2$  del polinomi  $X^2 + Y^2 - 1$  són els *punts reals* de la *circumferència* unitat. En aquest curs, ens limitem a l'estudi de les arrels dels polinomis en una sola indeterminada (i en anells commutatius), un problema de caire molt més aritmètic.

## 1.2 Divisió de polinomis

De la mateixa manera que moltes de les propietats bàsiques dels nombres enters, sobretot les relatives a la divisibilitat, es deriven de l'existència de divisió entera, així les propietats més importants de l'anell de polinomis de coeficients en un cos també es deriven de l'existència de la divisió entera de polinomis. Aquesta secció es dedica a aquest estudi.

**Proposició 1.2.1** (Divisió de polinomis). *Siguin  $k$  un cos i  $f(X), g(X) \in k[X]$  polinomis, amb  $g(X) \neq 0$ . Aleshores, existeixen polinomis  $q(X), r(X) \in k[X]$ , únics per als quals se satisfà que  $f(X) = g(X)q(X) + r(X)$  i que  $\text{gr}(r(X)) < \text{gr}(g(X))$ .*

DEMOSTRACIÓ: Comencem per provar-ne l'existència. Si  $\text{gr}(f(X)) < \text{gr}(g(X))$  i posem  $q(X) := 0, r(X) := f(X)$ , és clar que se satisfan les propietats enunciades. Suposem, doncs, que  $\text{gr}(f(X)) \geq \text{gr}(g(X))$ , i siguin  $f(X) =: a_0 + a_1X + \dots + a_nX^n, a_i \in k, g(X) =: b_0 + b_1X + \dots + b_mX^m, b_j \in k, a_n \neq 0, b_m \neq 0, i n \geq m$ . El polinomi

$$f(X) - g(X)\frac{a_n}{b_m}X^{n-m} =: c_0 + c_1X + \dots + c_{n-1}X^{n-1},$$

on  $c_0, \dots, c_{n-1} \in k$ , és de grau estrictament menor que el grau,  $n$ , de  $f(X)$ ; repetint el mateix procés, el polinomi

$$\begin{aligned} f(X) - g(X)\frac{a_n}{b_m}X^{n-m} - g(X)\frac{c_{n-1}}{b_m}X^{n-m-1} = \\ = f(X) - g(X)\left(\frac{a_n}{b_m}X^{n-m} - \frac{c_{n-1}}{b_m}X^{n-m-1}\right) \end{aligned}$$

és un polinomi de grau menor o igual que  $n - 2$ . Doncs, podem calcular recursivament un polinomi

$$q(X) := \frac{a_n}{b_m}X^{n-m} - \frac{c_{n-1}}{b_m}X^{n-m-1} + \dots;$$

el procés s'atura quan el grau de la diferència  $f(X) - g(X)q(X)$  és menor que el grau,  $m$ , de  $g(X)$  i el polinomi  $r(X)$  es defineix com aquesta diferència. Llavors, les propietats enunciades se satisfan per definició de  $q(X)$  i de  $r(X)$ .

Demostrem, ara, la unicitat. Suposem que

$$\begin{aligned} f(X) &= g(X)q_1(X) + r_1(X), & q_1(X), r_1(X) &\in k[X], & \text{gr}(r_1(X)) &< \text{gr}(g(X)), \\ &= g(X)q_2(X) + r_2(X), & q_2(X), r_2(X) &\in k[X], & \text{gr}(r_2(X)) &< \text{gr}(g(X)). \end{aligned}$$

De la igualtat  $r_2(X) - r_1(X) = g(X)(q_1(X) - q_2(X))$ , resulta que el grau de  $r_2(X) - r_1(X)$ , que és menor estricte que el grau de  $g(X)$ , coincideix amb el grau del producte del polinomi  $g(X)$  pel polinomi  $q_1(X) - q_2(X)$ ; però, si  $q_1(X) - q_2(X) \neq 0$ , el grau d'aquest producte és la suma dels graus dels dos factors, de manera que és més gran o igual que el grau de  $g(X)$ . Aquesta contradicció obliga que sigui  $q_1(X) = q_2(X)$  i, en conseqüència,  $r_1(X) = r_2(X)$ , com volíem provar.  $\square$

**1.2.2.** Un repàs acurat d'aquesta demostració ens ensenya que si no suposem que  $k$  és un cos, sinó només un anell commutatiu qualsevol, però, en canvi,  $b_m$  és un element invertible de  $k$ , el procés de la divisió es vàlid sense cap modificació; per tant, a més a més d'obtenir un algoritme per a calcular el quocient i el residu de la divisió entera de polinomis, hem demostrat també el resultat següent.

**Corol·lari 1.2.3.** *Sigui  $k$  un anell commutatiu. Donats polinomis  $f(X), g(X) \in k[X]$  tals que  $g(X)$  és mònic (i, per tant,  $g(X) \neq 0$ ), existeixen polinomis  $q(X), r(X) \in k[X]$  únics tals que  $f(X) = g(X)q(X) + r(X)$  i  $\text{gr}(r(X)) < \text{gr}(g(X))$ .  $\square$*

**Definició 1.2.4.** Una expressió de la forma  $f(X) = g(X)q(X) + r(X)$ , on  $f(X), g(X), q(X), r(X) \in A[X]$ ,  $g(X)$  mònic, i  $\text{gr}(r(X)) < \text{gr}(g(X))$ , s'anomena la *divisió entera* (o, simplement, divisió) de  $f(X)$  per  $g(X)$ ; els polinomis  $q(X)$  i  $r(X)$  s'anomenen, respectivament, el *quocient* i el *residu* de la divisió entera, mentre que  $f(X)$  i  $g(X)$  s'anomenen, respectivament, el *dividend* i el *divisor*.

**1.2.5.** Si l'anell  $A$  no és commutatiu, caldria donar sentit a les fraccions com  $\frac{a_n}{b_m}$  que apareixen a la demostració anterior; si fos que  $\frac{a_n}{b_m} = b_m^{-1}a_n$ , l'invers de  $b_m$  multiplicant a l'esquerra de  $a_n$ , i anàlogament les altres, obtindríem una divisió entera com la que hem escrit:  $f(X) = g(X)q(X) + r(X)$ ; i si fos  $\frac{a_n}{b_m} = a_nb_m^{-1}$ , ara, l'invers de  $b_m$  multiplicant a la dreta de  $a_n$ , obtindríem una divisió entera de la forma  $f(X) = q(X)g(X) + r(X)$ , amb l'ordre permutat entre el divisor i el quocient. No tractem el cas no commutatiu, de manera que no ens cal distingir entre les divisions enteres per l'esquerra o per la dreta.

**Corol·lari 1.2.6.** Per a tot cos  $k$ , l'anell de polinomis  $k[X]$  és un domini d'ideals principals (cf. A.3.18).

**DEMOSTRACIÓ:** Com que l'ideal  $\{0\}$  és principal, cal veure que tot ideal  $\mathfrak{a} \subseteq k[X]$ ,  $\mathfrak{a} \neq \{0\}$ , és principal. Sigui  $g(X) \in \mathfrak{a}$ ,  $g(X) \neq 0$ , un polinomi de grau mínim en  $\mathfrak{a} - \{0\}$ ; clarament, l'ideal  $\mathfrak{a}$  conté l'ideal  $g(X)k[X]$ . Recíprocament, donat  $f(X) \in \mathfrak{a}$ , la divisió entera de  $f(X)$  per  $g(X)$  ens proporciona un residu  $r(X) = f(X) - g(X)q(X) \in \mathfrak{a}$  de grau estrictament menor que  $\text{gr}(g(X))$ ; com que  $g(X)$  és un polinomi no nul de  $\mathfrak{a}$  de grau mínim en  $\mathfrak{a} - \{0\}$ , ha de ser  $r(X) = 0$ ; és a dir,  $f(X) = g(X)q(X) \in g(X)k[X]$ . Això prova l'altra inclusió i  $\mathfrak{a} = g(X)k[X]$ .  $\square$

**Exercici 1.2.7.** Es demana imitar la demostració anterior per a veure que l'anell dels nombres enters,  $\mathbb{Z}$ , és un domini d'ideals principals. (De fet, la demostració que hem fet per a l'anell de polinomis imita la demostració que es fa usualment d'aquest resultat per a l'anell dels nombres enters.)

## 1.3 Divisibilitat i arrels múltiples

Si calculem les solucions, en un cos  $K$ , de les equacions  $X^3 - X^2 = 0$ , o  $X^3 - 2X^2 + X = 0$ , o  $X^2 - X = 0$ , ens adonarem que totes tres tenen les mateixes solucions: 0 i 1. Però les tres equacions són diferents. Els conceptes de divisibilitat i de multiplicitat d'una arrel d'un polinomi ens ajuden a comprendre aquest fenomen. Ho tractem en aquesta secció.

**Definició 1.3.1.** Sigui  $A$  un anell commutatiu. Donats elements  $f, g \in A$ , es diu que  $g$  divideix  $f$ , o que  $g$  és un *divisor* de  $f$ , o que  $f$  és *divisible* per  $g$ , si existeix un element  $q \in A$ ,  $q \neq 0$ , tal que  $f = gq$ . Més generalment, donats elements  $f, g \in A$ , es diu que  $f$  és un *múltiple* de  $g$  si existeix un element  $q \in A$ , tal que  $f = gq$ . En aquest cas s'escriu  $g|f$ .

**1.3.2.** Notem que a la definició d'element múltiple d'un altre no es demana que sigui  $q \neq 0$ ; en particular, 0 és múltiple de qualsevol element de  $A$ . En canvi, 1 no és mai un divisor de 0, perquè  $1 \cdot q = 0$  implica  $q = 0$ . Aquesta definició, que estén la definició de divisibilitat de nombres enters, s'aplica a qualsevol anell commutatiu  $A$  i, en particular, als elements de  $A[X]$ ; és a dir, als polinomis de coeficients en  $A$ . I en aquest cas, hi ha una relació molt estreta entre la divisibilitat i les arrels dels polinomis.

**Proposició 1.3.3.** Sigui  $A$  un anell commutatiu i  $f(X) \in A[X]$ ,  $f(X) \neq 0$ , un polinomi no nul. Un element  $a \in A$  és una arrel del polinomi  $f(X)$  si, i només si, el polinomi  $f(X)$  és divisible pel polinomi  $X - a \in A[X]$ .

DEMOSTRACIÓ: Considerem la divisió entera de  $f(X)$  pel polinomi (mònic)  $X - a$ :

$$f(X) = (X - a)q(X) + r(X), \quad q(X), r(X) \in A[X], \quad \text{gr}(r(x)) < 1.$$

Notem que  $r(X)$  és un polinomi constant,  $r(X) =: r \in A$ . Ara, per a l'aplicació polinòmica definida per  $f(X)$ , se satisfà que  $f(a) = r$ , de manera que  $f(a) = 0$  si, i només si,  $r = 0$ ; i això és equivalent a dir que  $X - a$  divideix el polinomi  $f(X)$ .  $\square$

**Definició 1.3.4.** La igualtat  $f(X) = (X - a)q(X) + f(a)$  es coneix sovint com la *regla de Ruffini*. I el fet que el residu de la divisió sigui  $f(a)$  es coneix sovint com el *teorema del residu* (de la divisió de polinomis).

**1.3.5.** Suposem que  $a \in A$  és una arrel del polinomi no nul  $f(X)$ . Llavors, podem escriure  $f(X) = (X - a)q(X)$ , i el polinomi  $q(X) \in A[X]$  és únic. Pot succeir, o no, que  $a$  sigui una arrel de  $q(X)$ . Si ho és, existeix un polinomi no nul  $q_2(X)$  tal que  $q(X) = (X - a)q_2(X)$ ; o sigui,  $f(X) = (X - a)^2q_2(X)$ . Com que el grau de  $q_2(X)$  és una unitat menor que el grau de  $q(X)$  que, alhora, és una unitat menor que el grau de  $f(X)$ , aquest procés no pot continuar indefinidament; és a dir, existeix un nombre natural  $m \geq 1$  tal que  $(X - a)^m$  divideix el polinomi  $f(X)$  però  $(X - a)^{m+1}$  no divideix  $f(X)$ . I si  $a$  no és arrel de  $f(X)$ , aquest màxim és 0.

**Definició 1.3.6.** Siguin  $A$  un anell commutatiu,  $a \in A$  un element de  $A$ , i  $f(X) \in A[X]$ ,  $f(X) \neq 0$ , un polinomi no nul. S'anomena *multiplicitat* de  $a$  com a arrel de  $f(X)$  el màxim nombre natural  $m \geq 0$  tal que  $(X - a)^m$  divideix  $f(X)$ . Una arrel *simple* és una arrel de multiplicitat  $m = 1$ . Una arrel de multiplicitat  $m > 1$  s'anomena una arrel *múltiple* (*doble*, si  $m = 2$ ; *triple*, si  $m = 3$ ; etcètera).

**Definició 1.3.7.** Siguin  $A$  un anell i  $f(X) := a_0 + a_1X + \dots + a_nX^n \in A[X]$ , un polinomi de coeficients  $a_0, a_1, \dots, a_n \in A$ . El polinomi

$$D(f, X) := a_1 + 2a_2X + \dots + na_nX^{n-1} \in A[X]$$

s'anomena el *polinomi derivat* del polinomi  $f(X)$ .

**1.3.8.** Siguin  $A$  un anell i  $f(X), g(X) \in A[X]$ , polinomis qualssevol. La demostració de les propietats següents és un exercici senzill.

- (a)  $D(f + g, X) = D(f, X) + D(g, X)$ .
- (b)  $D(fg, X) = D(f, X)g(X) + f(X)D(g, X)$ .
- (c) Si  $f(X)$  és un polinomi constant, llavors  $D(f, X) = 0$ .

Però si hom intenta provar el recíproc de la darrera, hom es troba amb dificultats. Per a la discussió d'aquest fet, és convenient disposar del concepte de *característica d'un anell* (cf. **A.3.24**).

**Proposició 1.3.9.** Siguin  $A$  un domini d'integritat i  $f(X) \in A[X]$  un polinomi. Si  $A$  és de característica 0, llavors  $D(f, X) = 0$  si, i només si,  $f(X)$  és un polinomi constant. Però si  $A$  és de característica  $p > 0$ , llavors  $D(f, X) = 0$  si, i només si,  $f(X) = g(X^p)$ , per a algun polinomi  $g(X) \in A[X]$ ; és a dir, si els únics monomis no nuls de  $f(X)$  són de grau múltiple de  $p$ .

DEMOSTRACIÓ: Escriuem  $f(X) = a_0 + a_1X + \cdots + a_nX^n$ ,  $a_0, a_1, \dots, a_n \in A$ , i considerem el polinomi derivat,

$$D(f, X) = a_1 + 2a_2X + \cdots + pa_pX^{p-1} + \cdots + na_nX^{n-1}.$$

Aquest polinomi és nul si, i només si, els seus coeficients  $a_1, 2a_2, \dots, na_n$  són tots nuls. Però, com que  $A$  és un domini d'integritat,  $ka_k = 0$  si, i només si,  $k = 0 \in A$  o bé  $a_k = 0$ ; i la possibilitat  $k = 0 \in A$  es dona exactament per a  $k = 0$  i, si  $\text{car}(A) = p > 0$ , per als valors de  $k$  múltiples de  $p$ . Doncs, només per a aquests valors de  $k$ , el coeficient  $a_k$  del polinomi  $f(X)$  pot ésser qualsevol valor de  $A$ .  $\square$

**Observació 1.3.10.** Si l'anell  $A$  no és un domini d'integritat, encara hi pot haver més dificultats. Per exemple, el derivat del monomi  $3X^2 \in (\mathbb{Z}/6\mathbb{Z})[X]$  és el polinomi 0, tot i que el grau no és múltiple de la característica.

El resultat següent proporciona una caracterització de les arrels múltiples dels polinomis de coeficients en dominis d'integritat.

**Proposició 1.3.11.** *Siguin  $A$  un domini d'integritat,  $a \in A$  un element, i  $f(X) \in A[X]$  un polinomi no nul. L'element  $a$  és una arrel múltiple de  $f(X)$  si, i només si,  $a$  és una arrel de  $f(X)$  i, simultàniament, de  $D(f, X)$ .*

DEMOSTRACIÓ: Escriuem  $f(X) = (X - a)^m q(X)$ , on  $m \geq 1$  és la multiplicitat de  $a$  com a arrel de  $f(X)$ ; en particular,  $q(a) \neq 0$ . Llavors,

$$\begin{aligned} D(f, X) &= m(X - a)^{m-1}q(X) + (X - a)^m D(q, X) \\ &= (X - a)^{m-1}(mq(X) + (X - a)D(q, X)). \end{aligned}$$

Clarament, la multiplicitat de  $a$  com a arrel de  $D(f, X)$  és més gran o igual que  $m - 1$ . Per tant, si  $m > 1$ ,  $a$  també és arrel de  $D(f, X)$ . Recíprocament, si  $m = 1$ , llavors  $D(f, a) = q(a) \neq 0$ .  $\square$

**Teorema 1.3.12.** *Siguin  $A$  un domini d'integritat i  $f(X) \in A[X]$  un polinomi no nul. La suma de les multiplicitats de les arrels  $a \in A$  de  $f(X)$  és menor o igual que el grau de  $f(X)$ .*

DEMOSTRACIÓ: Si  $a \in A$  és una arrel de  $f(X)$ , i si anomenem  $m$  la seva multiplicitat, tenim que  $f(X) = (X - a)^m g(X)$ , amb  $g(X) \in A[X]$  tal que  $g(a) \neq 0$ , i se satisfà que  $\text{gr}(g(X)) = \text{gr}(f(X)) - m < \text{gr}(f(X))$ . Les arrels de  $f(X)$  diferents de  $a$  són exactament les arrels de  $g(X)$ , i les seves multiplicitats per a  $f(X)$  i per a  $g(X)$  coincideixen. Això ens diu que si la propietat que volem provar és vàlida per al polinomi  $g(X)$ , també ho és per al polinomi  $f(X)$ . Per tant, podem procedir per inducció sobre el grau del polinomi, perquè els polinomis de grau 0 no tenen arrels.  $\square$

**Observació 1.3.13.** Notem que no estem suposant que el domini d'integritat  $A$  sigui un domini de factorització única (cf. 1.4.13); per tant, cal anar en compte a l'hora de veure que la multiplicitat en  $f(X)$  d'una arrel de  $g(X)$  coincideix amb la multiplicitat com a arrel de  $g(X)$ . Però, si anomenem  $b \in A$  una arrel de  $g(X)$ , i  $n \geq 1$  la seva multiplicitat com a arrel de  $g(X)$ , podem escriure  $g(X) = (X - b)^n h(X)$ , per a  $h(X) \in A[X]$ ,  $h(b) \neq 0$ . Llavors, se satisfà la igualtat  $f(X) = (X - b)^n k(X)$ , on  $k(X) := h(X)(X - a)^m$ , i s'obté que  $k(b) = h(b)(b - a)^m \neq 0$ , perquè  $A$  és un domini d'integritat. Per tant, la multiplicitat de  $b$  com a arrel de  $f(X)$  és  $n$ .  $\square$



## 1.4 Factorització única a $k[X]$

De la mateixa manera que tot nombre enter no nul es pot escriure com a producte de nombres enters primers, i de manera única llevat de l'ordre i del signe dels factors, una cosa similar succeeix als polinomis de coeficients en un cos. Convé distingir, però, entre les nocions d'element primer i d'element irreductible que, encara que coincideixen en  $\mathbb{Z}$  (i també en  $k[X]$ ), no coincideixen en general. Recordem les definicions.

**Definició 1.4.1.** Sigui  $A$  un anell commutatiu. Un element  $p \in A$  s'anomena *primer* si no és invertible i tota relació de divisibilitat  $p \mid ab$ , amb  $a, b \in A$ , implica que  $p \mid a$  o bé  $p \mid b$ ; equivalentment, si l'ideal  $pA$  és un ideal primer (cf. **A.3.20**).

**Definició 1.4.2.** Sigui  $A$  un anell commutatiu qualsevol. Un element  $a \in A$  s'anomena *irreductible* si  $a$  no és invertible, i per a tota descomposició  $a = bc$ , on  $b, c \in A$ , és o bé  $b \in A^*$  o bé  $c \in A^*$ .

**1.4.3.** En particular, si  $k$  és un cos, un polinomi  $f(X) \in k[X]$  és irreductible si, i només si, no és divisible per cap polinomi no constant de grau estrictament més petit que el de  $f(X)$ . Per exemple, tot polinomi de grau 1 de  $k[X]$  és irreductible. D'altra banda, el polinomi  $2X \in \mathbb{Z}[X]$ , tot i que és un polinomi de grau 1, no és irreductible en  $\mathbb{Z}[X]$ , perquè descompon com a producte dels dos polinomis 2 i  $X$ , i cap dels dos no és invertible en  $\mathbb{Z}[X]$ . Notem que, en canvi, aquest polinomi és irreductible en  $\mathbb{Q}[X]$ .

**1.4.4.** El fet que un element sigui irreductible en un anell no vol dir que ho sigui en un altre anell que el conté com a subanell. Per exemple, considerem l'anell dels nombres enters de Gauss,  $\mathbb{Z}[i] := \{a + bi : a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$ , que conté  $\mathbb{Z}$  com a subanell. El nombre 2 és irreductible en  $\mathbb{Z}$ , mentre que admet la descomposició  $2 = (1 + i)(1 - i)$  en  $\mathbb{Z}[i]$ , i els elements  $1 + i, 1 - i \in \mathbb{Z}[i]$  són irreductibles (de fet,  $i$  és invertible en  $\mathbb{Z}[i]$  i es té que  $i(1 - i) = 1 + i$ ); per tant,  $2 = i(1 - i)^2$ , i aquesta és una descomposició de 2 com a producte d'elements irreductibles en  $\mathbb{Z}[i]$ . Per tant, el fet que un element sigui irreductible o no és un fet lligat molt estretament a l'anell en el qual el considerem.

**1.4.5.** El concepte d'element irreductible correspon al fet que l'element no sigui producte d'altres elements, llevat de productes trivials; i el concepte d'element primer correspon al fet que si un producte és múltiple d'un element primer, llavors algun dels factors ho és. Tot i que, per exemple, en  $\mathbb{Z}$  i en  $k[X]$ ,  $k$  cos, els elements primers no nuls i els elements irreductibles coincideixen, aquest fet no és general. Per exemple, si considerem l'anell  $A = \mathbb{Z}/6\mathbb{Z}$ , tenim que els elements 2, 3 i  $4 \in A$  són primers (de fet, generen ideals maximals, cf. **A.3.21**) però no són irreductibles, ja que  $2 = 2^3$ ,  $3 = 3^2$ , i  $4 = 2^2$ .

**Proposició 1.4.6** (cf. **A.3.22**). *Sigui  $A$  un anell commutatiu qualsevol. Tot ideal maximal és un ideal primer.*  $\square$

**Proposició 1.4.7.** *Sigui  $A$  un domini d'integritat qualsevol. Tot element primer no nul  $p \in A$ ,  $p \neq 0$ , és un element irreductible.*

DEMOSTRACIÓ: Suposem que  $p = bc$ , amb  $b, c \in A$ ; cal veure que  $b$ , o bé  $c$ , és invertible. Com que el producte  $bc$  és múltiple de  $p$ , o bé  $b$  és múltiple de  $p$ , o bé ho és  $c$ . Podem suposar que  $b$  és múltiple de  $p$ , de manera que existeix  $x \in A$  tal que  $b = px$ ; per tant,  $p = bc = pxc$ , d'on  $p(1 - xc) = 0$  i, com que  $A$  és un domini d'integritat i  $p \neq 0$ , ha de ser  $1 - xc = 0$ ; això és,  $xc = 1$ , de manera que  $c$  és invertible.  $\square$

**1.4.8.** Acabem de veure que tot ideal maximal és primer i que, en un domini d'integritat, tot element primer és irreductible. Els dominis d'ideals principals són especialment bons per a aquestes propietats. En efecte, se satisfà el recíproc i tot element irreductible genera un ideal maximal.

**Proposició 1.4.9.** *Siguin  $A$  un domini d'ideals principals i  $p \in A$  un element diferent de zero. Les propietats següents són equivalents:*

- (a) *L'ideal  $pA$  és maximal.*
- (b) *L'ideal  $pA$  és primer.*
- (c) *L'element  $p$  és irreductible.*

**DEMOSTRACIÓ:** Si apliquem els dos resultats anteriors, només resta veure que si  $p$  és irreductible, llavors l'ideal  $pA$  és maximal. Sigui  $\mathfrak{a} \subsetneq A$  un ideal de  $A$  que contingui  $pA$ ; cal veure que  $\mathfrak{a} = pA$ . Com que  $A$  és un anell d'ideals principals, existeix un element  $b \in A$  tal que  $\mathfrak{a} = bA$ ; i com que  $\mathfrak{a} \neq A$ , l'element  $b$  no és invertible. D'altra banda, la hipòtesi ens diu que  $p \in bA$ ; per tant, existeix  $x \in A$  tal que  $p = bx$ . Ara, com que  $p$  és irreductible i  $b$  no és invertible,  $x$  ha de ser invertible. Però això ens diu que  $b = px^{-1} \in pA$ ; és a dir, que  $\mathfrak{a} = bA \subseteq pA$ , d'on obtenim la igualtat  $\mathfrak{a} = pA$  perquè  $pA \subseteq \mathfrak{a}$ .  $\square$

**Definició 1.4.10.** Sigui  $A$  un anell commutatiu. Dos elements  $a, b \in A$  s'anomenen *associats* si existeix un element invertible  $u \in A$  tal que  $b = au$ .

**1.4.11.** Si dos elements d'un anell commutatiu  $A$  són associats, generen el mateix ideal. Si, a més a més,  $A$  és un domini d'integritat, se satisfà la propietat recíproca: si dos elements generen el mateix ideal, llavors són associats.

**1.4.12.** Si escrivim  $a \sim b$  per a denotar que  $a$  i  $b$  són elements associats, se satisfà que la relació  $\sim$  és d'equivalència, de manera que permet fer una partició de  $A$  en classes d'elements associats. Un element  $b \in A$  és múltiple d'un element  $a \in A$  si, i només si, cada element de la classe d'elements associats de  $b$  és múltiple de cada element de la classe d'elements associats de  $a$ . Podem dir, doncs, que la relació de divisibilitat es dona entre classes d'elements associats. Anàlogament, un element  $a \in A$  és irreductible (respectivament, primer) si, i només si, tots els elements associats a  $a$  ho són; podem parlar, doncs, de les classes d'elements irreductibles o de les classes d'elements primers.

**Definició 1.4.13.** Un domini d'integritat  $A$  s'anomena un *domini de factorització única* si tot element no nul i no invertible  $a \in A$  es pot escriure com un producte de la forma  $a = up_1p_2 \cdots p_r$ ,  $r \geq 1$ , on  $p_1, p_2, \dots, p_r \in A$  són elements irreductibles determinats a menys del producte per elements invertibles de  $A$ , i  $u \in A^*$  és un element invertible; és a dir, si tota classe d'elements associats diferent de la nul·la és producte, de manera única llevat de l'ordre, d'una quantitat finita de classes d'elements irreductibles associats.

**1.4.14.** No és veritat que tot domini d'integritat sigui un domini de factorització única. Per exemple, en  $\mathbb{Z}[\sqrt{-5}] := \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$ , els elements  $3$ ,  $2 + \sqrt{-5}$ , i  $2 - \sqrt{-5}$  són irreductibles (exercici) i no es transformen l'un en cap altre en multiplicar per un element invertible de  $\mathbb{Z}[\sqrt{-5}]$ ; i se satisfà la igualtat  $(2 + \sqrt{-5})(2 - \sqrt{-5}) = 9 = 3 \cdot 3$ . Per tant, encara que  $9$  admet descomposició com a producte d'elements irreductibles en aquest anell, la descomposició no és única. Més generalment, es pot provar que tot element no nul i no invertible de  $\mathbb{Z}[\sqrt{-5}]$  admet una descomposició com a producte d'elements irreductibles; però, en general, aquesta descomposició no és única.

**Teorema 1.4.15.** *Tot domini d'ideals principals és domini de factorització única.*

DEMOSTRACIÓ: Sigui  $A$  un domini d'ideals principals. Cal veure que tot element no nul de  $A$  admet una descomposició com a producte de factors irreductibles i que aquesta és única llevat de productes per elements invertibles. Provem en primer lloc l'existència de descomposició.

Per reducció a l'absurd, suposem que  $a_0 \in A$  és un element no nul i no invertible de  $A$  que no admet descomposició com a producte d'elements irreductibles de  $A$ . Anem a construir una successió infinita d'elements de  $A$  que no admeten una tal descomposició.

La hipòtesi feta sobre  $a_0$  implica, en particular, que  $a_0$  no és irreductible; per tant, existeixen elements  $a_1, b_1 \in A$ , tots dos no invertibles, tals que  $a_0 = a_1 b_1$ . Si cadascun dels dos elements  $a_1$  i  $b_1$  admetés descomposició com a producte d'elements irreductibles, en multiplicar-les obtindríem una descomposició per a  $a_0$ , fet que contradiria la hipòtesi feta sobre  $a_0$ ; per tant, algun dels dos elements  $a_1$  o bé  $b_1$  no admet descomposició, i podem suposar que  $a_1$  no n'admet. Repetim el procés amb  $a_1$ ; obtindrem un element  $a_2 \in A$  que no admet descomposició i tal que  $a_1$  és múltiple de  $a_2$ , de manera que podem escriure  $a_1 = a_2 b_2$ , amb  $b_2$  no invertible. I així successivament. Doncs, amb la hipòtesi que  $a_0$  no admet descomposició com a producte d'elements irreductibles de  $A$ , obtenim l'existència d'una successió d'elements  $\{a_n\}_{n \geq 0}$ ,  $a_n \in A$ , tal que  $a_n$  és múltiple de  $a_{n+1}$ , per a tot  $n \geq 0$ , i que  $a_n = a_{n+1} b_{n+1}$ , on  $b_{n+1} \in A$  no és invertible.

Aquesta successió d'elements ens proporciona la successió estrictament creixent d'ideals de  $A$ ,

$$a_0 A \subsetneq a_1 A \subsetneq \cdots \subsetneq a_n A \subsetneq a_{n+1} A \subsetneq \cdots .$$

Sigui  $\mathfrak{a} := \bigcup_{n \geq 0} a_n A \subseteq A$ ; llavors,  $\mathfrak{a}$  és un ideal de  $A$  que conté estrictament tots els ideals  $a_n A$ . Com que  $A$  és principal, existeix un element  $c \in A$  tal que  $\mathfrak{a} = cA$ . Però la definició de  $\mathfrak{a}$  ens diu que existeix  $n \geq 0$  tal que  $c \in a_n A$ , de manera que  $cA \subseteq a_n A$ ; i això contradia el fet que  $\mathfrak{a}$  conté estrictament  $a_n A$ . Aquesta contradicció acaba la reducció a l'absurd i, en conseqüència, tot element de  $A$  admet una descomposició com a producte d'elements irreductibles.

Per a veure la unicitat de les descomposicions, suposem que per a un element  $a \in A$ , no nul i no invertible, existeixen elements irreductibles  $p_1, p_2, \dots, p_r, q_1, q_2, \dots, q_s \in A$ ,  $r, s \geq 1$ , i elements invertibles  $u, v \in A^*$  tals que

$$a = up_1 p_2 \cdots p_r = vq_1 q_2 \cdots q_s.$$

Com que  $A$  és principal i  $p_1 \in A$  és irreductible, l'ideal  $p_1 A$  és primer i, com que el producte  $vq_1 q_2 \cdots q_s$  pertany a l'ideal  $p_1 A$  i  $v \notin p_1 A$ , algun dels elements  $q_j$  pertany a  $p_1 A$ ; podem suposar que  $q_1 \in p_1 A$ . Ara, com que  $q_1$  és múltiple de  $p_1$  i  $q_1$  és irreductible, tenim que els dos elements són iguals llevat del producte per un element invertible de  $A$ ; i, com que  $A$  és un domini d'integritat, podem simplificar  $p_1$  i  $q_1$  dels dos membres, a canvi de multiplicar-ne algun per un element invertible de  $A$ . Obtenim dues descomposicions d'un (altre) element no nul de  $A$  amb un factor irreductible menys a cada membre de la igualtat.

Això ho podem continuar fent mentre quedin elements irreductibles en algun dels dos membres de la igualtat; finalment, arribarem a una igualtat entre dos elements invertibles de  $A$ . És a dir, obtindrem que  $r = s$ , i que, llevat de l'ordre i del producte per elements invertibles,  $p_i = q_i$ . Això acaba la prova.  $\square$

**Observació 1.4.16.** Notem que en la prova de l'existència de descomposicions només es fa servir que l'anell  $A$  és un domini d'ideals principals per a arribar a una contradicció amb el fet de tenir una successió infinita estrictament creixent d'ideals principals. Doncs, si per a un domini d'integritat  $A$  no existeixen successions infinites estrictament creixents d'ideals principals, tot element admet una descomposició com a producte d'elements irreductibles, encara que potser no de manera única. De fet, existeixen exemples de dominis d'integritat d'ús ampli en matemàtiques en els quals hi ha elements que no admeten cap descomposició com a producte d'elements irreductibles.

**Corol·lari 1.4.17.** *Sigui  $k$  un cos qualsevol. L'anell de polinomis  $k[X]$  és un domini de factorització única.*  $\square$

**Corol·lari 1.4.18.** *L'anell  $\mathbb{Z}$  dels nombres enters és un domini de factorització única.*  $\square$

## 1.5 Factorització única a $A[X]$

Usualment treballem amb polinomis de coeficients enters; per tant, és convenient tenir un bon coneixement de l'anell de polinomis  $\mathbb{Z}[X]$ . D'una banda, ens interessa saber que hi ha factorització única; de l'altra, com es relacionen la irreductibilitat en  $\mathbb{Z}[X]$  i la irreductibilitat en  $\mathbb{Q}[X]$  dels polinomis de coeficients enters. Però no només treballem amb polinomis de coeficients enters. Sovint ho fem amb polinomis de coeficients en altres anells; especialment, en alguns dominis d'integritat. Els resultats d'aquesta secció són aplicables a moltes situacions generals; sobretot, en el cas de dominis de factorització única. Notem que, encara que treballem sobre un domini d'integritat qualsevol,  $A$ , l'anell de polinomis,  $k[X]$ , sobre el seu cos de fraccions,  $k$ , és un domini d'ideals principals i, per tant, un domini de factorització única. Però pot ser que el domini  $A$  ja sigui un domini de factorització única. En aquest cas, resulta que l'anell de polinomis  $A[X]$  també és de factorització única. Aquesta secció es dedica a la prova d'aquest resultat.

**Definició 1.5.1.** Sigui  $A$  un anell commutatiu. Donats elements  $a, b, d \in A$ , es diu que  $d$  és un *màxim comú divisor* de  $a$  i  $b$ , i s'escriu  $d = \text{mcd}(a, b)$ , si se satisfan les dues condicions següents.

- (a)  $a$  i  $b$  són múltiples de  $d$ ;
- (b) per a tot  $\delta \in A$ , si  $a$  i  $b$  són múltiples de  $\delta$ , llavors  $d$  és múltiple de  $\delta$ .

**Observació 1.5.2.** En general, donats elements  $a, b$ , d'un anell commutatiu  $A$ , no té per què existir cap màxim comú divisor de  $a$  i  $b$ ; ni tan sols en el cas que  $A$  sigui un domini d'integritat.

**1.5.3.** Com succeeix per als elements irreductibles, els elements primers o, en general, amb les qüestions relacionades amb la divisibilitat, un element  $d$  és un màxim comú divisor d'elements  $a, b \in A$  si, i només si, qualsevol element de la classe d'elements associats a  $d$  és un màxim comú divisor d'elements qualssevol  $a', b'$ , de les classes d'elements associats a  $a$  i  $b$ , respectivament. És a dir, el concepte de màxim comú divisor és, de fet, un concepte relatiu a classes d'elements associats. És només en aquest sentit que podem escriure l'expressió  $d = \text{mcd}(a, b)$ , expressió que és una igualtat que es dona entre les classes d'elements associats, però no necessàriament entre els elements de  $A$ . Així, per

exemple, de les dues expressions  $1 = \text{mcd}(2, 3)$  i  $-1 = \text{mcd}(2, 3)$ , vàlides en  $\mathbb{Z}$ , es dedueix l'expressió  $1 = -1$ , que és una igualtat de classes d'elements associats, però no, òbviament, de nombres enters.

**1.5.4.** Siguin  $A$  un domini de factorització única i  $a \in A$  un element no nul. El conjunt de classes d'elements irreductibles associats que divideixen  $a$  és finit. En conseqüència, el conjunt de classes de divisors de  $a$  és finit. Llavors, l'algoritme de l'escola que consisteix a prendre el producte dels factors irreductibles comuns a dos elements  $a, b \in A$ , tantes vegades com es pugui, en proporciona un màxim comú divisor. Això ens diu que en tot domini de factorització única se satisfà l'existència de màxim comú divisor. És a dir, se satisfà el resultat següent.

**Proposició 1.5.5.** *Si  $A$  és un domini de factorització única i  $a, b \in A$ , llavors existeix  $d \in A$  tal que  $d = \text{mcd}(a, b)$ .  $\square$*

**1.5.6** (L'algoritme d'Euclides). En general, tot i la seva existència sobre dominis de factorització única, no sabem calcular màxims comuns divisors d'elements donats. Però hi ha un cas molt important en què això se sap fer. Si  $k$  és un cos, disposem d'un algoritme per a calcular el màxim comú divisor de dos polinomis  $f(X), g(X) \in k[X]$ , l'algoritme d'Euclides. En efecte, donats polinomis qualssevol  $f(X), g(X), q(X) \in k[X]$ , se satisfà que  $\text{mcd}(f(X), g(X)) = \text{mcd}(f(X) - g(X)q(X), g(X))$ , i que  $\text{mcd}(f(X), 0) = f(X)$ . Si  $g(X) = 0$ , tenim que  $\text{mcd}(f(X), 0) = f(X)$ . I si  $g(X) \neq 0$ , fem servir la divisió entera de polinomis; obtenim una igualtat  $f(X) := g(X)q(X) + r(X)$ , on  $q(X), r(X) \in k[X]$ , i  $\text{gr}(r(X)) < \text{gr}(g(X))$ . Llavors, tenim que  $\text{mcd}(f(X), g(X)) = \text{mcd}(g(X), r(X))$ . I podem iterar el procés, canviant successivament la parella  $(f(X), g(X))$  per la parella  $(g(X), r(X))$ . El procés s'atura, com a màxim en tantes iteracions com el grau del polinomi  $g(X)$  inicial més una, quan obtenim un residu  $r(X) = 0$ , moment en el qual sabem que el màxim comú divisor cercat és el darrer polinomi  $g(X)$  considerat com a divisor. Si ara escrivim les igualtats successives que obtenim i substituïm enrere, obtenim una prova del resultat següent. Es proposa com a exercici escriure els detalls de la demostració.

**Corol·lari 1.5.7.** *Siguin  $k$  un cos,  $f(X), g(X) \in k[X]$  polinomis no nuls, i suposem que  $d(X) \in k[X]$  és un màxim comú divisor de  $f(X)$  i  $g(X)$ . Llavors, existeixen polinomis  $a(X), b(X) \in k[X]$ , tals que  $d(X) = f(X)a(X) + g(X)b(X)$ , i únics tals que, a més a més,  $\text{gr}(a(X)) < \text{gr}(g(X))$  i  $\text{gr}(b(X)) < \text{gr}(f(X))$ .  $\square$*

**Definició 1.5.8.** Una igualtat de la forma  $d(X) = f(X)a(X) + g(X)b(X)$ , per a polinomis  $a(X), b(X), d(X) \in k[X]$ , i  $d(X) = \text{mcd}(f(X), g(X))$ , s'anomena una *igualtat de Bézout* per a  $f(X), g(X)$  i  $d(X)$ .

**Definició 1.5.9.** Siguin  $A$  un domini de factorització única i  $f(X) \in A[X]$  un polinomi no nul. S'anomena *contingut* de  $f(X)$  el màxim comú divisor dels coeficients de  $f(X)$ . Escrivem  $\text{cont}(f(X))$  per a indicar el contingut del polinomi  $f(X)$ ; és una classe d'elements associats de  $A$ . Un polinomi no nul  $f(X) \in A[X]$  s'anomena *primitiu* si  $\text{cont}(f(X)) = 1$ .

**Observació 1.5.10.** Notem que si  $A$  és un domini de factorització única i  $f(X) \in A[X]$  és un polinomi de contingut  $c \in A$ , llavors podem escriure  $f(X) = cf'(X)$ , on el polinomi  $f'(X) \in A[X]$  és primitiu.

**Teorema 1.5.11** (Lema de Gauss, versió 1). *Siguin  $A$  un domini de factorització única i  $f(X), g(X) \in A[X]$  polinomis no nuls. Llavors,*

$$\text{cont}(f(X)g(X)) = \text{cont}(f(X)) \text{cont}(g(X)).$$

DEMOSTRACIÓ: Siguin  $c_f, c_g \in A$  els continguts de  $f(X), g(X)$ , respectivament; podem escriure, doncs,  $f(X) = c_f f'(X)$ ,  $g(X) = c_g g'(X)$ , amb  $f'(X), g'(X) \in A[X]$ , i  $\text{cont}(f'(X)) = \text{cont}(g'(X)) = 1$ ; o sigui, primitius. Llavors,  $f(X)g(X) = c_f c_g f'(X)g'(X)$ , i és suficient demostrar que  $\text{cont}(f'(X)g'(X)) = 1$ . O sigui, és suficient provar la versió 0 del lema de Gauss, que *el producte de polinomis primitius és un polinomi primitiu*. Per a tot element irreductible  $p \in A$ , tenim que  $f'(X) \not\equiv 0 \pmod{pA}$ , i  $g'(X) \not\equiv 0 \pmod{pA}$ , perquè  $\text{cont}(f'(X)) = \text{cont}(g'(X)) = 1$ . Com que  $A$  és un domini de factorització única, l'ideal  $pA$  és primer i, per tant, l'anell quocient  $A/pA$  és un domini d'integritat; en conseqüència,  $(A/pA)[X]$  és un domini d'integritat,  $f'(X)g'(X) \not\equiv 0 \pmod{pA}$ , i  $p$  no divideix  $\text{cont}(f'(X)g'(X))$ . Així,  $\text{cont}(f'(X)g'(X))$  no és divisible per cap element irreductible; doncs,  $\text{cont}(f'(X)g'(X)) = 1$ , com calia provar.  $\square$

**Corol·lari 1.5.12** (Lema de Gauss, versió 2). *Sigui  $A$  un domini de factorització única,  $K$  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, i tals que  $g(X) = c_g g'(X)$ ,  $h(X) = c_h h'(X)$ , 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  $A[X]$ .*

DEMOSTRACIÓ: Comencem per definir els elements  $c_g, c_h$ . Considerem un denominador comú de tots els coeficients de  $g(X)$ , posem  $d_g \in A$ , de manera que  $d_g g(X) \in A[X]$ ; sigui  $\delta_g \in A$  el contingut del polinomi  $d_g g(X)$  i posem  $d_g g(X) = \delta_g g'(X)$ , amb  $g'(X) \in A[X]$  de contingut 1; i, finalment, sigui  $c_g := \frac{\delta_g}{d_g} \in K$ . Definim  $d_h, \delta_h, h'(X)$  i  $c_h$  anàlogament.

És clar que  $f(X) = g(X)h(X) = c_g c_h g'(X)h'(X)$ . Com que  $g'(X)h'(X)$  és de contingut 1 (cf. el lema de Gauss, 1.5.11), el producte  $c_g c_h$  ha de ser el contingut del polinomi  $f(X)$ , de manera que  $c_g c_h \in A$ . En efecte, si escrivim  $c_g c_h = \frac{a}{b}$ , amb  $a, b \in A$ , primers entre si, tenim que  $bf(X) = ag'(X)h'(X)$ , i d'aquesta igualtat es dedueix immediatament que  $a = \text{cont}(ag'(X)h'(X)) = \text{cont}(bf(X)) = b \cdot \text{cont}(f(X))$ , d'on és clar que  $a$  és múltiple de  $b$ . Però com que  $A$  és un domini de factorització única i  $\text{mcd}(a, b) = 1$ ,  $b$  ha d'ésser invertible en  $A$ , de manera que  $c_g c_h = \frac{a}{b} \in A$ .  $\square$

**Corol·lari 1.5.13** (Lema de Gauss, versió 3). *Sigui  $A$  un domini de factorització única,  $K$  el seu cos de fraccions, i  $f(X) \in A[X]$  un polinomi no constant. Si  $f(X)$  és irreductible en  $A[X]$ , també ho és en  $K[X]$ ; d'altra banda, si  $f(X)$  és irreductible en  $K[X]$ , ho és en  $A[X]$  si, i només si, és de contingut 1.  $\square$*

Aquest resultat ens permet provar un resultat molt important que, en particular, ens diu que l'anell de polinomis  $\mathbb{Z}[X_1, \dots, X_n]$  i, per a qualsevol cos  $k$ , els anells de polinomis  $k[X_1, \dots, X_n]$  són de factorització única.

**Teorema 1.5.14** (Lema de Gauss, versió 4). *Si  $A$  és un domini de factorització única, l'anell de polinomis  $A[X]$  també és un domini de factorització única. A més a més, els elements irreductibles de  $A[X]$  són els elements irreductibles de  $A$  i els polinomis de  $A[X]$  de contingut 1 que són irreductibles en  $K[X]$ , on  $K$  designa el cos de fraccions de  $A$ .*

DEMOSTRACIÓ: Sigui  $f(X) \in A[X]$ ,  $f(X) \neq 0$ . Com que l'anell  $K[X]$  és de factorització única, els corol·laris anteriors, 1.5.12 i 1.5.13, ens ensenyen que, a partir d'una descomposició de  $f(X)$  com a producte de factors irreductibles en  $K[X]$ , existeix una descomposició

de  $f(X)$  de la forma  $f(X) = cg_1(X) \cdots g_n(X)$ , on  $c \in A$  i  $g_i(X) \in A[X]$  és un polinomi de contingut 1 i irreductible en  $K[X]$ . Ara, com que  $A$  és un domini de factorització única, l'element  $c$  es pot escriure de manera única (llevat de producte per elements invertibles de  $A$ ) com a producte d'elements irreductibles de  $A$ . Això dona una descomposició de  $f(X)$ ; en efecte, d'una banda, els elements de  $A$  només poden descompondre en  $A[X]$  com ho fan en  $A$ , ja que són polinomis de grau zero; per tant, els elements irreductibles de  $A$  també són irreductibles en  $A[X]$ ; d'altra banda, si un polinomi descompon en  $A[X]$ , la mateixa descomposició val en  $K[X]$ , de manera que un polinomi de  $A[X]$  de contingut 1 i irreductible en  $K[X]$  és irreductible en  $A[X]$ .

Resta veure la unicitat de la descomposició. Per a això, suposem que podem escriure  $f(X) = cg_1(X) \cdots g_n(X) = dh_1(X) \cdots h_m(X)$ , amb  $g_i(X), h_j(X) \in A[X]$ , de contingut 1, i irreductibles en  $K[X]$ . D'una banda,  $c, d$  són el contingut de  $f(X)$ , de manera que són associats; d'altra banda, la igualtat val en  $K[X]$ , que és de factorització única; per tant,  $n = m$  i, llevat de permutació dels polinomis,  $g_i(X)$  és associat de  $h_i(X)$  en  $K[X]$ ; però, llavors, en virtut del lema de Gauss (1.5.12),  $g_i(X)$  i  $h_i(X)$  són associats en  $A[X]$ . Això, juntament amb la factorització única en  $A$  per al contingut de  $f(X)$ , demostra la unicitat de la descomposició.  $\square$

**Corol·lari 1.5.15.** *Per a tot  $n \geq 0$ , l'anell de polinomis  $\mathbb{Z}[X_1, X_2, \dots, X_n]$  és un domini de factorització única.  $\square$*

**Corol·lari 1.5.16.** *Per a tot cos  $k$  i tot  $n \geq 1$ , l'anell de polinomis  $k[X_1, X_2, \dots, X_n]$  és un domini de factorització única.  $\square$*

**Observació 1.5.17.** Notem que hem etiquetat uns quants resultats diferents com a *Lema de Gauss*. La raó és que, de fet, la demostració que es presenta aquí del resultat principal (teorema 1.5.14) és, essencialment, una demostració de Gauss (cf., per exemple, [vW 1970, Chap. 5.4]). D'altra banda, qualsevol d'ells es podria trobar etiquetat d'aquesta manera en alguna font bibliogràfica, tot i que majoritàriament s'hi troba així el teorema 1.5.11 (cf., per exemple, [Ar 1991, Chap. 11, Thm. 3.3], [Ja 1974, Chap. 2.16, Lemma 2], [La 1984, Chap. V, § 6, Thm. 6.1]).

## 1.6 Criteris d'irreductibilitat de polinomis

Fins ara, no hem parlat de com es pot saber si un polinomi és irreductible, ni tan sols en el cas de coeficients en un cos; només ho sabem per als polinomis de grau 1. En aquesta secció, donem alguns criteris per a reconèixer si un polinomi és o no irreductible, almenys, per a alguns casos particulars.

**Teorema 1.6.1** (Criteri d'Eisenstein). *Siguin  $A$  un domini de factorització única,  $K$  el seu cos de fraccions, i  $f(X) = a_0 + a_1X + \cdots + a_nX^n \in A[X]$ ,  $a_0, a_1, \dots, a_n \in A$ ,  $a_n \neq 0$ , un polinomi. Suposem que existeix un element irreductible  $p \in A$  tal que  $a_n$  no és múltiple de  $p$ , cadascun dels  $a_0, a_1, \dots, a_{n-1}$  és múltiple de  $p$ , i  $a_0$  no és múltiple de  $p^2$ . Llavors,  $f(X)$  és irreductible en  $K[X]$ . I si, a més a més,  $f(X)$  és primitiu,  $f(X)$  és irreductible en  $A[X]$ .*

**DEMOSTRACIÓ:** Per reducció a l'absurd, suposem que  $f(X)$ , a més a més de satisfer les hipòtesis de l'enunciat, no és irreductible en  $K[X]$ . Llavors, existeixen polinomis no

constants,  $g(X), h(X) \in K[X]$ , de manera que  $f(X) = g(X) \cdot h(X)$ . I, pel lema de Gauss (cf. **1.5.12**), podem modificar els polinomis, multiplicant-los per constants adequades de  $K$ , de manera que  $g(X), h(X)$  siguin de coeficients en  $A$ .

Ara, podem reduir la igualtat  $f(X) = g(X) \cdot h(X)$  mòdul  $pA$ . Per hipòtesi, la reducció mòdul  $pA$  de  $f(X)$  és el polinomi  $uX^n$ , on  $u \in A/pA$  és un element no nul (de fet,  $u \equiv a_n \pmod{pA}$ ). D'altra banda, si designem per  $\bar{g}(X), \bar{h}(X)$  la reducció mòdul  $pA$  dels polinomis  $g(X), h(X)$ , tenim que

$$\text{gr}(\bar{g}(X)) = \text{gr}(g(X)), \quad \text{i} \quad \text{gr}(\bar{h}(X)) = \text{gr}(h(X)),$$

ja que això mateix succeeix amb el polinomi producte; en particular, aquestes reduccions són polinomis no constants.

Ara,  $A/pA$  no és necessàriament un cos, però és un domini d'integritat i podem considerar el seu cos de fraccions,  $k$ . L'anell de polinomis  $k[X]$  és un domini de factorització única, i de la descomposició

$$uX^n = \bar{g}(X) \cdot \bar{h}(X)$$

en  $(A/pA)[X] \subseteq k[X]$ , obtenim que existeixen elements no nuls  $v, w \in A/pA$  tals que

$$\bar{g}(X) = v \cdot X^k, \quad \text{i} \quad \bar{h}(X) = w \cdot X^{n-k},$$

on  $0 < k = \text{gr}(g(X)) < n$ , i  $0 < n - k = \text{gr}(h(X)) < n$ .

Això implica que tots els coeficients de  $g(X)$  i de  $h(X)$ , excepte els del monomi de grau màxim de cadascun d'ells, són divisibles per  $p$ , en  $A$ ; en particular, els termes constants dels polinomis  $g(X)$  i  $h(X)$  són divisibles per  $p$ . Però d'això se segueix immediatament que el terme constant del polinomi  $f(X)$  és divisible per  $p^2$ , perquè és el producte dels termes constants dels polinomis  $g(X)$  i  $h(X)$ ; i això contradiu la hipòtesi feta sobre el polinomi  $f(X)$ . Aquesta contradicció demostra que si el polinomi  $f(X)$  satisfà les condicions de l'enunciat, llavors és irreductible en  $K[X]$ .

Finalment, si, a més a més,  $f(X)$  és primitiu, com que és irreductible en  $K[X]$ , una nova aplicació del lema de Gauss (cf. **1.5.13**) ens diu que també és irreductible en  $A[X]$ .  $\square$

**Definició 1.6.2.** Un polinomi per al qual se satisfan les hipòtesis del teorema s'anomena un *polinomi d'Eisenstein* per al primer  $p$ .

**Exemple 1.6.3.** Sigui  $a \in \mathbb{Z}$ ,  $a \neq 0, 1, -1$ , un nombre enter lliure de quadrats; és a dir, tal que per a tot nombre primer  $p \in \mathbb{Z}$ , el nombre  $p^2$  no divideix  $a$ . Per a tot nombre natural  $n \geq 1$  el polinomi  $X^n - a$  és irreductible en  $\mathbb{Z}[X]$  i en  $\mathbb{Q}[X]$ , perquè és un polinomi d'Eisenstein per a qualsevol nombre natural primer  $p$  que divideix  $a$ .

Més generalment, si  $a \in \mathbb{Z}$  és un nombre enter,  $a \neq 0, 1, -1$ , per al qual existeix un nombre primer  $p$  tal que  $p$  divideix  $a$  però  $p^2$  no divideix  $a$ , llavors  $X^n - a$  és un polinomi d'Eisenstein per al primer  $p$  i, per tant, irreductible en  $\mathbb{Q}[X]$ , i en  $\mathbb{Z}[X]$ .

Destaquem els dos resultats següents que, encara que immediats, són útils molt sovint.

**1.6.4.** Siguin  $A$  un domini d'integritat i  $\varphi : A[X] \rightarrow A[X]$  un isomorfisme qualssevol. Un polinomi  $f(X) \in A[X]$  és irreductible si, i només si, ho és  $\varphi(f(X))$ .  $\square$



**1.6.5.** Siguin  $A$  un anell commutatiu, i  $u, v \in A$ ,  $u$  invertible. Existeix un únic morfisme d'anells  $\varphi : A[X] \rightarrow A[X]$  tal que  $\varphi(a) = a$ , per a tot  $a \in A$ , i  $\varphi(X) = uX + v$ ; aquest morfisme és un isomorfisme.  $\square$

**Corollari 1.6.6.** Siguin  $A$  un domini d'integritat i  $f(X) \in A[X]$  un polinomi no nul. Llavors,  $f(X)$  és irreductible si, i només si, per a algun element  $a \in A$ ,  $f(X - a)$  és irreductible; si, i només si, per a tot element  $a \in A$ ,  $f(X - a)$  és irreductible.  $\square$

**Proposició 1.6.7.** Sigui  $p$  un nombre natural primer. Llavors, el polinomi ciclotòmic  $\Phi_p(X) := 1 + X + X^2 + \dots + X^{p-1} \in \mathbb{Z}[X]$  és irreductible (cf. **3.2.6** i **3.2.23**).

DEMOSTRACIÓ: Notem que  $\Phi_p(X) = \frac{X^p - 1}{X - 1}$ , i sigui  $g(X) := \Phi_p(X + 1)$ . Llavors,  $g(X) = \frac{(X + 1)^p - 1}{(X + 1) - 1} = \frac{(X + 1)^p - 1}{X} = \sum_{i=1}^p \binom{p}{i} X^{i-1}$ . Com que  $p$  és primer, els nombres combinatoris  $\binom{p}{i}$ ,  $1 \leq i \leq p - 1$ , són divisibles per  $p$ , i  $\binom{p}{1} = p$  no és divisible per  $p^2$ , de manera que  $g(X)$  és un polinomi d'Eisenstein per al primer  $p$ ; per tant,  $g(X)$  és irreductible; en conseqüència,  $\Phi_p(X)$  és irreductible.  $\square$

**Teorema 1.6.8.** Siguin  $A, B$  dominis d'integritat,  $\varphi : A \rightarrow B$  un morfisme qualsevol d'anells, i  $L$ , el cos de fraccions de  $B$ . Anomenem també  $\varphi : A[X] \rightarrow B[X]$  el morfisme d'anells que s'obté en aplicar  $\varphi$  als coeficients dels polinomis de  $A[X]$ . Sigui  $f(X) \in A[X]$  un polinomi tal que  $\varphi(f(X)) \neq 0$  i  $\text{gr}(\varphi(f(X))) = \text{gr}(f(X))$ . Llavors, si el polinomi  $\varphi(f(X))$  és irreductible en  $L[X]$ ,  $f(X)$  no admet cap factorització en  $A[X]$  de la forma  $f(X) = g(X)h(X)$ , amb  $g(X), h(X) \in A[X]$ ,  $\text{gr}(g(X)) \geq 1$  i  $\text{gr}(h(X)) \geq 1$ .

DEMOSTRACIÓ: Si  $f(X)$  tingués una factorització com la de l'enunciat, en aplicar  $\varphi$  obtindríem una factorització,  $\varphi(f(X)) = \varphi(g(X))\varphi(h(X))$ , de  $\varphi(f(X))$  en  $L[X]$ ; com que es té que  $\text{gr}(\varphi(g(X))) \leq \text{gr}(g(X))$  i també que  $\text{gr}(\varphi(h(X))) \leq \text{gr}(h(X))$ , i, simultàniament,  $\text{gr}(\varphi(g(X))\varphi(h(X))) = \text{gr}(g(X)h(X))$ , s'haurien de satisfer les propietats  $\text{gr}(\varphi(g(X))) = \text{gr}(g(X)) \geq 1$  i  $\text{gr}(\varphi(h(X))) = \text{gr}(h(X)) \geq 1$ , de manera que obtindríem una descomposició no trivial de  $\varphi(f(X))$  en  $L[X]$ , contràriament a la hipòtesi que  $\varphi(f(X))$  és irreductible.  $\square$

**Corollari 1.6.9** (Criteri de reducció). Siguin  $f(X) \in \mathbb{Z}[X]$  un polinomi no nul i  $p \in \mathbb{Z}$  un nombre primer que no divideix el coeficient del monomi principal de  $f(X)$ . Suposem que per reducció mòdul  $p$  dels coeficients de  $f(X)$  s'obté un polinomi irreductible en  $(\mathbb{Z}/p\mathbb{Z})[X]$ ; llavors,  $f(X)$  és irreductible en  $\mathbb{Q}[X]$ . Si, a més a més,  $f(X)$  és primitiu,  $f(X)$  és irreductible en  $\mathbb{Z}[X]$ .  $\square$

**Exemple 1.6.10.** Siguin  $a, b \in \mathbb{Z}$  nombres senars. Els polinomis  $X^2 + aX + b$ ,  $X^3 + aX + b$ ,  $X^3 + aX^2 + b \in \mathbb{Z}[X]$  són irreductibles en  $\mathbb{Z}[X]$  i en  $\mathbb{Q}[X]$ . En efecte, les seves reduccions mòdul 2 són els polinomis  $X^2 + X + 1$ ,  $X^3 + X + 1$  i  $X^3 + X^2 + 1 \in (\mathbb{Z}/2\mathbb{Z})[X]$ , que són irreductibles (cf. l'exercici **1.8.4**).

## 1.7 Un mètode de factorització en $\mathbb{Z}[X]$

En general, els algorismes coneguts per a determinar si un polinomi és o no irreductible no són gaire eficients. Per a polinomis de coeficients enters, però, es pot donar un algorisme

que no només serveix per a decidir si un polinomi donat és irreductible o no, sinó que, en cas de ser reductible, en proporciona la descomposició. Aquest algoritme, que descrivim en aquesta secció, està basat en el càlcul de factoritzacions d'alguns nombres enters; i la seva eficiència depèn de com se sàpiga resoldre aquest problema de manera eficient.

Sigui  $f(X) := a_0 + a_1X + \dots + a_nX^n \in \mathbb{Z}[X]$ ,  $a_0, a_1, \dots, a_n \in \mathbb{Z}$ ,  $a_n \neq 0$ ,  $n \geq 0$ , un polinomi no nul qualsevol del qual volem trobar els seus factors irreductibles.

**1.7.1.** En primer lloc, podem calcular el contingut del polinomi i factoritzar aquest nombre enter. D'aquesta manera obtenim un factor constant del polinomi descompost en factors irreductibles i un polinomi de contingut 1 de  $\mathbb{Z}[X]$  que cal descompondre.

**1.7.2.** A continuació, calculem el polinomi derivat  $D(f, X)$  i, amb l'algoritme d'Euclides en  $\mathbb{Q}[X]$ , calculem el màxim comú divisor de  $f(X)$  i  $D(f, X)$  en  $\mathbb{Q}[X]$ , i en  $\mathbb{Z}[X]$ . Si posem  $d(X) := \text{mcd}(f(X), D(f, X)) \in \mathbb{Z}[X]$ , llavors el polinomi  $g(X) := \frac{f(X)}{d(X)} \in \mathbb{Z}[X]$  té els mateixos factors irreductibles que  $f(X)$ , però tots són de multiplicitat 1. Al final, per divisió, podem calcular la multiplicitat de cadascun dels factors múltiples de  $f(X)$ .

**1.7.3.** Doncs, a partir d'aquest punt, podem suposar que  $f(X) \in \mathbb{Z}[X]$  és un polinomi primitiu i sense factors irreductibles múltiples. I si el grau  $n$  de  $f(X)$  és 0 o bé 1, ja hem acabat, perquè  $f(X)$  és irreductible. En cas contrari, com que  $f(X)$  és de grau  $n \geq 2$ , si  $f(X)$  no és irreductible, ha de tenir algun divisor de grau menor o igual que la meitat de  $n$ . El procés de càlcul dels factors irreductibles de  $f(X)$  es fa cercant successivament els factors irreductibles de grau 1, després els de grau 2, i així successivament, fins als de grau  $[n/2]$ . Cada cop que trobem un factor de  $f(X)$ , posem  $h(X)$ , canviem el polinomi  $f(X)$  per  $\frac{f(X)}{h(X)}$ , de manera que el nou polinomi  $f(X)$  és de grau menor que el grau del polinomi  $f(X)$  anterior; per tant, la fita  $[n/2]$  va decreixent a mesura que anem trobant factors.

**1.7.4.** Comencem el procés amb el càlcul dels factors irreductibles de grau 1 del polinomi  $f(X)$ . Això és equivalent a calcular les arrels racionals de  $f(X)$  i és ben conegut que si  $\frac{a}{b} \in \mathbb{Q}$  és una arrel de  $f(X)$  en  $\mathbb{Q}$ , amb  $a, b \in \mathbb{Z}$ ,  $b > 0$ , i  $\text{mcd}(a, b) = 1$ , llavors  $a \mid a_0$  i  $b \mid a_n$ ; la descomposició en factors primers de  $a_0$  ens dóna una quantitat finita de possibilitats per a  $a$ , i la descomposició en factors primers de  $a_n$ , una quantitat finita de possibilitats per a  $b$ ; llavors, el mètode de divisió de Ruffini aplicat a totes les fraccions  $\frac{a}{b}$  ens diu immediatament quines d'aquestes possibilitats proporcionen realment factors de  $f(X)$  de grau 1, necessàriament irreductibles.

**1.7.5.** Un cop completat aquest pas, obtenim un nou polinomi  $f(X)$  que no és divisible per polinomis de grau 1. Si aquest nou polinomi és de grau 2 o bé de grau 3, ja hem acabat la descomposició. En cas contrari, cerquem un conjunt finit de polinomis de grau 2 que contingui tots els divisors de grau 2 del polinomi  $f(X)$ .

Per a això, suposem que  $g(X) := aX^2 + bX + c$  és un polinomi de coeficients enters  $a, b, c$ , tals que  $a \neq 0$  i que  $g(X)$  divideix  $f(X)$ . Llavors, per a tot nombre enter  $z$ , el nombre enter  $g(z)$  divideix  $f(z)$  (en efecte, si  $h(X) \in \mathbb{Z}[X]$  és tal que  $f(X) = g(X)h(X)$ , també és  $f(z) = g(z)h(z)$ ). Aquest fet ens proporciona les condicions de divisibilitat  $z^2a + zb + c \mid f(z)$ , una per a cada nombre enter  $z \in \mathbb{Z}$ . Per exemple, podem obtenir les relacions  $c \mid a_0$  (que correspon a fer  $z = 0$ ),  $a + b + c \mid a_0 + a_1 + \dots + a_n$  (que

correspon a fer  $z = 1$ ),  $a - b + c \mid a_0 - a_1 + \dots + (-1)^n a_n$  (que correspon a fer  $z = -1$ ),  $4a + 2b + c \mid a_0 + 2a_1 + \dots + 2^n a_n$  (que correspon a fer  $z = 2$ ), etcètera. De cadascuna d'aquestes relacions de divisibilitat, i si tenim en compte que, per a tot  $z \in \mathbb{Z}$ , el nombre de divisors de  $f(z)$  és finit (observem que  $f(z) \neq 0$  perquè  $f(X)$  no té arrels en  $\mathbb{Z}$ ), obtenim una quantitat finita d'equacions lineals. És a dir, per a cada nombre enter  $z$ , s'ha de satisfer que  $az^2 + bz + c$  sigui igual a algun dels divisors de  $f(z)$ .

Triem ara tres nombres enters diferents  $z_1, z_2, z_3$  i, per a cadascun d'ells, considerem un divisor, que anomenem  $d(z_i)$ , de  $f(z_i)$ ; d'aquesta manera obtenim un sistema d'equacions lineals de matriu

$$\begin{bmatrix} z_1^2 & z_1 & 1 & \mid & d(z_1) \\ z_2^2 & z_2 & 1 & \mid & d(z_2) \\ z_3^2 & z_3 & 1 & \mid & d(z_3) \end{bmatrix},$$

on el vector columna  $[d(z_1), d(z_2), d(z_3)]^t$  és el terme independent del sistema i el determinant del qual és el determinant de Vandermonde

$$\begin{vmatrix} z_1^2 & z_1 & 1 \\ z_2^2 & z_2 & 1 \\ z_3^2 & z_3 & 1 \end{vmatrix} = (z_1 - z_3)(z_2 - z_3)(z_1 - z_2) \neq 0.$$

En conseqüència, el sistema és de Cramer i té solució única. Així, per a cada família  $\{d(z_i)\}_{i=1,2,3}$ , obtenim una solució racional  $(a, b, c)$  del sistema. Si descartem les solucions que no siguin enteres, obtenim els possibles polinomis de grau 2 de  $\mathbb{Z}[X]$  que divideixen  $f(X)$ ; i, per divisió, obtenim efectivament els divisors irreductibles de grau 2 de  $f(X)$ .

**Observacions 1.7.6.** Notem que cal factoritzar els nombres enters  $f(z_i)$ ; aquests nombres creixen de la mateixa manera que  $z_i^n$ , on  $n$  és el grau del polinomi  $f(X)$ ; per tant, pot ésser costós de factoritzar-los. Però tenim el recurs de canviar de valor  $z_i$  tantes vegades com vulguem. Així, si per a un valor  $z$  no aconseguim factoritzar el nombre  $f(z)$ , podem canviar de valor i intentar-ho amb un nou valor de  $z$ .

D'altra banda, un cop haguem obtingut una llista de possibles polinomis  $aX^2 + bX + c$  divisors de  $f(X)$ , i si la llista és molt llarga, podem garbellar-la sense necessitat de més factoritzacions abans de procedir a les divisions. En efecte, per a cadascun dels polinomis obtinguts, i per a tots els nombres enters  $z$ , cal que se satisfaci que  $az^2 + bz + c$  sigui un divisor de  $f(z)$ . Doncs, per a uns quants valors de  $z$ , la comprovació que aquesta propietat de divisibilitat no se satisfà permet descartar el polinomi  $aX^2 + bX + c$  com a possible divisor de  $f(X)$ .

**1.7.7.** Un cop obtinguts tots els divisors de grau 2 de  $f(X)$ , si el polinomi que resta és de grau menor o igual que 5, automàticament és irreductible (perquè no té divisors de graus 1 ni 2). En cas contrari, provem la divisibilitat per un polinomi  $g(X) = aX^3 + bX^2 + cX + d$  de coeficients indeterminats, de la mateixa manera que ho hem fet per a grau 2; ara cal usar un mínim de quatre nombres enters diferents  $z_1, z_2, z_3, z_4$  per a obtenir un sistema lineal de matriu

$$\begin{bmatrix} z_1^3 & z_1^2 & z_1 & 1 & \mid & d(z_1) \\ z_2^3 & z_2^2 & z_2 & 1 & \mid & d(z_2) \\ z_3^3 & z_3^2 & z_3 & 1 & \mid & d(z_3) \\ z_4^3 & z_4^2 & z_4 & 1 & \mid & d(z_4) \end{bmatrix},$$

també de Cramer, etcètera.

**1.7.8.** I així successivament, mentre el grau  $n$  del polinomi que resti sigui més gran o igual que  $2k + 1$ , on  $k$  és el grau dels factors irreductibles que volem trobar en aquest pas.

**Exemple 1.7.9.** Intentem factoritzar el polinomi  $f(X) = X^8 - X^4 + 1$ .

Clarament, el polinomi no té factors irreductibles múltiples, perquè no té arrels complexes múltiples. Cerquem les seves arrels enteres. Com que el polinomi és mònic, les arrels de  $f(X)$  només poden ser els divisors del terme independent; és a dir, 1, o  $-1$ ; però  $f(1) = f(-1) = 1 \neq 0$ . Per tant,  $f(X)$  no té divisors de grau 1.

Cerquem divisors de grau 2. Tot divisor de  $f(X)$  en  $\mathbb{Z}[X]$  és associat a un polinomi mònic; per tant, només cal cercar els divisors de grau 2 de la forma  $g(X) = X^2 + bX + c$ . Si prenem per a  $z$  els valors 0, 1, obtenim les relacions de divisibilitat  $c = g(0) \mid f(0) = 1$  i  $1 + b + c = g(1) \mid f(1) = 1$ . Per tant, tenim quatre sistemes de dues equacions lineals:

$$\left. \begin{array}{l} c = 1 \\ 1 + b + c = 1 \end{array} \right\} \quad \left. \begin{array}{l} c = -1 \\ 1 + b + c = 1 \end{array} \right\}$$

$$\left. \begin{array}{l} c = 1 \\ 1 + b + c = -1 \end{array} \right\} \quad \left. \begin{array}{l} c = -1 \\ 1 + b + c = -1 \end{array} \right\}$$

El primer té solució  $(c, b) = (1, -1)$ , el segon,  $(c, b) = (-1, 1)$ , el tercer,  $(c, b) = (1, -3)$ , i el quart,  $(c, b) = (-1, -1)$ . Per tant, els únics polinomis de grau 2 que poden dividir  $f(X)$  són els polinomis  $X^2 - X + 1$ ,  $X^2 + X - 1$ ,  $X^2 - 3X + 1$ ,  $X^2 - X - 1$ . Si provem de fer les divisions, obtenim que cap d'aquests polinomis no divideix  $f(X)$ ; per tant,  $f(X)$  no té divisors de grau 2 de coeficients enters (ni racionals).

Repetim aquest procediment per al polinomi de grau 3 de coeficients indeterminats  $g(X) = X^3 + bX^2 + cX + d$ ; per a  $z = 0, 1, -1$ , obtenim les condicions  $d \in \{1, -1\}$ ,  $1 + b + c + d \in \{1, -1\}$ ,  $-1 + b - c + d \in \{1, -1\}$ , que donen lloc als 8 sistemes de tres equacions

$$\left. \begin{array}{l} d = 1 \\ 1 + b + c + d = 1 \\ -1 + b - c + d = 1 \end{array} \right\} \quad \left. \begin{array}{l} d = -1 \\ 1 + b + c + d = 1 \\ -1 + b - c + d = 1 \end{array} \right\}$$

$$\left. \begin{array}{l} d = 1 \\ 1 + b + c + d = 1 \\ -1 + b - c + d = -1 \end{array} \right\} \quad \left. \begin{array}{l} d = -1 \\ 1 + b + c + d = 1 \\ -1 + b - c + d = -1 \end{array} \right\}$$

$$\left. \begin{array}{l} d = 1 \\ 1 + b + c + d = -1 \\ -1 + b - c + d = 1 \end{array} \right\} \quad \left. \begin{array}{l} d = -1 \\ 1 + b + c + d = -1 \\ -1 + b - c + d = 1 \end{array} \right\}$$

$$\left. \begin{array}{l} d = 1 \\ 1 + b + c + d = -1 \\ -1 + b - c + d = -1 \end{array} \right\} \quad \left. \begin{array}{l} d = -1 \\ 1 + b + c + d = -1 \\ -1 + b - c + d = -1 \end{array} \right\}$$

El càlcul de les solucions d'aquests sistemes dóna com a solucions les ternes de nombres enters  $(b, c, d) \in \{(0, -1, 1), (-1, 0, 1), (-1, -2, 1), (-2, -1, 1), (2, -1, -1), (1, 0, -1), (1, -2, -1), (0, -1, -1)\}$ , de manera que obtenim els 8 possibles polinomis que divideixen  $f(X)$ :  $X^3 - X + 1$ ,  $X^3 - X^2 + 1$ ,  $X^3 - X^2 - 2X + 1$ ,  $X^3 - 2X^2 - X + 1$ ,  $X^3 + 2X^2 - X - 1$ ,  $X^3 + X^2 - 1$ ,  $X^3 + X^2 - 2X - 1$ ,  $X^3 - X - 1$ . Fetes les divisions, trobem que cap d'aquests polinomis no divideix  $f(X)$ , de manera que  $f(X)$  no és divisible per cap polinomi de  $\mathbb{Z}[X]$  de grau 3.

**Observació 1.7.10.** Abans de fer les divisions, podem garbellar aquests polinomis; per exemple, si prenem  $z = 2$ , tenim que  $f(2) = 241$ , mentre que els valors de  $g(2)$  són, respectivament, 7, 5, 1,  $-1$ , 13, 11, 7, i 5; d'aquests, els únics divisors de 241 són 1 i  $-1$ , de manera que els únics polinomis que poden dividir  $f(X)$  són els polinomis  $X^3 - X^2 - 2X + 1$  i  $X^3 - 2X^2 - X + 1$ . Si calculem els valors que prenen aquests dos polinomis en  $z = -2$ , obtenim els valors  $-7$  i  $-13$ , respectivament, que no són divisors de  $f(-2) = 241$ ; per tant, cap dels dos polinomis no és tampoc un divisor de  $f(X)$ . Ens hem estalviat, doncs, totes les divisions per polinomis.

**Exercici 1.7.11.** Es demana completar l'algorisme amb un polinomi de grau 4 de coeficients indeterminats per a deduir que  $f(X)$  és irreductible.

**Observació 1.7.12.** En un capítol posterior veurem que aquest polinomi, al qual donarem el nom de  $\Phi_{24}(X)$ , forma part d'una família infinita de polinomis irreductibles: els polinomis ciclotòmics (cf. 3.2.5 i 3.2.23).

## 1.8 Exercicis

Hom pot estar temptat de pensar que si un polinomi primitiu de  $\mathbb{Z}[X]$  és irreductible, llavors també ho és mòdul  $p$  per a algun nombre primer  $p$ , de manera que una cerca de la irreductibilitat mòdul  $p$  per a suficients nombres primers  $p$  resoldria el problema de la irreductibilitat sobre  $\mathbb{Z}$ . L'exercici següent mostra que això no és així: es poden trobar polinomis mònicos i irreductibles de  $\mathbb{Z}[X]$  tals que, per a tot nombre primer  $p$ , són reductibles en reduir-los mòdul  $p$ .

**Exercici 1.8.1.** (a) El polinomis  $X^4 - 10X^2 + 1$ ,  $X^4 + 1$  són irreductibles en  $\mathbb{Z}[X]$ .

(b) Aquests polinomis factoritzen en  $\mathbb{Z}/p\mathbb{Z}[X]$ , per a tot nombre primer  $p$ .

**Exercici 1.8.2.** (a) Els polinomis  $X^5 - 4X + 2$ ,  $3X^5 - 15$  i  $2X^{10} - 21$  són irreductibles en  $\mathbb{Q}[X]$ . Ho són en  $\mathbb{Z}[X]$ ?

(b) El polinomi  $X^6 + X^3 + 1$  és irreductible en  $\mathbb{Q}[X]$ .

(c) Per a tot nombre natural  $n \geq 1$ , si  $m \neq \pm 1$  és un nombre enter lliure de quadrats, el polinomi  $X^n - m$  és irreductible en  $\mathbb{Q}[X]$  (cf. 1.6.3).

**Exercici 1.8.3.** Quins dels polinomis següents són irreductibles sobre  $\mathbb{Q}$ ? D'aquells que no ho siguin, es demana determinar-ne la factorització com a producte de polinomis irreductibles:

(a)  $X^4 - 2X^3 + 2X^2 + X + 4$ ;

(b)  $X^4 - 5X^3 + 3X - 2$ ;

(c)  $3X^5 - 4X^3 - 6X^2 + 6$ ;

(d)  $5X^5 - 6X^4 - 3X^2 + 9X - 15$ ;

(e)  $X^6 + 12X^5 + 49X^4 + 96X^3 + 99X^2 + 54X + 15$ ;

(f)  $X^5 + X^4 + 2X^3 + 2X^2 + 2X + 3$ .

**Exercici 1.8.4.** Es demana provar que a l'anell de polinomis  $(\mathbb{Z}/2\mathbb{Z})[X]$ , els polinomis

$$X^2 + X + 1, \quad X^3 + X + 1, \quad X^3 + X^2 + 1,$$

són irreductibles, i trobar tots els polinomis irreductibles de grau 4.

**Exercici 1.8.5.** Es demana trobar les arrels de cadascun dels polinomis següents:

(a)  $X^3 + 6X^2 + 11X + 6$ , en  $\mathbb{Z}/12\mathbb{Z}$ ;

(b)  $3X^3 - 4X^2 - X + 4$ , en  $\mathbb{Z}/5\mathbb{Z}$ ;

(c)  $5X^4 + 2X^2 - 3$ , en  $\mathbb{Z}/7\mathbb{Z}$ ;

(d)  $X^3 + X + 1$ , en  $\mathbb{Z}/2\mathbb{Z}$ .

# Capítol 2

## Teorema fonamental de l'Àlgebra

En el capítol introductori hem deixat pendent de demostració el teorema fonamental de l'Àlgebra (cf. **0.2.2**). D'altra banda, en el capítol anterior hem introduït formalment l'anell de polinomis i hem provat que si considerem polinomis de coeficients en un cos, l'anell de polinomis en una quantitat finita d'indeterminades és un domini de factorització única.

A l'anell de polinomis en  $n$  indeterminades hi ha uns polinomis especials, els anomenats polinomis simètrics, la importància dels quals es fa evident al llarg dels capítols següents. De fet, han esdevingut, històricament, una eina fonamental per al càlcul algebraic: fórmules de Viète (cf. **2.2.7**), polinomis simètrics elementals (cf. **2.2.6**), polinomis i fórmules de Newton (cf. **2.6.1**), teorema de Waring (cf. **2.3.1**), o resultant de dos polinomis (cf. **2.6.5**), són conceptes o resultats íntimament relacionats amb els polinomis simètrics. En particular, permeten introduir còmodament el discriminant d'un polinomi qualsevol (cf. **2.4.3**). Dediquem, doncs, aquest capítol al seu estudi i, com a conseqüència, podem proporcionar una demostració senzilla del teorema fonamental de l'Àlgebra (cf. **2.5.1**). O potser és amb aquesta excusa, que fem l'estudi dels polinomis simètrics. En qualsevol cas, els dos temes són prou interessants.

### 2.1 Polinomis simètrics

El fet de treballar amb anells commutatius fa que l'expressió d'un polinomi com a producte dels seus factors lineals  $X - \alpha$ , on  $\alpha$  recorre la successió de les arrels del polinomi comptades cadascuna amb la seva multiplicitat corresponent, no depengui de l'ordre en què considerem aquestes; és a dir, l'expressió és invariant per permutació de les arrels del polinomi. Aquest fet es reflecteix còmodament en el concepte de polinomi simètric, i és l'objecte principal d'atenció d'aquesta secció.

**2.1.1.** Siguin  $B$  un anell commutatiu qualsevol,  $n \geq 1$  un nombre enter,  $B[X_1, \dots, X_n]$  l'anell de polinomis de coeficients en  $B$  en les indeterminades  $X_1, \dots, X_n$ , i  $S_n$  el grup simètric, de les permutacions de  $\{1, 2, \dots, n\}$ . L'acció per l'esquerra del grup  $S_n$  en el conjunt  $\{X_1, \dots, X_n\}$ , definida per l'assignació  $(\sigma, X_i) \mapsto X_{\sigma(i)}$ ,  $1 \leq i \leq n$ , (cf. **A.1.43**), es pot estendre a una nova aplicació  $S_n \times B[X_1, \dots, X_n] \longrightarrow B[X_1, \dots, X_n]$ , definida per l'assignació  $(\sigma, f) \mapsto \sigma f$ , on  $\sigma f(X_1, \dots, X_n) := f(X_{\sigma(1)}, \dots, X_{\sigma(n)})$ , que també és una acció per l'esquerra del grup  $S_n$  en el conjunt  $B[X_1, \dots, X_n]$ , de tots els polinomis en

$\{X_1, \dots, X_n\}$ . Per tant, podem veure-la com un morfisme del grup  $S_n$  en el grup de les bijeccions del conjunt  $B[X_1, \dots, X_n]$  (cf. **A.1.44**).

**Proposició 2.1.2.** *Per a tot  $\sigma \in S_n$ , l'assignació  $f \mapsto \sigma f$  defineix un  $B$ -automorfisme de  $B[X_1, \dots, X_n]$ ; és a dir, un automorfisme que deixa invariant cada element de  $B$ ; o sigui, un automorfisme de  $B$ -àlgebres. El morfisme de grups  $S_n \longrightarrow \text{Aut}_B(B[X_1, \dots, X_n])$  és injectiu; o sigui,  $S_n$  actua fidelment com a grup de  $B$ -automorfismes de  $B[X_1, \dots, X_n]$ .*

DEMOSTRACIÓ: La demostració d'aquest resultat és rutinària. En efecte, donades permutacions  $\sigma, \tau, 1 = \text{id} \in S_n$  i un polinomi  $f(X_1, \dots, X_n) \in B[X_1, \dots, X_n]$ , és clar que

$$\begin{aligned} \tau(\sigma f)(X_1, \dots, X_n) &= \tau f(X_{\sigma(1)}, \dots, X_{\sigma(n)}) \\ &= f(X_{\tau(\sigma(1))}, \dots, X_{\tau(\sigma(n))}) \\ &= \tau \sigma f(X_1, \dots, X_n), \\ 1f(X_1, \dots, X_n) &= f(X_1, \dots, X_n); \end{aligned}$$

doncs, l'assignació  $(\sigma, f) \mapsto \sigma f$  determina una acció per l'esquerra de  $S_n$  en  $B[X_1, \dots, X_n]$ . D'altra banda, per a tot  $\sigma \in S_n$  i tota parella de polinomis  $f, g \in B[X_1, \dots, X_n]$ , és

$$\begin{aligned} \sigma(f + g)(X_1, \dots, X_n) &= (f + g)(X_{\sigma(1)}, \dots, X_{\sigma(n)}) \\ &= f(X_{\sigma(1)}, \dots, X_{\sigma(n)}) + g(X_{\sigma(1)}, \dots, X_{\sigma(n)}) \\ &= \sigma f(X_1, \dots, X_n) + \sigma g(X_1, \dots, X_n) \\ &= (\sigma f + \sigma g)(X_1, \dots, X_n), \\ \sigma(fg)(X_1, \dots, X_n) &= (fg)(X_{\sigma(1)}, \dots, X_{\sigma(n)}) \\ &= f(X_{\sigma(1)}, \dots, X_{\sigma(n)}) g(X_{\sigma(1)}, \dots, X_{\sigma(n)}) \\ &= \sigma f(X_1, \dots, X_n) \sigma g(X_1, \dots, X_n) \\ &= (\sigma f \sigma g)(X_1, \dots, X_n), \end{aligned}$$

de manera que, com que  $\sigma 1 = 1$ , l'aplicació  $B[X_1, \dots, X_n] \longrightarrow B[X_1, \dots, X_n]$  donada per  $f \mapsto \sigma f$  és un morfisme d'anells. A més a més, resulta que, per a tot  $\sigma \in S_n$ , és  $\sigma^{-1}(\sigma f) = f$ , de manera que l'aplicació  $f \mapsto \sigma f$  és un automorfisme de  $B[X_1, \dots, X_n]$ , amb invers  $f \mapsto \sigma^{-1}f$ . I és clar que els polinomis constants són invariants per a qualsevol permutació de les indeterminades; és a dir, que es tracta de  $B$ -automorfismes. A més a més, si una permutació  $\sigma$  actua com la identitat en  $B[X_1, \dots, X_n]$ , resulta que  $X_{\sigma(i)} = X_i$ , per a tot índex  $i$ ; o sigui, que  $\sigma$  és la identitat, i el morfisme de grups  $S_n \longrightarrow \text{Aut}_B(B[X_1, \dots, X_n])$  és injectiu.  $\square$

**Definició 2.1.3.** Escrivim  $B[X_1, \dots, X_n]^{S_n}$  per a indicar el subconjunt format per tots els polinomis fixos per l'acció de  $S_n$ ; és a dir,

$$B[X_1, \dots, X_n]^{S_n} = \{f \in B[X_1, \dots, X_n] : \text{per a tot } \sigma \in S_n, \sigma f = f\}.$$

Es té que  $B[X_1, \dots, X_n]^{S_n}$  és un subanell de  $B[X_1, \dots, X_n]$ , i que conté  $B$  com a subanell. Els polinomis  $f(X_1, \dots, X_n) \in B[X_1, \dots, X_n]^{S_n}$  s'anomenen els *polinomis simètrics* en  $X_1, \dots, X_n$  (i coeficients en  $B$ ).

**2.1.4.** En particular, per a tot  $\sigma \in S_n$ , l'assignació  $f \mapsto \sigma f$  és un  $B[X_1, \dots, X_n]^{S_n}$ -automorfisme de  $B[X_1, \dots, X_n]$ ; doncs, l'acció es pot veure com un morfisme injectiu de grups de  $S_n$  en  $\text{Aut}_{B[X_1, \dots, X_n]^{S_n}}(B[X_1, \dots, X_n])$ . Per tant,  $S_n$  actua fidelment com a grup de  $B[X_1, \dots, X_n]^{S_n}$ -automorfismes de  $B[X_1, \dots, X_n]$ .



**Exemple 2.1.5.** Els polinomis  $X_1 + \dots + X_n$ ,  $X_1 \cdots X_n$ , suma i producte, respectivament, de les indeterminades, són simètrics. En canvi, els polinomis

$$X_1X_2 + X_3X_4, \quad X_1X_3 + X_2X_4, \quad X_1X_4 + X_2X_3 \in \mathbb{Z}[X_1, X_2, X_3, X_4],$$

no són simètrics; per exemple, el primer no és invariant per la transposició (1, 3), i el segon i el tercer no ho són per la transposició (1, 2). Però la seva suma,

$$V_4(X_1, X_2, X_3, X_4) := X_1X_2 + X_1X_3 + X_1X_4 + X_2X_3 + X_2X_4 + X_3X_4$$

és invariant per a les transposicions (1, 2), (1, 3) i (1, 4); com que aquestes transposicions generen  $S_4$ , el polinomi és invariant per tot  $S_4$ ; es tracta, doncs, d'un polinomi simètric de  $\mathbb{Z}[X_1, X_2, X_3, X_4]$ . Notem que no és invariant com a polinomi de  $\mathbb{Z}[X_1, \dots, X_n]$ , per a  $n \geq 5$ .

## 2.2 Fórmules de Viète

**Proposició 2.2.1.** *Sigui  $A$  un anell commutatiu, i considerem  $B := A[Y_1, \dots, Y_m]$  l'anell de polinomis de coeficients en  $A$  i indeterminades  $Y_1, \dots, Y_m$ . Llavors,*

$$A[Y_1, \dots, Y_m][X_1, \dots, X_n]^{S_n} = A[X_1, \dots, X_n]^{S_n}[Y_1, \dots, Y_m].$$

**Observació 2.2.2.** És a dir, els polinomis simètrics en  $X_1, \dots, X_n$  i coeficients polinomis en  $Y_1, \dots, Y_m$  són els polinomis en  $Y_1, \dots, Y_m$  i coeficients polinomis simètrics en  $X_1, \dots, X_n$ .

DEMOSTRACIÓ: Per inducció sobre  $m$ , és clar que és suficient provar el cas  $m = 1$ , ja que si

$$A[Y_1, \dots, Y_i][X_1, \dots, X_n]^{S_n} = A[X_1, \dots, X_n]^{S_n}[Y_1, \dots, Y_i]$$

i el resultat per a  $m = 1$  (i qualsevol anell de coeficients) és cert, llavors

$$\begin{aligned} A[Y_1, \dots, Y_i, Y_{i+1}][X_1, \dots, X_n]^{S_n} &= A[Y_1, \dots, Y_i][Y_{i+1}][X_1, \dots, X_n]^{S_n} \\ &= A[Y_1, \dots, Y_i][X_1, \dots, X_n]^{S_n}[Y_{i+1}] \\ &= A[X_1, \dots, X_n]^{S_n}[Y_1, \dots, Y_i][Y_{i+1}] \\ &= A[X_1, \dots, X_n]^{S_n}[Y_1, \dots, Y_{i+1}]. \end{aligned}$$

Ara, notem que

$$A[Y][X_1, \dots, X_n]^{S_n} \subseteq A[Y][X_1, \dots, X_n] = A[X_1, \dots, X_n][Y]$$

i que

$$A[X_1, \dots, X_n]^{S_n}[Y] \subseteq A[X_1, \dots, X_n][Y];$$

és a dir, que estem tractant amb subanells de  $A[X_1, \dots, X_n][Y]$ . Considerem, doncs, un polinomi qualsevol  $f(X_1, \dots, X_n, Y) \in A[X_1, \dots, X_n][Y]$ , que podem escriure de manera única en la forma

$$f(X_1, \dots, X_n, Y) = \sum_{i=0}^r a_i(X_1, \dots, X_n)Y^i, \quad a_i(X_1, \dots, X_n) \in A[X_1, \dots, X_n].$$

En fer actuar una permutació  $\sigma \in S_n$ , tenim que

$$\begin{aligned}\sigma f(X_1, \dots, X_n, Y) &= f(X_{\sigma(1)}, \dots, X_{\sigma(n)}, Y) \\ &= \sum_{i=0}^r a_i(X_{\sigma(1)}, \dots, X_{\sigma(n)}) Y^i \\ &= \sum_{i=0}^r \sigma a_i(X_1, \dots, X_n) Y^i;\end{aligned}$$

per tant,  $\sigma f = f$  si, i només si,  $\sigma a_i = a_i$ , per a  $0 \leq i \leq r$ . Així,  $f \in A[Y][X_1, \dots, X_n]^{S_n}$  si, i només si,  $a_i \in A[X_1, \dots, X_n]^{S_n}$ , per a  $0 \leq i \leq r$ ; o sigui, equivalentment, si, i només si,  $f \in A[X_1, \dots, X_n]^{S_n}[Y]$ , com calia provar.  $\square$

**Proposició 2.2.3.** *Siguin  $a, T, X_1, \dots, X_n$  indeterminades sobre un anell commutatiu qualsevol,  $A$ . Llavors,*

$$f(X_1, \dots, X_n)(T) := a(T - X_1) \cdots (T - X_n) \in A[a][X_1, \dots, X_n]^{S_n}[T].$$

DEMOSTRACIÓ: Això correspon al cas  $m = 1$  de la proposició anterior, sobre l'anell  $A[a]$ ; tenim que  $A[a][X_1, \dots, X_n]^{S_n}[T] = A[a, T][X_1, \dots, X_n]^{S_n}$ . Ara es tracta de veure que el polinomi

$$f(X_1, \dots, X_n)(T) := a(T - X_1) \cdots (T - X_n)$$

hi pertany. Però aquest fet és evident per causa de la commutativitat de l'anell de polinomis; per a tota permutació  $\sigma \in S_n$ , és

$$a(T - X_{\sigma(1)}) \cdots (T - X_{\sigma(n)}) = a(T - X_1) \cdots (T - X_n). \square$$

**Definició 2.2.4** (Polinomi general de grau  $n$  sobre  $A$ ). Sigui  $A$  un anell commutatiu qualsevol. S'anomena *polinomi general* de grau  $n$  sobre  $A$  el polinomi

$$a(T - X_1) \cdots (T - X_n) \in A[a][X_1, \dots, X_n]^{S_n}[T].$$

**Observació 2.2.5.** Notem que el polinomi general de grau  $n$  sobre  $A$  no és “qualsevol polinomi” sobre  $A$  ni “un polinomi qualsevol” de coeficients en  $A$ , sinó un polinomi molt concret, i no és de coeficients en  $A$ , sinó en  $A[a][X_1, \dots, X_n]^{S_n}$ . Encara més, si  $Z \subseteq A$  és l'anell primer de  $A$  (el subanell generat per 1), llavors

$$a(T - X_1) \cdots (T - X_n) \in Z[a][X_1, \dots, X_n]^{S_n}[T].$$

**Definició 2.2.6.** Sigui  $Z$  un anell primer; és a dir,  $Z = \mathbb{Z}$ , o bé  $Z = \mathbb{Z}/m\mathbb{Z}$ , per a algun nombre enter  $m \geq 2$ . Els polinomis

$$\begin{aligned}s_0(X_1, \dots, X_n) &= 1, \\ s_1(X_1, \dots, X_n) &= X_1 + \cdots + X_n, \\ s_2(X_1, \dots, X_n) &= \sum_{1 \leq i < j \leq n} X_i X_j, \\ s_3(X_1, \dots, X_n) &= \sum_{1 \leq i_1 < i_2 < i_3 \leq n} X_{i_1} X_{i_2} X_{i_3}, \\ &\dots \\ s_{n-1}(X_1, \dots, X_n) &= \sum_{1 \leq i_1 < \dots < i_{n-1} \leq n} X_{i_1} \cdots X_{i_{n-1}}, \\ s_n(X_1, \dots, X_n) &= X_1 \cdots X_n,\end{aligned}$$

de l'anell  $Z[X_1, \dots, X_n]$ , són simètrics; és a dir, pertanyen a  $Z[X_1, \dots, X_n]^{S_n}$ ; s'anomenen els *polinomis simètrics elementals* en  $X_1, \dots, X_n$ .

**Proposició 2.2.7** (Fórmules de Viète). *Siguin  $A$  un anell commutatiu, considerem indeterminades  $a, T, X_1, \dots, X_n$ , sobre  $A$ , i posem  $b_0, \dots, b_n$  per als coeficients del polinomi general de grau  $n$  sobre  $A$ ; és a dir, escrivim-lo en la forma*

$$a(T - X_1) \cdots (T - X_n) =: \sum_{k=0}^n b_k T^k \in A[a][X_1, \dots, X_n]^{S_n}[T],$$

$b_k \in A[a][X_1, \dots, X_n]^{S_n}$ , per a  $0 \leq k \leq n$ . Llavors, si  $s_k(X_1, \dots, X_n)$ ,  $0 \leq k \leq n$ , denoten els polinomis simètrics elementals en  $X_1, \dots, X_n$ , resulta que

$$b_k = (-1)^{n-k} a s_{n-k}(X_1, \dots, X_n).$$

DEMOSTRACIÓ: En desenvolupar el producte  $a(T - X_1) \cdots (T - X_n)$ , resulta que el coeficient de  $T^k$  és el producte del factor  $(-1)^{n-k} a$  per la suma per a tots els subconjunts  $C_k \subseteq \{X_1, \dots, X_n\}$  de cardinal  $n - k$ , del producte dels elements del subconjunt. I això és exactament l'expressió proposada.  $\square$

## 2.3 Teorema de Waring

**Teorema 2.3.1.** *Sigui  $B$  un anell commutatiu i considerem l'anell de polinomis en  $n$  indeterminades  $X_1, \dots, X_n$ . Es té que*

$$B[X_1, \dots, X_n]^{S_n} = B[s_1(X_1, \dots, X_n), \dots, s_n(X_1, \dots, X_n)].$$

Més concretament:

(a) *Per a tot polinomi  $P(Y_1, \dots, Y_n) \in B[Y_1, \dots, Y_n]$ , és*

$$P(s_1(X_1, \dots, X_n), \dots, s_n(X_1, \dots, X_n)) \in B[X_1, \dots, X_n]^{S_n}.$$

(b) *Per a tot polinomi simètric  $f(X_1, \dots, X_n) \in B[X_1, \dots, X_n]^{S_n}$ , existeix un polinomi  $P(Y_1, \dots, Y_n) \in B[Y_1, \dots, Y_n]$  tal que*

$$f(X_1, \dots, X_n) = P(s_1(X_1, \dots, X_n), \dots, s_n(X_1, \dots, X_n)).$$

(c) *Si el grau total del polinomi simètric  $f(X_1, \dots, X_n)$  és  $m \leq n$ , es pot prendre el polinomi  $P(Y_1, \dots, Y_m) \in B[Y_1, \dots, Y_m]$ , de manera que*

$$f(X_1, \dots, X_n) = P(s_1(X_1, \dots, X_n), \dots, s_m(X_1, \dots, X_n)).$$

DEMOSTRACIÓ (Mètode de Waring): Ordenem el conjunt dels monomis  $aX_1^{r_1} \cdots X_n^{r_n}$ , amb  $r_1, \dots, r_n \geq 0$ ,  $a \in B$ , de la manera següent. Donats exponents  $r_1, \dots, r_n \geq 0$ , i també  $k_1, \dots, k_n \geq 0$ , direm que el monomi  $aX_1^{r_1} \cdots X_n^{r_n}$ ,  $a \neq 0$ , és més petit que (o, si es vol, anterior a) el monomi  $bX_1^{k_1} \cdots X_n^{k_n}$ ,  $b \neq 0$ , si  $r_1 + \cdots + r_n < k_1 + \cdots + k_n$  o bé, en el cas que sigui  $r_1 + \cdots + r_n = k_1 + \cdots + k_n$ , quan per al primer índex  $i$  tal que  $r_i \neq k_i$  sigui  $r_i < k_i$ . És immediat comprovar que es tracta d'un ordre total en el conjunt dels monomis  $X_1^{r_1} \cdots X_n^{r_n}$ ; i que, per causa de la condició  $r_1 + \cdots + r_n < k_1 + \cdots + k_n$ , donat un monomi qualsevol, només hi ha una quantitat finita de monomis mòncics més petits.

Ara, donat un polinomi simètric no nul qualsevol,  $f(X_1, \dots, X_n)$ , considerem-ne el monomi no nul  $aX_1^{r_1} \cdots X_n^{r_n}$ ,  $a \in B$ ,  $a \neq 0$ , més gran entre tots els monomis no nuls de  $f(X_1, \dots, X_n)$ . En particular, el fet que  $f(X_1, \dots, X_n)$  sigui simètric implica que  $r_1 \geq r_2 \geq \cdots \geq r_n \geq 0$ . D'aquestes desigualtats es dedueixen de manera senzilla les relacions  $e_1 := r_1 - r_2 \geq 0$ ,  $e_2 := r_2 - r_3 \geq 0$ ,  $\dots$ ,  $e_{n-1} := r_{n-1} - r_n \geq 0$ ,  $e_n := r_n \geq 0$ , i podem considerar el polinomi, òbviament simètric,

$$g(X_1, \dots, X_n) := f(X_1, \dots, X_n) - a s_1(X_1, \dots, X_n)^{e_1} \cdots s_n(X_1, \dots, X_n)^{e_n}.$$

Com que el monomi no nul més gran d'un producte de polinomis mòncics s'obté en multiplicar els monomis no nuls més grans dels factors, resulta que el monomi no nul més gran de

$$s_1(X_1, \dots, X_n)^{e_1} \cdots s_n(X_1, \dots, X_n)^{e_n}$$

és exactament

$$X_1^{e_1} (X_1 X_2)^{e_2} \cdots (X_1 \cdots X_n)^{e_n} = X_1^{r_1} \cdots X_n^{r_n};$$

en conseqüència, el monomi no nul més gran de  $g(X_1, \dots, X_n)$  és estrictament menor que el monomi no nul més gran de  $f(X_1, \dots, X_n)$ . I podem acabar la demostració per inducció sobre l'ordre del monomi no nul més gran: per hipòtesi d'inducció, podem suposar que

$$g(X_1, \dots, X_n) \in B[s_1(X_1, \dots, X_n), \dots, s_n(X_1, \dots, X_n)];$$

i llavors,

$$f(X_1, \dots, X_n) \in B[s_1(X_1, \dots, X_n), \dots, s_n(X_1, \dots, X_n)].$$

Finalment, com que el grau total de polinomi  $s_m(X_1, \dots, X_n)$  és exactament  $m$ , si un polinomi simètric  $f(X_1, \dots, X_n)$  és de grau total  $m < n$ , en la seva expressió com a polinomi en  $s_1(X_1, \dots, X_n), \dots, s_n(X_1, \dots, X_n)$ , no pot aparèixer cap dels polinomis  $s_{m+1}(X_1, \dots, X_n), \dots, s_n(X_1, \dots, X_n)$ . Això acaba la prova.  $\square$

**Observació 2.3.2.** Encara més, si el grau màxim amb què apareix  $X_1$  en algun dels monomis no nuls de  $f(X_1, \dots, X_n)$  és  $m$ , llavors en l'expressió de  $f(X_1, \dots, X_n)$  com a polinomi en  $s_1(X_1, \dots, X_n), \dots, s_n(X_1, \dots, X_n)$  no pot aparèixer cap dels polinomis  $s_{m+1}(X_1, \dots, X_n), \dots, s_n(X_1, \dots, X_n)$ , ja que aquests tenen el grau de  $X_1$  més gran que  $m$ . I tampoc no pot aparèixer cap producte que contingui estrictament més de  $m$  d'entre els polinomis  $s_1(X_1, \dots, X_n), \dots, s_n(X_1, \dots, X_n)$ , perquè el grau en  $X_1$  seria més gran que  $m$ .

Acabarem la secció amb un resultat que no hauria de ser sorprenent, tot i que a primer cop d'ull ho pugui semblar.

**Teorema 2.3.3.** *Siguin  $B$  un anell commutatiu qualsevol i considerem indeterminades  $X_1, \dots, X_n, Y_1, \dots, Y_n$ , sobre  $B$ . Llavors, l'únic morfisme d'anells*

$$\varphi_n : B[Y_1, \dots, Y_n] \longrightarrow B[s_1(X_1, \dots, X_n), \dots, s_n(X_1, \dots, X_n)]$$

*tal que per a  $a \in B$  és  $\varphi_n(a) = a$ , i  $\varphi_n(Y_i) = s_i(X_1, \dots, X_n)$ , per a  $1 \leq i \leq n$ , és un isomorfisme.*

DEMOSTRACIÓ: Clarament, el morfisme d'anells  $\varphi_n$  és exhaustiu, perquè els generadors sobre  $B$ ,  $s_i(X_1, \dots, X_n)$ ,  $1 \leq i \leq n$ , pertanyen a la imatge de  $\varphi_n$ . Procedirem per inducció sobre  $n$  a partir del cas, immediat,  $n = 1$ . Suposem, doncs, que  $n \geq 2$  i que hem provat el resultat per a tots els anells de polinomis de menys de  $n$  indeterminades. Volem veure que el nucli de  $\varphi_n$  és trivial; és a dir, que si per a un polinomi  $f(Y_1, \dots, Y_n) \in B[Y_1, \dots, Y_n]$  és

$$f(s_1(X_1, \dots, X_n), \dots, s_n(X_1, \dots, X_n)) = 0,$$

llavors és  $f(Y_1, \dots, Y_n) = 0$ .

Podem escriure  $f(Y_1, \dots, Y_n)$  de manera única en la forma

$$f(Y_1, \dots, Y_n) = \sum_{k=0}^d a_k(Y_1, \dots, Y_{n-1}) Y_n^k,$$

per a certs polinomis  $a_k(Y_1, \dots, Y_{n-1}) \in B[Y_1, \dots, Y_{n-1}]$ ,  $0 \leq k \leq d$ . En substituir  $X_n$  per 0 (és a dir, en compondre amb el morfisme d'anells

$$B[X_1, \dots, X_n] \longrightarrow B[X_1, \dots, X_{n-1}]$$

determinat unívocament per  $X_i \mapsto X_i$ , si  $1 \leq i \leq n-1$ ,  $X_n \mapsto 0$ , i  $a \mapsto a$ , per a tot  $a \in B$ ), obtenim que

$$f(s_1(X_1, \dots, X_{n-1}, 0), \dots, s_n(X_1, \dots, X_{n-1}, 0)) = 0;$$

o sigui, que la suma

$$\sum_{k=0}^d a_k(s_1(X_1, \dots, X_{n-1}, 0), \dots, s_{n-1}(X_1, \dots, X_{n-1}, 0)) s_n(X_1, \dots, X_{n-1}, 0)^k$$

és nul·la. Ara bé, com que  $s_n(X_1, \dots, X_{n-1}, 0) = 0$ , resulta que per a tot valor de  $k > 0$  és  $s_n(X_1, \dots, X_{n-1}, 0)^k = 0$ ; per tant, obtenim que

$$a_0(s_1(X_1, \dots, X_{n-1}, 0), \dots, s_{n-1}(X_1, \dots, X_{n-1}, 0)) = 0.$$

Però (per exemple, a partir de les fórmules de Viète), és clar que

$$s_j(X_1, \dots, X_{n-1}, 0) = s_j(X_1, \dots, X_{n-1}), \quad 1 \leq j \leq n-1.$$

(Notem que els polinomis  $s_j$  de l'esquerra són els polinomis simètrics en  $n$  indeterminades, mentre que els de la dreta són els polinomis simètrics en  $n-1$  indeterminades.) Ara podem aplicar la hipòtesi d'inducció: tenim que la imatge del polinomi  $a_0(Y_1, \dots, Y_{n-1})$  pel morfisme  $\varphi_{n-1}$  és zero; o sigui, que  $a_0(Y_1, \dots, Y_{n-1}) = 0$ , perquè  $\varphi_{n-1}$  és injectiu, per hipòtesi d'inducció.

Si portem aquest fet a l'expressió de  $f(Y_1, \dots, Y_n)$ , obtenim que el coeficient del terme constant (en  $Y_n$ ) és nul; o sigui, que el polinomi  $f(Y_1, \dots, Y_n)$  és múltiple de  $Y_n$ , si  $d \geq 1$ , o directament zero, si  $d = 0$ ; i en aquest darrer cas ja hem acabat. Així, existeix un polinomi  $f_1(Y_1, \dots, Y_n) \in B[Y_1, \dots, Y_n]$  tal que  $f(Y_1, \dots, Y_n) = Y_n f_1(Y_1, \dots, Y_n)$ . Ara, el polinomi  $f_1(Y_1, \dots, Y_n)$  és de grau (en  $Y_n$ ) menor estricta que el grau (en  $Y_n$ ) de  $f(Y_1, \dots, Y_n)$ , i també és  $f_1(Y_1, \dots, Y_n) \in \ker(\varphi_n)$ ; o sigui, admet una expressió com la de  $f(Y_1, \dots, Y_n)$ , on  $d$  es pot canviar per  $d-1$ . Si repetim l'argument  $d$  vegades, obtenim que  $f(Y_1, \dots, Y_n) = 0$ , perquè  $f(Y_1, \dots, Y_n) = Y_n^d f_d(Y_1, \dots, Y_{n-1})$ , amb  $f_d(Y_1, \dots, Y_{n-1}) \in \ker(\varphi_{n-1}) = \{0\}$ .  $\square$

## 2.4 Discriminant d'un polinomi

Donat un polinomi quadràtic,  $aX^2 + bX + c$ , acostumem a anomenar discriminant del polinomi l'element  $b^2 - 4ac$ . El concepte de discriminant va més enllà dels polinomis quadràtics. Es tracta de fer-ne l'estudi.

**Proposició 2.4.1.** *Siguin  $a, X_1, \dots, X_n$  indeterminades sobre  $\mathbb{Z}$ . Considerem el polinomi general de grau  $n$ ,*

$$f(T) = \sum_{k=0}^n a_k T^k := a(T - X_1) \cdots (T - X_n),$$

de coeficients  $a_k = (-1)^{n-k} a_{n-k}(X_1, \dots, X_n)$ , donats per les fórmules de Viète (cf. 2.2.7) a partir dels polinomis simètrics elementals en  $X_1, \dots, X_n$ . I considerem el polinomi

$$\Delta_0(X_1, \dots, X_n) = \prod_{i < j} (X_i - X_j) \in \mathbb{Z}[X_1, \dots, X_n].$$

Llavors, per a tota permutació  $\sigma \in S_n$  se satisfà que

$$\Delta_0(X_{\sigma(1)}, \dots, X_{\sigma(n)}) = \text{sig}(\sigma) \Delta_0(X_1, \dots, X_n),$$

on  $\text{sig}(\sigma)$  és el signe de la permutació.

**DEMOSTRACIÓ:** Com que tota permutació és producte de transposicions, és suficient provar que si  $\sigma$  és una transposició, llavors  $\Delta_0(X_{\sigma(1)}, \dots, X_{\sigma(n)}) = -\Delta_0(X_1, \dots, X_n)$ .

Sigui, doncs,  $\sigma = (r, s)$  una transposició, amb  $1 \leq r < s \leq n$ . En aplicar la transposició als factors  $X_i - X_j$  del producte tals que  $\{i, j\} \cap \{r, s\} = \emptyset$ , el factor transformat és idèntic al de partida; per tant, només cal preocupar-se de què succeeix amb els factors que contenen  $X_r$  o  $X_s$ . Aquests factors són exactament els  $X_i - X_r$  i  $X_i - X_s$ , per a  $1 \leq i \leq r-1$ , que es transformen entre si bijectivament; els factors  $X_r - X_j$  i  $X_j - X_s$ , per a  $r < j < s$ , que es transformen els uns en els altres amb un canvi de signe per a cadascun  $i$ , en conseqüència, es produeix una quantitat parella de canvis de signe; el factor  $X_r - X_s$ , que es transforma en el factor  $X_s - X_r$ , de manera que es produeix un canvi de signe; i els factors  $X_r - X_j$  i  $X_s - X_j$ , per a  $j > s$ , que també es transformen bijectivament entre ells. Per tant, l'aplicació de la transposició produeix un canvi de signe en el producte, com calia veure.  $\square$

**Observació 2.4.2.** Per tant,  $\Delta_0(X_{\sigma(1)}, \dots, X_{\sigma(n)})$  no és pas un polinomi simètric, si  $n > 1$ . Però, en canvi,  $a^{2n-2} \Delta_0(X_1, \dots, X_n)^2 \in \mathbb{Z}[X_1, \dots, X_n]^{S_n}$ ; és a dir, el polinomi

$$\Delta(f) := \Delta(a_0, \dots, a_n) := a^{2n-2} \Delta_0(X_1, \dots, X_n)^2 \in \mathbb{Z}[a_0, \dots, a_n],$$

és un polinomi simètric en  $X_1, \dots, X_n$ .

**Definició 2.4.3.** El polinomi

$$\Delta(f) = \Delta(a_0, \dots, a_n) := a^{2n-2} \Delta_0(X_1, \dots, X_n)^2 \in \mathbb{Z}[a_0, \dots, a_n]$$

s'anomena el *discriminant* del polinomi general de grau  $n$ .

**Corollari 2.4.4.** *Amb les notacions anteriors, se satisfà la igualtat*

$$\Delta(f) = a_n^{2n-2} \prod_{i < j} (X_i - X_j)^2 = (-1)^{n(n-1)/2} a_n^{2n-2} \prod_{i \neq j} (X_i - X_j). \square$$

**Definició 2.4.5.** Siguin  $A$  un domini d'integritat,  $K$  el seu cos de fraccions, i considerem un polinomi qualsevol,  $g(X) = b_0 + b_1X + \dots + b_{n-1}X^{n-1} + b_nX^n \in A[X]$ , de grau  $n$ , i coeficients  $b_0, b_1, \dots, b_{n-1}, b_n \in A$ ,  $b_n \neq 0$ . S'anomena *discriminant* del polinomi  $g(X) \in A[X]$  la imatge de  $\Delta(a_0, \dots, a_n)$  en  $A$  per l'únic morfisme d'anells que aplica  $a_i$  en  $b_i$ . És, doncs, un element de  $A$ .

**Corollari 2.4.6.** *El discriminant d'un polinomi  $g(X) \in A[X]$  s'anul·la si, i només si, el polinomi té alguna arrel múltiple.*  $\square$

## 2.5 Prova del teorema fonamental de l'Àlgebra

Recordem l'enunciat que es tracta de provar.

**Teorema 2.5.1.** *El cos  $\mathbb{C}$  dels nombres complexos és algebraicament tancat; és a dir, tot polinomi no constant  $f(X) \in \mathbb{C}[X]$  té alguna arrel en  $\mathbb{C}$ .*

Farem la demostració per passos. El primer pas consisteix a reduir la prova al cas de polinomis de coeficients reals.

**Lema 2.5.2.** *Si tot polinomi no constant de coeficients reals té una arrel en  $\mathbb{C}$ , llavors tot polinomi de coeficients complexos té una arrel en  $\mathbb{C}$ .*

**DEMOSTRACIÓ:** Suposem que  $f(X) \in \mathbb{C}[X]$  és un polinomi no constant; cal veure que  $f(X)$  té una arrel en  $\mathbb{C}$ . Considerem  $\bar{f}(X)$ , el polinomi que s'obté de  $f(X)$  en aplicar als seus coeficients la conjugació complexa; i sigui  $g(X) := f(X)\bar{f}(X)$ . El polinomi  $g(X) \in \mathbb{R}[X]$  és un polinomi de coeficients reals; per hipòtesi, existeix  $\alpha \in \mathbb{C}$  arrel de  $g(X)$ ; és a dir, existeix  $\alpha \in \mathbb{C}$  tal que  $g(\alpha) = 0$ . Ara bé, se satisfà la igualtat  $f(\alpha)\bar{f}(\alpha) = g(\alpha) = 0$ , de manera que  $f(\alpha) = 0$ , o bé  $\bar{f}(\alpha) = 0$ ; en el primer cas, el polinomi  $f(X)$  té una arrel complexa i hem acabat la prova; en el segon, obtenim que  $\bar{f}(\alpha) = 0$ ; per tant,  $f(\bar{\alpha}) = \overline{\bar{f}(\alpha)} = 0$ , de manera que  $\bar{\alpha} \in \mathbb{C}$  és una arrel de  $f(X)$ . Això acaba la prova.  $\square$

El segon pas de la prova consisteix a veure que tot polinomi de coeficients reals i grau senar té una arrel real; però això és un fet conegut dels cursos d'anàlisi, on aquest fet és una conseqüència directa del teorema de Bolzano.

A continuació, podem veure que tot polinomi de grau 2 i coeficients complexos té una arrel en  $\mathbb{C}$ .

**Lema 2.5.3.** *Siguin  $b, c \in \mathbb{R}$ , i  $f(X) := X^2 + bX + c \in \mathbb{R}[X]$ . El polinomi  $f(X)$  admet una arrel en  $\mathbb{C}$ .*

**DEMOSTRACIÓ:** Com que  $\mathbb{R}$  és de característica zero, les arrels de  $f(X)$  s'expressen en la forma  $\frac{-b + \alpha}{2}, \frac{-b - \alpha}{2}$ , on  $\alpha^2 = b^2 - 4c$ . Si  $b^2 - 4c \geq 0$ , existeix  $\alpha \in \mathbb{R}$  tal que  $\alpha^2 = b^2 - 4c$ , de manera que les dues arrels de  $f(X)$  pertanyen a  $\mathbb{R}$  (una nova aplicació dels resultats

dels cursos d'anàlisi). Si, en canvi,  $b^2 - 4c < 0$ , i si  $i \in \mathbb{C}$  és tal que  $i^2 = -1$ , existeix  $\beta \in \mathbb{R}$  tal que  $(i\beta)^2 = b^2 - 4c$ , i  $\alpha := i\beta \in \mathbb{C}$ ; per tant,  $f(X)$  té les seves arrels en  $\mathbb{C}$ , com volíem veure.  $\square$

**Lema 2.5.4.** *Siguin  $b, c \in \mathbb{C}$ , i  $f(X) := X^2 + bX + c \in \mathbb{C}[X]$ . El polinomi  $f(X)$  admet una arrel en  $\mathbb{C}$ .*

DEMOSTRACIÓ: Clarament, és suficient veure que tot nombre complex admet una arrel quadrada complexa. Però, si  $A, B \in \mathbb{R}$ , llavors  $A^2 + B^2 \geq 0$ , de manera que existeix  $\sqrt{A^2 + B^2} \in \mathbb{R}$  tal que  $\sqrt{A^2 + B^2} \mp A \geq 0$ ; per tant, existeixen  $x := \sqrt{\frac{\sqrt{A^2 + B^2} + A}{2}}$ ,  
 $y := \text{sig}(B)\sqrt{\frac{\sqrt{A^2 + B^2} - A}{2}} \in \mathbb{R}$ , on  $\text{sig}(B) = 1$  si  $B \geq 0$ , i  $\text{sig}(B) = -1$  si  $B < 0$ ; i és immediat comprovar que  $(x + iy)^2 = A + iB$ ; és a dir, tot nombre complex  $A + iB$ ,  $A, B \in \mathbb{R}$ , admet alguna arrel quadrada  $x + iy \in \mathbb{C}$ .  $\square$

Finalment, procedim a fer una demostració del teorema fonamental de l'Àlgebra en la formulació següent.

**Teorema 2.5.5.** *Sigui  $f(X) \in \mathbb{R}[X]$  un polinomi mònic i no constant de coeficients reals. Llavors, existeix  $\alpha \in \mathbb{C}$  tal que  $f(\alpha) = 0$ .*

DEMOSTRACIÓ: Posem  $n = 2^v n'$ , amb  $2 \nmid n'$ , el grau del polinomi  $f(X)$ . Treballem per inducció sobre  $v$ . Si  $v = 0$ , el polinomi  $f(X)$  és de grau senar i, en conseqüència, té una arrel real; per tant, té una arrel en  $\mathbb{C}$ . Suposem, doncs, que  $v \geq 1$ , i que el teorema se satisfà per a tots els polinomis de coeficients reals de grau no divisible per  $2^v$ .

Siguin  $\theta_1, \dots, \theta_n$  les arrels del polinomi  $f(X)$  en un cert cos  $K$ , que podem suposar que conté  $\mathbb{C}$  (cf. **B.0.28** o bé **3.4.12**). Per a cada nombre real  $r$ , i cada parella d'índexs diferents  $i, j$ ,  $i < j$ , considerem l'element  $\alpha_{i,j}(r) := \theta_i \theta_j + r(\theta_i + \theta_j) \in K$ ; amb aquests elements, formem el polinomi  $f_r(X) := \prod_{i < j} (X - \alpha_{i,j}(r)) \in K[X]$ . La quantitat de factors

lineals que conté aquest polinomi és el nombre de subconjunts de 2 elements d'entre els  $1, 2, \dots, n$ ; per tant, el grau del polinomi  $f_r(X)$  és  $\binom{n}{2} = \frac{n(n-1)}{2} = 2^{v-1} n'(n-1)$ ; com

que  $v \geq 1$ ,  $n'(n-1)$  és un nombre senar, de manera que  $2^v$  no divideix el grau del polinomi  $f_r(X)$ ; així, aquest polinomi satisfà la hipòtesi d'inducció que fa referència al grau. Si veiem que  $f_r(X)$  és de coeficients reals, obtenim que  $f_r(X)$  satisfà les hipòtesis d'inducció, per a tot nombre real  $r$ ; en aquest cas, tenim que per a tot  $r \in \mathbb{R}$ , existeix una parella d'índexs diferents  $i, j$  tals que  $\alpha_{i,j}(r) \in \mathbb{C}$ . Ara bé, com que el conjunt de parelles  $(i, j)$  és finit, i  $\mathbb{R}$  és infinit, resulta que existeixen dos índexs diferents  $i, j$  i dos nombres reals diferents  $r, r'$ , tals que  $\alpha_{i,j}(r), \alpha_{i,j}(r') \in \mathbb{C}$ . En particular,  $\theta_i + \theta_j = \frac{\alpha_{i,j}(r) - \alpha_{i,j}(r')}{r - r'} \in \mathbb{C}$ ,

i  $\theta_i \theta_j = \frac{r' \alpha_{i,j}(r) - r \alpha_{i,j}(r')}{r - r'} \in \mathbb{C}$ , de manera que  $\theta_i, \theta_j$  són les dues arrels d'un polinomi de grau 2 i de coeficients complexos; en virtut del lema anterior,  $\theta_i, \theta_j \in \mathbb{C}$ ; i això acaba la demostració.

Per tant, només cal veure que  $f_r(X)$  és de coeficients reals. Però això és senzill. En efecte, els coeficients del polinomi  $f_r(X)$  són els polinomis simètrics elementals en les expressions  $\alpha_{i,j}(r)$ ; per tant, són polinomis (de coeficients reals) en  $\theta_1, \dots, \theta_n$ ; si veiem que aquests coeficients són polinomis simètrics en els  $\theta_1, \dots, \theta_n$ , tenim que els coeficients



de  $f_r(X)$  són polinomis en els coeficients, reals, de  $f(X)$ , de manera que són nombres reals, com volem veure. Ara bé, en aplicar a  $f_r(X)$  una transposició qualsevol del conjunt  $\{\theta_1, \dots, \theta_n\}$  s'obté una permutació dels elements  $\alpha_{i,j}(r)$ , de manera que els coeficients de  $f_r(X)$ , efectivament, no varien.  $\square$

## 2.6 Exercicis

**Exercici 2.6.1** (Fórmules de Newton). Siguin  $T, X_1, \dots, X_n$  indeterminades,  $n \geq 1$ . Per a tot nombre enter  $m \geq 0$ , posem

$$t_m = t_m(X_1, \dots, X_n) := \sum_{i=1}^n X_i^m,$$

la suma de les potències  $m$ -èsimes de les indeterminades (que s'anomena el  $m$ -èsim polinomi de Newton en  $X_1, \dots, X_n$ ), i considerem els polinomis simètrics elementals,  $s_m = s_m(X_1, \dots, X_n)$ , com a la proposició **2.2.7**. Notem que  $t_0(X_1, \dots, X_n) = n$ . Posem, també,

$$f(T) := (T - X_1) \cdots (T - X_n) \in \mathbb{Z}[X_1, \dots, X_n][T],$$

el polinomi mònic general de grau  $n$  sobre  $\mathbb{Z}$ , i  $g_i(T) := \frac{f(T)}{T - X_i}$ ,  $1 \leq i \leq n$ .

- Es demana demostrar que  $D(f, T) = g_1(T) + \cdots + g_n(T)$  (el polinomi derivat de  $f(T)$ , com a polinomi en  $T$ ).
- Es demana calcular, per a tot índex  $i$ ,  $1 \leq i \leq n$ , els coeficients de  $g_i(T)$  en funció de  $X_i, s_1, s_2, \dots, s_n$  (es pot utilitzar la divisió pel mètode de Ruffini).
- Es demana deduir dels dos apartats anteriors les fórmules de Newton

$$t_m - t_{m-1}s_1 + t_{m-2}s_2 - \cdots + (-1)^{m-1}t_1s_{m-1} + (-1)^mms_m = 0,$$

per a  $1 \leq m \leq n - 1$ .

- Es demana demostrar les fórmules de Newton

$$t_m - t_{m-1}s_1 + t_{m-2}s_2 - \cdots + (-1)^nt_{m-n}s_n = 0, \quad m \geq n.$$

- Sigui  $k$  un cos de característica no divisor de  $n!$ ; és a dir, de característica 0 o bé un nombre primer  $p > n$ . Tot polinomi simètric  $p(X_1, \dots, X_n) \in k[X_1, \dots, X_n]^{S_n}$ , i de grau total  $m$ , es pot escriure com un polinomi, de coeficients en  $k$ , en  $t_1, \dots, t_m$ , si  $m \leq n$ , i en  $t_1, \dots, t_n$ , si  $m \geq n$ .

Aquest resultat es pot interpretar com una versió del teorema dels polinomis simètrics per als polinomis de Newton en lloc dels polinomis simètrics elementals.

**Exercici 2.6.2.** (a) Quina és la suma de les potències cinquenes de les arrels del polinomi

$$X^8 - 15X^6 + X^5 - 31X^4 - 12X^3 + 14X^2 - 13X + 1?$$

- (b) D'un polinomi mònic de grau 5, sabem que per a les seves arrels  $\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5$ , se satisfà que

$$\sum_{i=1}^5 \alpha_i = 0, \quad \sum_{i=1}^5 \alpha_i^2 = 10, \quad \sum_{i=1}^5 \alpha_i^3 = 0, \quad \sum_{i=1}^5 \alpha_i^4 = 34, \quad \sum_{i=1}^5 \alpha_i^5 = 0.$$

Quin és el polinomi?

*Observació:* En aquest enunciat no hi ha restriccions a la característica del cos de coeficients.

**Exercici 2.6.3.** (a) Es demana calcular, com a polinomi en  $a, b, c, d$ , el discriminant del polinomi general cúbic  $f(X) := aX^3 + bX^2 + cX + d \in \mathbb{Z}[a, b, c, d][X]$ ;

- (b) i deduir que  $\Delta(X^3 + pX + q) = -4p^3 - 27q^2$ .

**Exercici 2.6.4.** Es demana comprovar que  $\Delta(X^n + a) = (-1)^{n(n-1)/2} n^n a^{n-1}$ .

**Exercici 2.6.5** (El resultant de dos polinomis). Sigui  $A$  un domini d'integritat i considerem polinomis  $f(X) := a_0 + a_1X + \dots + a_nX^n$ ,  $g(X) := b_0 + b_1X + \dots + b_mX^m \in A[X]$ ,  $a_0, \dots, a_n, b_0, \dots, b_m \in A$ ,  $a_n, b_m \neq 0$ , de graus  $n, m \geq 0$ . Es defineix el resultant de  $f(X)$  i  $g(X)$  com el determinant

$$R(f(X), g(X)) := \begin{vmatrix} a_n & a_{n-1} & \dots & a_1 & a_0 & 0 & \dots & 0 \\ 0 & a_n & a_{n-1} & \dots & a_1 & a_0 & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \dots & a_n & a_{n-1} & \dots & a_1 & a_0 \\ b_m & b_{m-1} & \dots & b_1 & b_0 & 0 & \dots & 0 \\ 0 & b_m & b_{m-1} & \dots & b_1 & b_0 & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \dots & b_m & b_{m-1} & \dots & b_1 & b_0 \end{vmatrix} \in A,$$

on hi ha  $m = \text{gr}(g(X))$  files amb els coeficients de  $f(X)$  i  $n = \text{gr}(f(X))$  files amb els coeficients de  $g(X)$ . Aquesta matriu s'anomena la matriu de Sylvester associada als dos polinomis  $f(X)$  i  $g(X)$ . Es demana demostrar els enunciats següents.

- (a) Els polinomis  $f(X)$  i  $g(X)$  tenen alguna arrel comuna (en algun cos algebraicament tancat que contingui  $A$  com a subanell) si, i només si,  $R(f(X), g(X)) = 0$ .
- (b) Per a tot element  $\lambda \in A$  se satisfà que  $R(\lambda f(X), g(X)) = \lambda^m R(f(X), g(X))$  i que  $R(f(X), \lambda g(X)) = \lambda^n R(f(X), g(X))$ .
- (c)  $R(f(X), g(X))$  és un polinomi homogeni de grau  $m$  en les indeterminades  $a_0, \dots, a_n$ , i, alhora, homogeni de grau  $n$  en les indeterminades  $b_0, \dots, b_m$ .
- (d)  $R(f(X), g(X)) = a_n^m b_0^n +$  suma de monomis que no contenen  $a_n^m b_0^n$ .

**Exercici 2.6.6.** Amb les notacions i les hipòtesis de l'exercici 2.6.5, existeixen polinomis  $\phi(X), \psi(X) \in A[X]$  tals que  $R(f(X), g(X)) = \phi(X)f(X) + \psi(X)g(X)$ ,  $\text{gr}(\phi(X)) < m$ , i  $\text{gr}(\psi(X)) < n$ , que, a més a més, són únics si  $R(f(X), g(X)) \neq 0$ .

**Exercici 2.6.7.** Amb les notacions i les hipòtesis de l'exercici 2.6.5, sigui  $\bar{k}$  un cos algebraicament tancat que conté  $A$ , i siguin  $\alpha_1, \dots, \alpha_n \in \bar{k}$ , les arrels del polinomi  $f(X)$ , i  $\beta_1, \dots, \beta_m \in \bar{k}$  les arrels del polinomi  $g(X)$ . Llavors,

$$R(f(X), g(X)) = a_n^m b_m^n \prod_{i,j} (\alpha_i - \beta_j).$$

**Exercici 2.6.8** (Resultant i discriminant). Sigui  $A$  un domini d'integritat i considerem un polinomi no nul  $f(X) := a_0 + a_1X + \dots + a_nX^n \in A[X]$ ,  $a_0, \dots, a_n \in A$ ,  $a_n \neq 0$ . Per al polinomi derivat de  $f(X)$ ,  $D(f, X)$ , se satisfà que

$$R(f(X), D(f, X)) = (-1)^{n(n-1)/2} a_n \Delta(f(X)),$$

on  $D(f, X)$  com un polinomi de grau virtual  $n - 1$ , i  $\Delta(f(X))$  és el discriminant del polinomi  $f(X)$ .

**Exercici 2.6.9.** Es demana calcular, a partir del resultat de l'exercici anterior (2.6.8), el discriminant del polinomi  $X^n + aX + b$ , per a  $a, b \in A$  i  $n \geq 2$ .

**Exercici 2.6.10.** Amb les notacions i les hipòtesis de l'exercici 2.6.5, es demana demostrar les propietats següents.

- (a)  $R(g(X), f(X)) = (-1)^{nm} R(f(X), g(X))$ .
- (b)  $R(f_1(X)f_2(X), g(X)) = R(f_1(X), g(X))R(f_2(X), g(X))$ .
- (c)  $R(f(X), X^m) = (-1)^{nm} a_0^m$ .
- (d) Siguin  $f(X), g(X), q(X), r(X) \in A[X]$  polinomis tals que  $f(X) = g(X)q(X) + r(X)$ ,  $g(X) \neq 0$ , i  $\text{gr}(r(X)) \leq n = \text{gr}(f(X)) > 0$ . Llavors,

$$R(f(X), g(X)) = (-1)^{nm} b_m^{n-\text{gr}(r(X))} R(g(X), r(X)).$$



# Capítol 3

## Arrels de la unitat

Si deixem de banda les equacions quadràtiques, potser les més senzilles són les de la forma  $X^n - 1 = 0$ . La causa és que el conjunt de les arrels  $n$ -èsimes de la unitat d'un cos té una estructura extra natural: és un grup cíclic. Dediquem la primera secció a establir aquesta estructura, i la segona a la definició i l'estudi dels polinomis ciclotòmics  $\Phi_d(X)$ ; en particular, provem que són polinomis de coeficients enters; a més a més, fem notar que la factorització del polinomi  $X^n - 1$  com a producte de polinomis ciclotòmics permet reduir la resolució en  $\mathbb{C}$  de l'equació  $X^n - 1 = 0$  a la de les equacions  $\Phi_d(X) = 0$ , per a tots els divisors  $d$  de  $n$ . A la secció tercera, fem la prova de la irreductibilitat dels polinomis ciclotòmics sobre  $\mathbb{Q}$  i aprofitem l'ocasió per a la introducció de la terminologia i les propietats bàsiques relacionades amb els nombres algebraics. A les seccions quarta i cinquena introduïm el llenguatge d'extensions de cossos i fem l'estudi del comportament del grau per a les extensions finites en general i, en particular, per al cas dels cossos ciclotòmics. A la secció sisena, procedim a la classificació de les extensions quadràtiques en el cas de característica diferent de 2, classificació que serveix de motivació i, alhora, d'exemple, de la teoria de Kummer de la classificació de les extensions cíclics que fem al capítol següent. A la secció setena, introduïm i estudiem el grup de Galois per al cas de les extensions ciclotòmiques del cos dels nombres racionals; en particular, establim l'anomenat caràcter ciclotòmic, que proporciona un isomorfisme natural i explícit del grup de Galois de l'extensió ciclotòmica de  $\mathbb{Q}$  generada per les arrels  $n$ -èsimes de la unitat amb el grup dels elements invertibles de l'anell  $\mathbb{Z}/n\mathbb{Z}$ .

A la secció vuitena, ens plantegem la qüestió “què succeeix si en comptes d'una arrel d'un polinomi irreductible en considerem una altra” i, per a donar-ne una resposta, iniciem l'estudi de les immersions de cossos i donem la definició del grup de Galois d'una extensió finita qualsevol. Aquest estudi serveix com a motivació per a la consideració de les extensions normals de cossos i l'extensió algebraica de morfismes, que fem a la secció novena. Finalment, dediquem la secció desena a l'estudi dels cossos finits, tots els elements dels quals són arrels de la unitat. Després de caracteritzar-ne l'existència i d'establir-ne les propietats bàsiques, definim l'automorfisme de Frobenius d'una extensió qualsevol de cossos finits i provem que aquest automorfisme és un generador del grup de Galois de l'extensió que, per tant, és cíclic; com a conseqüència, obtenim de manera natural i immediata una demostració del teorema fonamental de la teoria de Galois per al cas de les extensions finites de cossos finits.

### 3.1 Arrels de la unitat

**Definició 3.1.1.** Siguin  $k$  un cos i  $n \geq 1$  un nombre natural. Un element  $x \in k$  s'anomena una *arrel  $n$ -èsima de la unitat* si  $x^n = 1$ ; és a dir, si és arrel del polinomi  $X^n - 1 \in k[X]$ . Un element  $x \in k$  s'anomena una *arrel de la unitat* si existeix un nombre natural  $n \geq 1$  tal que  $x^n = 1$ . S'acostuma a denotar per  $\mu_n(k)$  el conjunt de les arrels  $n$ -èsimes de la unitat que pertanyen a  $k$  i per  $\mu(k) := \bigcup_{n \geq 1} \mu_n(k) \subseteq k^*$  el conjunt de totes les arrels de la unitat de  $k$ .

**3.1.2.** Si  $k$  és un cos, el grup multiplicatiu  $k^*$  és un grup abelià i, per tant, per a tot nombre enter  $n$ , l'aplicació d'elevat a  $n$ ,  $k^* \xrightarrow{[n]} k^*$ , que envia  $x$  a  $x^n$ , és un morfisme de grups. El seu nucli,  $\ker[n] = \{x \in k : x^n = 1\} = \mu_n(k)$ , és, doncs, un subgrup de  $k^*$ ; i, com que, per a  $n \geq 1$ , el polinomi  $X^n - 1$  no pot tenir més de  $n$  arrels en  $k$ ,  $\mu_n(k)$  és un subgrup finit de  $k^*$  d'ordre menor o igual que  $n$ .

**3.1.3.** Per a tot cos  $k$ , és  $\mu_2(k) = \{x \in k : x^2 - 1 = 0\} = \{1, -1\}$ . Notem que  $1 = -1$  si, i només si,  $\text{car}(k) = 2$ , ja que el polinomi  $X^2 - 1$  té una arrel doble en  $k$  si  $\text{car}(k) = 2$ , i dues arrels simples si  $\text{car}(k) \neq 2$ .

**3.1.4. Arrels de la unitat de  $\mathbb{Q}$ .** És ben conegut que tot nombre enter diferent de zero admet una descomposició única com a producte de nombres primers i, potser,  $-1$  (teorema fonamental de l'Aritmètica); per tant, tot nombre racional diferent de zero,  $q \in \mathbb{Q}$ ,  $q \neq 0$ , es pot escriure de manera única en la forma  $q = (-1)^{a_0} p_1^{a_1} \cdots p_r^{a_r}$ , on  $p_1, p_2, \dots, p_r$  denoten nombres naturals primers diferents dos a dos,  $a_0 \in \{0, 1\}$ , i  $a_1, \dots, a_r \in \mathbb{Z}$  són nombres enters diferents de zero. D'aquí es dedueix que, per a  $n \geq 1$ ,  $q^n = 1$  si, i només si,  $r = 0$  i  $a_0 n$  és parell; en conseqüència,  $\mu(\mathbb{Q}) = \mu_2(\mathbb{Q}) = \{1, -1\}$ .

**3.1.5.** Si  $k$  és un cos finit, el grup abelià  $k^*$  és finit i, si  $n$  és l'ordre de  $k^*$ , per a tot  $x \in k$ ,  $x \neq 0$ , és  $x^n = 1$ ; així,  $\mu(k) = \mu_n(k) = k^*$ . Dit d'una altra manera, tots els elements diferents de zero d'un cos finit són arrels de la unitat.

**3.1.6.** Per a tot cos  $k$ ,  $\mu(k) \subseteq k^*$  és un subgrup de  $k^*$ , ja que  $1 \in \mu(k)$  i si  $x^n = y^m = 1$ , llavors  $(xy^{-1})^{nm} = 1$ . El grup  $\mu(k)$  pot ésser un grup finit o no; per exemple, si  $k$  és algebraicament tancat, el grup  $\mu(k)$  és numerable, però no és finit.

**Proposició 3.1.7.** Siguin  $k$  un cos qualsevol i  $G \subseteq k^*$  un subgrup finit del grup multiplicatiu de  $k$ . Llavors,  $G$  és un grup cíclic, i  $G \subseteq \mu(k)$ .

**DEMOSTRACIÓ:** Com que  $G$  és finit, podem considerar un element  $\zeta \in G$  d'ordre màxim, posem  $n$ . I, com que  $G$  és un grup abelià, tot element  $x \in G$  és d'ordre divisor de  $n$  (exercici); és a dir, tot element de  $G$  és arrel del polinomi  $X^n - 1$ . Llavors, per al subgrup generat per  $\zeta$  és  $\langle \zeta \rangle \subseteq G \subseteq \mu_n(k)$ . Però  $\langle \zeta \rangle$  és un grup d'ordre  $n$  i  $\mu_n(k)$  és d'ordre menor o igual que  $n$ ; això ens diu que les inclusions anteriors són igualtats; és a dir,  $G$  és el grup cíclic generat per  $\zeta$ .  $\square$

**Corol·lari 3.1.8.** El grup de les arrels  $n$ -èsimes complexes de la unitat,  $\mu_n(\mathbb{C})$ , és cíclic d'ordre  $n$ .

**DEMOSTRACIÓ:** Per a tot nombre natural  $n \geq 1$ , el polinomi  $X^n - 1$  no té arrels múltiples en  $\mathbb{C}$ , ja que  $\text{mcd}(X^n - 1, nX^{n-1}) = 1$ ; per tant, té exactament  $n$  arrels diferents en  $\mathbb{C}$ .  $\square$

**Corollari 3.1.9** (Petit teorema de Fermat). *Sigui  $\mathbb{F}$  un cos finit i  $n := \#\mathbb{F}$ . Per a tot element  $x \in \mathbb{F}$  és  $x^n = x$ ; i per a tot element  $x \in \mathbb{F}^*$  és  $x^{n-1} = 1$ .*

DEMOSTRACIÓ: L'afirmació és clara per a  $x = 0$ ; d'altra banda,  $\mathbb{F}^*$  és un subgrup finit d'ordre  $n - 1$  i, per tant, per a tot  $x \in \mathbb{F}^*$ , és  $x^{n-1} = 1$ . L'altra igualtat s'obté en multiplicar aquesta per  $x$ .  $\square$

**Corollari 3.1.10.** *Sigui  $p$  un nombre enter primer. Per a tot polinomi  $f(X) \in (\mathbb{Z}/p\mathbb{Z})[X]$  és  $f(X)^p = f(X^p)$ .*

DEMOSTRACIÓ: La fórmula del binomi ens ensenya que, si  $a, b \in (\mathbb{Z}/p\mathbb{Z})[X]$ , llavors  $(a + b)^p = a^p + b^p$ , perquè els nombres combinatoris  $\binom{p}{i}$  són nombres naturals múltiples de  $p$ , per a  $1 \leq i \leq p - 1$ . En conseqüència, si  $f(X) = \sum_{i=0}^n a_i X^i$ , on  $a_i \in \mathbb{Z}/p\mathbb{Z}$ , llavors

$$f(X)^p = \sum_{i=0}^n a_i^p X^{ip} = \sum_{i=0}^n a_i X^{pi} = f(X^p), \text{ ja que } a_i^p = a_i, \text{ per a tot } a_i \in \mathbb{Z}/p\mathbb{Z}. \square$$

## 3.2 Polinomis ciclotòmics

**3.2.1.** Si  $k$  és un cos algebraicament tancat de característica  $p > 0$ , i si  $n$  és un múltiple de  $p$ , el grup  $\mu_n(k)$  és d'ordre estrictament menor que  $n$ . En efecte, tota arrel del polinomi  $X^n - 1$  és una arrel múltiple, perquè el derivat del polinomi  $X^n - 1$  és el polinomi  $nX^{n-1} = 0$ . Però si  $n$  no és múltiple de  $p$  o bé si  $k$  és de característica 0, les arrels del polinomi  $X^n - 1$  són simples, de manera que  $\#\mu_n(k) = n$ .

**Definició 3.2.2.** Sigui  $k$  un cos algebraicament tancat. Per a tot nombre natural  $n \geq 1$ , s'anomena *arrel primitiva  $n$ -èsima de la unitat* tot element de  $k^*$  d'ordre  $n$ , si n'hi ha; és a dir, tot generador de  $\mu_n(k)$ , si  $\#\mu_n(k) = n$ .

**3.2.3.** Si  $\zeta \in k^*$  és una arrel primitiva  $n$ -èsima de la unitat, les arrels  $n$ -èsimes de la unitat diferents són els nombres  $\zeta^m$ , per a  $1 \leq m \leq n$ ; i les arrels primitives  $n$ -èsimes de la unitat, els  $\zeta^m$ , per a  $1 \leq m \leq n$  tals que  $\text{mcd}(n, m) = 1$ . És a dir, les arrels primitives  $n$ -èsimes de la unitat són els generadors del grup cíclic de les arrels  $n$ -èsimes de la unitat.

**3.2.4.** Per exemple, les arrels  $n$ -èsimes de la unitat de  $\mathbb{C}$  es poden expressar en la forma  $\cos\left(\frac{2m\pi}{n}\right) + i \sin\left(\frac{2m\pi}{n}\right)$ , per a  $1 \leq m \leq n$  (fórmules de de Moivre). I són primitives  $n$ -èsimes si  $\text{mcd}(m, n) = 1$ .

**Definició 3.2.5.** Com que les arrels en  $\mathbb{C}$  del polinomi  $X^n - 1 \in \mathbb{Z}[X]$  són simples, aquest polinomi admet la descomposició, en  $\mathbb{C}[X]$ ,

$$X^n - 1 = \prod_{\zeta \in \mu_n(\mathbb{C})} (X - \zeta),$$

el producte està a totes les arrels  $n$ -èsimes de la unitat. El polinomi

$$\Phi_n(X) := \prod_{\zeta} (X - \zeta) \in \mathbb{C}[X],$$

on ara  $\zeta$  només recorre el conjunt de les arrels  $n$ -èsimes primitives de la unitat de  $\mathbb{C}$ , s'anomena el  *$n$ -èsim polinomi ciclotòmic*.

**3.2.6.** És clar que  $\Phi_1(X) = X - 1$ . D'altra banda, si  $p$  és un nombre primer, tots els elements de  $\mu_p(\mathbb{C})$  diferents de 1 són arrels primitives  $p$ -èsimes de la unitat; per tant,

$$\Phi_p(X) = \prod_{\zeta^p=1, \zeta \neq 1} (X - \zeta) = \frac{X^p - 1}{X - 1} = 1 + X + X^2 + \dots + X^{p-1}.$$

**Definició 3.2.7.** La funció  $\varphi$  d'Euler és l'aplicació  $\varphi : \mathbb{N} - \{0\} \rightarrow \mathbb{Z}$  definida per  $\varphi(n) := \#\{m : 1 \leq m \leq n, \text{mcd}(n, m) = 1\}$ .

**Corol·lari 3.2.8.** Si  $G$  és un grup cíclic d'ordre  $n \geq 1$ , llavors el nombre d'elements  $g \in G$  tals que  $G = \langle g \rangle$  és  $\varphi(n)$ .  $\square$

**Corol·lari 3.2.9.** El grau del polinomi ciclotòmic  $\Phi_n(X)$  és  $\varphi(n)$ .  $\square$

**3.2.10.** Ens proposem donar fórmules per a calcular els polinomis ciclotòmics. Sigui  $n \geq 1$  un nombre natural. El polinomi  $X^n - 1$  té per arrels totes les arrels  $n$ -èsimes de la unitat, primitives o no. Però tota arrel  $n$ -èsima de la unitat és arrel primitiva  $d$ -èsima per a algun divisor  $d$  de  $n$ ; per tant, tota arrel de  $X^n - 1$  és arrel d'un polinomi  $\Phi_d(X)$  per a un únic divisor  $d$  de  $n$ . I recíprocament, les arrels dels polinomis  $\Phi_d(X)$ , per a  $d \mid n$ , són arrels de  $X^n - 1$ . Això ens diu que els polinomis  $X^n - 1$  i  $\prod_{d \mid n} \Phi_d(X)$  tenen exactament les mateixes arrels. Com que totes són simples en tots dos polinomis i tots dos polinomis són mònic, obtenim la igualtat següent.

**Proposició 3.2.11.**  $X^n - 1 = \prod_{d \mid n} \Phi_d(X)$ .  $\square$

El càlcul del grau del polinomi  $X^n - 1$  a partir d'aquesta relació proporciona el resultat següent sobre la funció  $\varphi$  d'Euler.

**Corol·lari 3.2.12.** Per a tot nombre natural  $n \geq 1$  és  $\sum_{d \mid n} \varphi(d) = n$ .  $\square$

**Observació 3.2.13.** La igualtat  $X^n - 1 = \prod_{d \mid n} \Phi_d(X)$  ens diu que el polinomi  $X^n - 1$

és divisible pel polinomi mònic  $\prod_{d \mid n, d < n} \Phi_d(X)$ ; per tant, la divisió té sentit en l'anell de

polinomis i obtenim l'expressió equivalent  $\Phi_n(X) = \frac{X^n - 1}{\prod_{d \mid n, d < n} \Phi_d(X)}$ , de manera que podem

calcular els polinomis ciclotòmics de manera recursiva.

**Exemples 3.2.14.** Ja hem calculat més amunt els polinomis  $\Phi_1(X) = X - 1$  i, per a tot nombre primer  $p \geq 2$ ,  $\Phi_p(X) = 1 + X + X^2 + \dots + X^{p-1}$ . A continuació fem el càlcul recursiu d'alguns altres.

$$\begin{aligned} \Phi_4(X) &= \frac{X^4 - 1}{\Phi_2(X)\Phi_1(X)} = \frac{X^4 - 1}{(X + 1)(X - 1)} = X^2 + 1, \\ \Phi_6(X) &= \frac{X^6 - 1}{\Phi_3(X)\Phi_2(X)\Phi_1(X)} = \frac{X^6 - 1}{(X^2 + X + 1)(X + 1)(X - 1)} \\ &= X^2 - X + 1, \end{aligned}$$



$$\begin{aligned}
\Phi_8(X) &= \frac{X^8 - 1}{\Phi_4(X)\Phi_2(X)\Phi_1(X)} = \frac{X^8 - 1}{(X^2 + 1)(X + 1)(X - 1)} = X^4 + 1, \\
\Phi_9(X) &= \frac{X^9 - 1}{\Phi_3(X)\Phi_1(X)} = \frac{X^9 - 1}{(X^2 + X + 1)(X - 1)} = X^6 + X^3 + 1, \\
\Phi_{10}(X) &= \frac{X^{10} - 1}{\Phi_5(X)\Phi_2(X)\Phi_1(X)} \\
&= \frac{X^{10} - 1}{(X^4 + X^3 + X^2 + X + 1)(X + 1)(X - 1)} \\
&= X^4 - X^3 + X^2 - X + 1, \\
\Phi_{12}(X) &= \frac{X^{12} - 1}{\Phi_6(X)\Phi_4(X)\Phi_3(X)\Phi_2(X)\Phi_1(X)} \\
&= \frac{X^{12} - 1}{(X^2 - X + 1)(X^2 + 1)(X^2 + X + 1)(X + 1)(X - 1)} \\
&= X^4 - X^2 + 1.
\end{aligned}$$

Ens interessa obtenir una fórmula per al càlcul no recursiu dels polinomis ciclotòmics; l'expressió que obtenim fa ús de la funció de Möbius.

**Definició 3.2.15.** La funció  $\mu : \mathbb{N} - \{0\} \rightarrow \{0, 1, -1\}$  definida per

$$\mu(n) := \begin{cases} 1, & \text{si } n = 1, \\ 0, & \text{si } n \text{ és divisible per algun quadrat diferent de 1,} \\ (-1)^r, & \text{si } n \text{ és producte de } r \text{ nombres primers diferents,} \end{cases}$$

s'anomena la *funció  $\mu$  de Möbius*.

**Proposició 3.2.16.** Per a tot nombre natural  $n \geq 1$  és

$$\sum_{d|n} \mu(d) = \begin{cases} 1, & \text{si } n = 1, \\ 0, & \text{si } n > 1. \end{cases}$$

**DEMOSTRACIÓ:** El resultat és evident si  $n = 1$ . Suposem, doncs, que  $n \geq 1$  i que  $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$  és la descomposició de  $n$  en factors primers diferents,  $p_1, p_2, \dots, p_r$ . Els divisors positius de  $n$  són els nombres  $d = p_1^{b_1} p_2^{b_2} \cdots p_r^{b_r}$  tals que  $0 \leq b_i \leq a_i$ ,  $1 \leq i \leq r$ ; i els únics que corresponen a sumands no nuls són els  $d$  tals que  $0 \leq b_i \leq 1$ ,  $1 \leq i \leq r$ .

D'aquests divisors, i per a  $0 \leq k \leq r$ , n'hi ha  $\binom{r}{k}$  que són el producte d'exactament  $k$  nombres primers diferents; per tant, i com que  $r \geq 1$ , resulta que la suma que volem calcular val  $\sum_{k=0}^r \binom{r}{k} (-1)^k = (1 - 1)^r = 0$ .  $\square$

**Corol·lari 3.2.17.** Sigui  $n \geq 1$  un nombre natural. El polinomi ciclotòmic  $\Phi_n(X)$  es pot calcular per la fórmula

$$\Phi_n(X) = \prod_{d|n} (X^d - 1)^{\mu(n/d)} = \prod_{d|n} (X^{\frac{n}{d}} - 1)^{\mu(d)}.$$

DEMOSTRACIÓ: Evidentment, els dos productes de l'enunciat són iguals; calculem el segon.

$$\begin{aligned} \prod_{d|n} (X^{\frac{n}{d}} - 1)^{\mu(d)} &= \prod_{d|n} \prod_{\delta|\frac{n}{d}} \Phi_{\delta}(X)^{\mu(d)} \\ &= \prod_{\delta|n} \prod_{d|\frac{n}{\delta}} \Phi_{\delta}(X)^{\mu(d)} \\ &= \prod_{\delta|n} \Phi_{\delta}(X)^{\sum_{d|\frac{n}{\delta}} \mu(d)}. \end{aligned}$$

Ara, la suma de l'exponent val 0, llevat que  $\delta = n$ , cas en què val 1. Això acaba la prova.  $\square$

**Exemple 3.2.18.** Podem recuperar, a partir d'aquesta fórmula, els polinomis ciclotòmics  $\Phi_n(X)$ , per a  $n \in \{4, 6, 8, 9, 10, 12\}$ . Notem que aquest càlcul és més senzill que l'anterior.

$$\begin{aligned} \Phi_4(X) &= \frac{X^4 - 1}{X^2 - 1} = X^2 + 1, \\ \Phi_6(X) &= \frac{(X^6 - 1)(X - 1)}{(X^3 - 1)(X^2 - 1)} = X^2 - X + 1, \\ \Phi_8(X) &= \frac{X^8 - 1}{X^4 - 1} = X^4 + 1, \\ \Phi_9(X) &= \frac{X^9 - 1}{X^3 - 1} = X^6 + X^3 + 1, \\ \Phi_{10}(X) &= \frac{(X^{10} - 1)(X - 1)}{(X^5 - 1)(X^2 - 1)} = X^4 - X^3 + X^2 - X + 1, \\ \Phi_{12}(X) &= \frac{(X^{12} - 1)(X^2 - 1)}{(X^6 - 1)(X^4 - 1)} = X^4 - X^2 + 1. \end{aligned}$$

**Corol·lari 3.2.19.** Per a tot nombre natural  $n \geq 1$  és  $\frac{\varphi(n)}{n} = \sum_{d|n} \frac{\mu(d)}{d}$ .

DEMOSTRACIÓ: El càlcul del grau de  $\Phi_n(X)$  mitjançant la relació anterior ens proporciona la igualtat  $\varphi(n) = \sum_{d|n} \frac{n}{d} \mu(d)$  i només cal dividir per  $n$ .  $\square$

**Corol·lari 3.2.20.** Per a tot  $n \geq 1$ , el polinomi ciclotòmic  $\Phi_n(X)$  és de coeficients enters.

DEMOSTRACIÓ: La fórmula  $\Phi_n(X) = \prod_{d|n} (X^{\frac{n}{d}} - 1)^{\mu(d)}$  ens permet calcular  $\Phi_n(X)$  dividint dos polinomis mòncics de coeficients enters. Per tant, el quocient és un polinomi mònic de coeficients enters.  $\square$

**3.2.21.** Notem que també podem obtenir aquest resultat per inducció, a partir del fet que  $\Phi_1(X) = X - 1 \in \mathbb{Z}[X]$  i la fórmula  $\Phi_n(X) = \frac{X^n - 1}{\prod_{d|n, d < n} \Phi_d(X)}$ .

**3.2.22.** Podem observar que tots els polinomis ciclotòmics dels exemples explícits anteriors són irreductibles en  $\mathbb{Z}[X]$  i en  $\mathbb{Q}[X]$ . Aquest fet és general.

**Teorema 3.2.23** (Irreductibilitat dels polinomis ciclotòmics).  *sigui  $n \geq 1$ . El polinomi ciclotòmic  $\Phi_n(X) \in \mathbb{Z}[X]$  és irreductible en  $\mathbb{Z}[X]$  i en  $\mathbb{Q}[X]$ .*

En fem una demostració a la secció següent.

### 3.3 Elements algebraics i elements transcendents

El cos dels nombres racionals és un cos numerable, mentre que el cos dels nombres complexos no ho és. A partir de la numerabilitat de  $\mathbb{Q}$ , obtenim que la quantitat d'equacions polinòmiques de coeficients racionals és numerable; si tenim en compte que cada una d'elles només té una quantitat finita de solucions complexes, ens adonem que totes les solucions possibles de totes les equacions polinòmiques de coeficients racionals formen un subconjunt numerable de  $\mathbb{C}$ . En conseqüència, la majoria dels nombres complexos no són solució de cap equació polinòmica de coeficients racionals. Convé donar noms, i ho farem en general.

**Definició 3.3.1.** Siguin  $K$  un cos qualsevol i  $k \subseteq K$  un subcòs. Un element  $\theta \in K$  s'anomena *algebraic sobre  $k$*  si existeix un polinomi  $f(X) \in k[X]$ ,  $f(X) \neq 0$ , tal que  $f(\theta) = 0$ ; en cas contrari,  $\theta$  s'anomena *transcendent sobre  $k$* . En el cas dels nombres complexos que són algebraics sobre  $\mathbb{Q}$  es parla, simplement, dels *nombres algebraics*.

**3.3.2.** Siguin  $k \subseteq K$  cossos qualssevol i  $\theta \in K$  un element qualsevol de  $K$ . Podem avaluar tots els polinomis de  $k[X]$  en  $\theta$ ; és a dir, podem considerar l'aplicació  $\psi_\theta : k[X] \rightarrow K$  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  $a \in k$ .

**Definició 3.3.3.** Escriurem  $k[\theta] := \text{im}(\psi_\theta)$ ; es tracta del menor subanell de  $K$  que conté  $k$  i  $\theta$ ; o sigui, del subanell de  $K$  generat per  $k$  i  $\theta$ . Escriurem  $k(\theta)$  per a denotar el cos de fraccions de  $k[\theta]$ ; és el menor subcòs de  $K$  que conté  $k$  i  $\theta$ ; o sigui, el subcòs de  $K$  generat per  $k$  i  $\theta$ .

**3.3.4.** Notem que  $\ker(\psi_\theta)$  és el conjunt de tots els polinomis  $f(X) \in k[X]$  tals que  $f(\theta) = 0$ ; això implica que el conjunt de tots els polinomis de  $k[X]$  que tenen  $\theta$  com a arrel és un ideal de l'anell de polinomis  $k[X]$ . En particular, el morfisme  $\psi_\theta$  és injectiu si, i només si,  $\theta$  no és arrel de cap polinomi no nul de  $k[X]$ ; és a dir, si  $\theta$  és transcendent sobre  $k$ . En aquest cas, tenim un isomorfisme  $k[\theta] \cong k[X]$ ; i, en conseqüència,  $k(\theta)$  és isomorf al cos de fraccions de l'anell de polinomis en una indeterminada sobre  $k$ .

**3.3.5.** En cas contrari, és a dir, si  $\theta$  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, si  $f(X)$  és un generador qualsevol de  $\ker(\psi_\theta)$ , obtenim que  $k[X]/(f(X)) \cong k[\theta] \subseteq K$ . A més 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,  $k[\theta] = k(\theta)$ .

**Definició 3.3.6.** Per a un element  $\theta \in K$  algebraic sobre  $k$ , s'anomena *polinomi minimal de  $\theta$  sobre  $k$*  el polinomi mònic que genera l'ideal  $\ker(\psi_\theta)$ ; és un polinomi irreductible de  $k[X]$  que denotarem per  $\text{Irr}(\theta, k)(X)$ .

**Corollari 3.3.7.** Siguin  $K$  un cos,  $k \subseteq K$  un subcòs,  $\theta \in K$  un element algebraic sobre  $k$ , i  $f(X) := \text{Irr}(\theta, k)(X) \in k[X]$  el polinomi minimal de  $\theta$  sobre  $k$ . Si  $g(X) \in k[X]$  és un polinomi tal que  $g(\theta) = 0$ , llavors  $f(X) | g(X)$ .

**DEMOSTRACIÓ:** La hipòtesi  $g(\theta) = 0$  ens diu que  $g(X) \in \ker(\psi_\theta) = (f(X))$ ; és a dir, que  $f(X) | g(X)$ .  $\square$

Procedim, ara, a la demostració de la irreductibilitat dels polinomis ciclotòmics que hem promès a la secció anterior.

**DEMOSTRACIÓ** (del teorema **3.2.23**): Podem escriure  $\Phi_n(X) = f(X)g(X)$ , on  $f(X)$ ,  $g(X) \in \mathbb{Z}[X]$  són polinomis mònic i  $f(X)$  irreductible. Si veiem que  $f(X) = \Phi_n(X)$ , haurem acabat. I, per a això, és suficient veure que totes les arrels del polinomi  $\Phi_n(X)$  són arrels de  $f(X)$ .

Siguin  $\zeta \in \mathbb{C}$  una arrel de  $f(X)$  i  $p$  qualsevol nombre natural primer que no divideixi  $n$ . Com que  $\zeta$  és una arrel primitiva  $n$ -èsima de la unitat i  $\text{mcd}(p, n) = 1$ , la potència  $p$ -èsima  $\zeta^p$  també és una arrel primitiva  $n$ -èsima de la unitat, de manera que  $\zeta^p$  o bé és una arrel de  $f(X)$ , o bé és una arrel de  $g(X)$ . Vegem que  $f(\zeta^p) = 0$ .

Per reducció a l'absurd, suposem que fos  $f(\zeta^p) \neq 0$ ; tindríem que  $g(\zeta^p) = 0$ ; o sigui, que  $\zeta$  seria una arrel del polinomi mònic de coeficients enters  $g(X^p)$ . Com que  $f(X)$  és irreductible, se satisfà que  $f(X) = \text{Irr}(\zeta, \mathbb{Q})(X)$  i, per tant, tindríem que  $f(X) | g(X^p)$ . Com a conseqüència, obtindríem l'existència d'un polinomi mònic de coeficients enters,  $h(X) \in \mathbb{Z}[X]$ , tal que  $g(X^p) = f(X)h(X)$ . Considerem, ara, la reducció mòdul  $p$ . Com que  $g(X)^p \equiv g(X^p) \pmod{p}$ , tindríem que  $g(X)^p \equiv f(X)h(X) \pmod{p}$  i, per tant, tot factor irreductible de  $f(X) \pmod{p}$  ho seria de  $g(X) \pmod{p}$ . Ara, de la congruència  $\Phi_n(X) \equiv f(X)g(X) \pmod{p}$ , resulta que la reducció mòdul  $p$  de  $\Phi_n(X)$  tindria factors irreductibles en  $(\mathbb{Z}/p\mathbb{Z})[X]$  de multiplicitat més gran que 1; però això no pot ser, ja que  $\Phi_n(X) \pmod{p}$  divideix  $X^n - 1 \pmod{p}$ , i aquest darrer polinomi no té factors irreductibles de multiplicitat més gran que 1 en  $(\mathbb{Z}/p\mathbb{Z})[X]$ , perquè el seu polinomi derivat només té el factor irreductible  $X \pmod{p}$ , que no és factor de  $X^n - 1 \pmod{p}$ .

Doncs, hem provat que si  $\zeta$  és una arrel de  $f(X)$  i  $p$  és un nombre primer que no divideix  $n$ , també és  $f(\zeta^p) = 0$ . Si apliquem reiteradament aquest resultat tenint en compte que tot nombre natural  $r > 1$  primer amb  $n$  és producte de nombres primers  $p$  que no divideixen  $n$ , obtenim que, si  $\zeta$  és una arrel de  $f(X)$ , també és  $f(\zeta^r) = 0$ , per a tot nombre natural  $r$  tal que  $\text{mcd}(r, n) = 1$ . Ara bé, si  $\zeta$  és una arrel primitiva  $n$ -èsima de la unitat, tota altra arrel primitiva  $n$ -èsima de la unitat és de la forma  $\zeta^r$ , amb  $\text{mcd}(r, n) = 1$ ; per tant, totes les arrels primitives  $n$ -èsimes de la unitat són arrels de  $f(X)$ .  $\square$

**3.3.8.** Sigui  $K$  un cos,  $k \subseteq K$  un subcòs, i  $\theta \in K$  un element algebraic sobre  $k$ . Hem vist que, en aquest cas,  $k[\theta]$  és un subcòs de  $K$ . D'altra banda,  $k[\theta] \cong k[X]/(\text{Irr}(\theta, k)(X))$  és un  $k$ -espai vectorial de dimensió finita, igual al grau,  $n$ , de  $\text{Irr}(\theta, k)(X)$ , i  $\{1, \theta, \theta^2, \dots, \theta^{n-1}\}$  és una  $k$ -base de  $k[\theta]$ . En particular, per a tot element  $\beta \in k[\theta]$ ,  $\beta \neq 0$ , existeix un polinomi  $g(X) \in k[X]$ ,  $\text{gr}(g(X)) < n$ , tal que  $\beta = g(\theta)$ .

**Exercici 3.3.9.** Sigui  $\theta \in K$  un element algebraic sobre  $k$ , i  $\beta \in k[\theta]$ ,  $\beta \neq 0$  un element qualsevol. Es demana expressar l'element  $\beta^{-1} \in k[\theta]$  com a polinomi en  $\theta$  de coeficients en  $k$  a partir d'una expressió de  $\beta$  d'aquesta forma.

## 3.4 Extensions finites de cossos

La resolució de l'equació  $X^n = 1$  en  $\mathbb{C}$  ha estat reduïda a la resolució de les equacions  $\Phi_d(X) = 0$ , per a  $d | n$ , irreductibles en  $\mathbb{Q}[X]$ . Aquestes equacions satisfan una propietat especial: donada una arrel qualsevol,  $\zeta$ , del polinomi ciclotòmic  $\Phi_d(X)$ , les altres arrels del polinomi són potències de  $\zeta$ ; en conseqüència, les altres arrels pertanyen al menor subcòs de  $\mathbb{C}$  que conté  $\mathbb{Q}$  i  $\zeta$ .

**3.4.1.** Aquesta propietat dels polinomis ciclotòmics no és, ni de bon tros, general; per exemple, per a l'equació  $X^3 - 2 = 0$ , que és irreductible sobre  $\mathbb{Q}$ , una, i només una, de les seves tres solucions complexes és real, de manera que no totes les arrels d'un polinomi irreductible pertanyen al menor subcòs de  $\mathbb{C}$  que en conté una.

**Definició 3.4.2.** Si  $K$  és un cos i  $k \subseteq K$  un subcòs, també diem que  $K$  és *un cos extensió* de  $k$  i escriurem  $K|k$ . Diem que una extensió  $K|k$  de cossos és *algebraica* si tot element de  $K$  és algebraic sobre  $k$ ; en cas contrari, diem que  $K|k$  és una extensió *transcendent*. Podem parlar, doncs, d'extensions algebraiques de cossos o d'extensions transcendents de cossos.

**Exemples 3.4.3.** Les extensions  $\mathbb{C}|\mathbb{Q}$  i  $\mathbb{R}|\mathbb{Q}$  són transcendents, ja que la quantitat d'elements de  $\mathbb{R}$  o bé de  $\mathbb{C}$  que són algebraics sobre  $\mathbb{Q}$  és numerable.

D'altra banda, l'extensió  $\mathbb{C}|\mathbb{R}$  és algebraica, perquè donat  $\theta \in \mathbb{C}$ , podem escriure  $\theta = a + bi$ , amb  $a, b \in \mathbb{R}$  únics, i  $\theta$  és arrel del polinomi  $X^2 - 2aX + (a^2 + b^2) \in \mathbb{R}[X]$ .

**Definició 3.4.4.** Si  $K|k$  és una extensió qualsevol de cossos,  $K$  és un  $k$ -espai vectorial. S'anomena *grau* de l'extensió de cossos  $K|k$ , i es designa per  $[K : k]$ , la dimensió de  $K$  com a  $k$ -espai vectorial. Direm que l'extensió  $K|k$  és  *finita* si el grau  $[K : k]$  és finit.

**Observació 3.4.5.** En aquesta definició de grau com a nombre cardinal fem servir el resultat, que es discuteix en un apèndix, que tot espai vectorial té una base (cf. **B.0.25**), i també que dues bases d'un mateix espai vectorial tenen el mateix cardinal, resultat que es pot demostrar fàcilment amb l'ajuda de la teoria de nombres cardinals. Sovint només cal distingir cardinals diferents en el cas finit, de manera que podríem parlar d'extensions finites de grau donat i d'extensions no finites en general, i només caldria usar aquests dos resultats en el cas d'espais vectorials de dimensió finita, per als quals són ben coneguts dels cursos d'àlgebra lineal.

**Exemples 3.4.6.** El cos dels nombres complexos és un espai vectorial de dimensió 2 sobre el cos dels nombres reals; per tant,  $[\mathbb{C} : \mathbb{R}] = 2$ .

Siguin  $\bar{k}$  un cos algebraicament tancat,  $k \subseteq \bar{k}$  un subcòs, i  $f(X) \in k[X]$  un polinomi irreductible qualsevol. Si considerem  $\theta \in \bar{k}$  una arrel de  $f(X)$  i  $K := k[\theta] = k(\theta)$ , resulta que  $K \simeq k[X]/(f(X))$ , de manera que  $[K : k] = \text{gr}(f(X))$ . Per exemple, si  $n \geq 1$  i  $\zeta$  és una arrel primitiva  $n$ -èsima de la unitat en  $\mathbb{C}$ , tenim que  $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$ .

D'altra banda, com que tot espai vectorial de dimensió finita o numerable sobre un cos numerable és numerable, i com que ni  $\mathbb{R}$  ni  $\mathbb{C}$  no són numerables, tenim que  $[\mathbb{R} : \mathbb{Q}]$  i  $[\mathbb{C} : \mathbb{Q}]$  no són numerables; ni, molt menys, finits.

**Proposició 3.4.7.** *Sigui  $K|k$  una extensió finita de cossos. Llavors,  $K|k$  és algebraica.*

**DEMOSTRACIÓ:** Sigui  $\theta \in K$  un element qualsevol; volem veure que  $\theta$  és algebraic sobre  $k$ . La dimensió de  $K$  com a  $k$ -espai vectorial és finita, posem  $n := [K : k]$ . Llavors, el conjunt de les  $n+1$  primeres potències de  $\theta$ ,  $\{1, \theta, \theta^2, \dots, \theta^n\}$ , és  $k$ -linealment dependent i, en conseqüència, existeixen elements  $a_0, a_1, \dots, a_n \in k$ , no tots nuls, tals que  $\sum_{i=0}^n a_i \theta^i = 0$ ; és a dir, existeix un polinomi no nul  $f(X) := \sum_{i=0}^n a_i X^i \in k[X]$  tal que  $f(\theta) = 0$ . Per tant,  $\theta$  és algebraic sobre  $k$ .  $\square$

**Proposició 3.4.8** (Comportament del grau en torres d'extensions). *Siguin  $k \subseteq K \subseteq L$  extensions de cossos; se satisfà la igualtat  $[L : k] = [L : K][K : k]$ .*

DEMOSTRACIÓ: Siguin  $\{\eta_i\}_{i \in I}$  una  $k$ -base de  $K$  i  $\{\theta_j\}_{j \in J}$  una  $K$ -base de  $L$ , de manera que  $[K : k] = \#I$  i  $[L : K] = \#J$ . Si veiem que  $\{\eta_i \theta_j\}_{(i,j) \in I \times J}$  és una  $k$ -base de  $L$ , ja haurem acabat, perquè  $\#(I \times J) = \#I \times \#J$ .

Sigui  $\theta \in L$  un element qualsevol; com que  $\{\theta_j\}_{j \in J}$  és una  $K$ -base de  $L$ , existeix una família d'elements  $\{\alpha_j\}_{j \in J}$ ,  $\alpha_j \in K$ , gairebé tots nuls, tals que  $\theta = \sum_{j \in J} \alpha_j \theta_j$ . Ara, com que  $\{\eta_i\}_{i \in I}$  és una  $k$ -base de  $K$ , per a cada  $j \in J$  existeix una família d'elements  $\{a_{i,j}\}_{i \in I}$ ,  $a_{i,j} \in k$ , gairebé tots nuls, i tots nuls si  $\alpha_j = 0$ , tals que  $\alpha_j = \sum_{i \in I} a_{i,j} \eta_i$ . En conseqüència, el conjunt de parelles  $(i,j) \in I \times J$  tals que  $a_{i,j} \neq 0$  és finit i  $\theta = \sum_{(i,j) \in I \times J} a_{i,j} \eta_i \theta_j$ ; això és, el conjunt  $\{\eta_i \theta_j\}_{(i,j) \in I \times J}$  genera  $L$  com a  $k$ -espai vectorial.

D'altra banda, si  $\theta = 0$ , d'una expressió com  $0 = \sum_{(i,j) \in I \times J} a_{i,j} \eta_i \theta_j$ , obtenim que, per a tot  $j \in J$ , és  $\alpha_j := \sum_{i \in I} a_{i,j} \eta_i = 0$ , de manera que, per a tot  $j \in J$  i per a tot  $i \in I$ , és  $a_{i,j} = 0$ . Així, només hi ha una manera d'escriure 0 com a combinació  $k$ -lineal del conjunt  $\{\eta_i \theta_j\}_{(i,j) \in I \times J}$ ; per tant, aquests elements de  $L$  són  $k$ -linealment independents.  $\square$

**Corol·lari 3.4.9.** *Siguin  $k \subseteq K \subseteq L$  cossos tals que  $L|k$  és una extensió finita. Llavors, els graus  $[L : K]$  i  $[K : k]$  divideixen  $[L : k]$ .  $\square$*

**Observació 3.4.10.** Certament, aquesta proposició s'aplica d'una manera especial en el cas de les extensions finites; i les extensions finites de cossos tenen, per a nosaltres, una importància cabdal. En efecte; siguin  $\bar{k}$  un cos algebraicament tancat,  $k \subseteq \bar{k}$  un subcòs, i  $f(X) \in k[X]$  un polinomi no nul de coeficients en  $k$ . Siguin  $\theta_1, \dots, \theta_n$  les arrels de  $f(X)$  en  $\bar{k}$  i considerem la successió de subcossos de  $\bar{k}$

$$k \subseteq k(\theta_1) \subseteq k(\theta_1, \theta_2) \subseteq \dots \subseteq k(\theta_1, \dots, \theta_n).$$

Cada extensió  $k(\theta_1, \dots, \theta_{i+1})|k(\theta_1, \dots, \theta_i)$  és finita, de manera que, en virtut de la proposició,  $K := k(\theta_1, \dots, \theta_n)$  és un cos extensió finita de  $k$ .

**Corol·lari 3.4.11.** *Donat un polinomi  $f(X) \in k[X]$ , existeix una extensió finita  $K|k$  tal que  $K$  conté totes les arrels de  $f(X)$ .  $\square$*

**Definició 3.4.12.** Siguin  $k$  un subcòs d'un cos algebraicament tancat  $\bar{k}$ ,  $f(X) \in k[X]$  un polinomi no nul, i  $\theta_1, \theta_2, \dots, \theta_n \in \bar{k}$  les arrels de  $f(X)$  en  $\bar{k}$ . El subcòs  $k(\theta_1, \dots, \theta_n) \subseteq \bar{k}$  generat per  $k$  i les arrels de  $f(X)$  s'anomena el *cos de descomposició de  $f(X)$  en  $\bar{k}$* .

**3.4.13.** Si  $L|k$  és una extensió algebraica de cossos, llavors,  $L = \bigcup_K K$ , on  $K$  recorre els conjunt dels cossos  $k \subseteq K \subseteq L$  tals que  $K|k$  és una subextensió finita de  $L|k$ . En efecte; com que tot element  $\theta \in L$  és algebraic sobre  $k$ , la subextensió  $k(\theta)|k$  de  $L|k$  és finita, de manera que  $\theta \in \bigcup_K K$ ; això és,  $L \subseteq \bigcup_K K$ . L'altra inclusió és òbvia.

**Exercici 3.4.14.** Siguin  $K$  un cos i  $k \subseteq K$  un subcòs qualsevol. Llavors,  $K = \bigcup_F k(F)$ , on  $F$  recorre els subconjunts finits de  $K$  i, si  $F$  és el conjunt  $\{\theta_1, \dots, \theta_n\}$ ,  $k(F)$  denota el cos  $k(\theta_1, \dots, \theta_n)$ .

**Lema 3.4.15.** Siguin  $k \subseteq K \subseteq L$  extensions de cossos i  $\theta \in L$  un element algebraic sobre  $k$ . Llavors  $[K(\theta) : K] \leq [k(\theta) : k]$ .

DEMOSTRACIÓ: Sigui  $f(X) := \text{Irr}(\theta, k)(X) \in k[X]$  el polinomi minimal de  $\theta$  sobre  $k$ . Com que  $k \subseteq K$ , també és  $f(X) \in K[X]$  i  $f(\theta) = 0$ ; així, el polinomi  $\text{Irr}(\theta, K)(X)$  divideix  $f(X)$ ; i, per tant,  $[K(\theta) : K] = \text{gr}(\text{Irr}(\theta, K)(X)) \leq \text{gr}(f(X)) = [k(\theta) : k]$ .  $\square$

**Definició 3.4.16.** Siguin  $\bar{k}$  un cos algebraicament tancat, i  $k \subseteq K \subseteq \bar{k}$  i  $k \subseteq L \subseteq \bar{k}$  subcossos. Anomenarem *compost* de  $K$  i  $L$ , o bé *cos composició* de  $K$  i  $L$ , el subcòs  $KL \subseteq \bar{k}$  generat per  $K$  i  $L$ ; o sigui, el menor subcòs de  $\bar{k}$  que conté  $K$  i conté  $L$ .

**Proposició 3.4.17.** Mantinguem les notacions de la definició 3.4.16.

- (a) Comportament del grau per canvi de base. Si l'extensió  $L|k$  és finita, llavors l'extensió  $KL|K$  és finita i  $[KL : K] \leq [L : k]$ .
- (b) Comportament del grau per composició. Si les extensions  $K|k$  i  $L|k$  són finites, l'extensió  $KL|k$  és finita i  $[KL : k] \leq [L : k][K : k]$ .

**3.4.18.** Podem resumir aquest resultat en els diagrames següents.

Per al canvi de base, tenim que  $u \leq w$ ; en particular, si  $L|k$  és finita, llavors  $KL|K$  també és finita:

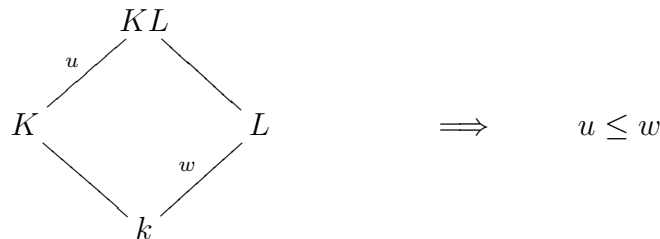


Diagrama 3.1: Comportament del grau per canvi de base

Per a la composició, tenim que  $m = u \cdot t = v \cdot w \leq t \cdot w$ ; en particular, si  $L|k$  i  $K|k$  són finites, llavors  $KL|k$  també és finita:

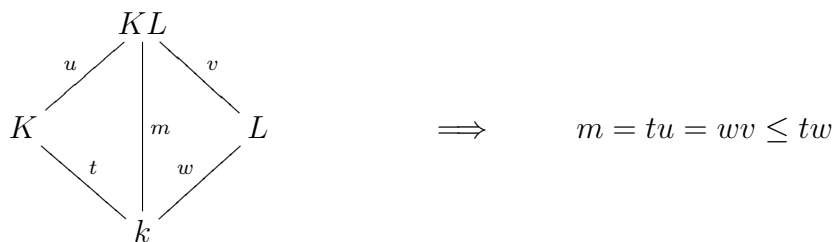


Diagrama 3.2: Comportament del grau per composició

DEMOSTRACIÓ: Si  $L|k$  és una extensió finita, existeixen elements de  $L$ , posem  $\theta_1, \dots, \theta_n$ , tals que  $L = k(\theta_1, \dots, \theta_n)$ ; llavors,  $KL = K(\theta_1, \dots, \theta_n)$ . Com que cada element  $\theta_i$  és algebraic sobre  $k$ , també ho és sobre  $K$ , i podem calcular els graus  $[KL : K]$  i  $[L : k]$  per multiplicació, respectivament, dels graus  $[K(\theta_1, \dots, \theta_{i+1}) : K(\theta_1, \dots, \theta_i)]$  i  $[k(\theta_1, \dots, \theta_{i+1}) : k(\theta_1, \dots, \theta_i)]$ . Com que els primers són, un a un, menors o iguals que els darrers, això demostra la primera afirmació. La segona es dedueix immediatament de la primera i de la multiplicativitat del grau en torres d'extensions:

$$[KL : k] = [KL : K][K : k] \leq [L : k][K : k]. \square$$

### 3.5 Cossos ciclotòmics

**Proposició 3.5.1.** *Siguin  $m, n \in \mathbb{N}$  nombres naturals no nuls i primers entre si. Se satisfà la igualtat  $\varphi(mn) = \varphi(m)\varphi(n)$ .*

DEMOSTRACIÓ: De la definició de la funció  $\varphi$  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  $\text{mcd}(m, n) = 1$ , el morfisme d'anells  $\mathbb{Z} \rightarrow (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$ , 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. Ara bé, com que  $((\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z}))^* = (\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*$ , resulta que  $\varphi(mn) = \varphi(m)\varphi(n)$ , com volem demostrar.  $\square$

**3.5.2 (Notació).** Per a tot nombre natural  $m$ , denotem per  $\zeta_m$  una arrel primitiva  $m$ -èsima qualsevol de la unitat de  $\mathbb{C}$ .

**Proposició 3.5.3.** *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  $\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}$ .*

DEMOSTRACIÓ: Podem considerar el diagrama d'inclusions de cossos

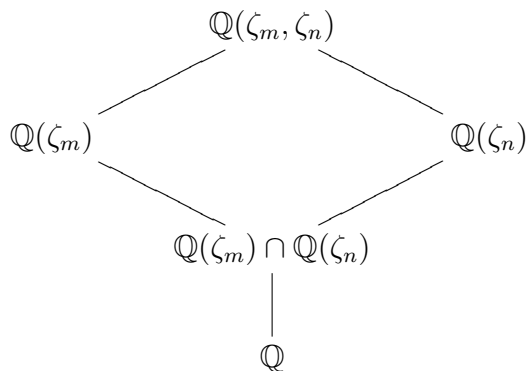


Diagrama 3.3: Composició de cossos ciclotòmics

Sigui  $\zeta := \zeta_m\zeta_n$ . Comencem per veure que  $\mathbb{Q}(\zeta_m, \zeta_n) = \mathbb{Q}(\zeta) = \mathbb{Q}(\zeta_{mn})$ . Com que



$\text{mcd}(m, n) = 1$ ,  $\zeta$  és una arrel primitiva  $mn$ -èsima de la unitat  $i$ , per tant,  $\mathbb{Q}(\zeta) = \mathbb{Q}(\zeta_{mn})$ . D'altra banda, la inclusió  $\mathbb{Q}(\zeta_m, \zeta_n) \supseteq \mathbb{Q}(\zeta)$  és clara, perquè  $\zeta = \zeta_m \zeta_n \in \mathbb{Q}(\zeta_m, \zeta_n)$ . I com que  $\zeta^m$  és una arrel primitiva  $n$ -èsima de la unitat,  $\zeta_n$  és una potència de  $\zeta^m$  i, per tant, una potència de  $\zeta$ , de manera que  $\mathbb{Q}(\zeta_n) \subseteq \mathbb{Q}(\zeta)$ . I, anàlogament,  $\mathbb{Q}(\zeta_m) \subseteq \mathbb{Q}(\zeta)$ ; per tant,  $\mathbb{Q}(\zeta_m, \zeta_n) \subseteq \mathbb{Q}(\zeta)$ .

La igualtat d'aquests cossos ens permet escriure les igualtats següents entre els graus:  $[\mathbb{Q}(\zeta_m, \zeta_n) : \mathbb{Q}(\zeta_n)]\varphi(n) = [\mathbb{Q}(\zeta_m, \zeta_n) : \mathbb{Q}(\zeta_n)][\mathbb{Q}(\zeta_n) : \mathbb{Q}] = [\mathbb{Q}(\zeta_m, \zeta_n) : \mathbb{Q}] = \varphi(mn) = \varphi(m)\varphi(n)$ ; per tant,  $[\mathbb{Q}(\zeta_m, \zeta_n) : \mathbb{Q}(\zeta_n)] = \varphi(m)$ . D'altra banda, totes les desigualtats  $\varphi(m) = [\mathbb{Q}(\zeta_m, \zeta_n) : \mathbb{Q}(\zeta_n)] \leq [\mathbb{Q}(\zeta_m) : \mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n)] \leq [\mathbb{Q}(\zeta_m) : \mathbb{Q}] = \varphi(m)$  són igualtats; o sigui,  $[\mathbb{Q}(\zeta_m) : \mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n)] = [\mathbb{Q}(\zeta_m) : \mathbb{Q}]$ ; i això implica la igualtat  $\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}$ .  $\square$

La demostració que hem fet d'aquest resultat es pot adaptar immediatament per a demostrar el resultat següent, més general.

**Proposició 3.5.4.** *Siguin  $\bar{k}$  un cos i  $k$ ,  $K_1, K_2$ , subcossos de  $\bar{k}$  tals que  $k \subseteq K_1 \cap K_2$ . Suposem que l'extensió  $K_1 K_2 | k$  és finita i que  $[K_1 K_2 : k] = [K_1 : k][K_2 : k]$ . Llavors,  $K_1 \cap K_2 = k$ .  $\square$*

**3.5.5.** Hom podria estar temptat de pensar que el recíproc del resultat anterior també és veritat; és a dir, que si  $K_1 \cap K_2 = k$ , llavors  $[K_1 K_2 : k] = [K_1 : k][K_2 : k]$ . Però això és, en general, fals.

Per a donar-ne un exemple, considerem  $\theta_1, \theta_2 \in \mathbb{C}$  dues arrels diferents del polinomi  $X^3 - 2 \in \mathbb{Q}[X]$  i siguin  $K_1 := \mathbb{Q}(\theta_1)$  i  $K_2 := \mathbb{Q}(\theta_2)$ . Anem a veure que:

- (a)  $[K_1 : \mathbb{Q}] = [K_2 : \mathbb{Q}] = 3$ .
- (b)  $K_1 \neq K_2$ .
- (c)  $K_1 \cap K_2 = \mathbb{Q}$ .
- (d)  $[K_1 K_2 : \mathbb{Q}] = 6$ .

El polinomi  $X^3 - 2$  és irreductible en  $\mathbb{Q}[X]$ , d'on  $[K_1 : \mathbb{Q}] = [K_2 : \mathbb{Q}] = \text{gr}(X^3 - 2) = 3$ .

Com que el grau de l'extensió  $K_1 | \mathbb{Q}$  és primer, no pot haver-hi cap cos entre  $\mathbb{Q}$  i  $K_1$  diferent dels  $\mathbb{Q}$  i  $K_1$ ; per tant, si veiem (b) també tenim (c). I per a veure (b), observem que per al nombre  $\rho := \frac{\theta_2}{\theta_1}$  tenim que  $\rho^2 + \rho + 1 = 0$ , perquè  $\rho^3 = 1$ , però  $\rho \neq 1$ . Ara, si fos  $K_1 = K_2$ , tindriem que  $\rho \in K_1$ , de manera que  $\mathbb{Q}(\rho) \subseteq K_1$ ; però  $\rho$  satisfà un polinomi irreductible de grau 2 sobre  $\mathbb{Q}$ , de manera que  $K_1$  contindria una extensió de grau 2, i aquest fet és impossible perquè el grau  $[K_1 : \mathbb{Q}]$  no és parell.

Finalment,  $K_1 K_2 = K_1(\rho)$ , ja que, si un cos conté  $\theta_1$ , condició necessària i suficient perquè contingui  $\theta_2$  és que contingui  $\rho$ . Així,  $K_1 K_2 | \mathbb{Q}$  és la composició de les extensions  $K_1 | \mathbb{Q}$ , de grau 3, i  $\mathbb{Q}(\rho) | \mathbb{Q}$ , de grau 2, de manera que  $[K_1 K_2 : \mathbb{Q}] \leq [K_1 : \mathbb{Q}][\mathbb{Q}(\rho) : \mathbb{Q}] = 6$ . Ara,  $K_1 K_2 | \mathbb{Q}$  és una extensió de grau menor o igual que sis, divisible per 3 (ja que conté  $K_1 | \mathbb{Q}$ ), i estrictament més gran que 3 (ja que  $K_1 K_2$  conté estrictament  $K_1$ , perquè  $K_1 \neq K_2$ ); per tant,  $[K_1 K_2 : \mathbb{Q}] = 6$ .  $\square$

**Observació 3.5.6.** La part final d'aquesta prova s'hauria pogut demostrar més fàcilment amb l'ajut del resultat següent, la demostració del qual es deixa com a exercici.

**Proposició 3.5.7.** *Siguin  $\bar{k}$  un cos, i  $k, K_1, K_2$ , subcossos de  $\bar{k}$  tals que  $k \subseteq K_1 \cap K_2$ . Suposem que les extensions  $K_1|k$  i  $K_2|k$  són finites i que  $[K_1 : k]$  i  $[K_2 : k]$  són primers entre si. Llavors,  $K_1 K_2|k$  és finita,  $[K_1 K_2 : k] = [K_1 : k][K_2 : k]$ , i  $K_1 \cap K_2 = k$ .  $\square$*

### 3.6 Cossos quadràtics

En aquesta secció classifiquem els cossos quadràtics sobre qualsevol cos  $k$  de característica diferent de 2.

**Proposició 3.6.1.** *Siguin  $\bar{k}$  un cos algebraicament tancat de característica diferent de 2 i  $k \subseteq K \subseteq \bar{k}$  subcossos tals que  $[K : k] = 2$ . Llavors, existeix  $\theta \in K$  tal que  $K = k(\theta)$ ,  $d := \theta^2 \in k$ , el polinomi  $f(X) := X^2 - d \in k[X]$  és irreductible en  $k[X]$ , i  $K$  és el cos de descomposició de  $f(X)$ .*

DEMOSTRACIÓ: Com que  $[K : k] = 2$ , existeix  $\eta \in K$  tal que  $\eta \notin k$ ; llavors,  $\{1, \eta\}$  és una  $k$ -base de  $K$  i  $\eta^2$  és combinació lineal, de coeficients en  $k$ , de 1 i  $\eta$ . Sigui  $b, c \in k$  tals que  $\eta^2 + b\eta + c = 0$ , i prenem  $\theta := 2\eta + b \in K$ ; llavors,  $\theta^2 = 4\eta^2 + 4b\eta + b^2 = b^2 - 4c =: d \in k$ ,  $K = k(\eta) = k(\theta)$ , el polinomi  $f(X) := X^2 - d \in k[X]$  és irreductible (ja que és de grau 2 i no té arrels en  $k$ ), i  $K$  és el seu cos de descomposició, perquè les arrels de  $f(X)$  són  $\theta$  i  $-\theta$ , pertanyen a  $K$ , i no pertanyen a  $k$ .  $\square$

**3.6.2.** Si  $\text{car}(\bar{k}) \neq 2$  i si  $\theta, \eta \in \bar{k}$  són elements tals que  $\theta^2, \eta^2 \in k$  però  $\theta, \eta \notin k$ , ens preguntem en quines condicions és  $k(\theta) = k(\eta)$ .

Suposem que se satisfà la igualtat  $k(\theta) = k(\eta)$ . Com que  $\{1, \theta\}$  és una  $k$ -base de  $k(\theta)$ , existeixen elements  $a, b \in k$  tals que  $\eta = a + b\theta$ ; i, com que  $\theta^2, (a^2 + b^2\theta^2) + 2ab\theta = \eta^2 \in k$ , ha d'ésser  $2ab = 0$ . Ara, si fos  $b = 0$ , seria  $\eta = a \in k$ , contràriament a la nostra suposició; per tant, és  $b \neq 0$  i, com que  $2 \neq 0$ , ha d'ésser  $a = 0$ , de manera que  $\eta = b\theta$ , amb  $b \in k$ ,  $b \neq 0$ .

Recíprocament, si  $\eta = b\theta$ , amb  $b \in k$ ,  $b \neq 0$ , és clar que  $k(\eta) = k(\theta)$  i que  $\eta^2 = b^2\theta^2 \in k$ .

**3.6.3.** Per tant, cada subcòs  $K \subseteq \bar{k}$  quadràtic sobre  $k$  determina unívocament una classe no trivial en  $k^*/k^{*2}$ : la classe d'un element  $d = \theta^2 \in k^*$  tal que  $K = k(\theta)$ . I aquesta assignació proporciona una aplicació injectiva del conjunt dels subcossos  $K \subseteq \bar{k}$  quadràtics sobre  $k$  en el conjunt  $k^*/k^{*2}$ .

D'altra banda, donat un element qualsevol  $d \in k^*$ , el cos de descomposició sobre  $k$  del polinomi  $X^2 - d \in k[X]$  només depèn de la classe de  $d$  en  $k^*/k^{*2}$  i és quadràtic sobre  $k$ , llevat del cas en què  $d \in k^{*2}$ , per al qual el cos de descomposició és el propi cos  $k$ . En conseqüència, l'aplicació anterior és exhaustiva en el conjunt de les classes no trivials de  $k^*/k^{*2}$ .

En resum, això prova el resultat següent.

**Proposició 3.6.4.** *Siguin  $\bar{k}$  un cos algebraicament tancat de característica diferent de 2 i  $k \subseteq \bar{k}$  un subcòs. Existeix una correspondència bijectiva entre el conjunt de les subextensions  $K|k$  de  $\bar{k}|k$  tals que  $[K : k] \leq 2$  i el grup abelià quocient  $k^*/k^{*2}$ ; la correspondència es pot establir de manera que el cos  $k$  es correspongui amb la classe  $k^{*2}$ , dels quadrats de  $k^*$ .  $\square$*

Per al cas de les extensions del cos dels nombres racionals, i com que podem caracteritzar el grup abelià quocient  $\mathbb{Q}^*/\mathbb{Q}^{*2}$  d'una manera molt senzilla, obtenim una descripció molt senzilla dels subcossos de  $\mathbb{C}$  quadràtics sobre  $\mathbb{Q}$ .

**Corol·lari 3.6.5.** *Existeix una correspondència bijectiva entre el conjunt dels subcossos de  $\mathbb{C}$  quadràtics sobre  $\mathbb{Q}$  i el conjunt dels nombres enters lliures de quadrats.*

**DEMOSTRACIÓ:** Donat un nombre enter lliure de quadrats,  $a$ , podem pensar en la seva classe en  $\mathbb{Q}^*/\mathbb{Q}^{*2}$ . Si  $a, b$  són nombres enters lliures de quadrats i diferents, les seves classes en  $\mathbb{Q}^*/\mathbb{Q}^{*2}$  també són diferents, ja que si  $a = bq^2$ , amb  $q \in \mathbb{Q}^*$ , i si posem  $q = \frac{r}{s}$ ,  $r, s \in \mathbb{Z}$ ,  $s \neq 0$ , és  $as^2 = br^2$ , de manera que, en virtut de la descomposició única en factors primers de  $\mathbb{Z}$ , és  $a = b$ . D'altra banda, donat  $q \in \mathbb{Q}^*$ , posem  $q = \frac{a}{b}$ , amb  $a, b \in \mathbb{Z}$ ,  $\text{mcd}(a, b) = 1$ ; llavors, en  $\mathbb{Q}^*/\mathbb{Q}^{*2}$ , és  $q = ab$ ; per tant, tot element de  $\mathbb{Q}^*/\mathbb{Q}^{*2}$  té un representant enter; i, encara, podem suposar que aquest representant no és divisible pel quadrat de cap nombre enter, excepte 1. Així, existeix una bijecció entre el conjunt dels nombres enters lliures de quadrats i  $(\mathbb{Q}^*/\mathbb{Q}^{*2}) - \{1\}$ .  $\square$

**Observació 3.6.6.** En el cas de característica 2 hom disposa d'un resultat similar, però no n'hi ha prou a considerar el grup quocient  $k^*/k^{*2}$ . Per exemple, si  $k = \mathbb{Z}/2\mathbb{Z}$ , en  $k[X]$  només hi ha un polinomi irreductible de grau 2, el polinomi  $X^2 + X + 1$ , que dóna una única extensió de  $k$  de grau 2, mentre que  $k^*/k^{*2}$  només té un element, que es correspon amb l'extensió trivial  $k | k$ . Discutim aquest cas en el capítol següent.

## 3.7 Grup de Galois dels cossos ciclotòmics

Sigui  $\zeta_n \in \mathbb{C}$  una arrel primitiva  $n$ -èsima qualsevol de la unitat,  $n \geq 2$ , i considerem el cos ciclotòmic  $\mathbb{Q}(\zeta_n)$ . Ja hem vist que, si  $r$  és un nombre natural primer amb  $n$ ,  $\zeta_n^r$  també és una arrel primitiva  $n$ -èsima de la unitat. Una pregunta que ens podem fer de manera natural és: quin efecte té el canvi de  $\zeta_n$  per  $\zeta_n^r$  en el cos  $\mathbb{Q}(\zeta_n)$ ? Dit d'una altra manera, canviar una solució de l'equació  $\Phi_n(X) = 0$  per una altra, quin efecte té en el cos que conté les solucions de l'equació?

**3.7.1.** Comencem per recordar que  $\mathbb{Q}(\zeta_n^r) \subseteq \mathbb{Q}(\zeta_n)$ ; però, si  $\text{mcd}(n, r) = 1$ , llavors  $\zeta_n$  també és una potència de  $\zeta_n^r$ , ja que  $\zeta_n^r$  és una arrel primitiva  $n$ -èsima de la unitat; per tant,  $\mathbb{Q}(\zeta_n^r) = \mathbb{Q}(\zeta_n)$ .

**3.7.2.** En segon lloc, l'isomorfisme  $\mathbb{Q}[X]/(\Phi_n(X)) \cong \mathbb{Q}(\zeta_n)$  s'obté identificant la classe de  $X$  amb  $\zeta_n$ ; d'altra banda, també és  $\mathbb{Q}[X]/(\Phi_n(X)) \cong \mathbb{Q}(\zeta_n^r)$ , i l'isomorfisme identifica la classe de  $X$  amb  $\zeta_n^r$ . Per tant, la composició d'un isomorfisme amb l'invers de l'altre proporciona un automorfisme de  $\mathbb{Q}(\zeta_n)$  que identifica  $\zeta_n$  amb  $\zeta_n^r$ . Podem resumir aquest fet en el resultat següent.

**Proposició 3.7.3.** *Siguin  $n, r$  nombres naturals tals que  $\text{mcd}(n, r) = 1$ ,  $\zeta_n \in \mathbb{C}$  una arrel primitiva  $n$ -èsima de la unitat, i  $\mathbb{Q}(\zeta_n)$  el  $n$ -èsim cos ciclotòmic sobre  $\mathbb{Q}$ . Existeix un únic automorfisme  $\sigma_r : \mathbb{Q}(\zeta_n) \rightarrow \mathbb{Q}(\zeta_n)$  tal que  $\sigma_r(\zeta_n) = \zeta_n^r$ .*

**DEMOSTRACIÓ:** Ja hem provat l'existència; vegem-ne la unicitat. Com que  $\zeta_n$  és un generador de  $\mathbb{Q}(\zeta_n)$  com a cos sobre  $\mathbb{Q}$ , un morfisme d'anells de  $\mathbb{Q}(\zeta_n)$  queda determinat

per la imatge dels elements de  $\mathbb{Q}$  i la imatge de  $\zeta_n$ . Però si  $\sigma$  és un morfisme de  $\mathbb{Q}$  en un anell qualsevol (per exemple, la restricció a  $\mathbb{Q}$  de  $\sigma_r$ ), ha de ser  $\sigma(1) = 1$ , de manera que  $\sigma(z) = z$ , per a tot nombre enter  $z$ , i, en conseqüència,  $\sigma(q) = q$ , per a tot nombre racional  $q$ . Per tant, la imatge de  $\zeta_n$  determina, com a màxim, un automorfisme de  $\mathbb{Q}(\zeta_n)$ .  $\square$

Així, doncs, el canvi de  $\zeta_n$  per  $\zeta_n^r$  proporciona un automorfisme de  $\mathbb{Q}(\zeta_n)$ . La pregunta immediata és: tot automorfisme de  $\mathbb{Q}(\zeta_n)$  és d'aquest tipus? La resposta és afirmativa; encara més, es pot calcular explícitament l'estructura del grup dels automorfismes del cos  $\mathbb{Q}(\zeta_n)$ .

**Definició 3.7.4.** S'anomena *grup de Galois* de l'extensió  $\mathbb{Q}(\zeta_n)|\mathbb{Q}$  el grup dels automorfismes de  $\mathbb{Q}(\zeta_n)$ , i es denota per  $\text{Gal}(\mathbb{Q}(\zeta_n)|\mathbb{Q})$ .

**3.7.5.** Sigui  $\sigma : \mathbb{Q}(\zeta_n) \rightarrow \mathbb{Q}(\zeta_n)$  un automorfisme qualsevol; la restricció de  $\sigma$  al grup  $\mathbb{Q}(\zeta_n)^*$  és un automorfisme de grups i, com a conseqüència,  $\sigma(\zeta_n)$  és un element d'ordre  $n$  de  $\mathbb{Q}(\zeta_n)^*$ ; és a dir,  $\sigma(\zeta_n)$  també és una arrel primitiva  $n$ -èsima de la unitat; per tant, existeix  $\chi(\sigma) \in \mathbb{Z}$ , definit mòdul  $n$  i primer amb  $n$ , tal que  $\sigma(\zeta_n) = \zeta_n^{\chi(\sigma)}$ . Notem que  $\chi(\sigma) \in (\mathbb{Z}/n\mathbb{Z})^*$ ; per tant, podem considerar una aplicació  $\chi : \text{Gal}(\mathbb{Q}(\zeta_n)|\mathbb{Q}) \rightarrow (\mathbb{Z}/n\mathbb{Z})^*$ .

**Proposició 3.7.6.** L'aplicació  $\chi : \text{Gal}(\mathbb{Q}(\zeta_n)|\mathbb{Q}) \rightarrow (\mathbb{Z}/n\mathbb{Z})^*$ , definida per la igualtat  $\sigma(\zeta_n) = \zeta_n^{\chi(\sigma)}$ , és un isomorfisme de grups, independent de l'arrel primitiva  $n$ -èsima de la unitat  $\zeta_n$  que considerem.

**DEMOSTRACIÓ:** Siguin  $\sigma, \tau \in \text{Gal}(\mathbb{Q}(\zeta_n)|\mathbb{Q})$  qualssevol; llavors, se satisfan les igualtats  $\zeta_n^{\chi(\sigma\tau)} = (\sigma \circ \tau)(\zeta_n) = \sigma(\tau(\zeta_n)) = \sigma(\zeta_n^{\chi(\tau)}) = \sigma(\zeta_n)^{\chi(\tau)} = (\zeta_n^{\chi(\sigma)})^{\chi(\tau)} = \zeta_n^{\chi(\sigma)\chi(\tau)}$ , de manera que  $\chi(\sigma \circ \tau) = \chi(\sigma)\chi(\tau)$ , en  $(\mathbb{Z}/n\mathbb{Z})^*$ ; per tant,  $\chi$  és un morfisme de grups.

D'altra banda, és clar que si  $\chi(\sigma) = \chi(\tau)$ , és  $\sigma(\zeta_n) = \tau(\zeta_n)$ ; però això implica que  $\sigma = \tau$ , ja que  $\sigma$  i  $\tau$  coincideixen sobre un generador de  $\mathbb{Q}(\zeta_n)$  com a cos. Això ens diu que  $\chi$  és un morfisme injectiu.

Finalment, ja hem vist que  $\chi$  és exhaustiu, perquè donat  $r \in (\mathbb{Z}/n\mathbb{Z})^*$ , existeix un automorfisme  $\sigma_r \in \text{Gal}(\mathbb{Q}(\zeta_n)|\mathbb{Q})$  tal que  $\sigma_r(\zeta_n) = \zeta_n^r$ , de manera que  $r = \chi(\sigma_r)$ .

Resta veure que l'isomorfisme  $\chi$  no depèn de l'arrel primitiva  $n$ -èsima de la unitat  $\zeta_n$  que considerem per a definir-lo. Però això és senzill, perquè si considerem que  $\zeta'_n$  és una altra arrel primitiva  $n$ -èsima de la unitat, aleshores existeix  $r \in \mathbb{Z}$  tal que  $\zeta'_n = \zeta_n^r$ ; i, llavors,  $\sigma(\zeta'_n) = \sigma(\zeta_n^r) = \sigma(\zeta_n)^r = \zeta_n^{r\chi(\sigma)} = \zeta_n^{r\chi(\sigma)}$ , com es vol demostrar.  $\square$

**Definició 3.7.7.** L'isomorfisme  $\chi_n : \text{Gal}(\mathbb{Q}(\zeta_n)|\mathbb{Q}) \rightarrow (\mathbb{Z}/n\mathbb{Z})^*$  s'anomena el  $n$ -èsim *caràcter ciclotòmic*.

**Corol·lari 3.7.8.** Per a tot  $n \geq 1$ , és  $\text{Gal}(\mathbb{Q}(\zeta_n)|\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*$ .  $\square$

Per a acabar aquesta secció, observem un cas particular d'un resultat que, més endavant, és clau.

**Proposició 3.7.9.** El subcòs de  $\mathbb{Q}(\zeta_n)$  format pels elements que són fixos per tots els automorfismes de  $\mathbb{Q}(\zeta_n)$  és exactament  $\mathbb{Q}$ .

**DEMOSTRACIÓ:** Siguin  $\zeta := \zeta_n$ ,  $G := \text{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q})$ , i  $K := \mathbb{Q}(\zeta)^G$ , el subcòs de  $\mathbb{Q}(\zeta)$  format pels elements fixos per tots els elements de  $G$ . Clarament,  $\mathbb{Q} \subseteq K \subseteq \mathbb{Q}(\zeta)$ , i

és suficient veure que  $[\mathbb{Q}(\zeta) : K] = [\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$ . En primer lloc, és clar que  $K(\zeta) = \mathbb{Q}(\zeta)$ , de manera que el grau  $[\mathbb{Q}(\zeta) : K]$  és el grau del polinomi  $\text{Irr}(\zeta, K)(X)$ . Sigui  $f(X) := \text{Irr}(\zeta, K)(X) \in K[X]$ ; donat  $\sigma \in G$ , és  $f(\sigma(\zeta)) = \sigma(f(\zeta)) = \sigma(0) = 0$ , ja que  $\sigma$  deixa fixos tots els coeficients de  $f(X)$ , perquè  $f(X) \in K[X]$ . Per tant, tots els elements  $\sigma(\zeta)$ , per a  $\sigma \in G$ , és a dir, totes les arrels primitives  $n$ -èsimes de la unitat, són arrels de  $f(X)$ ; això implica que el grau del polinomi  $f(X)$  és més gran o igual que  $\varphi(n)$ . Però, com que el grau  $[\mathbb{Q}(\zeta) : K]$  és menor o igual que el grau  $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$ , ha de ser  $\text{gr}(f(X)) = \varphi(n)$ , com es vol demostrar.  $\square$

## 3.8 Grup de Galois d'una extensió algebraica

Hem vist més amunt que el Grup de Galois de les extensions ciclotòmiques de  $\mathbb{Q}$  dona compte del canvi d'una solució de l'equació ciclotòmica  $\Phi_n(X) = 0$  per una altra. Ara tractem aquest fenomen amb més generalitat.

**Definició 3.8.1.** Siguin  $K|k$ ,  $L|k$ , extensions d'un mateix cos  $k$ . Anomenem *morfisme d'extensions* de  $K|k$  en  $L|k$ , o bé *k-immersió* del cos  $K$  en el cos  $L$ , tot morfisme de cossos  $\sigma : K \rightarrow L$  tal que  $\sigma(a) = a$ , per a tot  $a \in k$ . Si  $\sigma$  és un isomorfisme, diem que és un *k-isomorfisme* o un *isomorfisme d'extensions*.

**Definició 3.8.2.** Si  $\sigma : K \rightarrow L$  és qualsevol morfisme de cossos, denotem per  ${}^\sigma f(X)$  el polinomi de  $L[X]$  que s'obté en aplicar  $\sigma$  als coeficients del polinomi  $f(X) \in K[X]$ .

**3.8.3.** Si  $\theta \in K$  és una arrel d'un polinomi no nul  $f(X) \in K[X]$ , llavors  $\sigma(\theta) \in L$  és una arrel de  ${}^\sigma f(X)$ . En particular, si  $\sigma$  és una *k-immersió* i  $f(X) \in k[X]$ , llavors  ${}^\sigma f(X) = f(X)$ , de manera que  $\sigma(\theta)$  també és arrel de  $f(X)$ .

**Proposició 3.8.4.** Siguin  $k$  un cos,  $f(X) \in k[X]$  un polinomi irreductible, i  $\theta \in K$ ,  $\theta' \in L$ , arrels de  $f(X)$  en cossos extensió de  $k$ . Per als subcossos  $k(\theta) \subseteq K$  i  $k(\theta') \subseteq L$ , existeix un únic *k-isomorfisme*  $\sigma : k(\theta) \rightarrow k(\theta')$  tal que  $\sigma(\theta) = \theta'$ .

**DEMOSTRACIÓ:** L'isomorfisme  $k(\theta) \cong k[X]/(f(X))$  de (3.3.5) que identifica  $\theta$  amb la classe de  $X$  és un *k-isomorfisme*; per tant, la composició d'aquest amb l'invers de l'anàleg per a  $\theta'$  és un *k-isomorfisme* de  $k[\theta]$  en  $k[\theta']$  que transforma  $\theta$  en  $\theta'$ . A més a més, com que  $\theta$  genera  $k(\theta)$  com a cos extensió de  $k$ , la imatge de  $\theta$  i el fet que  $\sigma(a) = a$  per a tot  $a \in k$  determinen la imatge de tot element de  $k(\theta)$ ; la unicitat, doncs, és immediata.  $\square$

**3.8.5.** Així, el canvi d'una arrel d'un polinomi irreductible  $f(X) \in k[X]$  per una altra proporciona un *k-isomorfisme* entre el cossos que generen sobre  $k$  cadascuna de les arrels. Per tant, no importa quina arrel considerem, si l'afegim a  $k$  obtenim extensions isomorfes de  $k$ .

**3.8.6.** Donats un polinomi irreductible  $f(X) \in k[X]$ , una arrel  $\theta$  de  $f(X)$  en un cos  $K$  extensió de  $k$ , i una *k-immersió*  $\sigma : K \rightarrow L$ , on  $L|k$  és una extensió qualsevol de  $k$ ,  $\sigma(\theta)$  també és una arrel de  $f(X)$  i  $k(\theta)|k$  i  $k(\sigma(\theta))|k$  són extensions isomorfes. Això és, el cos  $\sigma(k(\theta))$  és el cos  $k(\sigma(\theta))$ , i  $\sigma(\theta)$  és una arrel de  $f(X)$ .

**3.8.7.** En el cas particular en què  $k = \mathbb{Q}$  i  $K = \mathbb{Q}(\zeta_n)$ , on  $\zeta_n \in \mathbb{C}$  és una arrel primitiva  $n$ -èsima de la unitat, hem vist que tota *k-immersió* de  $\mathbb{Q}(\zeta_n)$  en  $\mathbb{Q}(\zeta_n)$  és un automorfisme. Aquest resultat és més general, i s'aplica a totes les extensions algebraiques.

**Proposició 3.8.8.** *Sigui  $K|k$  qualsevol extensió algebraica de cossos. Tota  $k$ -immersió  $\sigma : K \rightarrow K$  és un  $k$ -automorfisme de  $K$ .*

DEMOSTRACIÓ: Com que  $\sigma$  és un morfisme d'anells d'un cos en un altre anell,  $\sigma$  és injectiu; vegem-ne l'exhaustivitat. El cas de les extensions finites  $K|k$  és immediat, perquè  $\sigma$  és, en particular, un endomorfisme injectiu del  $k$ -espai vectorial de dimensió finita  $K$  i, per tant, és exhaustiu. El cas general es dedueix del fet que tota extensió algebraica és la reunió de les seves subextensions finites. Vegem-ne els detalls.

Sigui  $\theta' \in K$  un element qualsevol, considerem  $f(X) := \text{Irr}(\theta', k)(X) \in k[X]$  el seu polinomi minimal, i denotem per  $K' \subseteq K$  el subcòs de  $K$  generat per  $k$  i totes les arrels de  $f(X)$  que pertanyin a  $K$ . Volem veure que  $\theta'$  és imatge per  $\sigma$  d'un element de  $K$ . Com que  $f(X)$  només té una quantitat finita d'arrels i totes elles són elements algebraics sobre  $k$ , l'extensió  $K'|k$  és finita. D'altra banda, la restricció de  $\sigma$  a  $K'$  és una  $k$ -immersió de  $K'$  en  $K$ ; però  $\sigma$  envia qualsevol arrel de  $f(X)$  que pertanyi a  $K$  a una altra arrel de  $f(X)$  que pertanyi a  $K$ , de manera que  $\sigma$  aplica  $K'$  en  $K'$ ; això és dir que la restricció de  $\sigma$  a  $K'$  és una  $k$ -immersió de  $K'$  en  $K'$ . Com que  $K'|k$  és finita,  $\sigma : K' \rightarrow K'$  és un automorfisme, de manera que existeix  $\theta \in K' \subseteq K$  tal que  $\sigma(\theta) = \theta'$ , com volem demostrar.  $\square$

**Corol·lari 3.8.9.** *Siguin  $\bar{k}$  un cos algebraicament tancat,  $k \subseteq \bar{k}$  un subcòs qualsevol,  $K|k$  una subextensió de  $\bar{k}|k$ ,  $\theta \in K$  un element algebraic sobre  $k$ ,  $f(X) := \text{Irr}(\theta, k)(X) \in k[X]$  el polinomi minimal de  $\theta$  sobre  $k$ , i  $n := \text{gr}(f(X))$ . El nombre de  $k$ -immersions de  $k(\theta)$  en  $\bar{k}$  és menor o igual que  $n$ .*

DEMOSTRACIÓ: Tota  $k$ -immersió de  $k(\theta)$  en  $\bar{k}$  és determinada per la imatge de  $\theta$  i, a més a més, la imatge de  $\theta$  ha d'ésser una arrel de  $f(X)$ . Per tant, la quantitat de  $k$ -immersions de  $k(\theta)$  en  $\bar{k}$  coincideix amb la quantitat d'arrels diferents de  $f(X)$  en  $\bar{k}$ ; i aquesta quantitat és menor o igual que el grau del polinomi  $f(X)$ .  $\square$

**Definició 3.8.10.** Sigui  $K|k$  una extensió algebraica de cossos. S'anomena *grup de Galois* de l'extensió  $K|k$  el grup  $\text{Gal}(K|k)$  format per tots els  $k$ -automorfismes de  $K$ .

**Corol·lari 3.8.11.** *Siguin  $\bar{k}$  un cos algebraicament tancat,  $k \subseteq \bar{k}$  un subcòs qualsevol, i  $\theta \in \bar{k}$  un element algebraic sobre  $k$ . Llavors,  $\#\text{Gal}(k(\theta)|k) \leq [k(\theta) : k]$ .  $\square$*

**3.8.12.** Hem vist que, en el cas en què  $k = \mathbb{Q}$  i  $\theta = \zeta_n$  és una arrel primitiva  $n$ -èsima de la unitat, se satisfà que  $\text{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*$  i que, en conseqüència, també tenim que  $\#\text{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q}) = \varphi(n) = [\mathbb{Q}(\zeta_n) : \mathbb{Q}]$ . Aquesta propietat no se satisfà per a tots els cossos del tipus  $k(\theta)$ , on  $\theta$  és un element algebraic sobre  $k$ . Per al grup de Galois d'una extensió  $k(\zeta)|k$ , per a una arrel  $n$ -èsima primitiva de la unitat  $\zeta$ , tenim el resultat següent.

**Corol·lari 3.8.13.** *Siguin  $n \geq 1$  un nombre natural,  $\bar{k}$  un cos algebraicament tancat de característica no divisor de  $n$ ,  $k \subseteq \bar{k}$  un subcòs qualsevol,  $\zeta$  una arrel primitiva  $n$ -èsima de la unitat de  $\bar{k}$ , i  $K_n := k(\zeta)$ . El grup de Galois  $\text{Gal}(K_n|k)$  és isomorf a un subgrup de  $(\mathbb{Z}/n\mathbb{Z})^*$ .*

DEMOSTRACIÓ: El caràcter ciclotòmic  $\chi : \text{Gal}(K_n|k) \rightarrow (\mathbb{Z}/n\mathbb{Z})^*$  pot ésser definit de la mateixa manera que per al cas  $\mathbb{Q}(\zeta)|\mathbb{Q}$ , i obtenim també un morfisme injectiu de grups (cf. 3.7.6).  $\square$

**3.8.14.** En general, no podem esperar que  $\chi$  sigui exhaustiu. Per exemple, si  $k := \mathbb{Q}(\zeta_n)$ , és clar que el grup  $\text{Gal}(k|k) = \{1\}$  no es pot aplicar de manera exhaustiva en  $(\mathbb{Z}/n\mathbb{Z})^*$ , per a  $n > 2$ . D'altra banda, pel què fa a la igualtat  $\#\text{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q}) = [\mathbb{Q}(\zeta) : \mathbb{Q}]$ , a continuació mostrem exemples que ens ensenyen que una igualtat anàloga no se satisfà en general.

**Exemple 3.8.15.** Sigui  $\theta \in \mathbb{C}$  una arrel del polinomi irreductible  $f(X) := X^3 - 2 \in \mathbb{Q}[X]$ . Llavors,  $[\mathbb{Q}(\theta) : \mathbb{Q}] = 3$ , mentre que  $\text{Gal}(\mathbb{Q}(\theta)|\mathbb{Q}) = \{1\}$ . En efecte, siguin  $\theta, \theta', \theta'' \in \mathbb{C}$  les tres arrels diferents de  $f(X)$  i  $K := \mathbb{Q}(\theta, \theta', \theta'') = \mathbb{Q}(\theta, \theta')$  el cos de descomposició de  $f(X)$  sobre  $\mathbb{Q}$ . Sigui  $\rho \in \mathbb{C}$  una arrel primitiva cúbica de la unitat de  $\mathbb{C}$ . Llavors,  $K = \mathbb{Q}(\theta, \rho)$ , de manera que  $[K : \mathbb{Q}] = 6$  (cf. l'exemple 3.5.5) i, com a conseqüència,  $K \neq \mathbb{Q}(\theta)$ . Això ens diu que  $\theta' \notin \mathbb{Q}(\theta)$  i, anàlogament,  $\theta'' \notin \mathbb{Q}(\theta)$ ; com que un automorfisme de  $\mathbb{Q}(\theta)$  és determinat per la imatge de  $\theta$  que, ahora, ha d'ésser una arrel de  $f(X)$ , un tal automorfisme ha d'ésser la identitat. D'on  $\text{Gal}(\mathbb{Q}(\theta)|\mathbb{Q}) = \{1\}$ .

**Exemple 3.8.16.** Siguin  $A := (\mathbb{Z}/2\mathbb{Z})[t]$  l'anell de polinomis en una indeterminada  $t$  i coeficients en  $\mathbb{Z}/2\mathbb{Z}$ ,  $k := (\mathbb{Z}/2\mathbb{Z})(t)$  el seu cos de fraccions.  $f(X) := X^2 - t \in k[X]$ ,  $\theta$  una arrel de  $f(X)$  en un cert cos algebraicament tancat que contingui  $k$ , i  $K$  el cos  $K := k(\theta)$ . El polinomi  $f(X)$  pertany a l'anell de polinomis  $A[X]$ ; per a l'element irreductible  $t \in A$ , el polinomi  $f(X)$  és  $t$ -Eisenstein, de manera que  $f(X)$  és irreductible en  $k[X]$ ; això implica que  $[K : k] = 2$ . D'altra banda, el polinomi  $f(X)$  té una arrel doble, ja que si  $\theta$  és una arrel de  $f(X)$ , llavors  $(X - \theta)^2 = X^2 - \theta^2 = X^2 - t = f(X)$ ; en conseqüència, l'única  $k$ -immersió possible de  $K$  en  $K$  és la identitat, ja que tota  $k$ -immersió de  $K$  en  $K$  ha d'enviar  $\theta$  a  $\theta$ . En conseqüència,  $\text{Gal}(K|k) = \{1\}$ , mentre que  $[K : k] = 2$ .

**3.8.17.** Disposem, doncs, de dos exemples en els quals succeeixen fets molt diferents. D'una banda, hem provat que si  $\theta$  és un element algebraic sobre un cos  $k$ , llavors  $\#\text{Gal}(k(\theta)|k) \leq [k(\theta) : k]_s \leq [k(\theta) : k]$ , on  $[k(\theta) : k]_s$  denota, momentàniament, el nombre de  $k$ -immersió diferents de  $k(\theta)$  en un cos algebraicament tancat que conté  $k$  i  $\theta$ . D'altra banda, en el cas en què  $\theta = \zeta_n$  és una arrel primitiva  $n$ -èsima de la unitat, hem vist que

$$\#\text{Gal}(\mathbb{Q}(\zeta_n)|\mathbb{Q}) = [\mathbb{Q}(\zeta_n) : \mathbb{Q}]_s = [\mathbb{Q}(\zeta_n) : \mathbb{Q}];$$

en el cas en què  $\theta$  és una arrel de  $X^3 - 2$ , hem vist que

$$\#\text{Gal}(\mathbb{Q}(\theta)|\mathbb{Q}) = 1 < [\mathbb{Q}(\theta) : \mathbb{Q}]_s = [\mathbb{Q}(\theta) : \mathbb{Q}] = 3;$$

i en el darrer cas, hem vist que

$$\#\text{Gal}(k(\theta)|k) = 1 = [k(\theta) : k]_s < [k(\theta) : k] = 2.$$

Encara es pot donar un altre cas. Si considerem  $A$  i  $k$  com en l'exemple (3.8.16), però canviem el polinomi  $f(X)$  pel polinomi  $g(X) := X^6 - t \in k[X]$  i  $K$  denota ara  $K := k(\theta)$ , per a una arrel  $\theta$  de  $g(X)$ , podem observar que  $g(X)$  té tres arrels diferents dobles, però  $K$  només en conté una; per tant, tenim que

$$\#\text{Gal}(k(\theta)|k) = 1 < [k(\theta) : k]_s = 3 < [k(\theta) : k] = 6.$$

## 3.9 Extensions normals

Convé que examinem més acuradament els exemples anteriors. Els casos en què se satisfà la igualtat  $\#\text{Gal}(k(\theta)|k) = [k(\theta) : k]_s$  són els casos en què el cos  $k(\theta)$  és el cos de

descomposició del polinomi irreductible  $\text{Irr}(\theta, k)(X) \in k[X]$ ; això és, els casos en què el cos generat sobre  $k$  per una arrel d'un polinomi irreductible  $f(X)$  és el mateix cos que el cos generat sobre  $k$  per totes les arrels de  $f(X)$ . I els casos en què  $\#\text{Gal}(k(\theta)|k) < [k(\theta) : k]_s$ , són els casos en què  $k(\theta)$  no és el cos de descomposició de  $\text{Irr}(\theta, k)(X) \in k[X]$ .

El comportament diferent del polinomi respecte de les seves arrels es fa, doncs, evident. Es tracta d'estudiar més a fons els cossos que són cos de descomposició d'un polinomi. Disposem del resultat següent, que els caracteritza.

**Teorema 3.9.1.** *Siguin  $\bar{k}$  un cos algebraicament tancat i  $k \subseteq K \subseteq \bar{k}$  subcossos tals que l'extensió  $K|k$  és algebraica. Les propietats següents són equivalents:*

- (a) *Existeix una família de polinomis no nuls,  $\{f_i(X)\}_{i \in I}$ ,  $f_i(X) \in k[X]$ , tal que  $K$  és el cos  $K = k(\{\theta \in \bar{k} : \text{existeix } i \in I \text{ i } f_i(\theta) = 0\})$ ; és a dir, el cos de descomposició de tots els polinomis  $f_i(X)$ .*
- (b) *Existeix una família de polinomis irreductibles  $\{f_i(X)\}_{i \in I}$ ,  $f_i(X) \in k[X]$ , tal que  $K$  és el cos de descomposició de tots els polinomis  $f_i(X)$ .*
- (c) *Si  $f(X) \in k[X]$  és un polinomi irreductible i  $K$  conté una arrel de  $f(X)$ , llavors  $K$  conté totes les arrels de  $f(X)$ .*
- (d) *Tota  $k$ -immersió de  $K$  en  $\bar{k}$  és un  $k$ -automorfisme de  $K$ ; és a dir, tota  $k$ -immersió de  $K$  en  $\bar{k}$  té imatge dins  $K$  i és automorfisme de  $K$ .*

*A més a més, si l'extensió  $K|k$  és finita, les propietats anteriors equivalen a la següent:*

- (e) *El nombre de  $k$ -immersions de  $K$  en  $\bar{k}$  coincideix amb  $\#\text{Gal}(K|k)$ .*

**DEMOSTRACIÓ:** La implicació (b)  $\implies$  (a) és evident. Per a veure que (a)  $\implies$  (b), només cal observar que si  $K$  és el cos de descomposició de la família de polinomis  $\{f_i(X)\}_{i \in I}$ ,  $f_i(X) \in k[X]$ , també ho és de la família formada per tots els polinomis irreductibles de  $k[X]$  que són factor d'algun polinomi dels  $f_i(X)$ .

Per a veure que (c)  $\implies$  (b), notem que  $K$  és el cos de descomposició de la família formada per tots els polinomis irreductibles  $\text{Irr}(\theta, k)(X) \in k[X]$  tals que  $\theta \in K$ .

Vegem que (b)  $\implies$  (d). Sigui  $\sigma : K \rightarrow \bar{k}$  una  $k$ -immersió. Volem veure que  $\sigma(K) = K$ . Per a això, considerem  $\theta \in K$  una arrel d'un polinomi  $f(X) := f_i(X) \in k[X]$ ,  $i \in I$ . Com que  $f(\theta) = 0$ , també és  $f(\sigma(\theta)) = 0$ , de manera que  $\sigma(\theta) \in K$ , per la hipòtesi sobre  $K$ ; per tant,  $\sigma(K) \subseteq K$ ; i, com que  $K|k$  és algebraica,  $\sigma : K \rightarrow K$  és un  $k$ -automorfisme de  $K$  (cf. 3.8.8).

Vegem que (d)  $\implies$  (c). Sigui  $f(X) \in k[X]$  un polinomi irreductible i  $\theta \in K$  una arrel de  $f(X)$ ; cal veure que  $K$  conté totes les arrels de  $f(X)$ . Per a això, donada una arrel qualsevol de  $f(X)$ ,  $\theta' \in \bar{k}$ , sigui  $\sigma : k(\theta) \rightarrow k(\theta') \subseteq \bar{k}$  l'únic  $k$ -isomorfisme tal que  $\sigma(\theta) = \theta'$ . Ara, per a veure que  $\theta' \in K$ , utilitzem el resultat següent, que provem més avall.

**Proposició 3.9.2** (Extensió algebraica de morfismes). *Siguin  $\bar{k}$  un cos algebraicament tancat,  $k \subseteq \bar{k}$  un subcòs qualsevol,  $k \subseteq K \subseteq L$  subcossos tals que  $L|k$  és una extensió algebraica, i  $\sigma : K \rightarrow \bar{k}$  una  $k$ -immersió qualsevol. Llavors, existeix una  $k$ -immersió  $\sigma' : L \rightarrow \bar{k}$  tal que la restricció a  $K$  de  $\sigma'$  és  $\sigma$ ; és a dir,  $\sigma'_K = \sigma$ .*



Usem aquesta proposició de la manera següent: Sigui  $\sigma : K \longrightarrow \bar{k}$  una extensió a  $K$  de  $\sigma : k(\theta) \longrightarrow k(\theta') \subseteq \bar{k}$ ; per hipòtesi,  $\sigma$  és un automorfisme de  $K$ , de manera que  $\theta' = \sigma(\theta) \in K$ , com volíem veure.

Resta veure que, en el cas que l'extensió  $K|k$  és finita, les propietats (a), (b), (c) i (d) equivalen a (e). Però és evident que la propietat (e) és equivalent a la propietat (d).  $\square$

**Observació 3.9.3.** Si  $K|k$  és finita, la quantitat de  $k$ -immersió de  $K$  en  $\bar{k}$  és finita. En efecte, existeix una quantitat finita d'elements  $\theta_1, \dots, \theta_n \in K$  tals que  $K = k(\theta_1, \dots, \theta_n)$ ; llavors, tota  $k$ -immersió de  $K$  és determinada per la imatge de tots els  $\theta_i$ , i, per a cada un d'aquests, hi ha una quantitat finita d'imatges possibles.

Cal veure, ara, l'extensió algebraica de morfismes. Per a això, comencem per veure'n un cas particular molt important.

**Lema 3.9.4.** Si  $\bar{K}, \bar{L}$ , són cossos algebraicament tancats,  $K \subseteq \bar{K}$ , un subcòs qualsevol,  $\theta \in \bar{K}$  un element algebraic sobre  $K$ , i  $\sigma : K \longrightarrow \bar{L}$  un morfisme qualsevol de cossos; existeix una extensió de  $\sigma$  a un morfisme  $K(\theta) \xrightarrow{\sigma'} \bar{L}$ .

DEMOSTRACIÓ: Siguin  $f(X) := \text{Irr}(\theta, K)(X) \in K[X]$  el polinomi minimal de  $\theta$  sobre  $K$ ,  $L := \sigma(K) \subseteq \bar{L}$  el cos imatge de  $K$  per  $\sigma$ ,  ${}^\sigma f(X) \in L[X]$  el polinomi que s'obté en aplicar  $\sigma$  als coeficients de  $f(X)$ , i  $\theta' \in \bar{L}$  una arrel de  ${}^\sigma f(X)$ . Com que  $\sigma$  és un isomorfisme de  $K$  en  $L$ , podem estendre  $\sigma$  a un únic isomorfisme  $\sigma : K[X] \longrightarrow L[X]$  tal que  $\sigma(X) = X$ , de manera que el polinomi  ${}^\sigma f(X)$  és irreductible en  $L[X]$ . Aleshores, obtenim isomorfismes de cossos  $K(\theta) \cong K[X]/(f(X)) \cong L[X]/({}^\sigma f(X)) \cong L(\theta')$ , que identifiquen, successivament,  $\theta$  amb la classe de  $X$  en  $K[X]/(f(X))$ , aquesta classe amb la classe de  $X$  en  $L[X]/({}^\sigma f(X))$ , i aquesta amb  $\theta'$ ; per tant, tenim un isomorfisme  $\sigma : K(\theta) \longrightarrow L(\theta') \subseteq \bar{L}$  tal que  $\sigma'(\theta) = \theta'$ . I és clar que la restricció de  $\sigma'$  a  $K$  és  $\sigma$ .  $\square$

Un cop vista l'extensió d'un morfisme de cossos  $\sigma : K \longrightarrow \bar{L}$  a una extensió algebraica de la forma  $K(\theta)$ , cal veure el cas general. La proposició que hem enunciat (i fet servir) més amunt és un cas particular del resultat més general següent, per a la demostració del qual usem el lema de Zorn, que es discuteix en un apèndix (cf. **B.0.23**).

**Proposició 3.9.5.** Sigui  $\bar{L}$  un cos algebraicament tancat,  $K|k$  una extensió algebraica de cossos, i  $\sigma : k \longrightarrow \bar{L}$  un morfisme qualsevol de cossos. Llavors, existeix una extensió de  $\sigma$  a un morfisme  $\sigma : K \longrightarrow \bar{L}$ .

DEMOSTRACIÓ: Sigui  $C$  el conjunt format per les parelles  $(K', \sigma')$  tals que  $k \subseteq K' \subseteq K$ , i  $\sigma' : K' \longrightarrow \bar{L}$  és un morfisme extensió de  $\sigma$ . El conjunt  $C$  conté, evidentment, la parella  $(k, \sigma)$ , de manera que  $C$  és un conjunt no buit.

Donades dues parelles  $(K', \sigma'), (K'', \sigma'') \in C$ , posem  $(K', \sigma') \leq (K'', \sigma'')$  si, i només si,  $K' \subseteq K''$  i la restricció de  $\sigma''$  a  $K'$  és  $\sigma'$ . Llavors, la relació  $\leq$  és una relació d'ordre en  $C$ . Per a aplicar el lema de Zorn al conjunt ordenat  $C$ , cal veure que l'ordre de  $C$  és un ordre inductiu.

Sigui, doncs,  $D \subseteq C$  un subconjunt no buit i totalment ordenat de  $C$ ; cal veure que existeix un element de  $C$  que és una fita superior per al conjunt  $D$ . Sigui  $F$  la reunió de tots els cossos  $K'$  tals que existeix una parella en  $D$  de la forma  $(K', \sigma')$ ; com que el conjunt  $D$  és totalment ordenat,  $F$  és un subcòs de  $K$  que conté  $k$ . D'altra banda, podem definir una aplicació  $\sigma_F : F \longrightarrow \bar{L}$  de la manera següent: donat un element qualsevol

$\theta' \in F$ , existeix una parella  $(K', \sigma') \in D$  tal que  $\theta' \in K'$ ; posem  $\sigma_F(\theta') := \sigma'(\theta')$ . Si  $(K'', \sigma'') \in D$  és una altra parella tal que  $\theta' \in K''$ , i com que l'ordre de  $D$  és total, tenim que  $(K', \sigma') \leq (K'', \sigma'')$  o bé que  $(K'', \sigma'') \leq (K', \sigma')$ ; i, per la definició de la relació  $\leq$ , tenim que  $\sigma'(\theta') = \sigma''(\theta')$ ; per tant,  $\sigma_F$  està ben definida.

Vegem, ara, que  $\sigma_F$  és un morfisme de cossos. Si  $\theta', \theta'' \in F$  són elements qualssevol, existeixen parelles  $(K', \sigma'), (K'', \sigma'') \in D$  tals que  $\theta' \in K'$  i  $\theta'' \in K''$ . De nou, com que  $D$  és un conjunt totalment ordenat, tenim que  $K' \subseteq K''$  o bé  $K'' \subseteq K'$ ; posem que sigui  $K'' \subseteq K'$ ; llavors,  $\theta', \theta'' \in K'$ , de manera que  $\theta' + \theta'', \theta'\theta'' \in K'$  i, en conseqüència,  $\sigma_F(\theta' + \theta'') = \sigma'(\theta' + \theta'') = \sigma'(\theta') + \sigma'(\theta'') = \sigma_F(\theta') + \sigma_F(\theta'')$ , i anàlogament per al producte  $\theta'\theta''$ . Per tant,  $\sigma_F$  és un morfisme de cossos que, clarament, és una extensió de  $\sigma'$ , per a tota parella  $(K', \sigma') \in D$ . Per tant, la parella  $(F, \sigma_F) \in C$  és una fita superior de  $D$ .

Així, el lema de Zorn ens permet deduir que en  $C$  hi ha un element maximal; això és, existeix una parella  $(F, \sigma_F)$  tal que  $k \subseteq F \subseteq K$  i, a més a més,  $\sigma_F : F \rightarrow \bar{L}$  és una extensió de  $\sigma$ , i tal que si  $(F, \sigma_F) \leq (F', \sigma_{F'})$ , per a alguna parella  $(F', \sigma_{F'}) \in C$ , llavors  $F = F'$  i  $\sigma_F = \sigma_{F'}$ . Per a acabar, és suficient veure que  $F = K$ .

Però això és conseqüència del lema anterior. En efecte, si fos  $F \subsetneq K$ , podríem considerar  $\theta \in K$  tal que  $\theta \notin F$ ; el lema ens permet assegurar, doncs, que existiria una extensió de  $\sigma_F$  a un morfisme  $\bar{\sigma}_F : F(\theta) \rightarrow \bar{L}$  que estén  $\sigma_F$ , ja que  $\theta$  és algebraic sobre  $k$  i, per tant, algebraic sobre  $F$ ; de manera que la parella  $(F, \sigma_F)$  no seria un element maximal de  $C$ . Això acaba la demostració.  $\square$

**Definició 3.9.6.** Sigui  $K|k$  una extensió algebraica de cossos. Es diu que l'extensió  $K|k$  és *normal* si satisfà les condicions equivalents del teorema.

**Proposició 3.9.7.** Una extensió finita de cossos  $K|k$  és normal si, i només si,  $K$  és el cos de descomposició d'un polinomi  $f(X) \in k[X]$ .

**DEMOSTRACIÓ:** Si l'extensió  $K|k$  és finita, existeixen elements  $\theta_1, \dots, \theta_n \in K$  tals que  $K = k(\theta_1, \dots, \theta_n)$ . Sigui  $f(X)$  el producte dels polinomis minimalis  $\text{Irr}(\theta_i, k)(X) \in k[X]$ ; llavors,  $f(X) \in k[X]$  i, si  $K$  és normal, llavors  $K$  és el cos de descomposició de  $f(X)$ . El recíproc és evident.  $\square$

**Exemples 3.9.8.** Tota extensió quadràtica de cossos és normal. D'altra banda, de les extensions de cossos considerades més amunt, les  $\mathbb{Q}(\zeta)|\mathbb{Q}$ ,  $k(\zeta)|k$ , per a qualsevol cos  $k$  i qualsevol arrel de la unitat  $\zeta$ , són extensions normals.

En canvi, si  $\theta \in \mathbb{C}$  és una arrel del polinomi  $f(X) := X^3 - 2$ , l'extensió  $\mathbb{Q}(\theta)|\mathbb{Q}$  no és normal, ja que el polinomi  $f(X)$  és irreductible en  $\mathbb{Q}[X]$ , té una arrel en  $\mathbb{Q}(\theta)$ , però no té totes les arrels en  $\mathbb{Q}(\theta)$ , de manera que contradiu la condició (c) del teorema 3.9.1.

La propietat equivalent (c) de la definició d'extensió normal de cossos es pot llegir en el sentit que si  $K|k$  és una extensió normal i si un polinomi irreductible  $f(X) \in k[X]$  admet un factor de grau 1 en  $K[X]$ , llavors tots els factors irreductibles de  $f(X)$  en  $K[X]$  són de grau 1. En tenim la generalització següent.

**Proposició 3.9.9.** Siguin  $\bar{k}$  un cos algebraicament tancat,  $k \subseteq K \subseteq \bar{k}$  subcossos tals que l'extensió  $K|k$  és normal,  $f(X) \in k[X]$  un polinomi irreductible, i  $g(X), h(X)$  polinomis mòncics irreductibles de  $K[X]$  que divideixen  $f(X)$ . Llavors, existeix un  $k$ -automorfisme  $\sigma \in \text{Gal}(K|k)$  tal que  $h(X) = \sigma g(X)$ .

DEMOSTRACIÓ: Siguin  $\theta, \theta' \in \bar{k}$  arrels respectives dels polinomis  $g(X), h(X)$ ; en particular,  $\theta, \theta'$  són arrels del polinomi irreductible  $f(X) \in k[X]$ , de manera que existeix un únic  $k$ -isomorfisme  $\sigma : k(\theta) \rightarrow k(\theta')$  tal que  $\sigma(\theta) = \theta'$ . Aquest  $k$ -isomorfisme ens proporciona una única  $k$ -immersió  $\sigma : k(\theta) \rightarrow k(\theta') \subseteq \bar{k}$  tal que  $\sigma(\theta) = \theta'$ . Com que l'extensió  $K|k$  és algebraica, també ho és l'extensió  $K(\theta)|k(\theta)$ , de manera que  $\sigma$  admet una extensió a una  $k$ -immersió  $\sigma : K(\theta) \rightarrow \bar{k}$  tal que  $\sigma(\theta) = \theta'$ .

La restricció a  $K$  de  $\sigma$  és una  $k$ -immersió  $\sigma : K \rightarrow \bar{k}$ , de manera que, per hipòtesi,  $\sigma$  és un  $k$ -automorfisme de  $K$ ; és a dir,  $\sigma \in \text{Gal}(K|k)$ .

Ara,  $\sigma$  s'estén a un únic automorfisme de  $K[X]$  tal que  $\sigma(X) = X$ , de manera que la imatge per  $\sigma$  d'un polinomi irreductible és un polinomi irreductible. Però com que  $g(X) = \text{Irr}(\theta, K)(X)$  té arrel  $\theta$ , resulta que  $\sigma(g(X))$  és un polinomi mònic irreductible de  $K[X]$  que té per arrel  $\sigma(\theta) = \theta'$ ; és a dir,  $\sigma(g(X)) = h(X)$ .  $\square$

**Corollari 3.9.10.** *Sigui  $K|k$  una extensió normal i  $f(X) \in k[X]$  un polinomi irreductible. Llavors, tots els divisors irreductibles de  $f(X)$  en  $K[X]$  són del mateix grau.*  $\square$

**Definició 3.9.11.** Sigui  $K|k$  una extensió algebraica de cossos. S'anomena *clausura normal* de l'extensió  $K|k$  la mínima de les extensions normals  $N|k$  que contenen  $K|k$ .

**3.9.12.** Acabem la secció amb les propietats de la normalitat respecte del canvi de base i de la composició, que resumim en un parell de diagrames.

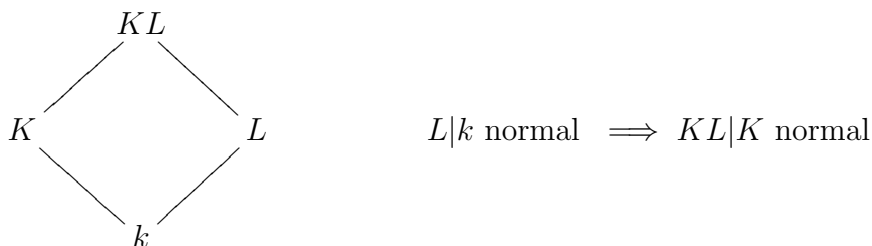


Diagrama 3.4: Comportament de la normalitat per canvi de base

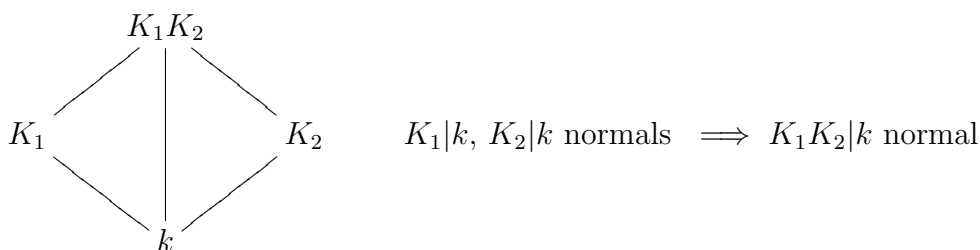


Diagrama 3.5: Comportament de la normalitat per composició

**Proposició 3.9.13.** *Sigui  $\bar{k}$  un cos algebraicament tancat, i  $k \subseteq K \subseteq \bar{k}$  i  $k \subseteq L \subseteq \bar{k}$  subcossos. Si l'extensió  $L|k$  és normal, llavors l'extensió  $KL|K$  és normal.*

DEMOSTRACIÓ: Si  $L$  és el cos de descomposició d'una família  $\{f_i(X)\}_{i \in I}$  de polinomis de  $k[X]$ , els polinomis pertanyen a  $K[X]$  i  $KL$  és el cos de descomposició de la família  $\{f_i(X)\}_{i \in I}$ .  $\square$

**Proposició 3.9.14.** *Siguin  $\bar{k}$  un cos algebraicament tancat, i  $k \subseteq K_1 \subseteq \bar{k}$  i  $k \subseteq K_2 \subseteq \bar{k}$  subcossos. Si les extensions  $K_1|k$  i  $K_2|k$  són normals, llavors l'extensió  $K_1K_2|k$  és normal.*

DEMOSTRACIÓ: Si  $K_1$  és el cos de descomposició d'una família  $\{f_i(X)\}_{i \in I}$  de polinomis de  $k[X]$ , i  $K_2$  és el cos de descomposició d'una família  $\{g_j(X)\}_{j \in J}$  de polinomis de  $k[X]$ , el cos compost  $K_1K_2$  és el cos de descomposició de la família reunió  $\{f_i(X)\}_{i \in I} \cup \{g_j(X)\}_{j \in J}$ .  $\square$

**Observació 3.9.15.** En canvi, la normalitat no es comporta bé per a torres d'extensions. Per exemple, per a  $\alpha \in \mathbb{C}$  tal que  $\alpha^4 = 2$ , l'extensió  $\mathbb{Q}(\alpha)|\mathbb{Q}$  no és normal (per exemple, perquè  $i \notin \mathbb{Q}(\alpha)$ ), mentre que les dues extensions  $\mathbb{Q}(\alpha)|\mathbb{Q}(\alpha^2)$  i  $\mathbb{Q}(\alpha^2)|\mathbb{Q}$  són normals (per exemple, perquè són quadràtiques).

### 3.10 Cossos finits

En aquesta secció, ens aturem una mica i fem l'estudi d'una família molt important de cossos: els cossos finits. Com que, en particular, els cossos finits proporcionen sempre extensions normals, obtenim exemples molt importants de la teoria de les extensions normals. D'altra banda, els cossos finits també proporcionen un exemple molt important (i motivador) del teorema fonamental de la teoria de Galois de les extensions de cossos.

**Proposició 3.10.1.** *Siguin  $\mathbb{F}$  un cos finit i  $q := \#\mathbb{F}$  el cardinal de  $\mathbb{F}$ . Llavors, existeixen un nombre natural primer  $p$  i un nombre natural  $f \geq 1$  tals que  $p = \text{car}(\mathbb{F})$  i  $q = p^f$ .*

DEMOSTRACIÓ: Si  $K$  és un cos qualsevol, llavors  $K$  conté un subcòs isomorf a  $\mathbb{Z}/p\mathbb{Z}$ , per a algun nombre primer  $p$ , o bé  $K$  conté un subcòs isomorf a  $\mathbb{Q}$ . Com que un cos finit no pot contenir  $\mathbb{Q}$ , tenim que  $\mathbb{F}$  és, en particular, de característica  $p > 0$ , per a algun nombre primer  $p$ . Així,  $\mathbb{F}$  conté  $\mathbb{Z}/p\mathbb{Z}$  com a subcòs i, per tant,  $\mathbb{F}$  és un  $\mathbb{Z}/p\mathbb{Z}$ -espai vectorial. Com que  $\mathbb{F}$  és un conjunt finit, la dimensió de  $\mathbb{F}$  com a  $\mathbb{Z}/p\mathbb{Z}$ -espai vectorial és finita, posem  $f \geq 1$ . Llavors, és clar que  $\#\mathbb{F} = p^f$ .  $\square$

El resultat anterior té un recíproc que caracteritza tots els cossos finits.

**Teorema 3.10.2.** *Sigui  $\bar{\mathbb{F}}$  un cos algebraicament tancat de característica  $p > 0$ . Se satisfan les propietats següents.*

- (a) *Per a tot nombre natural  $f \geq 1$ , existeix un únic subcòs  $\mathbb{F}_{p^f} \subseteq \bar{\mathbb{F}}$  de cardinal  $p^f$ .*
- (b) *El cos  $\mathbb{F}_{p^f}$  és el cos de descomposició del polinomi  $X^{p^f} - X \in \mathbb{F}_p[X]$ .*
- (c) *El cos  $\mathbb{F}_{p^f}$  és el conjunt de les arrels del polinomi  $X^{p^f} - X \in (\mathbb{Z}/p\mathbb{Z})[X]$  en  $\bar{\mathbb{F}}$ . En particular,  $\mathbb{F}_{p^f}^* = \mu_{p^f-1}(\bar{\mathbb{F}})$  és el conjunt de les arrels  $(p^f - 1)$ -èsimes de la unitat de  $\bar{\mathbb{F}}$ .*
- (d) *Per a nombres naturals  $f, n \geq 1$ , és  $\mathbb{F}_{p^f} \subseteq \mathbb{F}_{p^n}$  si, i només si,  $f$  és un divisor de  $n$ .*
- (e) *Per a nombres naturals  $f, n$  tals que  $f$  divideix  $n$ , l'extensió  $\mathbb{F}_{p^n}|\mathbb{F}_{p^f}$  és normal.*

DEMOSTRACIÓ: Siguin  $p$  un nombre natural primer,  $f \geq 1$  un nombre natural qualsevol, i posem  $q := p^f$ . El polinomi  $f(X) := X^q - X \in (\mathbb{Z}/p\mathbb{Z})[X]$  no té arrels múltiples, ja que el seu derivat, que és  $-1$ , no té arrels; per tant, el conjunt de les seves arrels en  $\overline{\mathbb{F}}$  és de cardinal  $q$ . Si veiem que les arrels de  $f(X)$  en  $\overline{\mathbb{F}}$  formen un cos, haurem provat l'existència de (a) i, a més a més, (c) i (b). D'altra banda, la unicitat de (a) és senzilla, ja que si  $\#\mathbb{F} = q$ , és  $\#\mathbb{F}^* = q - 1$ , de manera que tots els elements no nuls de  $\mathbb{F}$  són arrels del polinomi  $X^{q-1} - 1$ , que no té arrels múltiples i, en conseqüència,  $\mathbb{F}^* = \mu_{q-1}(\overline{\mathbb{F}})$ . Vegem, doncs, que el conjunt de les arrels de  $f(X)$  és un subcòs de  $\overline{\mathbb{F}}$ .

Siguin  $\theta, \theta'$  arrels de  $f(X)$  en  $\overline{\mathbb{F}}$ ; llavors, tenim que  $\theta^q = \theta$ ,  $\theta'^q = \theta'$ , de manera que  $(\theta\theta')^q = \theta^q\theta'^q = \theta\theta'$ , i  $(\theta + \theta')^q = \theta^q + \theta'^q = \theta + \theta'$ , ja que  $p = 0$  en  $\mathbb{F}$ . D'altra banda,  $(\theta^{-1})^q = (\theta^q)^{-1} = \theta^{-1}$  i  $(-\theta)^q = (-1)^q\theta^q = (-1)^q\theta = -\theta$ , ja que, si  $p$  és senar, també és  $(-1)^q = -1$ , i, si  $p = 2$ , és  $-1 = 1$ . Això ens diu que el conjunt de les arrels de  $f(X)$  en  $\overline{\mathbb{F}}$  és un subcòs de  $\overline{\mathbb{F}}$ , com volíem provar.

Per a veure (d), observem, primerament, que si  $f$  divideix  $n$ , llavors  $p^f - 1$  divideix  $p^n - 1$ . En efecte, el polinomi  $g(X) := X^f - 1 \in \mathbb{Z}[X]$  té per arrels totes les arrels  $f$ -èsimes de la unitat de  $\mathbb{C}$ ; per tant, les seves arrels ho són del polinomi  $h(X) := X^n - 1 \in \mathbb{Z}[X]$ ; així, el polinomi  $g(X)$  divideix el polinomi  $h(X)$  en  $\mathbb{Z}[X]$  i, en conseqüència,  $g(p)$  divideix  $h(p)$  en  $\mathbb{Z}$ . Aquesta propietat de divisibilitat ens diu que tota arrel  $(p^f - 1)$ -èsima de la unitat de  $\overline{\mathbb{F}}$  també és una arrel  $(p^n - 1)$ -èsima de la unitat de  $\overline{\mathbb{F}}$ ; per tant,  $\mathbb{F}_{p^f}^* \subseteq \mathbb{F}_{p^n}^*$ , de manera que  $\mathbb{F}_{p^f} \subseteq \mathbb{F}_{p^n}$ . Recíprocament, si  $\mathbb{F}_{p^f} \subseteq \mathbb{F}_{p^n}$ ,  $\mathbb{F}_{p^n}$  és un  $\mathbb{F}_{p^f}$ -espai vectorial, de manera que, si  $d$  n'és la dimensió, és  $\#\mathbb{F}_{p^n} = (\#\mathbb{F}_{p^f})^d$ ; és a dir,  $p^n = p^{fd}$ , d'on  $n = fd$ .

Resta veure (e). Ja hem vist que  $\mathbb{F}_{p^n}$  és el cos de descomposició de  $f(X) := X^{p^n} - X$  sobre  $\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$  i, per tant, l'extensió  $\mathbb{F}_{p^n}|\mathbb{F}_p$  és normal, per a tot  $n \geq 1$ . Ara bé, si  $f$  divideix  $n$ , el polinomi  $f(X)$  també té els seus coeficients en  $\mathbb{F}_{p^f}$ , de manera que  $\mathbb{F}_{p^n}$  també és el cos de descomposició sobre  $\mathbb{F}_{p^f}$  de  $f(X)$ . Això acaba la prova.  $\square$

**Exemples 3.10.3.** En particular, l'únic cos de cardinal  $p$ , primer, és  $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ .

Notem també que per a  $q := p^f$ ,  $f > 1$ , l'anell  $\mathbb{Z}/q\mathbb{Z}$  no és un cos, ja que  $p \neq 0$ , però  $p^f = 0$  en  $\mathbb{Z}/q\mathbb{Z}$ ; en particular,  $\mathbb{Z}/q\mathbb{Z}$  té divisors de zero. Per tant,  $\mathbb{F}_q \neq \mathbb{Z}/q\mathbb{Z}$ .

Si  $g(X) \in \mathbb{F}_p[X]$  és qualsevol polinomi irreductible de grau  $f$  i  $\theta$  és una arrel de  $g(X)$ , llavors  $\mathbb{F}_{p^f} = \mathbb{F}_p(\theta)$ .

**Proposició 3.10.4.** Siguin  $p$  un nombre natural primer,  $d \geq 1$  un nombre natural no divisible per  $p$ , i  $\zeta$  una arrel primitiva  $d$ -èsima de la unitat en un cos algebraicament tancat,  $\overline{\mathbb{F}}_p$ , que conté  $\mathbb{F}_p$ . Llavors,  $\mathbb{F}_p(\zeta) = \mathbb{F}_{p^f}$ , on  $f \geq 1$  és el menor nombre natural tal que  $d$  divideix  $p^f - 1$ .

DEMOSTRACIÓ: Com que  $\mathbb{F}_p(\zeta)$  és un cos extensió de  $\mathbb{F}_p$ , és de cardinal potència de  $p$ , posem  $p^f$ , amb  $f \geq 1$ . Llavors,  $\mathbb{F}_{p^f}^* = \mu_{p^f-1}(\overline{\mathbb{F}}_p)$  és un grup cíclic d'ordre  $p^f - 1$ , de manera que  $d$  divideix  $p^f - 1$ .

D'altra banda, si  $g \geq 1$  és un nombre natural tal que  $d$  divideix  $p^g - 1$ ,  $\zeta$  també és una arrel  $(p^g - 1)$ -èsima de la unitat, de manera que  $\zeta$  pertany al cos  $\mathbb{F}_{p^g}$ ; això implica que  $\mathbb{F}_{p^f} \subseteq \mathbb{F}_{p^g}$ , de manera que  $f$  divideix  $g$ ; per tant,  $f$  és el menor natural no nul tal que  $d|p^f - 1$ .  $\square$

**3.10.5.** Siguin  $p$  un nombre natural primer,  $n, f \geq 1$ , nombres naturals qualssevol, posem  $q := p^f$ , i considerem l'extensió de cossos  $\mathbb{F}_{q^n}|\mathbb{F}_q$  i el grup de Galois  $\text{Gal}(\mathbb{F}_{q^n}|\mathbb{F}_q)$ .

Ja hem vist que si  $\zeta \in \mathbb{F}_{q^n}$  és una arrel primitiva  $(q^n - 1)$ -èsima de la unitat, aleshores  $\mathbb{F}_{q^n} = \mathbb{F}_q(\zeta) = \mathbb{F}_p(\zeta)$ , tot automorfisme de  $\mathbb{F}_{q^n}$  és determinat per la imatge de  $\zeta$ , i el caràcter ciclotòmic  $\chi : \text{Gal}(\mathbb{F}_{q^n}|\mathbb{F}_q) \rightarrow (\mathbb{Z}/(q^n - 1)\mathbb{Z})^*$  identifica el grup de Galois  $\text{Gal}(\mathbb{F}_{q^n}|\mathbb{F}_q)$  amb un subgrup de  $(\mathbb{Z}/(q^n - 1)\mathbb{Z})^*$ . Es tracta de calcular la imatge d'aquest subgrup.

**3.10.6.** Sigui  $\varphi_q : \mathbb{F}_{q^n} \rightarrow \mathbb{F}_{q^n}$  l'aplicació definida per  $\varphi_q(x) := x^q$ , per a tot  $x \in \mathbb{F}_{q^n}$ . Com que  $q = p = 0$  en  $\mathbb{F}_{q^n}$ , per a  $x, y \in \mathbb{F}_{q^n}$ , és  $(x+y)^q = x^q + y^q$ ; i, com que, evidentment,  $(xy)^q = x^q y^q$ , i  $1^q = 1$ ,  $\varphi_q$  és un automorfisme de  $\mathbb{F}_{q^n}$ .

D'altra banda, els elements  $x \in \mathbb{F}_{q^n}$  tals que  $\varphi_q(x) = x$  són les arrels del polinomi  $X^q - X$ , és a dir, els elements de  $\mathbb{F}_q$ , de manera que tenim que  $\varphi_q \in \text{Gal}(\mathbb{F}_{q^n}|\mathbb{F}_q)$ .

**Definició 3.10.7.** L'automorfisme  $\varphi_q \in \text{Gal}(\mathbb{F}_{q^n}|\mathbb{F}_q)$  s'anomena *l'automorfisme de Frobenius de l'extensió  $\mathbb{F}_{q^n}|\mathbb{F}_q$* .

**Proposició 3.10.8.** *El grup de Galois  $\text{Gal}(\mathbb{F}_{q^n}|\mathbb{F}_q)$  és cíclic, d'ordre  $n$ , i generat per l'automorfisme de Frobenius  $\varphi_q$ .*

DEMOSTRACIÓ: Com que  $[\mathbb{F}_{q^n} : \mathbb{F}_q] = n$ , i com que el cos  $\mathbb{F}_{q^n}$  és generat sobre  $\mathbb{F}_q$  per  $\zeta$ , l'ordre  $\#\text{Gal}(\mathbb{F}_{q^n}|\mathbb{F}_q)$  és menor o igual que el nombre d'arrels de  $\text{Irr}(\zeta, \mathbb{F}_q)(X) \in \mathbb{F}_q[X]$ , és a dir, que  $[\mathbb{F}_{q^n} : \mathbb{F}_q]$ ; per tant, és suficient si demostrem que  $\varphi_q$  és un element d'ordre  $n$  de  $\text{Gal}(\mathbb{F}_{q^n}|\mathbb{F}_q)$ . Però això és senzill. En efecte, per a tot nombre natural  $k \geq 1$ , és  $\varphi_q^k = \varphi_{q^k}$ , ja que  $\varphi_q^k(\zeta) = \zeta^{q^k} = \varphi_{q^k}(\zeta)$ ; així, si  $\varphi_q^k$  és la identitat, ha de ser  $\zeta^{q^k} = \zeta$ , de manera que  $k$  ha de ser un múltiple de  $n$  perquè  $\zeta$  és una arrel primitiva  $(q^n - 1)$ -èsima de la unitat. Per tant,  $\varphi_q \in \text{Gal}(\mathbb{F}_{q^n}|\mathbb{F}_q)$  és d'ordre  $n$ , com volíem demostrar.  $\square$

**3.10.9.** Alternativament, per a veure que l'automorfisme de Frobenius és un automorfisme d'ordre  $n$ , és suficient observar que, per la definició del caràcter ciclotòmic, tenim que  $\chi(\varphi_q) = q \in (\mathbb{Z}/(q^n - 1)\mathbb{Z})^*$ ; però, evidentment,  $q$  és un element invertible i d'ordre  $n$  en  $(\mathbb{Z}/(q^n - 1)\mathbb{Z})^*$ ; per tant, l'ordre de  $\varphi_q$  en  $\text{Gal}(\mathbb{F}_{q^n}|\mathbb{F}_q)$  ha d'ésser un múltiple de  $n$  menor o igual que el grau  $n$  de l'extensió; és a dir, igual a  $n$ . En altres paraules, tenim que la imatge del caràcter ciclotòmic  $\chi : \text{Gal}(\mathbb{F}_{q^n}|\mathbb{F}_q) \rightarrow (\mathbb{Z}/(q^n - 1)\mathbb{Z})^*$  és el subgrup de  $(\mathbb{Z}/(q^n - 1)\mathbb{Z})^*$  generat per  $q$ , que és un subgrup cíclic d'ordre  $n$ .

**3.10.10.** Recordem que per a cada divisor  $d$  de  $n$  existeix una única subextensió  $\mathbb{F}_{q^d}|\mathbb{F}_q$  de  $\mathbb{F}_{q^n}|\mathbb{F}_q$ ; d'altra banda, observem que, per a cada divisor  $d$  de  $n$ , existeix un únic subgrup de  $\text{Gal}(\mathbb{F}_{q^n}|\mathbb{F}_q)$  d'ordre  $d$ , ja que  $\text{Gal}(\mathbb{F}_{q^n}|\mathbb{F}_q)$  és cíclic d'ordre  $n$ . La pregunta és, doncs, òbvia: hi ha alguna relació entre els subgrups de  $\text{Gal}(\mathbb{F}_{q^n}|\mathbb{F}_q)$  i les subextensions  $\mathbb{F}_{q^d}|\mathbb{F}_q$  de  $\mathbb{F}_{q^n}|\mathbb{F}_q$ ? La resposta és que sí. Vegem quina.

**3.10.11. Teorema fonamental de la teoria de Galois per als cossos finits.** Siguin  $\mathcal{S}(q^n, q)$  el conjunt dels subgrups de  $\text{Gal}(\mathbb{F}_{q^n}|\mathbb{F}_q)$  i  $\mathcal{C}(q^n, q)$  el conjunt de les subextensions de  $\mathbb{F}_{q^n}|\mathbb{F}_q$ .

Observem, en primer lloc, que si  $d|n$ , el grup de Galois  $\text{Gal}(\mathbb{F}_{q^n}|\mathbb{F}_{q^d})$  és un subgrup del grup de Galois  $\text{Gal}(\mathbb{F}_{q^n}|\mathbb{F}_q)$ , ja que si un automorfisme de  $\mathbb{F}_{q^n}$  deixa fix el cos  $\mathbb{F}_{q^d}$ , també deixa fix el cos  $\mathbb{F}_q$ . Per tant, podem definir una aplicació  $\mathcal{C}(q^n, q) \xrightarrow{f} \mathcal{S}(q^n, q)$  per l'assignació  $f(\mathbb{F}_{q^d}|\mathbb{F}_q) := \text{Gal}(\mathbb{F}_{q^n}|\mathbb{F}_{q^d})$ .

D'altra banda, podem definir una aplicació  $\mathcal{S}(q^n, q) \xrightarrow{g} \mathcal{C}(q^n, q)$  assignant a cada subgrup  $H$  de  $\text{Gal}(\mathbb{F}_{q^n}|\mathbb{F}_q)$  la subextensió  $\mathbb{F}_{q^n}^H|\mathbb{F}_q$ , on  $\mathbb{F}_{q^n}^H$  és el subcòs de  $\mathbb{F}_{q^n}$  format pels elements que són fixos per tots els automorfismes que pertanyen a  $H$ .

Com que  $\text{Gal}(\mathbb{F}_{q^n}|\mathbb{F}_q) = \langle \varphi_q \rangle$ , els seus subgrups són els  $\langle \varphi_q^d \rangle$ , per als divisors  $d$  de  $n$ . Així, el subcòs de  $\mathbb{F}_{q^n}$  format pels elements fixos per  $\langle \varphi_q^d \rangle$  és el cos de descomposició del polinomi  $X^{q^d} - X$ , és a dir,  $\mathbb{F}_{q^d}$ ; i el grup de Galois de l'extensió  $\mathbb{F}_{q^n}|\mathbb{F}_{q^d}$  és exactament  $\langle \varphi_q^d \rangle$ . Per tant, les dues aplicacions  $f$  i  $g$  són inverses l'una de l'altra. Això és una demostració del teorema següent.

**Teorema 3.10.12.** *Les aplicacions  $f$  i  $g$  són inverses l'una de l'altra, de manera que estableixen una bijecció entre el conjunt de les subextensions de  $\mathbb{F}_{q^n}|\mathbb{F}_q$  i el conjunt dels subgrups de  $\text{Gal}(\mathbb{F}_{q^n}|\mathbb{F}_q)$ .  $\square$*

**Observació 3.10.13.** Aquesta bijecció no es produeix, en general, per a totes les extensions de cossos. Per exemple, si  $K := \mathbb{Q}(\theta)$ , amb  $\theta^3 = 2$ , l'extensió  $K|\mathbb{Q}$  és de grau 3 i té grup de Galois trivial; per tant, el grup de Galois no té subgrups diferents de  $\{1\}$ , però, en canvi, tenim les dues subextensions  $K|\mathbb{Q}$  i  $\mathbb{Q}|\mathbb{Q}$ .

Fins i tot, per al cas d'extensions normals, tampoc no tenim un resultat similar. Per exemple, l'extensió  $k(\theta)|k$ , on  $k := \mathbb{F}_2(t)$  i  $\theta^2 = t$ , és normal, ja que és de grau 2, mentre que  $\text{Gal}(k(\theta)|k) = \{1\}$  (cf. l'exemple 3.8.16).

Més endavant, caracteritzem les extensions per a les quals se satisfà el teorema anterior (cf. 5.2.1).

## 3.11 Exercicis

**Exercici 3.11.1.** Siguin  $n > 1$  un nombre enter,  $\zeta_n$  una arrel primitiva  $n$ -èsima de la unitat, i  $\zeta_{2n}$  una arrel primitiva  $2n$ -èsima de la unitat. Si  $n$  és senar, llavors es té la igualtat  $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{2n})$ , mentre que si  $n$  és parell, llavors l'extensió  $\mathbb{Q}(\zeta_{2n})|\mathbb{Q}(\zeta_n)$  és de grau 2.

**Exercici 3.11.2.** Per a tot nombre natural  $k \geq 1$ , sigui  $\zeta_k$  una arrel primitiva  $k$ -èsima de la unitat. Siguin  $r, s$  nombres enters positius i considerem  $m := \text{mcm}(r, s)$ ,  $d := \text{mcd}(r, s)$ . Llavors,  $\mathbb{Q}(\zeta_r, \zeta_s) = \mathbb{Q}(\zeta_m)$  i  $\mathbb{Q}(\zeta_r) \cap \mathbb{Q}(\zeta_s) = \mathbb{Q}(\zeta_d)$  (cf. la proposició 3.5.3 per al cas particular en què  $d = 1$ ).

**Exercici 3.11.3.** Sigui  $\Phi_n(X)$  el polinomi ciclotòmic  $n$ -èsim.

(a) Per a tot nombre natural primer  $p$ , per a tot nombre natural  $n$  tal que  $p$  no divideix  $n$ , i per a tot  $r \geq 1$ , es té que

$$\Phi_{np^r}(X) = \Phi_{np}(X^{p^{r-1}}).$$

(b) D'aquí es dedueix que, per a tot nombre primer  $p$  i tot  $r \geq 1$ ,

$$\Phi_{p^r}(X) = \sum_{j=0}^{p-1} X^{p^{r-1}j}.$$

(c) Per a tot nombre senar  $n \geq 3$  es té que

$$\Phi_{2n}(X) = \Phi_n(-X).$$

Què succeeix en el cas  $n = 1$ ?

- (d) Per a tot nombre natural  $n$  i per a tot nombre primer  $p$  tals que  $p$  no divideix  $n$ , es té que

$$\Phi_{np}(X) = \frac{\Phi_n(X^p)}{\Phi_n(X)}.$$

**Exercici 3.11.4.** Sigui  $\Phi_n(X)$  el polinomi ciclotòmic  $n$ -èsim. Quin és el nombre  $n$  més petit tal que algun dels coeficients de  $\Phi_n(X)$  és diferent de 0, 1 i  $-1$ ?

*Indicació:* Dels exercicis anteriors es dedueix que aquest  $n$  haurà de ser compost, senar i lliure de quadrats.

**Exercici 3.11.5.** Siguin  $n, m$  nombres enters positius,  $\Phi_n(X)$  el polinomi ciclotòmic  $n$ -èsim, i suposem que  $p$  és un nombre primer tal que  $p \mid \Phi_n(m)$ .

- (a) Llavors,  $m^n \equiv 1 \pmod{p}$ ; en particular,  $p \nmid m$ .
- (b) Sigui  $d$  l'ordre de  $m$  en el grup multiplicatiu  $(\mathbb{Z}/p\mathbb{Z})^*$ . Llavors,  $d \mid n$  i, si  $n/d > 1$ , aleshores

$$\Phi_n(X) \mid \sum_{i=0}^{\frac{n}{d}-1} X^{di}.$$

D'aquí es dedueix que si  $n/d > 1$ , aleshores  $p \mid n$ .

- (c) Si  $p \nmid n$ , aleshores  $p \equiv 1 \pmod{n}$ . En particular, si  $p \mid \Phi_n(n)$ , llavors  $p \equiv 1 \pmod{n}$ .
- (d) Siguin  $n > 1$  un nombre enter,  $x \geq 2$  un nombre real i  $\Phi_n(X)$  el polinomi ciclotòmic  $n$ -èsim. Llavors,  $|\Phi_n(x)| > x - 1$ .
- (e) Per a qualsevol nombre enter positiu  $n$ , el conjunt dels nombres primers  $p$  tals que  $p \equiv 1 \pmod{n}$  és infinit.

*Indicació:* Es pot considerar la successió de nombres enters  $\Phi_{kn}(kn)$ , per a  $k \geq 1$ , enter.

**Exercici 3.11.6** (Fórmula d'inversió de Möbius). Siguin  $f, g : \mathbb{N} - \{0\} \rightarrow A$  funcions aritmètiques de valors en un anell  $A$ . Llavors,

$$g(n) = \sum_{d \mid n} f(d), \quad \forall n \geq 1 \quad \Leftrightarrow \quad f(n) = \sum_{d \mid n} g(d)\mu(n/d), \quad \forall n \geq 1,$$

on  $\mu : \mathbb{N} - \{0\} \rightarrow A$  indica la funció de Möbius (cf. la definició 3.2.15).

**Observació:** Es defineix el producte de Dirichlet (també anomenat convolució de Dirichlet) de dues funcions aritmètiques  $f, g$  per la fórmula

$$(f * g)(n) := \sum_{d \mid n} f(d)g(n/d), \quad \forall n \geq 1,$$

la suma estesa sobre tots els divisors naturals de  $n$ ; llavors, el resultat enunciat és equivalent a dir que, a l'anell de les funcions aritmètiques de valors en  $A$ , amb la suma habitual de funcions i el producte de Dirichlet, la funció  $\mu$  és invertible amb inversa la funció constant de valor 1; és a dir, la funció definida per  $u(n) := 1$ , per a tot  $n \geq 1$ . En efecte, l'element unitat d'aquest anell de funcions és la funció  $\delta$  definida per  $\delta(1) := 1$ ,  $\delta(n) := 0$ , si  $n > 1$ .



**Exercici 3.11.7** (Nombre de polinomis irreductibles sobre  $\mathbb{F}_q$ ). Sigui  $\mathbb{F}_q$  el cos finit de  $q$  elements.

(a) Si  $f_d(X) \in \mathbb{F}_q[X]$  és un polinomi mònic irreductible de grau  $d$ , llavors  $f_d(X)$  divideix  $X^{q^n} - X$  si, i només si,  $d$  divideix  $n$ .

(b) Per a tot nombre natural  $n \geq 1$ , se satisfà la identitat

$$X^{q^n} - X = \prod_{d|n} \prod_{f_d} f_d(X),$$

on, en el segon producte,  $f_d$  recorre tots els polinomis mònics irreductibles de grau  $d$  de  $\mathbb{F}_q[X]$ .

(c) Si  $\psi_q(d)$  designa el nombre de polinomis mònics irreductibles de grau  $d$  de  $\mathbb{F}_q[X]$ , llavors, per a tot nombre natural  $n \geq 1$  es té que

$$q^n = \sum_{d|n} d\psi_q(d).$$

(d) Per a tot nombre natural  $n \geq 1$ , és

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

on  $\mu$  és la funció de Möbius.

(e) Si  $\text{mcd}(q, n) = 1$ , llavors el nombre de polinomis mònics irreductibles de grau  $n$  de  $\mathbb{F}_q[X]$  és múltiple de  $q$ .



# Capítol 4

## Radicals

Si deixem de banda l'equació  $X^n = 1$ , la més senzilla és l'equació  $X^n = a$ , per a  $a \neq 0, 1$ . Dedicuem aquest capítol a fer el seu estudi.

A la secció primera, n'estudiem la resolució i fem el càlcul del cos de descomposició del polinomi  $X^n - a$  i la reducció de l'estudi de l'equació al cas d'exponent  $n = p$ , primer. Dedicuem la secció segona a la irreductibilitat dels polinomis  $X^{p^r} - a$ ,  $a \in k$ ,  $p$  primer, i  $r \geq 1$ .

A continuació, estudiem els conceptes d'element separable i de grau de separabilitat d'una extensió algebraica de cossos, concepte que ja ha aparegut una mica de passada en el capítol anterior (cf. **3.8.17**), tot i que allà no n'hem donat la definició formal ni n'hem estudiat les propietats, i dediquem la secció quarta a l'estudi del concepte d'extensió algebraica separable de cossos i, en particular, al comportament d'aquest concepte per a torres d'extensions, per al canvi de base, per a la composició i per al pas a la clausura normal.

A la secció cinquena, introduïm el concepte d'element primitiu i demostrem l'existència d'elements primitius per a totes les extensions finites i separables de cossos (teorema de l'element primitiu).

L'objecte de la secció sisena és l'estudi de la traça i de la norma d'una extensió finita de cossos; el seu càlcul permet caracteritzar les extensions separables, cosa que fem a la secció setena, en la qual provem, a més a més, el teorema d'independència lineal de caràcters.

Dedicuem la secció vuitena a la prova del teorema 90 de Hilbert, en les seves formes additiva i multiplicativa, que fem servir a la secció novena per a l'estudi de les extensions cícliques de cossos i, en particular, per a la demostració del teorema d'Artin-Schreier.

A la secció desena, establim la teoria de Kummer de la classificació de les extensions cícliques de cossos quan el cos base conté prou arrels de la unitat.

Finalment, a les seccions onzena i dotzena fem l'estudi bàsic dels radicals, de les extensions radicals, i de les extensions resolubles per radicals; aquesta és la part central de la teoria que serveix per a caracteritzar les equacions resolubles per radicals, teoria que acabem de desenvolupar en el capítol següent amb l'ús del teorema fonamental de la teoria de Galois.

## 4.1 L'equació $X^n = a$

Siguin  $k$  un cos,  $a \in k$  un element qualsevol, i  $\bar{k}$  un cos algebraicament tancat que conté  $k$ . Per a  $a = 0$ , l'equació  $X^n = a$  només té la solució  $\alpha = 0$  en  $\bar{k}$ , a partir d'ara, doncs, suposarem que  $a \neq 0$ .

**4.1.1.** Mirem-nos les solucions de l'equació. Suposem que  $\alpha, \alpha' \in \bar{k}$  són solucions de l'equació  $X^n = a$ ; com que  $a \neq 0$ , ha de ser  $\alpha, \alpha' \neq 0$ , de manera que té sentit considerar el quocient  $\frac{\alpha'}{\alpha} \in \bar{k}$ ; i aquest quocient és una solució de l'equació  $X^n = 1$ ; això és, existeix una arrel  $n$ -èsima de la unitat,  $\zeta \in \bar{k}$ , tal que  $\alpha' = \zeta\alpha$ . I, recíprocament, si  $\alpha$  és una solució de  $X^n = a$  i  $\zeta$  és una arrel  $n$ -èsima de la unitat, llavors  $\alpha' := \alpha\zeta$  també és una solució de l'equació  $X^n = a$ . Aquests dos fets ens ensenyen que el càlcul de les solucions de l'equació  $X^n = a$  es redueix al càlcul d'una solució particular de l'equació i de totes les arrels  $n$ -èsimes de la unitat. Notem el paral·lelisme amb la resolució de les equacions lineals, les solucions de les quals s'obtenen a partir d'una solució particular en sumar-hi totes les solucions de l'equació homogènia associada; en el cas que tractem ara, el paper de l'equació homogènia és representat per l'equació  $X^n = 1$ .

**Corollari 4.1.2.** *Siguin  $\bar{k}$  un cos algebraicament tancat,  $k \subseteq \bar{k}$  un subcòs qualsevol,  $a \in k$ , un element no nul,  $n \geq 2$  un nombre enter, i  $\mu_n(\bar{k})$  el grup de les arrels  $n$ -èsimes de la unitat de  $\bar{k}$ . El cos de descomposició sobre  $k$  del polinomi  $X^n - a \in k[X]$  és el cos  $k(\zeta, \alpha)$ , on  $\zeta$  és un generador qualsevol del grup  $\mu_n(\bar{k})$ , i  $\alpha \in \bar{k}$  és una arrel qualsevol del polinomi  $X^n - a$ .  $\square$*

**4.1.3.** Si  $\text{car}(k)$  no divideix  $n$ , en  $\bar{k}$  hi ha exactament  $n$  arrels  $n$ -èsimes diferents de la unitat (cf. **3.2.1**), de manera que l'equació  $X^n = a$  també té  $n$  solucions diferents. En canvi, si  $\text{car}(k) = p > 0$  i escrivim  $n$  en la forma  $n = p^r n'$ , amb  $n'$  no divisible per  $p$ , el polinomi  $X^n - a$  té exactament  $n'$  arrels diferents, totes elles múltiples i de la mateixa multiplicitat  $p^r$ .

**Corollari 4.1.4.** *Suposem que  $\text{car}(k) = p > 0$ , primer, i que  $n = p^r n'$ , on  $n' \geq 1$  és un nombre natural no divisible per  $p$  i  $r \geq 1$  és un nombre natural. Sigui  $\alpha \in \bar{k}$  l'únic element tal que  $\alpha^{p^r} = a$ . Llavors, el polinomi  $X^n - a$  admet una descomposició en  $\bar{k}[X]$  del tipus  $X^n - a = (X^{n'} - \alpha)^{p^r}$ , i el polinomi  $X^{n'} - \alpha$  té  $n'$  arrels diferents en  $\bar{k}$ .*

**DEMOSTRACIÓ:** El polinomi derivat del polinomi  $X^{n'} - \alpha$  és  $n'X^{n'-1}$ ; com que  $p$  no divideix  $n'$ , és  $n' \neq 0$ , de manera que el polinomi  $n'X^{n'-1}$  només té l'arrel 0, que no és arrel de  $X^{n'} - \alpha$ ; per tant, el polinomi  $X^{n'} - \alpha$  té exactament  $n'$  arrels diferents. D'altra banda, i com que  $\text{car}(k) = p$ , es té que  $(X^{n'} - \alpha)^{p^r} = (X^{n'})^{p^r} - \alpha^{p^r} = X^n - a$ .  $\square$

Un cop vist quin cos és el cos de descomposició del polinomi  $X^n - a$ , volem estudiar la irreductibilitat del polinomi  $X^n - a$  i, també, la resolució de l'equació  $X^n = a$ .

**Proposició 4.1.5.** *Siguin  $k$  un cos,  $a \in k$  un element no nul, i  $m, n \geq 1$  nombres naturals primers entre si. El polinomi  $X^{mn} - a$  és irreductible en  $k[X]$  si, i només si, els polinomis  $X^m - a$  i  $X^n - a$  són irreductibles en  $k[X]$ .*

**DEMOSTRACIÓ:** Suposem que  $X^m - a$  no és irreductible en  $k[X]$  i sigui  $g(X) \in k[X]$  un divisor propi i no trivial de  $f(X) := X^m - a$ . Llavors,  $g(X^n) \in k[X]$  és un divisor propi i no trivial del polinomi  $f(X^n) = X^{mn} - a$ , de manera que  $X^{mn} - a$  tampoc no és irreductible en  $k[X]$ .

Recíprocament, suposem que  $X^m - a$  i  $X^n - a$  són irreductibles en  $k[X]$ . Si  $\alpha$  és una arrel qualsevol de  $X^{mn} - a$ , llavors  $\alpha^n$  és una arrel de  $X^m - a$  i  $[k(\alpha^n) : k] = m$ ; i, anàlogament,  $[k(\alpha^m) : k] = n$ . Com que  $m, n$  són primers entre si, obtenim que per al cos composició és  $[k(\alpha^m, \alpha^n) : k] = mn$ . D'altra banda, com que  $\text{mcd}(m, n) = 1$ , existeixen nombres enters  $x, y$  tals que  $mx + ny = 1$ , de manera que  $\alpha = (\alpha^m)^x (\alpha^n)^y$  pertany al cos  $k(\alpha^m, \alpha^n)$  i, en conseqüència,  $k(\alpha^m, \alpha^n) = k(\alpha)$ . Finalment, el fet que sigui  $[k(\alpha) : k] = mn$  ens diu que  $X^{mn} - a = \text{Irr}(\alpha, k)(X) \in k[X]$ ; en particular, doncs, que  $X^{mn} - a$  és irreductible.  $\square$

**4.1.6.** Notem que si sabem calcular les solucions de les equacions  $X^m = a$  i  $X^n = a$ , on  $\text{mcd}(m, n) = 1$ , també sabem calcular les de l'equació  $X^{mn} = a$ . En efecte, si  $\alpha, \beta \in \bar{k}$  són solucions particulars de les equacions  $X^m = a$  i  $X^n = a$ , respectivament, i si prenem  $x, y \in \mathbb{Z}$  tals que  $mx + ny = 1$  i posem  $\gamma := \alpha^y \beta^x$ , aleshores se satisfan les igualtats  $\gamma^{mn} = \alpha^{ymn} \beta^{xmn} = a^{yn} a^{xm} = a^{mx+ny} = a$ , de manera que  $\gamma \in \bar{k}$  és una solució particular de  $X^{mn} = a$ .

Així, doncs, podem reduir l'estudi de les equacions  $X^n = a$  al cas en què l'exponent  $n$  és una potència d'un nombre primer.

**Observació 4.1.7.** Suposem que sabem resoldre totes les equacions  $X^p = a$  per a tot nombre primer  $p$  i tot element no nul  $a$  de tot cos  $k$ . Llavors, també sabem resoldre de manera recursiva totes les equacions  $X^n = a$  per a tot nombre natural  $n \geq 1$  i tot element no nul  $a$  de tot cos  $k$ . En efecte, és clar que si  $p$  és un nombre primer que divideix  $n$  i si  $n = pm$ , amb  $m \in \mathbb{N}$ , llavors les arrels del polinomi  $X^n - a$  són les arrels dels polinomis  $X^p - \alpha$ , quan  $\alpha$  recorre el conjunt de les arrels del polinomi  $X^m - a$ , i és  $m < n$ . Així, doncs, l'objecte principal d'estudi d'aquest capítol són les equacions  $X^p = a$ , on  $a \in k$ ,  $a \neq 0$ , i  $p$  és un nombre natural primer.

## 4.2 Irreductibilitat de $X^{p^r} - a$

En aquesta secció, es tracta d'estudiar la irreductibilitat dels polinomis  $X^{p^r} - a \in k[X]$ , per a  $p$  primer, i de donar una descripció del grup de Galois del cos de descomposició del polinomi  $X^n - a \in k[X]$ , per a  $n \geq 1$  qualsevol.

**Proposició 4.2.1.** *Siguin  $k$  un cos,  $p$  un nombre natural primer,  $r \geq 1$  un nombre natural,  $a \in k$  un element no nul, i suposem que el polinomi  $X^p - a \in k[X]$  no té cap arrel en  $k$ . Llavors, en els casos (a)  $p \neq 2$ ; (b)  $p = 2$  i  $\text{car}(k) = 2$ ; i (c)  $p = 2$ ,  $\text{car}(k) \neq 2$ , i  $r = 1$ ; el polinomi  $X^{p^r} - a$  és irreductible en  $k[X]$ . En el cas (d)  $p = 2$ ,  $\text{car}(k) \neq 2$ , i  $r \geq 2$ , el polinomi  $X^{2^r} - a$  és irreductible en  $k[X]$  si, i només si, cap dels polinomis  $X^p - a \in k[X]$  i  $X^4 + 4a \in k[X]$  no té arrels en  $k$ .*

**Observació 4.2.2.** Doncs, en el cas  $p = 2$  i  $\text{car}(k) \neq 2$ , la irreductibilitat del polinomi  $X^{2^r} - a$ ,  $r \geq 2$ , és equivalent al fet que els dos polinomis  $X^4 + 4a$  i  $X^2 - a$  no tinguin arrels en  $k$ , de manera similar a com, en tots els altres casos, la irreductibilitat del polinomi  $X^{p^r} - a$  és equivalent al fet que el polinomi  $X^p - a$  no tingui arrels en  $k$ .

Demostrem la proposició 4.2.1 per inducció sobre l'exponent  $r$ . Per al cas  $r = 1$ , cal establir la irreductibilitat del polinomi  $X^p - a$ .

**Lema 4.2.3.** *Si un polinomi  $X^p - a \in k[X]$ ,  $p$  primer, no té arrels en  $k$ , llavors és irreductible en  $k[X]$ .*

DEMOSTRACIÓ: Òbviament, si el polinomi  $X^p - a$  té una arrel  $\alpha \in k$ , llavors és divisible, en  $k[X]$ , per  $X - \alpha$ , de manera que no és irreductible en  $k[X]$ , perquè és de grau  $p > 1$ .

Suposem, recíprocament, que  $X^p - a$  és divisible per un polinomi mònic  $f(X) \in k[X]$ , de grau  $d$ ,  $1 \leq d \leq p - 1$ ; es tracta de provar que el polinomi  $X^p - a$  té alguna arrel en  $k$ . Obtindrem aquesta arrel a partir del terme constant de  $f(X)$ . Per a calcular aquest terme constant, considerem  $\alpha \in \bar{k}$  una arrel de  $X^p - a$  en un cos algebraicament tancat  $\bar{k}$  que conté  $k$ . Les arrels d'aquest polinomi en  $\bar{k}$  són de la forma  $\alpha\zeta$ , on  $\zeta \in \bar{k}$  és alguna arrel  $p$ -èsima de la unitat; per tant,  $f(X)$  és el producte de  $d$  factors de la forma  $X - \alpha\zeta$ , on  $\alpha$  és fix i  $\zeta$ , que pot variar, és tal que  $\zeta^p = 1$ . En particular, obtenim una igualtat de la forma  $b := (-1)^d f(0) = \alpha^d \zeta$ , on  $b \in k$  i  $\zeta^p = 1$ . Com que  $\text{mcd}(d, p) = 1$ , existeixen nombres enters  $x, y$  tals que  $dx + py = 1$ , i podem definir  $\beta := \alpha\zeta^x$ ; així, tenim que  $\beta = \alpha^{py} \alpha^{dx} \zeta^x = \alpha^y b^x \in k$  i que  $\beta^p = a$ , de manera que el polinomi  $X^p - a$  té l'arrel  $\beta$  en  $k$ .  $\square$

Per a establir l'argument inductiu de la demostració de la proposició 4.2.1, fem servir el resultat següent.

**Lema 4.2.4.** *Suposem que un polinomi  $X^p - a \in k[X]$ ,  $p$  primer, no té arrels en  $k$  i sigui  $\alpha \in \bar{k}$  una arrel de  $X^p - a$  en un cos algebraicament tancat  $\bar{k}$  que conté  $k$ . En els casos (a) i (b), en què o bé  $p \neq 2$  o bé  $p = 2$  i  $\text{car}(k) = 2$ , el polinomi  $X^p - \alpha$  no té arrels en  $k(\alpha)$ ; en canvi, en el cas  $p = 2$  i  $\text{car}(k) \neq 2$ , el polinomi  $X^2 - \alpha$  té arrels en  $k(\alpha)$  si, i només si, el polinomi  $X^4 + 4a$  té arrels en  $k$ .*

DEMOSTRACIÓ: Com que, en virtut del lema anterior, el polinomi  $X^p - a$  és irreductible en  $k[X]$ , tenim que  $[k(\alpha) : k] = p$  i  $\text{Irr}(\alpha, k)(X) = X^p - a$ . També ara distingirem casos, però no els mateixos que abans. El cas més simple és el cas en què  $\text{car}(k) = p$ . En efecte, tot element  $\beta \in k(\alpha)$  es pot escriure en la forma  $\beta = g(\alpha)$ , on  $g(X) \in k[X]$  és un polinomi de grau menor o igual que  $p - 1$ ; ara, si  $h(X) \in k[X]$  és el polinomi que s'obté de  $g(X)$  en elevar els seus coeficients a la potència  $p$ -èsima, és  $h(X) \in k[X]$  i si és  $\text{car}(k) = p$ , llavors tenim que  $\beta^p = g(\alpha)^p = h(\alpha^p) = h(a) \in k$ . Així, si  $\beta$  fos una arrel de  $X^p - \alpha$  en  $k(\alpha)$ , obtindríem que  $\alpha = \beta^p \in k$ , contràriament a la hipòtesi. Per tant, en el cas en què  $\text{car}(k) = p$ , el polinomi  $X^p - \alpha$  no té arrels en  $k(\alpha)$ , com es tracta de demostrar.

Estudiem ara el cas en què  $\text{car}(k) \neq p$ . Siguin  $\zeta$  una arrel primitiva  $p$ -èsima de la unitat,  $K := k(\zeta)$ , i  $L := K(\alpha) = k(\zeta, \alpha)$ , el cos de descomposició del polinomi  $X^p - a \in k[X]$ .

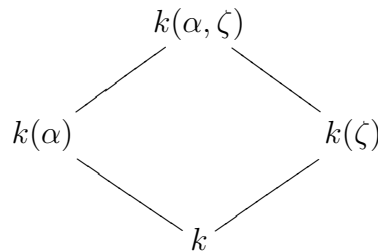


Diagrama 4.1: Cos de descomposició de  $X^p - a$

Com que el polinomi  $X^p - a$  és irreductible en  $k[X]$  i com que el grau  $[K : k]$  és menor o igual que  $p - 1$  i, per tant, primer amb  $p$ , tenim que  $[L : K] = p$  i, en conseqüència,

el polinomi  $X^p - a$  coincideix amb  $\text{Irr}(\alpha, K)(X)$  i és, per tant, irreductible en  $K[X]$ . I, com que l'extensió  $L|k$  és normal, per a tot  $i \in \{0, 1, \dots, p-1\}$  podem considerar un  $k$ -automorfisme  $\sigma_i \in \text{Gal}(L|k)$ , extensió a  $L$  de l'única  $k$ -immersió  $\sigma_i : k(\alpha) \rightarrow L$  tal que  $\sigma_i(\alpha) = \zeta^i \alpha$ .

Com més amunt, suposem que existeix alguna arrel  $\beta \in k(\alpha)$  del polinomi  $X^p - a$ . Com que  $k(\beta) \subseteq k(\alpha)$ , el grau  $[k(\alpha) : k] = p$  és primer, i  $\beta \notin k$  perquè  $\beta^p = a \notin k$ , tenim que  $k(\alpha) = k(\beta)$  i, en conseqüència, el polinomi  $\text{Irr}(\beta, k)(X)$  és de grau  $p$ . A més a més, si posem  $\beta_i := \sigma_i(\beta) \in L$ ,  $0 \leq i \leq p-1$ , i tenim en compte que els elements  $\beta_i^p = \sigma_i(\beta)^p = \sigma_i(\beta^p) = \sigma_i(a) = \zeta^i a$  són tots diferents, tenim que els elements  $\beta_i$ ,  $0 \leq i \leq p-1$ , també són tots diferents; i com que  $\sigma_i(\beta)$  és arrel del polinomi  $\text{Irr}(\beta, k)(X)$ ,

ha d'ésser  $\text{Irr}(\beta, k)(X) = \prod_{i=0}^{p-1} (X - \beta_i)$ . En particular, el coeficient del monomi de grau

zero d'aquest polinomi pertany a  $k$ ; és a dir,  $\gamma := \prod_{i=0}^{p-1} \beta_i \in k$ . A més a més, la potència

$p$ -èsima de  $\gamma$  és  $\gamma^p = \prod_{i=0}^{p-1} (\zeta^i \alpha) = \alpha^p \zeta^S = a \zeta^S$ , on  $S = \sum_{i=0}^{p-1} i = \frac{p(p-1)}{2}$ . Estudiem, ara, aquesta igualtat  $\gamma^p = a \zeta^S$ .

Si  $p \neq 2$ ,  $S$  és un nombre enter múltiple de  $p$ , de manera que  $\zeta^S = 1$  i  $\gamma \in k$  és una arrel de  $X^p - a$ , contràriament a la hipòtesi. Això acaba la prova en el cas  $p \neq 2$ . En el cas que resta (això és  $p = 2$  i  $\text{car}(k) \neq 2$ ), tenim que  $\zeta = -1$  i que  $S = 1$ , de manera que  $\gamma^2 = -a \in k$ . Ara hem de veure que el polinomi  $X^4 + 4a \in k[X]$  té alguna arrel en  $k$ . Com que  $p = 2$ , el conjunt  $\{1, \alpha\}$  és una  $k$ -base de  $k(\alpha)$  i existeixen  $x, y \in k$  tals que  $\beta = x + y\alpha$ ; aleshores, de l'equació  $\beta^2 = \alpha$ , és  $x^2 + ay^2 = 0$  i  $2xy = 1$ . La primera equació, multiplicada per  $4x^2$ , proporciona, tenint en compte la segona, la nova igualtat  $4x^4 + a = 4x^4 + 4x^2 y^2 a = 0$ , que dóna que  $-4a = 16x^4 = (2x)^4$  i ens ensenya que  $2x \in k$  és una arrel del polinomi  $X^4 + 4a \in k[X]$ .

Per a acabar la prova, només resta veure que si el polinomi  $X^4 + 4a$  té arrels en  $k$ , llavors  $X^2 - \alpha$  també en té en  $k(\alpha)$ ; però això és immediat, ja que si  $\theta \in k$  és tal que  $\theta^4 = -4a$ , llavors  $\beta := \frac{\theta}{2} + \alpha\theta^{-1} \in k(\alpha)$  i  $\beta^2 = \frac{\theta^2}{4} + a\theta^{-2} + \alpha = \frac{\theta^4 + 4a}{4\theta^2} + \alpha = \alpha$ , de manera que el polinomi  $X^2 - \alpha$  té una arrel  $\beta$  en  $k(\alpha)$ .  $\square$

Ara, amb l'ús dels lemes **4.2.3** i **4.2.4**, podem acabar la demostració de la proposició **4.2.1**.

**DEMOSTRACIÓ** de la proposició **4.2.1**: Argumentem per inducció sobre  $r$ ; notem que el cas  $r = 1$  ja ha estat provat en tots els casos (cf. el lema **4.2.3**).

Suposem, doncs, que  $r \geq 2$ , sigui  $\theta \in \bar{k}$  una arrel qualsevol del polinomi  $X^{p^r} - a$ , i posem  $\alpha := \theta^{p^{r-1}}$ . Llavors,  $\alpha^p = a$  i, com que, també en virtut del lema **4.2.3**, el polinomi  $X^p - a$  és irreductible, tenim que  $[k(\alpha) : k] = p$ . En els casos  $p \neq 2$  i  $p = 2 = \text{car}(k)$ , el lema **4.2.4** ens diu que el polinomi  $X^p - \alpha$  no té arrels en  $k(\alpha)$ , de manera que podem aplicar la hipòtesi d'inducció al cos base  $k(\alpha)$  i el polinomi  $X^{p^{r-1}} - \alpha$ ; obtenim que aquest polinomi és irreductible sobre  $k(\alpha)$ , però això implica que  $[k(\theta) : k(\alpha)] = p^{r-1}$ , de manera que  $[k(\theta) : k] = p^r$  i el polinomi  $X^{p^r} - a$ , del qual  $\theta$  n'és una arrel, és irreductible en  $k[X]$ . Això demostra els apartats (a) i (b) de la proposició. I l'apartat (c) és cobert pel lema **4.2.3**. Demostrem, finalment, (d).

Suposem, doncs, que  $p = 2$ , que  $\text{car}(k) \neq 2$ , i que el polinomi  $X^4 + 4a$  té alguna arrel  $\beta \in k$ . Si posem  $\alpha := \frac{\beta}{2} \in k$ , tenim que  $-4\alpha^4 = a$  i, llavors, el polinomi  $X^{2^r} - a$  admet la descomposició

$$X^{2^r} - a = X^{2^r} + 4\alpha^4 = (X^{2^{r-1}} + 2\alpha X^{2^{r-2}} + 2\alpha^2)(X^{2^{r-1}} - 2\alpha X^{2^{r-2}} + 2\alpha^2)$$

en  $k[X]$ , com es comprova immediatament.

Recíprocament, suposem que  $p = 2$ , que  $\text{car}(K) \neq 2$ , i que els polinomis  $X^4 + 4a$  i  $X^2 - a$  no tenen arrels en  $k$ ; cal veure que  $X^{2^r} - a$  és irreductible en  $k[X]$ . Si, com més amunt, posem que  $\theta$  sigui una arrel del polinomi  $X^{2^r} - a$  i  $\alpha := \theta^{2^{r-1}}$ , tenim que  $[k(\alpha) : k] = 2$ , i només cal veure que  $[k(\theta) : k(\alpha)] = 2^{r-1}$ . En el cas  $r = 2$ , obtenim això si veiem que  $X^2 - \alpha$  no té arrels en  $k(\alpha)$ ; en el cas  $r > 2$ , ho obtenim en aplicar la hipòtesi d'inducció al cos base  $k(\alpha)$ , si veiem que els polinomis  $X^4 + 4a$  i  $X^2 - \alpha$  no tenen arrels en  $k(\alpha)$ .

En aquest darrer cas, observem que si el polinomi  $X^4 + 4a$  té una arrel  $\beta \in k(\alpha)$ , llavors és  $\frac{\beta^2}{2} \in k(\alpha)$  i  $\left(\frac{\beta^2}{2}\right)^2 = -a$ , de manera que el polinomi  $X^2 + \alpha$  també té una arrel en  $k(\alpha)$ . Ara, observem que si el polinomi  $X^2 - \alpha$  no té arrels en  $k(\alpha)$ , el polinomi  $X^2 + \alpha$  tampoc no té arrels en  $k(\alpha)$ . En efecte, com que  $\alpha, -\alpha$  són les arrels del polinomi irreductible  $X^2 - a \in k[X]$ , existeix un únic  $k$ -automorfisme  $\tau : k(\alpha) \rightarrow k(\alpha)$  tal que  $\tau(\alpha) = -\alpha$ ; en conseqüència, el polinomi  $X^2 - \alpha$  és irreductible en  $k(\alpha)[X]$  si, i només si, ho és  $X^2 + \alpha$ .

Així, doncs, hem reduït la part final de la demostració a veure que el polinomi  $X^2 - \alpha$  no té arrels en  $k(\alpha)$ ; però això es veu a la demostració del lema 4.2.4, quan es prova que si  $X^2 - \alpha$  té una arrel  $\beta = x + y\alpha \in k(\alpha)$ ,  $x, y \in k$ , llavors  $2x \in k$  és una arrel del polinomi  $X^4 + 4a$ .  $\square$

Un cop hem caracteritzat la irreductibilitat dels polinomis  $X^n - a \in k[X]$ , descrivim el grup de Galois del seu cos de descomposició, en tots els casos.

**Proposició 4.2.5.** *Siguin  $\bar{k}$  un cos algebraicament tancat,  $k \subseteq \bar{k}$  un subcòs,  $n \geq 2$  un nombre natural no divisible per  $\text{car}(k)$ ,  $a \in k$ ,  $a \neq 0, 1$ , i  $L$  el cos de descomposició sobre  $k$  del polinomi  $X^n - a$ . El grup de Galois de l'extensió  $L|k$  és isomorf a un subgrup del grup de les matrius de la forma  $\begin{bmatrix} * & * \\ 0 & 1 \end{bmatrix}$  de  $\mathbf{GL}(2, \mathbb{Z}/n\mathbb{Z})$ .*

**DEMOSTRACIÓ:** Com que  $\text{car}(k)$  no divideix  $n$ , existeixen arrels primitives  $n$ -èsimes de la unitat en  $\bar{k}$ . Siguin  $\zeta \in \bar{k}$  una arrel primitiva  $n$ -èsima de la unitat,  $\alpha \in \bar{k}$  una arrel qualsevol de  $X^n - a$ ,  $K := k(\zeta)$ , i  $L = k(\alpha, \zeta) = K(\alpha)$ , el cos de descomposició sobre  $k$  del polinomi  $X^n - a$ . En particular, tot automorfisme  $\sigma \in \text{Gal}(L|k)$  és determinat pels valors  $\sigma(\alpha)$  i  $\sigma(\zeta)$ . Ara bé, si  $\chi : \text{Gal}(K|k) \rightarrow (\mathbb{Z}/n\mathbb{Z})^*$  és el  $n$ -èsim caràcter ciclotòmic sobre  $k$  (cf. el corollari 3.8.13), sabem que  $\sigma(\zeta) = \zeta^{\chi(\sigma)}$  i que  $\chi(\sigma) \in (\mathbb{Z}/n\mathbb{Z})^*$  no depèn de l'arrel primitiva  $n$ -èsima de la unitat  $\zeta$  que triem. D'altra banda, com que  $\alpha$  és una arrel del polinomi  $X^n - a \in k[X]$ ,  $\sigma(\alpha)$  també ha de ser una arrel d'aquest polinomi; per tant, el quocient  $\frac{\sigma(\alpha)}{\alpha}$  és una arrel  $n$ -èsima de la unitat; és a dir, existeix  $\tau(\sigma) \in \mathbb{Z}/n\mathbb{Z}$ , determinat unívocament per  $\sigma$  i  $\alpha$  (de fet, depèn de l'elecció de l'arrel  $\alpha$  del polinomi  $X^n - a$ ), tal que  $\sigma(\alpha) = \alpha\zeta^{\tau(\sigma)}$ . En particular, la matriu  $\rho(\sigma) := \begin{bmatrix} \chi(\sigma) & \tau(\sigma) \\ 0 & 1 \end{bmatrix}$  és un



element de  $\mathbf{GL}(2, \mathbb{Z}/n\mathbb{Z})$  i l'aplicació  $\rho : \text{Gal}(L|k) \rightarrow \mathbf{GL}(2, \mathbb{Z}/n\mathbb{Z})$  definida d'aquesta manera és un morfisme injectiu de grups, amb imatge continguda, per definició, en el subgrup de les matrius de la forma  $\begin{bmatrix} * & * \\ 0 & 1 \end{bmatrix}$ .  $\square$

**4.2.6.** Suposem que  $\text{car}(k) = p > 0$  i que  $n = p^r n'$ , amb  $r \geq 1$  i  $n'$  no divisible per  $p$ . Llavors, si  $\beta \in \bar{k}$  és l'únic element tal que  $\beta^{p^r} = a$ , les arrels del polinomi  $X^n - a$  sobre  $k$  són les arrels del polinomi  $X^{n'} - \beta$  sobre  $k(\beta)$ ; i, com que  $n'$  no és divisible per la característica de  $k(\beta)$ , el grup de Galois del cos de descomposició del polinomi  $X^n - a = (X^{n'} - \beta)^{p^r}$  sobre  $k(\beta)$  és de la forma descrita; és a dir, un subgrup  $H$  del subgrup de les matrius de la forma  $\begin{bmatrix} * & * \\ 0 & 1 \end{bmatrix}$  de  $\mathbf{GL}(2, \mathbb{Z}/n'\mathbb{Z})$ . Ara bé, qualsevol  $k$ -immersió de  $k(\beta)$  és la identitat en  $k(\beta)$ , ja que la imatge de  $\beta$  ha de ser una arrel del polinomi  $X^{p^r} - a = (X - \beta)^{p^r}$ ; per tant, qualsevol  $k$ -automorfisme de  $L$ , el cos de descomposició de  $X^n - a$  sobre  $k$ , és un  $k(\beta)$ -automorfisme, i el grup de Galois  $\text{Gal}(L|k)$  coincideix amb  $\text{Gal}(L|k(\beta))$ ; és a dir, és isomorf a  $H$ . Obtenim, doncs, una descripció del grup de Galois cos de descomposició del polinomi irreductible  $X^n - a \in k[X]$ , també en el cas en què  $\text{car}(k)$  divideix  $n$ .

**Proposició 4.2.7.** *Siguin  $\bar{k}$  un cos algebraicament tancat de característica  $p > 0$ ,  $k \subseteq \bar{k}$  un subcòs,  $n = p^r n'$  un nombre natural, on  $r \geq 1$  i  $n'$  no és divisible per  $p$ ,  $a \in k$ ,  $a \neq 0, 1$ , i  $L$  el cos de descomposició sobre  $k$  del polinomi  $X^n - a$ . El grup de Galois de l'extensió  $L|k$  és isomorf a un subgrup del grup de les matrius de la forma  $\begin{bmatrix} * & * \\ 0 & 1 \end{bmatrix}$  de  $\mathbf{GL}(2, \mathbb{Z}/n'\mathbb{Z})$ .*  $\square$

**Corollari 4.2.8.** *Suposem que  $k$  conté una arrel  $n$ -èsima primitiva de la unitat,  $\zeta$ , i que el polinomi  $X^n - a \in k[X]$  és irreductible. Sigui  $\alpha \in \bar{k}$  una arrel de  $X^n - a$ . Llavors, el grup de Galois de l'extensió  $k(\alpha)|k$  és cíclic d'ordre  $n$ .*

**DEMOSTRACIÓ:** L'acció del grup de Galois sobre les arrels  $n$ -èsimes de la unitat és trivial en aquest cas, ja que pertanyen al cos base; és a dir,  $\chi(\sigma) = 1$ , per a tot  $\sigma \in \text{Gal}(L|k)$ ; per tant, el grup de Galois de l'extensió s'identifica amb un subgrup del grup de les matrius de la forma  $\begin{bmatrix} 1 & * \\ 0 & 1 \end{bmatrix} \subseteq \mathbf{GL}(2, \mathbb{Z}/n\mathbb{Z})$ . Però aquest grup és isomorf al grup additiu  $\mathbb{Z}/n\mathbb{Z}$

(l'isomorfisme identifica la matriu  $\begin{bmatrix} 1 & z \\ 0 & 1 \end{bmatrix}$  amb l'element  $z$  de  $\mathbb{Z}/n\mathbb{Z}$ ). Per tant, el grup de Galois és isomorf a un subgrup de  $\mathbb{Z}/n\mathbb{Z}$ . Ara bé, com que existeix un  $k$ -automorfisme de  $k(\alpha)$  que transforma  $\alpha$  en  $\alpha\zeta$ , el generador  $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$  del grup  $\begin{bmatrix} 1 & * \\ 0 & 1 \end{bmatrix}$  pertany a la imatge de  $\text{Gal}(k(\alpha)|k)$ ; per tant, l'aplicació  $\rho : \text{Gal}(k(\alpha)|k) \rightarrow \begin{bmatrix} 1 & * \\ 0 & 1 \end{bmatrix}$  és un isomorfisme de grups.  $\square$

**Observació 4.2.9.** En general, el grup de Galois de l'extensió  $k(\alpha, \zeta)|k$ , quan  $\alpha^n \in k$ ,  $\zeta$  és una arrel  $n$ -èsima primitiva de la unitat, i el polinomi  $X^n - a$  és irreductible en  $k[X]$ , no és pas abelià. Per exemple, podem considerar  $n = 3$ ,  $k = \mathbb{Q}$ , i  $a = 2$  i, en aquest cas,  $\text{Gal}(\mathbb{Q}(\alpha, \zeta)|\mathbb{Q}) \simeq S_3$ , el grup de permutacions de tres elements. Aquest fet és essencialment diferent del que succeeix en el cas de l'equació  $X^n = 1$ , en què el grup de Galois sempre és abelià. Això reflecteix el fet (de fet, n'és la causa) que l'equació  $X^n = a$  és, en general, més difícil que l'equació  $X^n = 1$ .

### 4.3 Separabilitat

En l'estudi de les equacions  $X^n = 1$  i  $X^n = a$ , ens hem trobat algunes vegades amb el cas de polinomis irreductibles que tenen arrels múltiples. Convé estudiar aquest cas amb més detall.

**Definició 4.3.1.** Siguin  $K|k$  una extensió de cossos i  $\theta \in K$  un element algebraic sobre  $k$ . Es diu que  $\theta$  és *separable* sobre  $k$  si  $\theta$  és arrel d'un polinomi de  $k[X]$  que no té arrels múltiples; equivalentment, si el polinomi  $\text{Irr}(\theta, k)(X) \in k[X]$  no té arrels múltiples.

En molts casos, tots els elements algebraics són separables; per exemple, sobre tots els cossos de característica zero i sobre tots els cossos finits.

**Proposició 4.3.2.** *Sigui  $k$  un cos de característica zero o bé un cos finit. Tot element algebraic sobre  $k$  és separable.*

**DEMOSTRACIÓ:** Suposem que  $f(X) \in k[X]$  és un polinomi mònic que té alguna arrel múltiple; cal veure que  $f(X)$  no és irreductible. El polinomi derivat de  $f(X)$  també s'anul·la sobre aquesta arrel múltiple, de manera que o bé  $D(f, X) = 0$ , o bé el polinomi no nul  $\text{mcd}(f(X), D(f, X))$  té alguna arrel comuna amb  $f(X)$  i, en conseqüència, és un divisor propi i no trivial de  $f(X)$ . Això acaba la prova en el cas de característica zero, perquè el derivat d'un polinomi mònic que té arrels no és mai el polinomi zero.

Però si  $k$  és finit, encara hi ha la possibilitat que sigui  $D(f, X) = 0$ . En aquest cas, existeix un polinomi  $h(X) \in k[X]$  tal que  $f(X) = h(X^p)$ , on posem  $p := \text{car}(k) > 0$ . L'exhaustivitat de l'automorfisme de Frobenius  $\varphi_p : k \rightarrow k$  (cf. **3.10.7**) proporciona l'existència d'un polinomi  $g(X) \in k[X]$  tal que  $h(X)$  s'obté en elevar els coeficients de  $g(X)$  a la potència  $p$ -èsima; així,  $f(X) = h(X^p) = g(X)^p$ , de manera que  $f(X)$  no és irreductible.  $\square$

**Exemple 4.3.3.** En canvi, hi ha cossos  $k$  per als quals existeixen polinomis mònic irreductibles que tenen arrels múltiples. Per exemple, si  $p$  és un nombre primer i prenem  $k := \mathbb{F}_p(t)$ , el cos de fraccions de l'anell de polinomis en una indeterminada  $t$ , llavors el polinomi  $X^p - t \in k[X]$  és irreductible i només té una arrel, de multiplicitat  $p$ ; per tant, l'arrel d'aquest polinomi és un element algebraic i no separable sobre  $k$ .

**4.3.4.** En el capítol anterior (cf. per exemple, **3.8.17**), apareix algunes vegades el nombre de  $k$ -immersions d'un cos de la forma  $k(\theta)$ ,  $\theta$  algebraic sobre  $k$ , en algun cos algebraicament tancat  $\bar{k}$  que conté  $k$ , nombre que allà hem denotat per  $[k(\theta) : k]_s$ , per al qual hem vist que se satisfà la desigualtat  $[k(\theta) : k]_s \leq [k(\theta) : k]$ , i que és el nombre d'arrels diferents en  $\bar{k}$  del polinomi mònic irreductible de  $k[X]$  que té  $\theta$  per arrel. Estudiem aquest nombre més de prop; en primer lloc, veiem que no depèn del cos algebraicament tancat  $\bar{k}$  que considerem.

**Proposició 4.3.5.** *Sigui  $K|k$  una extensió algebraica qualsevol de cossos. El cardinal del conjunt de  $k$ -immersions de  $K$  en un cos algebraicament tancat  $\bar{k}$  que conté  $k$  no depèn de  $\bar{k}$ .*

**DEMOSTRACIÓ:** Siguin  $\bar{k}$  i  $k^a$  cossos algebraicament tancats que contenen  $k$ , suposem que  $K \subseteq \bar{k}$ , i sigui  $N|k$  la clausura normal en  $\bar{k}$  de l'extensió  $K|k$ . Podem pensar la identitat de  $k$  com una  $k$ -immersió de  $k$  en  $k^a$ , de manera que l'extensió algebraica de

morfismes (cf. la proposició **3.9.2**) proporciona una  $k$ -immersió  $\sigma_0 : N \rightarrow k^a$ . Llavors, per a  $N' := \sigma_0(N)$ , l'extensió  $N'|k$  és la clausura normal en  $k^a$  de l'extensió  $\sigma_0(K)|k$ , i  $\sigma_0 : N \rightarrow N'$  és un  $k$ -isomorfisme. Notem que si l'extensió algebraica  $K|k$  és generada per una certa família d'elements algebraics sobre  $k$ , llavors  $N$  és el cos de descomposició en  $\bar{k}$  dels polinomis minimalis sobre  $k$  dels elements d'aquesta família; i  $N'$  és el cos de descomposició en  $k^a$  dels mateixos polinomis de  $k[X]$ . En particular, tota  $k$ -immersió de  $K$  en  $\bar{k}$  té imatge inclosa en  $N$  i tota  $k$ -immersió de  $K$  en  $k^a$  té imatge inclosa en  $N'$ .

Ara, la composició amb  $\sigma_0$  transforma una  $k$ -immersió de  $K$  en  $\bar{k}$  en una  $k$ -immersió de  $K$  en  $k^a$  i, recíprocament, la composició amb  $\sigma_0^{-1}$  transforma una  $k$ -immersió de  $K$  en  $k^a$  en una  $k$ -immersió de  $K$  en  $\bar{k}$ . S'obté, d'aquesta manera, una aplicació bijectiva entre els conjunts de les  $k$ -immersions de  $K$  en  $\bar{k}$  i en  $k^a$ .  $\square$

Aquest resultat ens permet definir en general el grau de separabilitat d'una extensió algebraica de cossos, no necessàriament de la forma  $k(\theta)|k$ , o sigui, no necessàriament generada per un sol element algebraic.

**Definició 4.3.6.** Sigui  $K|k$  una extensió algebraica qualsevol de cossos. S'anomena *grau de separabilitat* de l'extensió  $K|k$  el cardinal del conjunt de  $k$ -immersions de  $K$  en qualsevol cos algebraicament tancat  $\bar{k}$  que conté  $k$ ; es designa amb el símbol  $[K : k]_s$ .

**Observació 4.3.7.** D'entre les extensions finites de cossos, podem caracteritzar les extensions normals  $K|k$  pel fet que l'ordre del grup de Galois  $\text{Gal}(K|k)$  coincideixi amb el grau de separabilitat  $[K : k]_s$  de l'extensió. En efecte, el grau de separabilitat  $[K : k]_s$  és el nombre de  $k$ -immersions de  $K$  en un cos algebraicament tancat  $\bar{k}$  que contingui  $k$ , l'ordre del grup de Galois  $\text{Gal}(K|k)$  és el nombre de  $k$ -automorfismes de  $K$ , i l'extensió  $K|k$  és normal si, i només si, tota  $k$ -immersió de  $K$  en  $\bar{k}$  és un  $k$ -automorfisme de  $K$ .

El grau de separabilitat es comporta bé per a cadenes d'extensions; és a dir, podem establir el resultat bàsic següent.

**Proposició 4.3.8.** *Siguin  $K|k$  i  $L|K$  extensions algebraiques qualssevol. Aleshores, se satisfà la igualtat  $[L : k]_s = [L : K]_s [K : k]_s$ .*

DEMOSTRACIÓ: Sigui  $\bar{k}$  un cos algebraicament tancat que conté  $L$ , i siguin  $S(k, K)$ ,  $S(k, L)$ ,  $S(K, L)$ , respectivament, els conjunts de totes les  $k$ -immersions de  $K$  en  $\bar{k}$ , de totes les  $k$ -immersions de  $L$  en  $\bar{k}$ , i de totes les  $K$ -immersions de  $L$  en  $\bar{k}$ . Cal veure que el cardinal del conjunt  $S(k, L)$  és el producte dels cardinals dels altres dos conjunts,  $S(k, K)$  i  $S(K, L)$ . I per a això, és suficient establir una aplicació exhaustiva  $S(k, L) \rightarrow S(k, K)$  tal que l'antiimatge de tot element de  $S(k, K)$  sigui un conjunt del mateix cardinal que  $S(K, L)$ .

Podem definir una aplicació  $f : S(k, L) \rightarrow S(k, K)$  per  $f(\sigma) := \sigma|_K$ , on  $\sigma|_K$  indica la restricció a  $K$  de  $\sigma$ . Com que l'extensió  $L|K$  és algebraica, tota  $k$ -immersió de  $K$  en  $\bar{k}$  s'estén a una  $k$ -immersió de  $L$  en  $\bar{k}$  (cf. la proposició **3.9.2**), de manera que l'aplicació  $f$  és exhaustiva. Per tant, només cal comprovar que l'antiimatge per  $f$  de qualsevol element de  $S(k, K)$  és un conjunt del mateix cardinal que  $S(K, L)$ .

Sigui  $N|k$  la clausura normal en  $\bar{k}$  de l'extensió  $L|k$ . Per a tota  $k$ -immersió  $\sigma$  de  $L$  en  $\bar{k}$ , l'axioma de l'elecció (cf. **B.0.17** i **B.0.18**) ens permet fixar una extensió  $\sigma'$  de  $\sigma$  a una  $k$ -immersió de  $N$  en  $\bar{k}$ ; com que  $N|k$  és normal, tenim que  $\sigma'$  és un  $k$ -automorfisme de  $N$ . Ara, siguin  $\sigma_1, \sigma_2 \in S(k, L)$  dos elements qualssevol tals que  $f(\sigma_1) = f(\sigma_2)$ ; és a

dir, tals que  $\sigma_{1|K} = \sigma_{2|K}$ ; llavors,  $\sigma'_1(K) = \sigma'_2(K)$  i, a més a més, la restricció a  $K$  de la composició  $\sigma'_1{}^{-1} \circ \sigma'_2$  és la identitat, de manera que la restricció a  $L$  de  $\sigma'_1{}^{-1} \circ \sigma'_2$  és un element de  $S(K, L)$ . Recíprocament, si  $\tau \in S(K, L)$  és un element qualsevol, també és  $\tau \in S(k, L)$ , de manera que té sentit considerar-ne una extensió  $\tau'$  a  $N$ , i la restricció a  $L$  de la composició  $\sigma'_1 \circ \tau'$  és una  $k$ -immersió de  $L$  en  $\bar{k}$  tal que la seva restricció a  $K$  és  $\sigma_1$ . Així, la composició amb  $\sigma'_1{}^{-1}$ , ens proporciona una bijecció de l'antiimatge de  $f(\sigma_1) = \sigma_{1|K}$  en el conjunt  $S(K, L)$ , amb inversa donada per la composició amb  $\sigma'_1$ ; per tant, aquests dos conjunts tenen el mateix cardinal, com volíem demostrar.  $\square$

**Corollari 4.3.9.** *Sigui  $K|k$  una extensió finita. Llavors,  $[K : k]_s \leq [K : k]$ .*

DEMOSTRACIÓ: Siguin  $\theta_1, \theta_2, \dots, \theta_n \in K$  elements tals que  $K = k(\theta_1, \dots, \theta_n)$ ; tenim que

$$[K : k] = \prod_{i=0}^{n-1} [k(\theta_1, \dots, \theta_{i+1}) : k(\theta_1, \dots, \theta_i)].$$

D'altra banda, la proposició anterior ens diu que

$$[K : k]_s = \prod_{i=0}^{n-1} [k(\theta_1, \dots, \theta_{i+1}) : k(\theta_1, \dots, \theta_i)]_s.$$

Però en el cas de les extensions de la forma  $k(\theta)|k$ , el resultat ja ha estat provat (i utilitzat) anteriorment (cf., per exemple, **3.8.9** i **3.8.17**); per tant, per a  $0 \leq i \leq n-1$ , és

$$[k(\theta_1, \dots, \theta_{i+1}) : k(\theta_1, \dots, \theta_i)]_s \leq [k(\theta_1, \dots, \theta_{i+1}) : k(\theta_1, \dots, \theta_i)],$$

i obtenim la propietat desitjada per multiplicació.  $\square$

**Corollari 4.3.10.** *Sigui  $k \subseteq K \subseteq L$  cossos tals que l'extensió  $L|k$  és finita. Aleshores,  $[L : k]_s = [L : k]$  si, i només si,  $[L : K]_s = [L : K]$  i  $[K : k]_s = [K : k]$ .  $\square$*

**Proposició 4.3.11.** *Sigui  $K|k$  una extensió finita qualsevol de cossos. Llavors,  $[K : k]_s$  divideix  $[K : k]$ .*

DEMOSTRACIÓ: Com que podem escriure  $K$  en la forma  $K = k(\theta_1, \dots, \theta_n)$ , per a certs elements  $\theta_1, \dots, \theta_n \in K$ , és suficient provar el resultat per a les extensions de la forma  $k(\theta)|k$ , amb  $\theta$  algebraic sobre  $k$ , per a qualsevol cos  $k$  i tenir en compte la multiplicativitat dels graus

$$[k(\theta_1, \dots, \theta_{i+1}) : k(\theta_1, \dots, \theta_i)] \quad \text{i} \quad [k(\theta_1, \dots, \theta_{i+1}) : k(\theta_1, \dots, \theta_i)]_s.$$

Sigui, doncs,  $k$  un cos qualsevol,  $\theta$  un element algebraic sobre  $k$ ,  $K := k(\theta)$ , i posem  $f(X) := \text{Irr}(\theta, k)(X) \in k[X]$  per al polinomi minimal de  $\theta$  sobre  $k$ ; llavors,  $[k(\theta) : k]_s$  és exactament el nombre d'arrels diferents de  $f(X)$ . Si  $\theta$  és separable,  $[k(\theta) : k]_s$  és, doncs, el grau del polinomi  $f(X)$ , que coincideix amb el grau  $[k(\theta) : k]$ ; per tant, obtenim la igualtat  $[k(\theta) : k]_s = [k(\theta) : k]$ , i això acaba la prova en aquest cas.

Suposem, doncs, que  $\theta$  no és separable. Això implica que  $D(f, X) = 0$  i que  $f(X)$  és de la forma  $f(X) = h(X^{p^r})$ , on  $h(X) \in k[X]$  és un polinomi, per força irreductible,  $p = \text{car}(k) > 0$ , i  $r \geq 1$  és un nombre natural, que podem considerar que és el màxim per al qual se satisfà aquesta propietat. Aquesta maximalitat de  $r$  implica que  $\theta^{p^r}$ , que és arrel de

$h(X)$ , és un element de  $k(\theta)$  separable sobre  $k$ , de manera que  $[k(\theta^{p^r}) : k]_s = [k(\theta^{p^r}) : k]$ . D'altra banda,  $\theta$  és l'única arrel del polinomi  $X^{p^r} - \theta^{p^r} \in k(\theta^{p^r})[X]$ , també per força irreductible; per tant,  $[k(\theta) : k(\theta^{p^r})] = p^r$  i l'única  $k(\theta^{p^r})$ -immersió de  $k(\theta)$  és la identitat; és a dir,  $[k(\theta) : k(\theta^{p^r})]_s = 1$ . Per tant, obtenim que

$$[k(\theta) : k]_s = [k(\theta^{p^r}) : k]_s = [k(\theta^{p^r}) : k]$$

és un divisor de  $[k(\theta) : k]$ , com volíem veure.  $\square$

## 4.4 Extensions separables

Acabem de veure que, per a tota extensió finita de cossos  $K|k$ ,  $[K : k]_s$  divideix  $[K : k]$ . Es tracta de veure en quines condicions se satisfà la igualtat.

**Proposició 4.4.1.** *Sigui  $K|k$  una extensió finita de cossos. Les dues propietats següents són equivalents.*

(a) *Tot element de  $K$  és separable sobre  $k$ .*

(b)  $[K : k]_s = [K : k]$ .

**DEMOSTRACIÓ:** Suposem que tot element  $\theta \in K$  és separable sobre  $k$ . Com que l'extensió  $K|k$  és finita, podem pensar  $K = k(\theta_1, \dots, \theta_n)$ , per a certs elements  $\theta_i \in K$ . Per hipòtesi, cadascun dels elements  $\theta_i$  és separable sobre  $k$ , de manera que  $\theta_{i+1}$  és separable sobre  $k(\theta_1, \dots, \theta_i)$ . Així, obtenim que

$$[k(\theta_1, \dots, \theta_{i+1}) : k(\theta_1, \dots, \theta_i)]_s = [k(\theta_1, \dots, \theta_{i+1}) : k(\theta_1, \dots, \theta_i)],$$

per a  $0 \leq i \leq n-1$ ; per la multiplicativitat del grau i la del grau de separabilitat, obtenim que  $[K : k]_s = [K : k]$ , com volíem veure.

Recíprocament, suposem que  $[K : k]_s = [K : k]$  i vegem que tot element  $\theta \in K$  és separable sobre  $k$ . Però això és immediat, de nou per la multiplicativitat dels graus i dels graus de separabilitat, en aplicar-les a la torre d'extensions  $k \subseteq k(\theta) \subseteq K$ : obtenim que  $[k(\theta) : k]_s = [k(\theta) : k]$ , de manera que  $\theta$  és separable sobre  $k$ .  $\square$

**Definició 4.4.2.** Sigui  $K|k$  una extensió algebraica de cossos. Es diu que l'extensió  $K|k$  és *separable* si tot element de  $K$  és separable sobre  $k$ . En particular, per a les extensions finites, això equival a dir que el grau de separabilitat coincideix amb el grau de l'extensió.

**Corol·lari 4.4.3.** *Una extensió finita  $K|k$  és normal i separable si, i només si, se satisfà la igualtat  $\#\text{Gal}(K|k) = [K : k]$ .  $\square$*

A la demostració de la proposició anterior hem provat, en particular, que si  $K$  és un cos generat sobre  $k$  per una família finita d'elements separables sobre  $k$ , llavors l'extensió  $K|k$  és separable. El resultat no es restringeix a famílies finites d'elements.

**Proposició 4.4.4.** *Sigui  $K|k$  una extensió algebraica de cossos tal que  $K$  és generat sobre  $k$  per una família qualsevol d'elements separables sobre  $k$ ; és a dir, suposem que existeix una família  $\{\theta_i\}_{i \in I}$  d'elements  $\theta_i \in K$ , separables sobre  $k$ , tals que  $K = k(\{\theta_i\}_{i \in I})$ . Llavors, l'extensió  $K|k$  és separable.*

**DEMOSTRACIÓ:** Donat un element  $\theta \in K$ , existeix un subconjunt finit  $J \subseteq I$  tal que  $\theta \in k(\{\theta_j\}_{j \in J})$ ; com que aquest cos és generat sobre  $k$  per una família finita d'elements separables sobre  $k$ , tots els elements d'aquest cos són separables sobre  $k$ ; en particular,  $\theta$  és separable sobre  $k$ .  $\square$

**Definició 4.4.5.** Un cos  $k$  s'anomena *perfecte* si tota extensió algebraica  $K|k$  és separable; equivalentment, si tota extensió finita  $K|k$  és separable.

Per la seva importància, destaquem el resultat següent.

**Corollari 4.4.6.** *Tota extensió algebraica d'un cos de característica zero o bé finit és separable; és a dir, tots els cossos de característica zero i tots els cossos finits són perfectes.*  $\square$

**Definició 4.4.7.** Si  $K|k$  és una extensió finita de cossos, hem vist més amunt (cf. la proposició 4.3.11) que  $[K : k]_s$  divideix  $[K : k]$ . S'anomena *grau d'inseparabilitat* de l'extensió  $K|k$  el quocient  $[K : k]_i := \frac{[K : k]}{[K : k]_s}$ .

**Observació 4.4.8.** El grau d'inseparabilitat d'una extensió finita de cossos  $K|k$ , o bé és 1 (i això pot succeir en característica qualsevol) o bé  $k$  és un cos de característica positiva  $p := \text{car}(k) > 0$  i el grau d'inseparabilitat és una potència de  $p$ . En efecte, tot polinomi irreductible de grau primer amb la característica té les arrels simples, ja que el seu derivat és diferent de zero. D'altra banda, ja hem vist (cf. la demostració de la proposició 4.3.11) que si  $\theta \in K$  no és separable sobre  $k$ , llavors existeix un nombre natural  $r \geq 1$  tal que  $\theta^{p^r}$  és separable sobre  $k$ , o sigui, que  $k(\theta^{p^r})|k$  és separable, que  $[k(\theta) : k(\theta^{p^r})]_s = 1$ , que  $X^{p^r} - \theta^{p^r}$  és irreductible sobre  $k(\theta^{p^r})$  i que  $[k(\theta) : k(\theta^{p^r})] = p^r$ , de manera que el grau d'inseparabilitat de  $k(\theta)|k$ , que coincideix amb aquest grau, és una potència de  $p$ . Això demostra l'enunciat per a les extensions de la forma  $k(\theta)|k$ ; el cas general s'obté, de nou, per la multiplicativitat dels graus i dels graus de separabilitat.

Acabem la secció amb un estudi del comportament de la separabilitat en situacions diverses: per al canvi de base, per a torres d'extensions, per a la composició d'extensions, i per pas a la clausura normal.

**Proposició 4.4.9** (Comportament de la separabilitat per canvi de base). *Siguin  $K|k$  i  $L|k$  extensions algebraiques de cossos tals que existeix un cos  $\bar{k}$  que conté  $K$  i  $L$ . Si l'extensió  $L|k$  és separable, llavors  $KL|K$  també és separable.*

**DEMOSTRACIÓ:** Podem elegir una família  $\{\theta_i\}_{i \in I}$  d'elements  $\theta_i \in L$  de manera que sigui  $L = k(\{\theta_i\}_{i \in I})$ . Comque, per hipòtesi, els elements  $\theta_i$  són separables sobre  $k$ ; també ho són sobre  $K$ , de manera que  $K(\{\theta_i\}_{i \in I})|K$  també és separable; però  $K(\{\theta_i\}_{i \in I}) = KL$ .  $\square$

**Proposició 4.4.10** (Comportament de la separabilitat per a torres d'extensions). *Siguin  $L|K$  i  $K|k$  extensions algebraiques separables de cossos. Llavors, l'extensió  $L|k$  també és separable.*

**DEMOSTRACIÓ:** Sigui  $\theta \in L$  un element qualsevol. Cal veure que  $\theta$  és separable sobre  $k$ . Considerem el polinomi  $\text{Irr}(\theta, K)(X) \in K[X]$ , i siguin  $\alpha_0, \dots, \alpha_n \in K$  els seus coeficients; com que  $K|k$  és separable, els elements  $\alpha_i$ ,  $0 \leq i \leq n$ , són separables sobre  $k$ , de manera que l'extensió finita  $k(\alpha_0, \dots, \alpha_n)|k$  és separable. D'altra banda, el polinomi

$\text{Irr}(\theta, K)(X) \in K[X]$  no té arrels múltiples, té  $\theta$  per arrel, i pertany a  $k(\alpha_0, \dots, \alpha_n)[X]$ ; per tant,  $\theta$  és separable sobre  $k(\alpha_0, \dots, \alpha_n)$ . En conseqüència,

$$\begin{aligned} [k(\alpha_0, \dots, \alpha_n, \theta) : k]_s &= [k(\alpha_0, \dots, \alpha_n, \theta) : k(\alpha_0, \dots, \alpha_n)]_s [k(\alpha_0, \dots, \alpha_n) : k]_s \\ &= [k(\alpha_0, \dots, \alpha_n, \theta) : k(\alpha_0, \dots, \alpha_n)] [k(\alpha_0, \dots, \alpha_n) : k] \\ &= [k(\alpha_0, \dots, \alpha_n, \theta) : k]. \end{aligned}$$

Per tant,  $\theta$  és separable sobre  $k$ , com volíem veure.  $\square$

**4.4.11.** Resumim en un diagrama el comportament de la separabilitat per canvi de base.

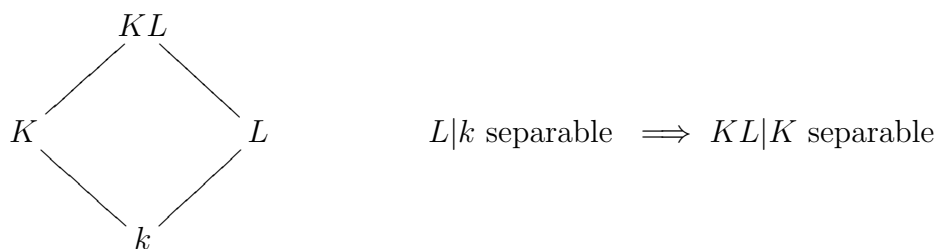


Diagrama 4.2: Comportament de la separabilitat per canvi de base

**4.4.12.** Resumim en un diagrama el comportament de la separabilitat per a torres d'extensions.

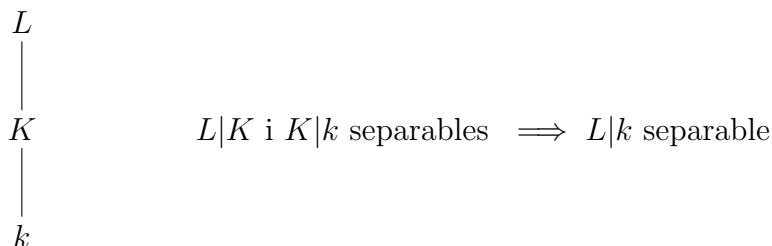


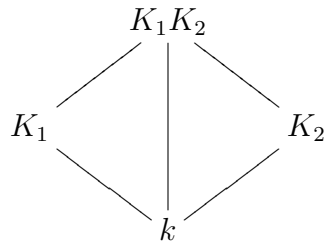
Diagrama 4.3: Comportament de la separabilitat per a torres d'extensions

El fet que la separabilitat es comporti bé per canvi de base i també es comporti bé per a torres d'extensions fa que, automàticament, es comporti bé per a la composició d'extensions. Veiem-ho. La demostració és gairebé tautològica.

**Proposició 4.4.13** (Comportament de la separabilitat per composició). *Siguin  $K_1|k$  i  $K_2|k$  extensions algebraiques de cossos tals que existeix un cos  $\bar{k}$  que conté  $K_1$  i  $K_2$ . Si les extensions  $K_1|k$  i  $K_2|k$  són separables, la composició  $K_1K_2|k$  també és separable.*

**DEMOSTRACIÓ:** En efecte; les extensions  $K_1|k$  i  $K_1K_2|K_1$  són separables, la primera per hipòtesi i la segona per canvi de base. Com que la separabilitat es comporta bé per a torres d'extensions, l'extensió  $K_1K_2|k$  també és separable.  $\square$

4.4.14. Resumim en un diagrama el comportament de la separabilitat per composició.



$$K_1|k, K_2|k \text{ separables} \implies K_1K_2|k \text{ separable}$$

Diagrama 4.4: Comportament de la separabilitat per composició

**Corol·lari 4.4.15.** *Sigui  $K|k$  una extensió finita. El conjunt  $K_s$  format per tots els elements  $\theta \in K$  separables sobre  $k$  és un subcòs de  $K$  que conté  $k$ ; l'extensió  $K_s|k$  és la màxima subextensió de  $K|k$  que és separable.  $\square$*

Més generalment, tenim el resultat següent.

**Corol·lari 4.4.16.** *Sigui  $K|k$  una extensió algebraica. El conjunt  $K_s$  format per tots els elements  $\theta \in K$  separables sobre  $k$  és un subcòs de  $K$  que conté  $k$ ; l'extensió  $K_s|k$  és la màxima subextensió de  $K|k$  que és separable.  $\square$*

**Definició 4.4.17.** La màxima subextensió separable  $K_s|k$  de  $K|k$  s'anomena la *clausura separable* de  $k$  en  $K$ .

**Proposició 4.4.18** (Comportament de la separabilitat per clausura normal). *Sigui  $K|k$  una extensió algebraica separable de cossos, i suposem que  $K$  està inclòs en un cos algebraicament tancat  $\bar{k}$ . Llavors, la clausura normal  $N|k$  de  $K|k$  també és separable.*

DEMOSTRACIÓ: Podem escriure  $K = k(\{\theta_i\}_{i \in I})$  per a una certa família,  $\{\theta_i\}_{i \in I}$ , tal que per a tot  $i \in I$ , l'element  $\theta_i \in K$  i és algebraic i separable sobre  $k$ . Això implica que totes les arrels dels polinomis  $\text{Irr}(\theta_i, k)(X) \in k[X]$  són elements separables sobre  $k$ . Ara bé, la clausura normal  $N|k$  de l'extensió  $K|k$  és tal que el cos  $N$  és el cos de descomposició de la família de polinomis  $\{\text{Irr}(\theta_i, k)(X)\}_{i \in I}$ ; per tant, l'extensió  $N|k$  és separable.  $\square$

4.4.19. Resumim en un diagrama el comportament de la separabilitat per pas a la clausura normal.

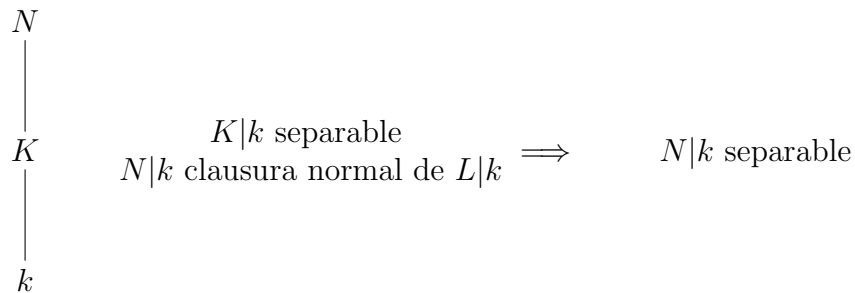


Diagrama 4.5: Clausura normal d'una extensió separable



## 4.5 El teorema de l'element primitiu

Hem vist més amunt que el cos generat sobre  $k$  per totes les arrels  $n$ -èsimes de la unitat coincideix amb el cos generat sobre  $k$  per una arrel primitiva  $n$ -èsima de la unitat; també que, en el cas que  $m, n$  siguin nombres naturals primers entre si, el cos generat sobre  $k$  per una arrel primitiva  $n$ -èsima de la unitat i una arrel primitiva  $m$ -èsima de la unitat coincideix amb el cos generat sobre  $k$  per una arrel primitiva  $mn$ -èsima de la unitat (cf. 3.5.3); i també que el cos generat sobre  $k$  per una arrel del polinomi  $X^n - a \in k[X]$  i una del polinomi  $X^m - a$ , coincideix amb el cos generat sobre  $k$  per una arrel del polinomi  $X^{nm} - a$  (cf. la demostració de la proposició 4.1.5). En altres paraules, hem vist que podem trobar un sol generador per a alguns cossos generats, en principi, per més d'un element. La pregunta natural és si aquest fet és general; és a dir, si podem canviar qualsevol sistema de generadors d'un cos sobre un altre per un únic generador.

Així formulada, la pregunta té resposta negativa; en efecte, si una extensió algebraica  $K|k$  és tal que existeix un element  $\theta \in K$  per al qual és  $K = k(\theta)$ , llavors l'extensió  $K|k$  és, per força, finita. Però la pregunta encara té sentit per a les extensions finites  $K|k$ . És veritat que, donada una extensió finita  $K|k$ , existeix un element  $\theta \in K$  tal que  $K = k(\theta)$ ?

**Definició 4.5.1.** Sigui  $K|k$  una extensió algebraica finita. Si existeix un element  $\theta \in K$  tal que  $K = k(\theta)$ , es diu que  $\theta$  és un *element primitiu* per a l'extensió  $K|k$ .

El propòsit d'aquesta secció és, d'una banda, caracteritzar les extensions finites  $K|k$  per a les quals existeix algun element primitiu; i de l'altra, demostrar que les extensions finites i separables sempre admeten element primitiu. Abans de començar per la primera caracterització, provem un resultat que és important per si mateix.

**Proposició 4.5.2.** *Siguin  $L|k$  una extensió finita que admet un element primitiu,  $\theta$ , i  $K \subseteq L$  un subcòs de  $L$  que conté  $k$ . Llavors, podem recuperar el cos  $K$  com el cos generat sobre  $k$  pel conjunt dels coeficients del polinomi  $\text{Irr}(\theta, K)(X) \in K[X]$ . És a dir, si escrivim  $\text{Irr}(\theta, K)(X) = \alpha_0 + \alpha_1 X + \dots + \alpha_{n-1} X^{n-1} + X^n \in K[X]$ , amb  $\alpha_0, \dots, \alpha_{n-1} \in K$ , llavors  $K = k(\alpha_0, \dots, \alpha_{n-1})$ .*

**DEMOSTRACIÓ:** Notem que  $\theta$  també és un element primitiu de l'extensió  $L|K$  i que, en conseqüència, el grau  $[L : K]$  és el grau del polinomi  $\text{Irr}(\theta, K)(X) \in K[X]$ . Sigui  $K_0 := k(\alpha_0, \dots, \alpha_{n-1}) \subseteq K$  el subcòs de  $K$  generat sobre  $k$  pels coeficients de  $\text{Irr}(\theta, K)(X)$ ; en particular,  $\text{Irr}(\theta, K)(X) \in K_0[X]$ , de manera que és irreductible en  $K_0[X]$  (un factor no constant del polinomi en  $K_0[X]$  seria un factor en  $K[X]$ , no constant). Però també és  $L = K_0(\theta)$ , de manera que el grau  $[L : K_0]$  és el grau d'aquest polinomi, que és el grau  $[L : K]$ ; com que  $K_0 \subseteq K \subseteq L$ , ha de ser  $K_0 = K$ , com volem demostrar.  $\square$

**Proposició 4.5.3** (Criteri d'existència d'element primitiu). *Sigui  $L|k$  una extensió finita. L'extensió  $L|k$  admet un element primitiu si, i només si, el conjunt format per totes les subextensions  $K|k$  de  $L|k$  és finit.*

**DEMOSTRACIÓ:** En primer lloc, suposem que  $L$  és un cos finit; és clar que el conjunt de les subextensions de  $L|k$  és finit; però també sabem que el grup multiplicatiu dels elements no nuls de  $L$  és cíclic, de manera que un generador d'aquest grup és un element primitiu de l'extensió  $L|k$ . Per tant, no hi ha res a provar. Així, podem suposar que el cos  $L$ , i, en conseqüència, el cos  $k$ , és infinit.

Signin  $\theta \in L$  un element primitiu de  $L|k$  i  $f(X) := \text{Irr}(\theta, k)(X) \in k[X]$  el seu polinomi minimal sobre  $k$ . Per a cada subextensió  $K|k$  de  $L|k$  el polinomi  $\text{Irr}(\theta, K)(X) \in K[X]$  és un divisor mònic del polinomi  $f(X)$  en  $K[X]$  (doncs, també un divisor en  $L[X]$ ) i  $K$  és generat sobre  $k$  pels coeficients d'aquest polinomi (cf. la proposició 4.5.2). Per tant, a cada subextensió  $K|k$  de  $L|k$  li podem fer correspondre un divisor, en  $L[X]$ , del polinomi  $f(X)$ , i recuperem el cos  $K$  a partir dels coeficients d'aquest divisor; així, obtenim una aplicació injectiva del conjunt de les subextensions  $K|k$  de  $L|k$  en el conjunt dels divisors mòncics de  $f(X)$  en  $L[X]$ . Ara bé, el conjunt dels divisors mòncics d'un polinomi qualsevol és finit, de manera que el conjunt de subextensions  $K|k$  de  $L|k$  és finit.

Recíprocament, suposem que el conjunt de les subextensions  $K|k$  de  $L|k$  és finit, i siguin  $\theta_1, \theta_2 \in K$  elements qualssevol. Com que el conjunt de les subextensions de  $K|k$  de la forma  $k(\theta_1 + c\theta_2)|k$ , quan  $c$  recorre  $k$ , és finit, i com que  $k$  és infinit, existeixen elements diferents  $c_1, c_2 \in k$  tals que  $k(\theta_1 + c_1\theta_2) = k(\theta_1 + c_2\theta_2)$ . Observem que aquest cos és un subcòs de  $k(\theta_1, \theta_2)$ . Recíprocament, qualsevol cos que contingui  $k, \theta_1 + c_1\theta_2$  i  $\theta_1 + c_2\theta_2$  també conté la diferència  $(c_2 - c_1)\theta_2$  i, com que  $c_2 - c_1 \neq 0$  i  $c_2 - c_1 \in k$ , conté l'element  $\theta_2$ , de manera que conté l'element  $\theta_1 = (\theta_1 + c_1\theta_2) - c_1\theta_2$ ; és a dir,  $k(\theta_1, \theta_2) = k(\theta_1 + c_1\theta_2)$ .

Hem provat, doncs, que si un subcòs  $K \subseteq L$  és generat sobre  $k$  per dos elements  $\theta_1, \theta_2 \in L$ , aleshores, existeix algun element  $c_1 \in k$  tal que  $K = k(\theta_1 + c_1\theta_2)$ .

Podem aplicar aquest fet inductivament a tota subextensió  $K|k$  de  $L|k$ , perquè, com que  $K|k$  és una extensió finita, és finitament generada sobre  $k$  per elements de  $L$ . En particular, també s'aplica a l'extensió  $L|k$ , i obtenim que, si  $L = k(\theta_1, \dots, \theta_n)$ , llavors existeixen elements  $c_2, \dots, c_n \in k$  tals que, per a  $\theta := \theta_1 + c_2\theta_2 + \dots + c_n\theta_n \in L$ , és  $L = k(\theta)$ .  $\square$

**Teorema 4.5.4** (Teorema de l'element primitiu). *Tota extensió finita i separable de cossos admet un element primitiu.*

DEMOSTRACIÓ: En la demostració del criteri anterior (4.5.3) hem vist de passada que tota extensió finita de cossos finits admet un element primitiu; per tant, podem suposar que els cossos involucrats són infinits. Signi, doncs,  $K|k$  una extensió finita i separable de cossos infinits, i siguin  $\theta_1, \dots, \theta_m \in K$  elements tals que  $K = k(\theta_1, \dots, \theta_m)$ . Per inducció sobre  $m$ , i anàlogament a la demostració del criteri, és suficient provar que per a tota parella d'elements  $\theta_1, \theta_2 \in K$ , l'extensió  $k(\theta_1, \theta_2)|k$  admet un element primitiu. Com que  $\theta_1, \theta_2 \in K$  i l'extensió  $K|k$  és separable, per hipòtesi, el grau de separabilitat de l'extensió  $k(\theta_1, \theta_2)|k$  coincideix amb el seu grau, posem  $n$ . Signi, doncs,  $\sigma_1, \dots, \sigma_n$  les  $n$   $k$ -immersions diferents de  $k(\theta_1, \theta_2)$  en un cos algebraicament tancat  $\bar{k}$  que conté  $k$ . Posem

$$f(X) := \prod_{i \neq j} (\sigma_i(\theta_1) + \sigma_i(\theta_2)X - \sigma_j(\theta_1) - \sigma_j(\theta_2)X).$$

Si un factor  $(\sigma_i(\theta_1) + \sigma_i(\theta_2)X - \sigma_j(\theta_1) - \sigma_j(\theta_2)X)$  del polinomi fos nul, hauria de ser  $\sigma_i(\theta_1) = \sigma_j(\theta_1)$  i  $\sigma_i(\theta_2) = \sigma_j(\theta_2)$ , de manera que  $\sigma_i$  i  $\sigma_j$  coincidirien sobre  $\theta_1$ , i sobre  $\theta_2$ , que generen  $k(\theta_1, \theta_2)$  sobre  $k$ ; per tant, hauria de ser  $\sigma_i = \sigma_j$ , d'on  $i = j$ . Hem provat, doncs, que  $f(X) \neq 0$ . Com que el cos  $k$  és infinit, i com que un polinomi no nul només pot tenir una quantitat finita d'arrels en  $k$ , existeix  $c \in k$  tal que  $f(c) \neq 0$ . En particular, per a  $i \neq j$  és  $\sigma_i(\theta_1 + c\theta_2) \neq \sigma_j(\theta_1 + c\theta_2)$ . Així, l'element  $\theta_1 + c\theta_2 \in k(\theta_1, \theta_2)$  admet, almenys,  $n$  transformats diferents per  $k$ -immersions. En conseqüència, el grau del polinomi  $\text{Irr}(\theta_1 + c\theta_2, k)(X) \in k[X]$  és, com a mínim,  $n$  i, per tant,  $[k(\theta_1 + c\theta_2) : k] \geq n$ .

Ara, com que  $k(\theta_1 + c\theta_2) \subseteq k(\theta_1, \theta_2)$  i com que  $[k(\theta_1, \theta_2) : k] = n$ , és  $k(\theta_1, \theta_2) = k(\theta_1 + c\theta_2)$ , com volem demostrar.  $\square$

**Observació 4.5.5.** Notem que si  $\text{car}(k) = 0$ , els elements  $c$  es poden prendre nombres naturals, perquè el polinomi  $f(X)$  no pot anul·lar-se en tots els nombres naturals.

## 4.6 Normes i traces

**4.6.1.** Sigui  $K|k$  una extensió finita de cossos. Podem pensar  $K$  com un espai vectorial sobre  $k$  i considerar, per a tot element  $\theta \in K$ , l'aplicació  $k$ -lineal de multiplicació per  $\theta$ ,  $m_\theta : K \rightarrow K$ ; és a dir, l'aplicació donada per  $m_\theta(x) := \theta x$ , per a tot  $x \in K$ . Llavors, l'aplicació  $m : K \rightarrow \text{End}_k(K)$  donada per  $m(\theta) := m_\theta$  és un morfisme d'anells (de fet, de  $k$ -àlgebres); és a dir, se satisfan les propietats  $m_{\theta_1 + \theta_2} = m_{\theta_1} + m_{\theta_2}$ ,  $m_{\theta_1 \theta_2} = m_{\theta_1} \circ m_{\theta_2}$ , i  $m_1 = 1$ . I com que, si  $\theta \neq 0$ ,  $m_\theta$  és un automorfisme  $k$ -lineal de  $K$ ,  $m$  també es pot veure com un morfisme de grups  $m : K^* \rightarrow \mathbf{GL}(K)$ , on  $\mathbf{GL}(K)$  indica el grup dels automorfismes  $k$ -lineals de  $K$ .

En particular, per a cada element  $\theta \in K$  podem considerar el polinomi característic de  $m_\theta$ ,  $\det(m_\theta - X\text{id}) \in k[X]$ ; és un polinomi de  $k[X]$  que té  $\theta$  per arrel i que, si posem  $n := [K : k]$  i escrivim

$$\det(m_\theta - X\text{id}) = a_0(\theta) - a_1(\theta)X + \cdots + (-1)^{n-1}a_{n-1}(\theta)X^{n-1} + (-1)^n X^n,$$

amb  $a_0(\theta), a_1(\theta), \dots, a_{n-1}(\theta) \in k$ , dóna lloc a  $n$  aplicacions  $a_i : K \rightarrow k$ ,  $0 \leq i \leq n-1$ . Per causa de les seves propietats, les aplicacions  $a_0$  i  $a_{n-1}$  són especialment interessants. D'una banda, podem considerar l'aplicació  $a_0$  com el determinant de  $m$ ; és a dir,  $a_0$  és la composició  $K^* \xrightarrow{m} \mathbf{GL}(K) \xrightarrow{\det} k^*$ , i és un morfisme de grups. De l'altra, l'aplicació  $a_{n-1}$  és la traça de  $m$ ; és a dir,  $a_{n-1}$  és la composició  $K \xrightarrow{m} \text{End}_k(K) \xrightarrow{\text{tr}} k$ , i és  $k$ -lineal. Aquestes dues aplicacions es coneixen amb els noms de norma i traça de l'extensió  $K|k$ , d'acord amb la definició següent.

**Definició 4.6.2.** Sigui  $K|k$  una extensió finita de cossos. S'anomena *norma* de  $K$  sobre  $k$  l'aplicació  $N_{K|k} : K \rightarrow k$  donada, sobre  $\theta \in K$ , pel determinant de la multiplicació per  $\theta$ . S'anomena *traça* de  $K$  sobre  $k$  l'aplicació  $k$ -lineal  $\text{Tr}_{K|k} : K \rightarrow k$  donada, sobre  $\theta \in K$ , per la traça de la multiplicació per  $\theta$ .

En particular, doncs, i si posem  $n := [K : k]$ , se satisfan les propietats següents. Per a  $\theta_1, \theta_2 \in K$ ,  $c_1, c_2 \in k$ , i si  $\theta \in k$ , és

- (a)  $N_{K|k}(\theta_1 \theta_2) = N_{K|k}(\theta_1) N_{K|k}(\theta_2)$ ;
- (b)  $\text{Tr}_{K|k}(c_1 \theta_1 + c_2 \theta_2) = c_1 \text{Tr}_{K|k}(\theta_1) + c_2 \text{Tr}_{K|k}(\theta_2)$ ;
- (c)  $N_{K|k}(\theta) = \theta^n$ ; i
- (d)  $\text{Tr}_{K|k}(\theta) = n\theta$ .

**Proposició 4.6.3** (Càlcul de normes i de traces). *Siguin  $K|k$  una extensió finita de cossos i  $\theta \in K$  un element qualsevol. Llavors,*

$$N_{K|k}(\theta) = N_{k(\theta)|k}(\theta)^{[K:k(\theta)]}, \quad \text{Tr}_{K|k}(\theta) = [K : k(\theta)] \text{Tr}_{k(\theta)|k}(\theta).$$

A més a més, si posem

$$\text{Irr}(\theta, k)(X) = X^n - a_{n-1}X^{n-1} + \dots + (-1)^{n-1}a_1X + (-1)^na_0,$$

amb  $a_0, \dots, a_{n-1} \in k$ , tenim que

$$N_{k(\theta)|k}(\theta) = a_0, \quad \text{Tr}_{k(\theta)|k}(\theta) = a_{n-1}.$$

DEMOSTRACIÓ: El menor subcòs de  $K$  on el càlcul de la traça i de la norma d'un element  $\theta \in K$  té sentit és el cos  $k(\theta)$ . Per a fer-lo, siguin  $\{\theta_i\}_{i \in I}$  una  $k$ -base de  $k(\theta)$  i  $M$  la matriu de la multiplicació per  $\theta$  en  $k(\theta)$  relativa a aquesta base. El polinomi característic de  $M$  pertany a  $k[X]$ , és de grau  $[k(\theta) : k]$  i s'anul·la en  $\theta$  (teorema de Cayley-Hamilton), de manera que, afectat del signe  $(-1)^n$ , coincideix amb el polinomi  $\text{Irr}(\theta, k)(X)$ . Per tant,

$$N_{k(\theta)|k}(\theta) = a_0, \quad \text{Tr}_{k(\theta)|k}(\theta) = a_{n-1}.$$

Els valors de la norma i de la traça de  $\theta$  relatives a l'extensió  $K|k$  s'obtenen fàcilment a partir dels valors de la norma i de la traça de  $\theta$  relatives a l'extensió  $k(\theta)|k$ . En efecte, si  $\{\eta_j\}_{j \in J}$  és una  $k(\theta)$ -base de  $K$ , llavors,  $\{\theta_i \eta_j\}_{(i,j) \in I \times J}$  és una  $k$ -base de  $K$  i la matriu

de la multiplicació per  $\theta$  en  $K$  relativa a aquesta base és de la forma

$$\begin{bmatrix} M & 0 & \dots & 0 \\ 0 & M & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & M \end{bmatrix}.$$

Per tant, el polinomi característic de la multiplicació per  $\theta$  en  $K$  és la potència  $[K : k(\theta)]$ -èsima del polinomi característic de  $M$ . En particular, per a la norma i la traça de  $\theta$ , obtenim les fórmules enunciades.  $\square$

**Proposició 4.6.4.** *Siguin  $K|k$  una extensió finita de cossos,  $\theta \in K$  un element qualsevol, i  $\tau_u$ ,  $1 \leq u \leq [K : k]_s$ , les  $k$ -immersións diferents de  $K$  en qualsevol cos algebraicament tancat  $\bar{k}$  que contingui  $k$ . Llavors,*

$$N_{K|k}(\theta) = \left( \prod_{u=1}^{[K:k]_s} \tau_u(\theta) \right)^{[K:k]_i}, \quad \text{Tr}_{K|k}(\theta) = [K : k]_i \sum_{u=1}^{[K:k]_s} \tau_u(\theta).$$

DEMOSTRACIÓ: Posem  $d := [k(\theta) : k]$  i siguin  $\theta_1 := \theta, \theta_2, \dots, \theta_d$  les  $d$  arrels del polinomi  $\text{Irr}(\theta, k)(X)$ . Notem que aquí, cadascuna de les arrels diferents està repetida tantes vegades com indica la seva multiplicitat, i que aquesta és la mateixa per a totes (cf. el final de la demostració de la proposició 4.3.11). Tenim que

$$\text{Tr}_{k(\theta)|k}(\theta) = \theta_1 + \dots + \theta_d, \quad N_{k(\theta)|k}(\theta) = \theta_1 \cdots \theta_d,$$

perquè

$$\text{Irr}(\theta, k)(X) = (-1)^d \det(m_\theta - X\text{Id}) = (X - \theta_1) \cdots (X - \theta_d).$$

Com que totes les arrels del polinomi  $\text{Irr}(\theta, k)(X)$  són de la mateixa multiplicitat, si  $d_s := [k(\theta) : k]_s$  designa el grau de separabilitat de l'extensió  $k(\theta)|k$ ,  $p^i$  designa el grau d'inseparabilitat de l'extensió  $k(\theta)|k$ , i  $\sigma_1, \dots, \sigma_{d_s}$  són les  $d_s$   $k$ -immersións diferents de  $k(\theta)$  en qualsevol cos algebraicament tancat  $\bar{k}$  que conté  $k$ , obtenim que

$$N_{k(\theta)|k}(\theta) = \left( \prod_{t=1}^{d_s} \sigma_t(\theta) \right)^{p^i}, \quad \text{Tr}_{k(\theta)|k}(\theta) = p^i \sum_{t=1}^{d_s} \sigma_t(\theta).$$

Notem que cada  $k$ -immersió de  $k(\theta)$  en  $\bar{k}$  s'estén a una  $k$ -immersió de  $K$  en  $\bar{k}$  exactament de  $[K : k(\theta)]_s$  maneres diferents. Per tant,

$$\prod_{u=1}^{[K:k]_s} \tau_u(\theta) = \left( \prod_{t=1}^{d_s} \sigma_t(\theta) \right)^{[K:k(\theta)]_s}, \quad \sum_{u=1}^{[K:k]_s} \tau_u(\theta) = [K : k(\theta)]_s \sum_{t=1}^{d_s} \sigma_t(\theta).$$

Com a conseqüència,

$$\begin{aligned} \left( \prod_{u=1}^{[K:k]_s} \tau_u(\theta) \right)^{[K:k]_i} &= \left( \prod_{t=1}^{d_s} \sigma_t(\theta) \right)^{[K:k(\theta)]_s [K:k]_i} = \left( \prod_{t=1}^{d_s} \sigma_t(\theta) \right)^{[k(\theta):k]_i [K:k(\theta)]} \\ &= (N_{k(\theta)|k}(\theta))^{[K:k(\theta)]} = N_{K|k}(\theta); \end{aligned}$$

i, anàlogament,

$$\begin{aligned} [K : k]_i \sum_{u=1}^{[K:k]_s} \tau_u(\theta) &= [K : k]_i [K : k(\theta)]_s \sum_{t=1}^{d_s} \sigma_t(\theta) \\ &= [K : k(\theta)] [k(\theta) : k]_i \sum_{t=1}^{d_s} \sigma_t(\theta) = [K : k(\theta)] \text{Tr}_{k(\theta)|k}(\theta) = \text{Tr}_{K|k}(\theta). \quad \square \end{aligned}$$

**Corol·lari 4.6.5.** *Si  $K|k$  és una extensió finita i no separable de cossos, llavors  $\text{Tr}_{K|k} = 0$ .*  
□

**Teorema 4.6.6** (Transitivitat de la traça i de la norma). *Siguin  $L|K$  i  $K|k$  extensions finites. Llavors,*

$$N_{L|k} = N_{K|k} \circ N_{L|K}, \quad \text{Tr}_{L|k} = \text{Tr}_{K|k} \circ \text{Tr}_{L|K}.$$

DEMOSTRACIÓ: Considerem els graus,  $n := [K : k]$ ,  $m := [L : K]$ , els graus de separabilitat,  $n_s := [K : k]_s$ ,  $m_s := [L : K]_s$ , i els graus d'inseparabilitat, i  $p^i := [K : k]_i$ ,  $p^j := [L : K]_i$ , de les dues extensions  $K|k$  i  $L|K$ . Així,  $n = p^i n_s$ ,  $m = p^j m_s$  i, a més a més,  $[L : k] = nm$ ,  $[L : k]_s = n_s m_s$  i  $[L : k]_i = p^{i+j}$ . Considerem una clausura normal  $N|k$  de l'extensió  $L|k$  i siguin  $\sigma_1, \dots, \sigma_{n_s} \in \text{Gal}(N|k)$  extensions a  $N$  de les  $n_s$   $k$ -immersions diferents de  $K$  en  $\bar{k}$ , i  $\tau_1, \dots, \tau_{m_s} \in \text{Gal}(N|K) \subseteq \text{Gal}(N|k)$  extensions a  $N$  de les  $m_s$   $K$ -immersions diferents de  $L$  en  $\bar{k}$ . Aleshores, les composicions  $\sigma_t \circ \tau_u \in \text{Gal}(N|k)$  són  $k$ -automorfismes diferents de  $N$  i les restriccions a  $L$  d'aquests automorfismes són exactament les  $n_s m_s$   $k$ -immersions diferents de  $L$  en  $\bar{k}$ . Amb aquestes notacions, el càlcul de la traça i de la norma de cadascuna d'aquestes extensions és senzill. Si  $\theta \in L$  és un element qualsevol, llavors

$$\begin{aligned} N_{L|k}(\theta) &= \left( \prod_{t,u} (\sigma_t \circ \tau_u)(\theta) \right)^{p^{i+j}} = \left( \prod_{t,u} \sigma_t(\tau_u(\theta))^{p^j} \right)^{p^i} \\ &= \left( \prod_t \sigma_t \left( \prod_u \tau_u(\theta) \right)^{p^j} \right)^{p^i} = \prod_t \sigma_t(N_{L|K}(\theta))^{p^i} = N_{K|k}(N_{L|K}(\theta)), \end{aligned}$$

i, anàlogament,

$$\begin{aligned} \text{Tr}_{L|k}(\theta) &= p^{i+j} \sum_{t,u} (\sigma_t \circ \tau_u)(\theta) = p^i \sum_{t,u} \sigma_t(p^j \tau_u(\theta)) = p^i \sum_t \sigma_t \left( p^j \sum_u \tau_u(\theta) \right) \\ &= p^i \sum_t \sigma_t(\text{Tr}_{L|K}(\theta)) = \text{Tr}_{K|k}(\text{Tr}_{L|K}(\theta)). \quad \square \end{aligned}$$

**Observació 4.6.7.** Notem que si només volguéssim establir la transitivitat per a la traça, podríem restringir la demostració al cas separable, perquè si alguna de les extensions és inseparable, llavors la traça és zero.

## 4.7 Separabilitat i traça

**4.7.1.** Donada una extensió finita de cossos  $K|k$ , podem considerar la forma  $k$ -lineal traça,  $\text{Tr}_{K|k} : K \rightarrow k$ . A partir d'aquesta forma  $k$ -lineal, i tenint en compte que el producte de  $K$  és  $k$ -bilineal i commutatiu, podem considerar la forma traça com a forma  $k$ -bilineal simètrica  $\text{Tr}_{K|k} : K \times K \rightarrow k$ , definida per l'assignació  $\text{Tr}_{K|k}(x, y) := \text{Tr}_{K|k}(xy)$ .

Si l'extensió  $K|k$  no és separable, la forma  $k$ -bilineal traça és nul·la (cf. el corol·lari 4.6.5); en canvi, si  $K|k$  és separable, la forma  $k$ -bilineal traça és no degenerada. Així, podem caracteritzar les extensions finites separables com aquelles per a les quals la forma traça és no degenerada. Per a això, comencem per demostrar el resultat següent.

**Teorema 4.7.2** (Independència lineal de caràcters). *Siguin  $G$  un grup,  $K$  un cos, i  $\chi_1, \dots, \chi_n : G \rightarrow K^*$  morfismes, diferents dos a dos, de grups. Llavors,  $\chi_1, \dots, \chi_n$  són aplicacions  $K$ -linealment independents de  $G$  en  $K$ .*

**DEMOSTRACIÓ:** Suposem que  $\chi_1, \dots, \chi_n$  siguin  $K$ -linealment dependents, i triem una combinació lineal  $\alpha_1\chi_1 + \dots + \alpha_m\chi_m = 0$  tal que  $\alpha_m \in K$  sigui diferent de zero i  $m$  sigui mínim amb aquesta propietat; això és, suposem que per a tota combinació lineal  $\beta_1\chi_1 + \dots + \beta_d\chi_d = 0$ , on  $\beta_i \in K$  i  $d < m$ , és  $\beta_i = 0$  per a tot índex  $i$ . Com que un sol morfisme de grups  $\chi : G \rightarrow K^*$  és una aplicació no nul·la, és  $K$ -linealment independent, de manera que tenim que és  $m > 1$ ; i, com que  $\chi_m \neq \chi_{m-1}$ , existeix  $g \in G$  tal que  $\chi_m(g) \neq \chi_{m-1}(g)$ . La relació  $\alpha_1\chi_1 + \dots + \alpha_m\chi_m = 0$  ens diu que, per a tot  $h \in G$ , és

$$\alpha_1\chi_1(h) + \dots + \alpha_m\chi_m(h) = 0;$$

en particular, com que  $gh \in G$ , és

$$\alpha_1\chi_1(gh) + \dots + \alpha_m\chi_m(gh) = 0,$$

per a tot  $h \in G$ ; equivalentment, i com que els  $\chi_j$  són morfismes de grups,

$$\alpha_1\chi_1(g)\chi_1(h) + \dots + \alpha_m\chi_m(g)\chi_m(h) = 0.$$

D'altra banda, si multipliquem la relació  $\alpha_1\chi_1(h) + \dots + \alpha_m\chi_m(h) = 0$  per  $\chi_m(g)$  i restem, obtenim que, per a tot  $h \in G$ , és

$$\alpha_1(\chi_1(g) - \chi_m(g))\chi_1(h) + \dots + \alpha_{m-1}(\chi_{m-1}(g) - \chi_m(g))\chi_{m-1}(h) = 0.$$

Però  $\chi_{m-1}(g) - \chi_m(g) \neq 0$ , de manera que obtenim una combinació lineal de la forma  $\beta_1\chi_1 + \dots + \beta_{m-1}\chi_{m-1} = 0$  amb  $\beta_{m-1} \neq 0$ , fet que contradueix l'elecció de  $m$ . Això acaba la demostració.  $\square$

**Proposició 4.7.3.** *Sigui  $K|k$  una extensió finita i separable de cossos. Llavors, la forma  $k$ -bilineal simètrica traça,  $\text{Tr}_{K|k} : K \times K \rightarrow k$ , donada per  $\text{Tr}_{K|k}(x, y) := \text{Tr}_{K|k}(xy)$ , és no degenerada.*

**DEMOSTRACIÓ:** És suficient provar que l'aplicació  $k$ -lineal  $\text{Tr}_{K|k}$  és no nul·la, ja que si  $x_0 \in K$  és tal que  $\text{Tr}_{K|k}(x_0) \neq 0$ , llavors, per a tot  $x \neq 0$ , existeix  $y := x^{-1}x_0 \in K$  tal que  $\text{Tr}_{K|k}(xy) = \text{Tr}_{K|k}(x(x^{-1}x_0)) \neq 0$ .

Com que l'extensió  $K|k$  és finita i separable, existeix un element primitiu; és a dir, existeix  $\theta \in K$  tal que  $K = k(\theta)$ , i podem suposar que  $\theta \neq 0$ . Siguin  $\theta_1 := \theta, \theta_2, \dots, \theta_n \neq 0$  les arrels del polinomi  $\text{Irr}(\theta, k)(X) \in k[X]$ , on  $n := [K : k]$  és el grau de l'extensió. Com que  $\theta$  és separable, tots els  $\theta_i$ ,  $1 \leq i \leq n$ , són diferents, i, per a tot  $r \in \mathbb{Z}$ , és

$$\text{Tr}_{K|k}(\theta^r) = \sum_{i=1}^n \theta_i^r.$$

Si fos  $\text{Tr}_{K|k} = 0$ , tindríem que, per a tot  $r \in \mathbb{Z}$ , seria  $\text{Tr}_{K|k}(\theta^r) = 0$ , de manera que  $\sum_{i=1}^n \theta_i^r = 0$ , per a tot  $r \in \mathbb{Z}$ . Així, si posem  $L := k(\theta_1, \dots, \theta_n)$ , els morfismes de grups  $f_i : \mathbb{Z} \rightarrow L^*$ , donats per  $f_i(r) := \theta_i^r$ , serien  $L$ -linealment dependents. Però, si  $i \neq j$  és  $f_i \neq f_j$ , ja que, per exemple,  $f_i(1) = \theta_i \neq \theta_j = f_j(1)$ , de manera que aquests morfismes són diferents dos a dos i obtindríem una contradicció amb el teorema d'independència lineal de caràcters.  $\square$

## 4.8 El teorema 90 de Hilbert

L'estudi de les traces i les normes de les extensions finites de cossos que hem fet en les seccions anteriors ens permet establir còmodament les formes multiplicativa i additiva del teorema conegut com "teorema 90 de Hilbert". Aquest resultat és bàsic per a l'obtenció que fem a la secció següent de la classificació de les extensions cícliques de cossos en el cas que el cos base contingui les arrels necessàries de la unitat.

**Definició 4.8.1.** Una extensió algebraica de cossos  $K|k$  s'anomena *de Galois* si és normal i separable. En el cas de les extensions finites, això equival a dir que l'ordre del grup de Galois  $\text{Gal}(K|k)$  coincideix amb el grau de l'extensió:  $\#\text{Gal}(K|k) = [K : k]$ .

**Definició 4.8.2.** Una extensió de Galois  $K|k$  s'anomena *cíclica* si el grup de Galois  $\text{Gal}(K|k)$  és cíclic; s'anomena *abeliana* si  $\text{Gal}(K|k)$  és commutatiu.

**Observació 4.8.3.** Notem que només definim extensió cíclica o extensió abeliana per a extensions de Galois. En general, per a extensions de Galois, s'utilitza un qualificatiu determinat per a l'extensió si per al grup s'utilitza aquell qualificatiu; per exemple, es parla d'extensions resolubles, o d'extensions nilpotents, quan l'extensió és de Galois i el grup de Galois és resoluble o nilpotent. Més endavant tractem el cas de les extensions resolubles. Ara ens interessen de manera especial les extensions cícliques.

**Teorema 4.8.4** (Teorema 90 de Hilbert). *Sigui  $K|k$  una extensió finita i cíclica de cossos,  $G := \text{Gal}(K|k)$  el seu grup de Galois,  $n := [K : k] \geq 2$  el seu grau, i  $\sigma \in G$  un generador del grup de Galois.*

- Forma multiplicativa. *Un element  $\theta \in K$  és tal que  $N_{K|k}(\theta) = 1$  si, i només si, existeix un element  $\alpha \in K$ ,  $\alpha \neq 0$ , tal que  $\theta = \frac{\alpha}{\sigma(\alpha)}$ .*
- Forma additiva. *Un element  $\theta \in K$  és tal que  $\text{Tr}_{K|k}(\theta) = 0$  si, i només si, existeix un element  $\alpha \in K$  tal que  $\theta = \alpha - \sigma(\alpha)$ .*

DEMOSTRACIÓ: Com que  $G = \{\sigma, \sigma^2, \dots, \sigma^n = \text{Id}\}$ , donat un element qualsevol  $\alpha \in K$  és  $N_{K|k}(\alpha) = \prod_{i=1}^n \sigma^i(\alpha)$  i  $\text{Tr}_{K|k}(\alpha) = \sum_{i=1}^n \sigma^i(\alpha)$ ; en particular, per a tot nombre enter  $r$ , se satisfan les igualtats  $\text{Tr}_{K|k}(\alpha) = \text{Tr}_{K|k}(\sigma^r(\alpha))$  i  $N_{K|k}(\alpha) = N_{K|k}(\sigma^r(\alpha))$ . Així, si existeix  $\alpha \in K$ ,  $\alpha \neq 0$ , tal que  $\theta = \frac{\alpha}{\sigma(\alpha)}$ , és  $N_{K|k}(\theta) = N_{K|k}\left(\frac{\alpha}{\sigma(\alpha)}\right) = \frac{N_{K|k}(\alpha)}{N_{K|k}(\sigma(\alpha))} = 1$ ; i, anàlogament per al cas additu, si existeix  $\alpha \in K$  tal que  $\theta = \alpha - \sigma(\alpha)$ , aleshores és  $\text{Tr}_{K|k}(\theta) = \text{Tr}_{K|k}(\alpha - \sigma(\alpha)) = \text{Tr}_{K|k}(\alpha) - \text{Tr}_{K|k}(\sigma(\alpha)) = 0$ .

Això demostra les implicacions senzilles de les dues formes del teorema: multiplicativa i additiva.

Recíprocament, suposem que existeix  $\theta \in K$  tal que  $N_{K|k}(\theta) = 1$ ; llavors, per a tot  $m \geq 1$ , és  $\theta\sigma(\theta) \cdots \sigma^m(\theta) \neq 0$ , de manera que, en virtut del teorema d'independència lineal de caràcters (cf. 4.7.2), l'aplicació

$$\varphi := \text{Id} + \theta\sigma + \theta\sigma(\theta)\sigma^2 + \cdots + \theta\sigma(\theta) \cdots \sigma^{n-2}(\theta)\sigma^{n-1}$$

és no nul·la; per tant, existeix un element  $\beta \in K$  tal que  $\alpha := \varphi(\beta) \neq 0$ . Per a aquest element  $\alpha$  se satisfà que

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

Ara bé, com que  $\theta\sigma(\theta)\sigma^2(\theta) \cdots \sigma^{n-1}(\theta) = N_{K|k}(\theta) = 1$  i  $\sigma^n = \text{Id}$ , és

$$\theta\sigma(\alpha) = \beta + \theta\sigma(\beta) + \theta\sigma(\theta)\sigma^2(\beta) + \cdots + \theta\sigma(\theta) \cdots \sigma^{n-2}(\theta)\sigma^{n-1}(\beta) = \alpha,$$

com volem veure, perquè  $\sigma(\alpha) \neq 0$  i, per tant,  $\theta = \frac{\alpha}{\sigma(\alpha)}$ .

Demostrem anàlogament la forma additiva del teorema. Sigui  $\theta \in K$  un element tal que  $\text{Tr}_{K|k}(\theta) = 0$ . Com que l'extensió  $K|k$  és separable, és  $\text{Tr}_{K|k} \neq 0$ , de manera que existeix  $\beta \in K$  tal que  $\text{Tr}_{K|k}(\beta) \neq 0$ ; és a dir,  $\sigma(\beta) + \sigma^2(\beta) + \cdots + \sigma^n(\beta) \neq 0$ . Posem

$$\alpha := \frac{1}{\text{Tr}_{K|k}(\beta)} (\theta\sigma(\beta) + (\theta + \sigma(\theta))\sigma^2(\beta) + \cdots + (\theta + \sigma(\theta) + \cdots + \sigma^{n-2}(\theta))\sigma^{n-1}(\beta)).$$

Llavors, se satisfà que  $\sigma(\alpha) =$

$$\begin{aligned} & \frac{1}{\text{Tr}_{K|k}(\beta)} (\sigma(\theta)\sigma^2(\beta) + (\sigma(\theta) + \sigma^2(\theta))\sigma^3(\beta) + \cdots + (\sigma(\theta) + \sigma^2(\theta) + \cdots + \sigma^{n-1}(\theta))\sigma^n(\beta)) \\ &= \frac{1}{\text{Tr}_{K|k}(\beta)} (\theta\sigma(\beta) + (\theta + \sigma(\theta))\sigma^2(\beta) + \cdots + (\theta + \sigma(\theta) + \cdots + \sigma^{n-1}(\theta))\sigma^n(\beta)) \\ & - \frac{1}{\text{Tr}_{K|k}(\beta)} (\theta\sigma(\beta) + \theta\sigma^2(\beta) + \cdots + \theta\sigma^n(\beta)); \end{aligned}$$

i, ara, com que  $\theta + \sigma(\theta) + \cdots + \sigma^{n-1}(\theta) = \text{Tr}_{K|k}(\theta) = 0$  tenim que

$$\begin{aligned} \sigma(\alpha) &= \frac{1}{\text{Tr}_{K|k}(\beta)} (\theta\sigma(\beta) + (\theta + \sigma(\theta))\sigma^2(\beta) + \cdots + (\theta + \sigma(\theta) + \cdots + \sigma^{n-2}(\theta))\sigma^{n-1}(\beta)) \\ & - \frac{1}{\text{Tr}_{K|k}(\beta)} \theta(\sigma(\beta) + \sigma^2(\beta) + \cdots + \sigma^n(\beta)) \\ &= \alpha - \theta, \end{aligned}$$

d'on  $\theta = \alpha - \sigma(\alpha)$ , com volem veure.  $\square$



**Observació 4.8.5.** El teorema 90 de Hilbert és la formulació multiplicativa del teorema 4.8.4; s'anomena d'aquesta manera perquè ocupa el lloc 90 entre els resultats retolats com a “teorema” en el llibre [Hi 1897], llibre conegut durant molt de temps, i encara ara, com el “Zahlbericht de Hilbert”. De fet, aquest resultat es continuarà coneixent com el “teorema 90 de Hilbert”, encara que aquí sigui l'apartat (a) del teorema 4.8.4 o, per exemple, en [La 1984] sigui el **Theorem 6.1**, o en [Ja 1974] sigui el **THEOREM 4.28**.

## 4.9 Extensions cíclicues

**4.9.1.** Siguin  $\bar{k}$  un cos algebraicament tancat,  $k \subseteq \bar{k}$  un subcòs,  $a \in k$  un element, i  $\alpha \in \bar{k}$  una arrel del polinomi  $X^n - a \in k[X]$ . Suposem que  $n$  no és divisible per la característica de  $k$ , que  $X^n - a$  és irreductible en  $k[X]$ , i que  $k$  conté una arrel primitiva  $n$ -èsima de la unitat,  $\zeta$ . En aquestes condicions, l'extensió  $k(\alpha)|k$  és cíclica de grau  $n$  i el grup de Galois  $\text{Gal}(k(\alpha)|k)$  és generat per l'únic  $k$ -automorfisme  $\sigma$  de  $k(\alpha)$  tal que  $\sigma(\alpha) = \zeta\alpha$  (cf. el corollari 4.2.8). Podem utilitzar el teorema 90 de Hilbert (cf. 4.8.4) per a precisar més aquell resultat. En efecte, ara podem establir el resultat següent.

**Teorema 4.9.2.** *Siguin  $\bar{k}$  un cos algebraicament tancat,  $n \geq 1$  un nombre natural no divisible per la característica de  $\bar{k}$ ,  $\zeta \in \bar{k}$  una arrel primitiva  $n$ -èsima de la unitat, i  $k \subseteq \bar{k}$  un subcòs tal que  $\zeta \in k$ .*

- (a) *Siguin  $a \in k^*$ ,  $\alpha \in \bar{k}$ , elements tals que  $\alpha^n = a$ . L'extensió  $k(\alpha)|k$  és cíclica, de grau  $d$  divisor de  $n$ ,  $\alpha^d \in k$ , i  $X^d - \alpha^d \in k[X]$  és irreductible.*
- (b) *Si  $K|k$  és una extensió de Galois cíclica de grau  $n$ , existeix un element primitiu  $\alpha \in K$  tal que  $\text{Irr}(\alpha, k)(X)$  és de la forma  $X^n - a \in k[X]$ .*

**DEMOSTRACIÓ:** Demostrem, en primer lloc, l'afirmació (a). Com que  $\zeta \in k$ , el cos  $k(\alpha)$  és el cos de descomposició del polinomi  $X^n - a \in k[X]$ , que no té arrels múltiples perquè  $n$  no és divisible per  $\text{car}(k)$ ; per tant, l'extensió  $k(\alpha)|k$  és de Galois. A més a més, l'aplicació  $\tau : \text{Gal}(k(\alpha)|k) \rightarrow \mathbb{Z}/n\mathbb{Z}$  definida per  $\sigma \mapsto \tau(\sigma)$ , on  $\tau(\sigma) \in \mathbb{Z}/n\mathbb{Z}$  és determinat per la igualtat  $\sigma(\alpha) = \zeta^{\tau(\sigma)}\alpha$ , és un morfisme injectiu de grups i identifica  $\text{Gal}(k(\alpha)|k)$  amb un subgrup  $G \subseteq \mathbb{Z}/n\mathbb{Z}$  (cf. el corollari 4.2.8). Com que  $\mathbb{Z}/n\mathbb{Z}$  és un grup cíclic d'ordre  $n$ , el grup de Galois  $\text{Gal}(k(\alpha)|k)$  és cíclic d'ordre  $d$  divisor de  $n$ .

El polinomi minimal de  $\alpha$  sobre  $k$  és  $\text{Irr}(\alpha, k)(X) = \prod_{m \in G} (X - \zeta^m \alpha)$ , el terme independent del qual és  $(-1)^d N_{k(\alpha)|k}(\alpha) = (-1)^d \alpha^d \prod_{m \in G} \zeta^m \in k$ . Com que  $G$  és l'únic subgrup de  $\mathbb{Z}/n\mathbb{Z}$  d'ordre  $d$ , és generat per  $\frac{n}{d}$  i, per tant,

$$S := \sum_{m \in G} m = \sum_{j=0}^{d-1} \frac{jn}{d} = \frac{n(d-1)}{2}.$$

Si  $n$  és senar,  $d$  és senar,  $\frac{d-1}{2} \in \mathbb{Z}$ , i  $S$  és múltiple de  $n$ , de manera que  $\zeta^S = 1 = (-1)^{d-1}$ ; i si  $n$  és parell, llavors  $\zeta^{\frac{n}{2}} = -1$ , de manera que  $\zeta^S = (-1)^{d-1}$ . En qualsevol cas, doncs,  $\prod_{m \in G} \zeta^m = \zeta^S = (-1)^{d-1}$ , i el terme independent del polinomi  $\text{Irr}(\alpha, k)(X)$  és donat

per  $(-1)^d \alpha^d \zeta^S = (-1)^{d+(d-1)} \alpha^d = -\alpha^d$ . Això demostra que  $\alpha^d \in k$ . Finalment, com que  $X^d - \alpha^d \in k[X]$  és un polinomi mònic de grau  $[k(\alpha) : k]$  que té  $\alpha$  per arrel, és  $X^d - \alpha^d = \text{Irr}(\alpha, k)(X)$  i, per tant, irreductible.

Demostrem, ara, l'afirmació (b). Sigui  $\sigma \in \text{Gal}(K|k)$  un generador del grup de Galois. Com que  $\zeta^{-1} \in k$  i  $[K : k] = n$ , és  $N_{K|k}(\zeta^{-1}) = \zeta^{-n} = 1$  i, en virtut de la formulació multiplicativa del teorema 90 de Hilbert (cf. el teorema 4.8.4, (a)), existeix  $\alpha \in K$  tal que  $\sigma(\alpha) = \zeta\alpha$ ; això implica que  $\sigma^i(\alpha) = \zeta^i\alpha$ , per a tot  $i \in \mathbb{Z}$ , ja que  $\zeta \in k$ . En particular, els  $n$  elements diferents  $\zeta^i\alpha \in K$ ,  $0 \leq i \leq n-1$ , són arrels de  $\text{Irr}(\alpha, k)(X) \in k[X]$  i, per tant,  $[k(\alpha) : k] \geq n$ . I com que  $n = [K : k]$  i  $k(\alpha) \subseteq K$ , ha de ser  $K = k(\alpha)$ . Finalment, com a la demostració de (a), resulta que el polinomi irreductible de  $\alpha$  sobre  $k$

és  $\text{Irr}(\alpha, k)(X) = \prod_{i=0}^{n-1} (X - \zeta^i\alpha) = X^n - \alpha^n$ , de manera que  $\alpha^n \in k$ , com volíem veure.  $\square$

A continuació, i a fi d'obtenir una descripció de les extensions cícliques en tots els casos, estudiem les extensions cícliques en el cas de grau igual a la característica.

**Teorema 4.9.3** (Artin–Schreier). *Siguin  $k$  un cos de característica  $p > 0$ , i  $\bar{k}$  un cos algebraicament tancat que conté  $k$ .*

- (a) *Per a tot element  $a \in k^*$ , el polinomi  $f(X) := X^p - X - a \in k[X]$  o bé té una arrel en  $k$  (i, en aquest cas, descompon en factors lineals en  $k[X]$ ), o bé és irreductible. En aquest darrer cas, si  $\alpha \in \bar{k}$  és una arrel de  $f(X)$ , l'extensió  $k(\alpha)|k$  és cíclica de grau  $p$ .*
- (b) *Si  $K|k$  és una extensió cíclica de grau  $p$ , existeix un element primitiu  $\alpha$  de l'extensió  $K|k$  tal que  $\alpha^p - \alpha \in k^*$ .*

DEMOSTRACIÓ: Comencem per la prova de (a). Sigui  $\alpha \in \bar{k}$  una arrel del polinomi  $f(X)$ . Per a tot element  $x \in \mathbb{F}_p \subseteq k$ , podem escriure  $f(\alpha + x) = (\alpha + x)^p - (\alpha + x) - a = \alpha^p + x^p - \alpha - x - a = f(\alpha) + (x^p - x) = x^p - x = 0$ ; per tant, se satisfà la igualtat  $f(X) = \prod_{x \in \mathbb{F}_p} (X - (\alpha + x))$ . En particular, el polinomi té les arrels diferents i totes

pertanyen al cos generat per  $\alpha$  sobre  $k$ . Això ens diu dues coses; d'una banda, que l'extensió  $k(\alpha)|k$  és de Galois i, de l'altra, que si  $\alpha \in k$ , llavors  $f(X)$  descompon en factors lineals en  $k[X]$ . A més a més, si el polinomi és irreductible, fet que veurem de seguida, l'extensió ha d'ésser obligatòriament cíclica, perquè és de grau primer. Suposem, doncs, que  $f(X)$  no té cap arrel en  $k$ . Si poguéssim descompondre  $f(X)$  com a producte  $f(X) = g(X)h(X)$  de dos polinomis mònic no constants  $g(X), h(X) \in k[X]$ , el factor  $g(X)$  hauria de ser de la forma  $g(X) = \prod_{x \in C} (X - (\alpha + x))$ , per a un cert subconjunt  $C \subseteq \mathbb{F}_p$

de cardinal igual al grau del polinomi  $g(X)$ ; en particular, la suma  $\sum_{x \in C} (\alpha + x)$ , que, potser llevat del signe, és un coeficient de  $g(X)$ , seria un element de  $k$ ; però aquesta suma és  $\#C\alpha + z$ , amb  $z \in \mathbb{F}_p \subseteq k$ . Això ens diu que  $\#C\alpha \in k$  i, com que  $\#C \neq 0$ , que  $\alpha \in k$ . Hem vist, doncs, que si  $f(X)$  descompon en  $k[X]$  de manera no trivial, llavors  $\alpha \in k$ ; això acaba la prova de (a).

Provem, ara, (b). Sigui  $\sigma \in \text{Gal}(K|k)$  un generador del grup de Galois. Com que  $-1 \in k$  i  $[K : k] = p = \text{car}(k)$ , és  $\text{Tr}_{K|k}(-1) = 0$ , i la forma additiva del teorema 90 de Hilbert (cf. el teorema 4.8.4, (b)), ens permet assegurar que existeix un element  $\alpha \in K$

tal que  $-1 = \alpha - \sigma(\alpha)$ ; és a dir, que  $\sigma(\alpha) = \alpha + 1$ . Llavors, per a  $0 \leq i \leq p - 1$ , és  $\sigma^i(\alpha) = \alpha + i$ , de manera que  $k(\alpha)$  conté, almenys,  $p$  transformats diferents de  $\alpha$  per  $k$ -immersions. Això implica que  $[k(\alpha) : k] \geq p$  i, per tant,  $K = k(\alpha)$ . Vegem que  $\alpha^p - \alpha \in k^*$ . El polinomi  $\text{Irr}(\alpha, k)(X) \in k[X]$  té per arrels els elements  $\sigma^i(\alpha) = \alpha + i$ , per a  $i \in \mathbb{F}_p$ ; és a dir,  $\text{Irr}(\alpha, k)(X) = \prod_{i \in \mathbb{F}_p} (X - (\alpha + i))$ . Ara bé, se satisfà la igualtat

$$\prod_{i \in \mathbb{F}_p} (X - (\alpha + i)) = \prod_{i \in \mathbb{F}_p} ((X - \alpha) - i) = (X - \alpha)^p - (X - \alpha),$$

ja que  $\prod_{i \in \mathbb{F}_p} (Y - i) = Y^p - Y \in \mathbb{F}_p[Y] \subseteq K[Y]$  i existeix un únic  $K$ -isomorfisme de  $K[Y]$  en  $K[X]$  que identifica  $Y$  amb  $X - \alpha$ . Per tant,

$$\text{Irr}(\alpha, k)(X) = X^p - X - (\alpha^p - \alpha) \in k[X],$$

de manera que  $\alpha^p - \alpha \in k$ ; i, a més a més,  $\alpha^p - \alpha \neq 0$  perquè el polinomi és irreductible. Aquest element  $\alpha$  és l'element primitiu que se cerca.  $\square$

## 4.10 Teoria (bàsica) de Kummer

Els resultats de la secció anterior permeten classificar totes les extensions cícliques de grau  $n$  sobre un cos de característica no divisor de  $n$  que conté les arrels  $n$ -èsimes de la unitat, de manera anàloga a com hem fet classificació de les extensions quadràtiques en el cas de característica diferent de 2 (cf. 3.6.2).

**Proposició 4.10.1.** *Considerem un cos algebraicament tancat,  $\bar{k}$ , un nombre natural  $n \geq 1$  no divisible per la característica de  $\bar{k}$ , una arrel primitiva  $n$ -èsima de la unitat,  $\zeta \in \bar{k}$ , i un subcòs  $k \subseteq \bar{k}$  tal que  $\zeta \in k$ .*

- (a) *Sigui  $\alpha \in \bar{k}$  un element tal que  $\alpha^n \in k$ . Llavors, per a tot element  $\beta$  de la forma  $\beta = x\alpha^s$ , amb  $x \in k^*$ ,  $0 \leq s \leq n - 1$ , i  $\text{mcd}(s, n) = 1$ , és  $\beta^n \in k$  i  $k(\beta) = k(\alpha)$ .*
- (b) *Sigui  $K|k$  una extensió cíclica de grau  $n$  i  $\alpha, \beta \in K^*$  elements primitius de l'extensió  $K|k$  tals que  $\alpha^n, \beta^n \in k$ . Llavors, existeixen un element  $x \in k^*$  i un nombre enter  $s$  tals que  $0 \leq s \leq n - 1$ ,  $\text{mcd}(s, n) = 1$ , i  $\beta = x\alpha^s$ .*

**DEMOSTRACIÓ:** Comencem per la prova de (a). Si  $\beta := x\alpha^s$ , amb  $x \in k^*$ , és clar que  $k(\beta) = k(\alpha^s) \subseteq k(\alpha)$ . D'altra banda, si  $\text{mcd}(s, n) = 1$ , existeixen nombres enters  $t, u$  tals que  $st + nu = 1$ ; llavors,  $\alpha = \alpha^{st}\alpha^{nu} \in k(\alpha^s)$ , ja que  $\alpha^{nu} \in k$ ; això prova la inclusió contrària,  $k(\alpha) \subseteq k(\alpha^s)$ .

Provem, ara, (b). Com que  $1, \alpha, \dots, \alpha^{n-1}$  és una  $k$ -base de  $k(\alpha)$ , podem escriure  $\beta \in k(\alpha)$  en la forma  $\beta = \sum_{i=0}^{n-1} x'_i \alpha^i$ , per a certs  $x'_i \in k$ ,  $0 \leq i \leq n - 1$ , i algun dels coeficients  $x'_i$  és diferent de zero, perquè  $\alpha, \beta \neq 0$ . Sigui  $s$  el menor índex tal que  $x'_s \neq 0$ . Llavors,  $0 \leq s \leq n - 1$  i, si posem  $x_i := x'_{i+s} \in k$  per a  $0 \leq i \leq n - 1 - s$ , i  $x_i = 0$  per a  $n - s \leq i \leq n - 1$ , obtenim que  $\beta\alpha^{-s} = \sum_{i=0}^{n-1} x_i \alpha^i$ , però, ara,  $x_0 = x'_s \neq 0$ . Volem

demostrar que  $\beta\alpha^{-s} \in k$  i que  $\text{mcd}(s, n) = 1$ ; però si demostrem que  $\beta\alpha^{-s} \in k$ , també és  $\text{mcd}(s, n) = 1$ . En efecte, si posem  $\delta := \text{mcd}(s, n)$  i tenim en compte que  $(\alpha^{-s})^{\frac{n}{\delta}} = (\alpha^n)^{-\frac{s}{\delta}} \in k$ , obtenim que  $[k(\alpha^{-s}) : k] \leq \frac{n}{\delta}$ . Ara, si  $\beta\alpha^{-s} \in k^*$ , és  $k(\alpha) = k(\beta) = k(\alpha^s)$ , de manera que  $n = [k(\alpha^s) : k] \leq \frac{n}{\delta}$ , fet que només pot succeir si  $\delta = 1$ .

Vegem, doncs, que  $\beta\alpha^{-s} \in k$ . Sigui  $f(X) := \text{Irr}(\beta\alpha^{-s}, k)(X) \in k[X]$ ; en virtut del teorema 4.9.2, i com que  $(\beta\alpha^{-s})^n \in k$ , l'extensió  $k(\beta\alpha^{-s})|k$  és cíclica de grau  $d$  divisor de  $n$  i  $(\beta\alpha^{-s})^d \in k$ ; per tant,  $f(X) = X^d - (\beta\alpha^{-s})^d$ . Si veiem que la suma de les arrels de  $f(X)$  no és nul·la, com que la suma de les arrels és, llevat del signe, el coeficient del monomi de grau  $d - 1$  de  $f(X)$ , haurà de ser  $d = 1$ , o sigui,  $\beta\alpha^{-s} \in k$ , i haurem acabat.

Sigui  $\sigma \in \text{Gal}(k(\alpha)|k)$  el generador del grup de Galois determinat per l'assignació  $\sigma(\alpha) = \alpha\zeta$ . Les  $d$  arrels del polinomi  $f(X)$  són alguns dels elements  $\sigma^j(\beta\alpha^{-s})$ ; és a dir, existeix un cert subconjunt no buit  $C \subseteq \{0, 1, \dots, n-1\}$ , de cardinal  $d$ , tal que les arrels de  $f(X)$  són els elements  $\sigma^j(\beta\alpha^{-s})$ , per a  $j \in C$ . Ara, la suma de les arrels de  $f(X)$  és l'element de  $k$

$$\begin{aligned} \sum_{j \in C} \sigma^j(\beta\alpha^{-s}) &= \sum_{j \in C} \sigma^j \left( \sum_{i=0}^{n-1} x_i \alpha^i \right) = \sum_{i=0}^{n-1} \sum_{j \in C} x_i \sigma^j(\alpha^i) = \sum_{i=0}^{n-1} \sum_{j \in C} x_i \alpha^i \zeta^{ij} \\ &= \sum_{i=0}^{n-1} \left( \sum_{j \in C} x_i \zeta^{ij} \right) \alpha^i = \sum_{j \in C} x_0 = x_0 d \neq 0, \end{aligned}$$

ja que, d'una banda, és un element de  $k$  i està expressat en la  $k$ -base  $\{1, \alpha, \dots, \alpha^{n-1}\}$  de  $k(\alpha)$ , de manera que  $\sum_{j \in C} x_i \zeta^{ij} = 0$  per a  $1 \leq i \leq n-1$ , i, de l'altra, és  $d \neq 0$ , perquè  $\text{car}(k)$  no divideix  $n$  i, per tant, no divideix  $d$ .  $\square$

La classificació de les extensions cíclics de  $k$  de grau  $n$  no divisible per la característica de  $k$  és donada, anàlogament al cas de les extensions quadràtiques (cf. la proposició 3.6.4), pel conjunt dels subgrups cíclics d'ordre  $n$  del grup abelià quocient  $k^*/k^{*n}$ .

**Corol·lari 4.10.2.** *Siguin  $\bar{k}$  un cos algebraicament tancat,  $n \geq 1$  un nombre natural no divisible per la característica de  $\bar{k}$ ,  $\zeta \in \bar{k}$  una arrel primitiva  $n$ -èsima de la unitat, i  $k \subseteq \bar{k}$  un subcòs tal que  $\zeta \in k$ . Sigui  $\mathfrak{C}_n(k)$  el conjunt de totes les extensions cíclics de grau  $n$  de  $k$  i  $\mathcal{C}_n(k)$  el conjunt format per tots els subgrups cíclics d'ordre  $n$  del grup abelià quocient  $k^*/k^{*n}$ . Llavors, existeix una aplicació bijectiva  $f : \mathfrak{C}_n(k) \rightarrow \mathcal{C}_n(k)$ .*

**DEMOSTRACIÓ:** La proposició anterior, 4.10.1, ens diu que donada una extensió cíclica de grau  $n$  de  $k$ ,  $K|k$ , existeix un element primitiu  $\alpha \in K$  tal que  $a := \alpha^n \in k^*$ . Vegem, en primer lloc, que l'ordre del subgrup cíclic de  $k^*/k^{*n}$  generat per la classe de  $a$  és  $n$ . En efecte, si, per a algun nombre natural  $d \geq 1$ , és  $a^d \in k^{*n}$ , llavors podem escriure  $a^d = b^n$ , per a algun element  $b \in k^*$ , de manera que se satisfà la igualtat  $\alpha^{dn} = b^n$  i, com que  $\zeta \in k$ , és  $\alpha^d \in k$ . Per tant, l'extensió  $K|k$  és cíclica de grau divisor de  $d$ , i això ens diu que  $n$  divideix  $d$ .

D'altra banda, si  $\beta \in K$  és un altre element primitiu de  $K|k$  tal que  $b := \beta^n \in k^*$ , la mateixa proposició 4.10.1 proporciona l'existència d'un nombre enter  $s$ ,  $0 \leq s \leq n-1$  i tal que  $\text{mcd}(s, n) = 1$ , i d'un element  $x \in k^*$ , tals que  $\beta = \alpha^s x$ ; llavors,  $b$  genera el mateix subgrup cíclic d'ordre  $n$  que  $a$  en  $k^*/k^{*n}$ ; en efecte, com que  $b = \beta^n = \alpha^{sn} x^n = a^s x^n$ , el

subgrup que genera  $b$  és el mateix que el subgrup que genera  $a^s$ , que és el mateix que el subgrup que genera  $a$ , perquè  $\text{mcd}(s, n) = 1$ .

Això permet definir una aplicació  $f$  com la desitjada. En efecte, per a cada extensió cíclica  $K|k$  de grau  $n$ , triem un element primitiu  $\alpha \in K$  tal que  $\alpha^n \in k^*$ , i a l'extensió  $K|k$  li fem correspondre el subgrup cíclic generat per  $\alpha^n$  en el grup quocient  $k^*/k^{*n}$ , que és d'ordre  $n$ ,

Recíprocament, donat un subgrup cíclic d'ordre  $n$  de  $k^*/k^{*n}$ , sigui  $a \in k^*$  un representant de qualsevol generador del subgrup. Llavors, una arrel  $\alpha$  del polinomi  $X^n - a \in k[X]$  genera una extensió cíclica  $k(\alpha)|k$  de grau  $d$  divisor de  $n$ . Ara bé, com que el subgrup generat per  $a$  en  $k^*/k^{*n}$  és d'ordre  $[k(\alpha) : k]$ , tenim que  $d = n$  i  $k(\alpha)|k$  és cíclica d'ordre  $n$ .

Clarament, en virtut de la proposició anterior, **4.10.1**, aquestes dues assignacions són inverses l'una de l'altra, de manera que l'aplicació  $f$  admet una inversa i, en conseqüència, és bijectiva.  $\square$

En el cas de característica positiva  $p = \text{car}(k)$ , podem fer una descripció semblant de les extensions cícliques de grau  $p$ ; això inclou el cas de les extensions quadràtiques per a  $p = 2$ . Ara, però, no serveix el grup multiplicatiu, perquè no hi ha arrels primitives  $n$ -èsimes de la unitat. Cal canviar el grup cíclic. Ho veiem en el teorema següent.

**Teorema 4.10.3.** *Siguin  $p > 0$  un nombre primer,  $k$  un cos de característica  $p$ , i  $\bar{k}$  un cos algebraicament tancat que conté  $k$ .*

- L'aplicació  $\wp : k \rightarrow k$  donada per  $\wp(x) := x^p - x$  és un morfisme de grups additius. Per tant, el conjunt dels elements de  $k$  de la forma  $x^p - x$ ,  $x \in k$ , és el subgrup imatge,  $\wp(k)$ , de  $k$ .*
- Sigui  $\alpha \in \bar{k}$  un element tal que  $\alpha^p - \alpha \in k$ . Per a tot element  $\beta \in \bar{k}$  de la forma  $\beta = s\alpha + x$ , on  $s \in \mathbb{Z}$  no és divisible per  $p$  i  $x \in k$ , és  $\beta^p - \beta \in k$  i  $k(\beta) = k(\alpha)$ .*
- Per a un element  $\alpha \in \bar{k}$  tal que  $\alpha^p - \alpha \in k$ , l'extensió  $k(\alpha)|k$  és trivial o bé cíclica de grau  $p$  segons que  $\alpha^p - \alpha \in \wp(k)$  o bé  $\alpha^p - \alpha \notin \wp(k)$ , respectivament.*
- Suposem que  $K|k$  és una extensió cíclica de grau  $p$ , i  $\alpha, \beta \in K$  són elements primitius de l'extensió  $K|k$  tals que  $\alpha^p - \alpha, \beta^p - \beta \in k$ . Llavors, existeixen un element  $x \in k$  i un nombre enter  $s$  no divisible per  $p$  tals que  $\beta = s\alpha + x$ .*
- Existeix una aplicació bijectiva del conjunt  $\mathfrak{C}_p(k)$ , de totes les extensions cícliques de grau  $p$  de  $k$  en el conjunt  $\mathcal{C}_p(k)$  dels subgrups cíclics d'ordre  $p$  del grup abelià quocient  $k/\wp(k)$ .*

**DEMOSTRACIÓ:** La comprovació de les propietats (a) i (b) és rutinària i immediata. I la propietat (c) és una conseqüència del teorema d'Artin-Schreier (cf. el teorema **4.9.3**, (a)), ja que el polinomi  $X^p - X - a$  té arrels en  $k$  si, i només si,  $a \in \wp(k)$ . Vegem ara la propietat (d).

Per a això, sigui  $K|k$  una extensió cíclica de grau  $p$  i suposem que  $\alpha, \beta \in K$  són tals que  $K = k(\alpha) = k(\beta)$ , i que  $a := \alpha^p - \alpha, b := \beta^p - \beta \in k$ . Notem que, per (c),  $a, b \notin \wp(k)$ , perquè  $\alpha, \beta \notin k$ , ja que  $[k(\beta) : k] = [k(\alpha) : k] = p > 1$ . Com que  $\{1, \alpha, \dots, \alpha^{p-1}\}$  és una  $k$ -base de  $k(\alpha)$ , existeixen elements  $a_0, a_1, \dots, a_{p-1} \in k$  tals que  $\beta = \sum_{i=0}^{p-1} a_i \alpha^i$ . Es tracta

de veure que  $a_2, \dots, a_{p-1} = 0$ , i que  $a_1 \in \mathbb{F}_p^*$ . Podem reescriure la igualtat  $b = \beta^p - \beta$  en la forma següent:

$$\begin{aligned} b &= \beta^p - \beta &= \sum_{i=0}^{p-1} a_i^p \alpha^{pi} - \sum_{i=0}^{p-1} a_i \alpha^i \\ &= \sum_{i=0}^{p-1} a_i^p (\alpha + a)^i - \sum_{i=0}^{p-1} a_i \alpha^i &= \sum_{i=0}^{p-1} a_i^p \sum_{j=0}^i \binom{i}{j} \alpha^j a^{i-j} - \sum_{j=0}^{p-1} a_j \alpha^j \\ &= \sum_{j=0}^{p-1} \sum_{i=j}^{p-1} \binom{i}{j} a_i^p a^{i-j} \alpha^j - \sum_{j=0}^{p-1} a_j \alpha^j &= \sum_{j=0}^{p-1} \left( \sum_{i=j}^{p-1} \binom{i}{j} a_i^p a^{i-j} - a_j \right) \alpha^j. \end{aligned}$$

Com que  $\{1, \alpha, \dots, \alpha^{p-1}\}$  és una  $k$ -base de  $k(\alpha)$ , i els coeficients d'aquesta combinació lineal pertanyen a  $k$ , s'ha de satisfer que  $\sum_{i=j}^{p-1} \binom{i}{j} a_i^p a^{i-j} - a_j = 0$ , per a  $1 \leq j \leq p-1$ , i

que  $\sum_{i=0}^{p-1} a_i^p a^i - a_0 = b$ , igualtat que correspon a  $j = 0$ .

En particular, per a  $j = p-1$ , obtenim la igualtat  $a_{p-1}^p - a_{p-1} = 0$ , de manera que  $a_{p-1} \in \mathbb{F}_p$ . Si  $p = 2$ , posem  $s := a_{p-1} = a_1$  i  $x := a_0$  i ja hem acabat, perquè  $s \neq 0$  (en cas contrari, seria  $\beta = a_0 \in k$ ).

Estudiem el cas  $p > 2$ . Considerem l'equació  $\sum_{i=j}^{p-1} \binom{i}{j} a_i^p a^{i-j} - a_j = 0$  per a  $j = p-2$ ;

obtenim la igualtat  $\binom{p-1}{p-2} a_{p-1}^p a + a_{p-2}^p - a_{p-2} = 0$ . Com que  $a_{p-1} \in \mathbb{F}_p$ , és  $a_{p-1}^p = a_{p-1}$ , de manera que  $(p-1)a_{p-1}a + a_{p-2}^p - a_{p-2} = 0$ ; això és,  $a_{p-1}a = a_{p-2}^p - a_{p-2} \in \wp(k)$ ; però  $a \notin \wp(k)$ , de manera que  $a_{p-1} = 0$  i  $a_{p-2}^p = a_{p-2}$ ; o sigui,  $a_{p-2} \in \mathbb{F}_p$ .

En repetir inductivament aquest argument, obtenim successivament que  $a_{p-2} = 0$  i  $a_{p-3} \in \mathbb{F}_p$ ; que  $a_{p-3} = 0$  i  $a_{p-4} \in \mathbb{F}_p$ ; etcètera. És a dir, que  $a_{p-1} = a_{p-2} = \dots = a_2 = 0$ , i  $a_1 \in \mathbb{F}_p$ . Notem que, en aquest punt, tenim que és  $\beta = a_1 \alpha + a_0$ , amb  $a_1 \in \mathbb{F}_p$ , i  $x := a_0 \in k$ . I ha d'ésser  $s := a_1 \neq 0$ , ja que  $k(\alpha) = k(\beta) \neq k$ . Això acaba la prova de (d). Doncs, ja només resta demostrar la propietat (e).

Donada una extensió cíclica  $K|k$  de grau  $p$ , i en virtut del teorema d'Artin-Schreier (4.9.3), existeix un element  $\alpha \in K$  tal que  $K = k(\alpha)$  i  $\alpha^p - \alpha \in k$ ; d'altra banda, si  $\beta \in K$  és un altre element tal que  $K = k(\beta)$  i  $\beta^p - \beta \in k$ , acabem de veure que existeix  $s \in \mathbb{Z}$  no divisible per  $p$  i existeix  $x \in k$  tals que  $\beta = s\alpha + x$ ; llavors, podem calcular  $\beta^p - \beta$  en la forma  $\beta^p - \beta = s^p \alpha^p + x^p - s\alpha - x = s(\alpha^p - \alpha) + (x^p - x)$ ; com que  $x^p - x \in \wp(k)$ ,  $\beta^p - \beta$  i  $s(\alpha^p - \alpha)$  generen el mateix subgrup de  $k/\wp(k)$ ; i, com que  $s$  no és divisible per  $p$ ,  $s(\alpha^p - \alpha)$  i  $\alpha^p - \alpha$  generen el mateix subgrup de  $k/\wp(k)$ , subgrup que és cíclic d'ordre  $p$ . Així, com que el subgrup no depèn de la tria de l'element  $\alpha$  tal que  $\alpha^p - \alpha \in k$ , podem definir una aplicació  $f : \mathfrak{C}_p(k) \rightarrow \mathfrak{C}_p(k)$  per  $f(K|k) := \langle \alpha^p - \alpha \rangle \subseteq k/\wp(k)$ , el subgrup generat per  $\alpha^p - \alpha$ .

Recíprocament, si  $a \in k$  és tal que el subgrup de  $k/\wp(k)$  generat per  $a$  és cíclic d'ordre  $p$  (és a dir, si  $a \notin \wp(k)$ ), i si  $\alpha$  és una arrel del polinomi  $X^p - X - a$ , l'apartat (c), que ja

hem provat, ens diu que l'extensió  $k(\alpha)|k$  és cíclica de grau  $p$  i tenim que  $f(k(\alpha)|k) = \langle a \rangle$ . Per tant,  $f$  és exhaustiva.

Finalment, per a veure que  $f$  és injectiva, suposem que  $k(\alpha)|k, k(\beta)|k$  són dues extensions cícliques de grau  $p$  tals que  $f(k(\alpha)|k) = f(k(\beta)|k)$ , i que  $a := \alpha^p - \alpha, b := \beta^p - \beta \in k$ . El fet que  $\langle a \rangle = \langle b \rangle \subseteq k/\wp(k)$  ens diu que ha de ser  $b = sa + y$ , per a un cert nombre enter  $s$  no divisible per  $p$  i un cert element  $y \in \wp(k)$  (apartat (d), ja provat); per tant, existeix  $x \in k$  tal que  $y = x^p - x$ , i  $(s\alpha + x)^p - (s\alpha + x) = s(\alpha^p - \alpha) + (x^p - x) = sa + y = b$ ; és a dir,  $s\alpha + x$  és una arrel de  $X^p - X - b$ ; com que  $k(\beta)|k$  és el cos de descomposició d'aquest polinomi, ha de ser  $k(\beta) = k(s\alpha + x) = k(s\alpha) = k(\alpha)$ , com volíem demostrar.  $\square$

## 4.11 Radicals en característica zero

Signin  $k$  un cos de característica diferent de 2,  $\bar{k}$  un cos algebraicament tancat que conté  $k$ , i  $f(X) := aX^2 + bX + c \in k[X]$ ,  $a, b, c \in k$ ,  $a \neq 0$ , un polinomi de grau 2. Les arrels de  $f(X)$  són els elements  $\frac{-b \pm \alpha}{2a} \in \bar{k}$ , on  $\alpha^2 = b^2 - 4ac \in k$ ; per tant, s'expressen com a funcions racionals d'arrels de polinomis de la forma  $X^2 - d$ , amb  $d \in k$  (cf. la proposició **0.3.1**).

Anàlogament, suposem que  $\text{car}(k) \neq 2, 3$ , considerem un polinomi de grau 3,  $f(X) := aX^3 + bX^2 + cX + d \in k[X]$ ,  $a, b, c, d \in k$ ,  $a \neq 0$ , i siguin  $p := \frac{c}{a} - \frac{b^2}{3a^2}$ ,  $q := \frac{d}{a} + \frac{2b^3}{27a^3} - \frac{bc}{3a^2}$ , i  $\Delta := -4p^3 - 27q^2$ . Si  $p \neq 0$ , les arrels del polinomi  $f(X)$  s'expressen en la forma

$$x_1 = \gamma - \frac{p}{3\gamma} - \frac{b}{3a}, \quad x_2 = \rho\gamma - \frac{p\rho^2}{3\gamma} - \frac{b}{3a}, \quad x_3 = \rho^2\gamma - \frac{p\rho}{3\gamma} - \frac{b}{3a},$$

on  $\gamma \in \bar{k}$  és tal que  $\gamma^3 = \frac{-27q + 3\alpha\beta}{54}$ , i  $\alpha, \beta \in \bar{k}$  tals que  $\alpha^2 = \Delta$ , i  $\beta^2 = -3$ . I, si  $p = 0$ , les arrels del polinomi  $f(X)$  s'expressen en la forma

$$x_1 = \theta - \frac{b}{3a}, \quad x_2 = \rho\theta - \frac{b}{3a}, \quad x_3 = \rho^2\theta - \frac{b}{3a}.$$

on  $\theta \in \bar{k}$  és tal que  $\theta^3 = -q$  i  $\rho := \frac{-1 + \beta}{2}$  (cf. la proposició **0.4.1**).

Doncs, amb algunes restriccions sobre la característica del cos  $k$ , les arrels de qualsevol polinomi  $f(X) \in k[X]$ , de grau 2 o bé 3, s'expressen com a funcions racionals d'arrels de polinomis de la forma  $X^2 - y$ ,  $X^3 - z$ , per a certs elements  $y, z \in \bar{k}$  que són arrels de polinomis d'aquesta mateixa forma i que es determinen a partir dels coeficients  $a, b, c, d$  del polinomi  $f(X)$ . Es diu que les equacions  $f(X) = 0$  són resolubles per radicals.

Ja des del Renaixement, en què es van conèixer fórmules per a expressar les solucions de les equacions de graus 2, 3 i 4 (primer només per a equacions de coeficients racionals i solucions reals), s'intentava cercar fórmules similars per a les equacions de grau superior; això és, se cercaven fórmules que *expressessin per radicals* les solucions de les equacions polinòmiques de grau més gran que 4. En particular, Gauss, en les *Disquisitiones Arithmeticae*, demostra que les equacions ciclotòmiques  $\Phi_p(X) = 0$ ,  $p$  primer, són "reductibles a pures" (cf. [Ga 1801], secció setena). I, més endavant, Abel prova que hi ha equacions de grau 5 que no són resolubles per radicals.

El propòsit de la part final del text és caracteritzar quines equacions són resolubles per radicals i quines no ho són; és a dir, caracteritzar per a quines equacions polinòmiques  $f(X) = 0$  les seves solucions es poden expressar com a funcions racionals d'arrels de polinomis de la forma  $X^n - a$ , per a certs elements  $a$  que es puguin obtenir com a arrels de polinomis de la mateixa forma, de manera recursiva, a partir dels coeficients del polinomi  $f(X)$ . Comencem per precisar la definició.

**Definició 4.11.1.** Siguin  $k$  un cos de característica zero,  $\bar{k}$  un cos algebraicament tancat que conté  $k$ , i  $f(X) \in k[X]$  un polinomi no nul. Direm que l'equació  $f(X) = 0$  és una *equació resoluble per radicals* sobre  $k$  si existeix una successió finita de cossos

$$k \subseteq k(\theta_1) \subseteq k(\theta_1, \theta_2) \subseteq \cdots \subseteq k(\theta_1, \dots, \theta_m) =: K \subseteq \bar{k},$$

tal que les arrels de  $f(X)$  pertanyen a  $K$  i, per a  $1 \leq i \leq m$ , existeix un nombre natural  $n_i \geq 1$  tal que  $a_i := \theta_i^{n_i} \in k(\theta_1, \dots, \theta_{i-1})$ . També anomenarem *resolució* de  $K|k$  d'exponents  $n_i$  una successió d'elements  $\theta_1, \theta_2, \dots, \theta_m \in K$  com aquesta, *extensió radical* de  $k$  qualsevol extensió com  $K|k$ , i *extensió resoluble per radicals* qualsevol subextensió d'una extensió radical.

En altres paraules, una equació polinòmica  $f(X) = 0$ , sobre un cos de característica zero, és resoluble per radicals si existeix una extensió radical  $K|k$  tal que  $K$  conté el cos de descomposició de  $f(X)$  sobre  $k$ ; és a dir, si el cos de descomposició sobre  $k$  del polinomi  $f(X)$  defineix una extensió de  $k$  resoluble per radicals. Notem que, en particular, tota extensió radical és finita; en conseqüència, tota extensió resoluble per radicals és finita.

**Observació 4.11.2.** La definició que donem d'extensió radical admet que alguns (o bé tots) dels elements  $\theta_i$  siguin arrels de la unitat, ja que no exclou la possibilitat  $\theta_i^{n_i} = 1$ . De fet, això no és necessari, i es podria exigir també que els polinomis  $X^{n_i} - \theta_i^{n_i}$  fossin irreductibles en  $k(\theta_1, \dots, \theta_{i-1})[X]$ , de manera que no s'admetrien, d'entrada, extensions per arrels de la unitat (notem que els polinomis  $X^n - 1$  no són irreductibles per a  $n > 1$ ). Sembla que aquesta és la situació que es plantejaven els matemàtics clàssics; en efecte, d'altra manera no tindria gaire sentit que Gauss es dediqués a provar que les equacions ciclotòmiques  $\Phi_p(X) = 0$  "són reductibles a pures". Veurem més endavant que les dues definicions són equivalents (cf. la proposició 5.5.1); és a dir, que per a totes les extensions  $k(\zeta)|k$ , on  $\zeta$  és una arrel de la unitat, existeix una extensió radical  $K|k$  per a la qual cada polinomi  $X^{n_i} - \theta_i^{n_i}$  és irreductible en  $k(\theta_1, \dots, \theta_{i-1})[X]$ .

**Proposició 4.11.3.** Siguin  $k$  un cos de característica zero, i  $\bar{k}$  un cos algebraicament tancat que conté  $k$ .

- (a) (Comportament per torres) Si  $k \subseteq K \subseteq L \subseteq \bar{k}$  són cossos tals que les extensions  $K|k$  i  $L|K$  són radicals (respectivament, resolubles per radicals), llavors, l'extensió  $L|k$  és radical (respectivament, resoluble per radicals).
- (b) (Comportament per canvi de base) Si  $k \subseteq K, L \subseteq \bar{k}$  són cossos tals que l'extensió  $L|k$  és radical (respectivament, resoluble per radicals), l'extensió  $KL|K$  també és radical (respectivament, resoluble per radicals).
- (c) (Comportament per composició) Si  $k \subseteq K_1, K_2 \subseteq \bar{k}$  són cossos tals que  $K_1|k, K_2|k$  són extensions radicals (respectivament, resolubles per radicals), l'extensió  $K_1K_2|k$  també és radical (respectivament, resoluble per radicals).  $\square$



**Corollari 4.11.4.** *Siguin  $k$  un cos de característica zero,  $f(X) \in k[X]$  un polinomi no nul, i  $P_1(X), \dots, P_m(X) \in k[X]$  els polinomis irreductibles diferents que divideixen  $f(X)$ . L'equació  $f(X) = 0$  és resoluble per radicals si, i només si, ho són totes les equacions  $P_1(X) = 0, \dots, P_m(X) = 0$ .  $\square$*

## 4.12 Extensions radicals

En aquesta secció fem un estudi més detallat de les extensions resolubles per radicals. En primer lloc, estudiarem la relació entre una extensió radical  $K|k$  i la seva clausura normal  $N|k$ .

**Proposició 4.12.1.** *Siguin  $k$  un cos de característica zero,  $\bar{k}$  un cos algebraicament tancat que conté  $k$ ,  $K|k$  una subextensió radical de  $\bar{k}|k$ , i  $N|k$  la clausura normal de  $K|k$ . Llavors, l'extensió  $N|k$  també és radical.*

DEMOSTRACIÓ: Siguin  $\theta_1, \dots, \theta_m \in \bar{k}$  una resolució de  $K$  d'exponents  $n_i$ ,  $\sigma : K \rightarrow \bar{k}$  una  $k$ -immersió qualsevol, i considerem una extensió a  $N$  de  $\sigma$ . Llavors  $\sigma : N \rightarrow N$  és un  $k$ -automorfisme i  $\sigma(K) = k(\sigma(\theta_1), \dots, \sigma(\theta_m))$  i  $\sigma(\theta_i)^{n_i} \in k(\sigma(\theta_1), \dots, \sigma(\theta_{i-1}))$ ; per tant, l'extensió  $\sigma(K)|k$  també és radical. Com que l'extensió  $N|k$  és la composició de les extensions  $\sigma(K)|k$ , per a totes les  $k$ -immersions  $\sigma$  de  $K$  en  $\bar{k}$ , l'extensió  $N|k$  és la composició d'una quantitat finita d'extensions radicals; per tant, és una extensió radical.  $\square$

**Corollari 4.12.2.** *Siguin  $k$  un cos de característica zero,  $K|k$  una extensió resoluble per radicals, i  $N|k$  una clausura normal de  $K|k$ . Llavors, l'extensió  $N|k$  també és resoluble per radicals.  $\square$*

L'ús de les extensions de la forma  $k(\zeta)|k$ , on  $\zeta$  és una arrel de la unitat, fa més senzilla la caracterització de les extensions resolubles per radicals.

**4.12.3.** *Siguin  $k$  un cos de característica zero,  $\bar{k}$  un cos algebraicament tancat que conté  $k$ ,  $K|k$  una extensió radical, i  $\theta_1, \dots, \theta_m \in K$  una resolució de  $K$  d'exponents  $n_i$ . Suposem, a més a més, que l'extensió  $K|k$  és normal.*

Siguin  $n := \text{mcm}(n_1, \dots, n_m)$ , i  $\zeta \in \bar{k}$  una arrel primitiva  $n$ -èsima de la unitat. Si fem el canvi de base a  $k(\zeta)$ , les extensions  $k(\zeta)(\theta_1, \dots, \theta_i)|k(\zeta)(\theta_1, \dots, \theta_{i-1})$ ,  $1 \leq i \leq m$ , són cíclics (cf. el teorema 4.9.2), cada una de grau divisor del nombre  $n_i$  corresponent. D'altra banda, l'extensió  $K(\zeta)|k(\zeta)$  és normal i per al seu grup de Galois podem considerar la cadena de subgrups

$$\begin{aligned} \text{Gal}(K(\zeta)|k(\zeta)) &\supseteq \text{Gal}(K(\zeta)|k(\zeta)(\theta_1)) \\ &\supseteq \text{Gal}(K(\zeta)|k(\zeta)(\theta_1, \theta_2)) \\ &\supseteq \dots \\ &\supseteq \text{Gal}(K(\zeta)|k(\zeta)(\theta_1, \dots, \theta_{m-1})) \\ &\supseteq \text{Gal}(K(\zeta)|K(\zeta)) = \{1\}. \end{aligned}$$

**Lema 4.12.4.** *Per a  $1 \leq i \leq n$ , el grup de Galois  $\text{Gal}(K(\zeta)|k(\zeta)(\theta_1, \dots, \theta_i))$  és un subgrup normal de  $\text{Gal}(K(\zeta)|k(\zeta)(\theta_1, \dots, \theta_{i-1}))$  i el grup quocient és cíclic, isomorf al grup de Galois  $\text{Gal}(k(\zeta)(\theta_1, \dots, \theta_i)|k(\zeta)(\theta_1, \dots, \theta_{i-1}))$ .*

Aquest resultat és un cas particular del següent, molt més general.

**Proposició 4.12.5.** *Siguin  $L|K$  i  $K|k$  extensions normals de cossos, no necessàriament finites ni de característica zero, i tals que l'extensió  $L|k$  sigui normal. Llavors,  $\text{Gal}(L|K)$  és un subgrup normal de  $\text{Gal}(L|k)$  i el grup quocient  $\text{Gal}(L|k)/\text{Gal}(L|K)$  és isomorf al grup de Galois  $\text{Gal}(K|k)$ .*

DEMOSTRACIÓ: Podem definir una aplicació  $\text{Gal}(L|k) \xrightarrow{\text{res}} \text{Gal}(K|k)$  per l'assignació  $\sigma \mapsto \sigma|_K$ , que assigna a cada automorfisme de  $L$  la seva restricció a  $K$ , perquè l'extensió  $K|k$  és normal i, per tant,  $\sigma|_K$  és un automorfisme de  $K$ . L'aplicació  $\text{res}$  és, clarament, un morfisme de grups, i és exhaustiu perquè l'extensió  $L|k$  és normal i, per tant, tot  $k$ -automorfisme de  $K$  s'estén a un  $k$ -automorfisme de  $L$  (cf. el teorema d'extensió algebraica de morfismes, **3.9.2**). A més a més, el nucli del morfisme  $\text{res}$  és exactament  $\text{Gal}(L|K)$ . En conseqüència,  $\text{Gal}(L|K)$  és un subgrup normal de  $\text{Gal}(L|k)$  i el quocient és isomorf a  $\text{Gal}(K|k)$ .  $\square$

**4.12.6.** Sigui  $\bar{k}$  un cos algebraicament tancat,  $k \subseteq \bar{k}$  un subcòs qualsevol, i  $f(X) \in k[X]$  un polinomi no nul. Suposem que  $\text{car}(k) = 0$  i que l'equació  $f(X) = 0$  és resoluble per radicals sobre  $k$ , i sigui  $\theta_1, \dots, \theta_m \in \bar{k}$  una resolució d'exponents  $n_i$  d'un cos  $K$  que contingui totes les arrels de  $f(X)$  i tal que l'extensió  $K|k$  sigui normal. A continuació, posem  $n := \text{mcm}(n_1, \dots, n_m)$ , considerem  $\zeta \in \bar{k}$  una arrel primitiva  $n$ -èsima de la unitat, i els cossos  $K_i := k(\zeta, \theta_1, \dots, \theta_i)$ , per a  $0 \leq i \leq m$ . Com que l'extensió  $K_m|k$  és la composició de les dues extensions normals  $K|k$  i  $K_0|k$ , l'extensió  $K_m|k$  és normal. Considerem la successió de cossos

$$k \subseteq K_0 \subseteq K_1 \subseteq \dots \subseteq K_m,$$

i la dels grups de Galois

$$\begin{aligned} \text{Gal}(K_m|k) &\supseteq \text{Gal}(K_m|K_0) \supseteq \text{Gal}(K_m|K_1) \supseteq \dots \\ &\dots \supseteq \text{Gal}(K_m|K_{m-1}) \supseteq \text{Gal}(K_m|K_m) = \{1\}. \end{aligned}$$

Si posem  $K_{-1} := k$ , obtenim que, per a  $0 \leq i \leq m$ , el grup de Galois  $\text{Gal}(K_m|K_i)$  és un subgrup normal de  $\text{Gal}(K_m|K_{i-1})$  i també que el quocient  $\text{Gal}(K_m|K_{i-1})/\text{Gal}(K_m|K_i)$ , que és isomorf a  $\text{Gal}(K_i|K_{i-1})$ , és un grup abelià. En efecte, per a  $1 \leq i \leq m$ , això ja ha estat vist (i, a més a més, en aquests casos, tenim que  $\text{Gal}(K_m|K_{i-1})/\text{Gal}(K_m|K_i)$  és cíclic), i, per a  $i = 0$ , podem aplicar la proposició anterior (**4.12.5**), de manera que  $\text{Gal}(K_m|K_{-1})/\text{Gal}(K_m|K_0) \cong \text{Gal}(k(\zeta)|k)$  és isomorf a un subgrup de  $(\mathbb{Z}/n\mathbb{Z})^*$ , i, per tant, abelià. Així, obtenim una demostració del resultat següent.

**Teorema 4.12.7.** *Siguin  $k$  un cos de característica zero i  $f(X) \in k[X]$  un polinomi no nul. Si l'equació  $f(X) = 0$  és resoluble per radicals, existeix una extensió normal finita  $K|k$  per a la qual se satisfan les condicions següents:*

- El cos  $K$  conté el cos de descomposició de  $f(X)$  sobre  $k$ .
- El grup  $G_0 := \text{Gal}(K|k)$  admet una successió decreixent  $G_0 \supseteq G_1 \supseteq \dots \supseteq G_m = \{1\}$  de subgrups tal que  $G_i$  és un subgrup normal de  $G_{i-1}$ , per a  $1 \leq i \leq m$ , i el quocient  $G_{i-1}/G_i$  és abelià.  $\square$

L'objectiu final és provar que aquesta condició necessària per a la resolubilitat per radicals de l'equació  $f(X) = 0$  també és suficient. Això ho farem en el capítol següent.

**Observació 4.12.8.** Notem que aquesta condició és dir que el grup de Galois  $G$  és un grup resoluble. De fet, el qualificatiu *resoluble* que s'atorga a un grup per al qual se satisfà aquesta condició prové del fet que l'equació és *resoluble per radicals*. Remetem a la secció (5.3) per al seu estudi.

## 4.13 Exercicis

**Exercici 4.13.1.** Siguin  $p$  un nombre natural primer, i  $t, u$ , indeterminades sobre el cos finit  $\mathbb{F}_p$ . Posem  $k := \mathbb{F}_p(t^p, u^p) \subseteq L := \mathbb{F}_p(t, u)$ . Se satisfan les propietats següents.

- (a) L'extensió  $L|k$  és de grau  $p^2$ .
- (b) Si  $\alpha \in L$ ,  $\alpha \notin k$ , llavors  $[k(\alpha) : k] = p$ .
- (c) L'extensió  $L|k$  admet una infinitat de subextensions finites. A més a més,
- (d) es demana determinar de manera explícita una família infinita de cossos intermedis  $k \subsetneq K \subsetneq L$ .

**Exercici 4.13.2.** Siguin  $\mathbb{Q}(\alpha_i)|\mathbb{Q}$ ,  $i = 1, 2$ , dues extensions de Galois amb  $\alpha_1 \cdot \alpha_2 \neq 0$  i tals que  $\mathbb{Q}(\alpha_1) \cap \mathbb{Q}(\alpha_2) = \mathbb{Q}$ . Si el grau d'alguna d'elles és senar, aleshores el grup de Galois de l'extensió  $\mathbb{Q}(\alpha_1, \alpha_2)|\mathbb{Q}(\alpha_1\alpha_2)$  és trivial; és a dir, el producte  $\alpha_1\alpha_2$  és un element primitiu de l'extensió  $\mathbb{Q}(\alpha_1, \alpha_2)|\mathbb{Q}$ .



# Capítol 5

## Teorema fonamental i aplicacions

Estem ja en disposició d'acabar la teoria empresa i caracteritzar les equacions resolubles per radicals. Per a això, comencem el capítol amb la demostració del teorema d'Artin que proporciona extensions de Galois a partir de grups finits d'automorfismes d'un cos. Fem servir aquest teorema per a demostrar, en la secció segona i per al cas d'extensions finites sobre un cos qualsevol, l'anomenat “teorema fonamental de la teoria de Galois”, que proporciona una bijecció entre, d'una banda, el conjunt de les subextensions d'una extensió finita i de Galois i, de l'altra, el conjunt dels subgrups del grup de Galois d'aquesta extensió. Notem que aquest teorema ja s'ha obtingut per al cas dels cossos finits (cf. el teorema **3.10.12**). D'altra banda, també estudiem el comportament general dels grups de Galois per canvi de base, per composició, i amb relació al cos intersecció.

A les seccions tercera i quarta, estudiem les propietats formals dels grups resolubles i establim el teorema que caracteritza les equacions resolubles per radicals com aquelles per a les quals el grup de Galois del seu cos de descomposició és un grup resoluble. I veiem, en la secció cinquena, de quina manera podem expressar per radicals les arrels de la unitat (en paraules de Gauss, “reduir a pures” les equacions ciclotòmiques) i així poder obviar aquestes en la definició d'equació resoluble per radicals i, per tant, poder demanar que els radicals siguin irreductibles.

A partir d'aquí, ens fixem en aplicacions de la teoria a diversos problemes. Dedicuem la secció sisena a identificar el grup de Galois d'una equació polinòmica amb un subgrup del grup de permutacions de les seves arrels, fet que ens permet representar els grups de Galois com a subgrups dels grups simètrics i demostrar, a la secció setena, que les equacions generals de grau més gran estrictament que 4 no són resolubles per radicals.

En canvi, a les seccions vuitena i novena, fem una deducció explícita de la solució de les equacions de graus 3 o 4, no tant per l'interès que puguin tenir les fórmules que expressen les seves arrels per radicals, com per a il·lustrar de quina manera es pot usar la teoria per a resoldre algunes equacions per radicals. Notem que fórmules per a les equacions cúbiques sobre un cos de característica diferent de 2 i de 3 ja s'han obtingut en **0.4.1**.

Les dues darreres seccions es destinen a l'exposició d'una variació de la teoria, la caracterització de les seccions del cercle construïbles amb regla i compàs; a la secció desena, mitjançant la introducció formal de les construccions amb regla i compàs i la discussió dels problemes clàssics de la duplicació del cub, de la trisecció de l'angle i de la quadratura del cercle, i, a l'onzena, amb la caracterització dels nombres naturals  $n \geq 1$

tals que el polígon regular de  $n$  costats es pot construir amb regla i compàs, fet que aprofitem per a la introducció del concepte de  $p$ -grup.

Finalment, per a arrodonir el tema de la impossibilitat de la quadratura del cercle amb regla i compàs i, alhora, per a donar un exemple molt important de nombre real no algebraic, proporcionem una demostració de la transcendència de  $\pi$ .

## 5.1 El teorema d'Artin

Per a un cos  $L$  i un grup  $H$  d'automorfismes de  $L$ , hem denotat per  $L^H$  el subcòs de  $L$  format pels elements que són fixos per tots els automorfismes de  $L$  (cf. la proposició **3.7.9** i el teorema **3.10.12**); és a dir,

$$L^H := \{x \in L : \sigma(x) = x, \text{ per a tot } \sigma \in H\}.$$

De fet, a la proposició **3.7.9** hem vist que, si  $\zeta$  és una arrel de la unitat, el subcòs de  $\mathbb{Q}(\zeta)$  fix per  $\text{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q})$  coincideix amb el cos base  $\mathbb{Q}$ ; és a dir, que  $\mathbb{Q}(\zeta)^{\text{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q})} = \mathbb{Q}$ . Aquest mateix fet succeeix també en el cas dels cossos finits: el subcòs de  $\mathbb{F}_{q^n}$  fix per l'automorfisme de Frobenius  $\varphi_q \in \text{Gal}(\mathbb{F}_{q^n}|\mathbb{F}_q)$  és el cos base  $\mathbb{F}_q$ ; i com que l'automorfisme de Frobenius és un generador del grup  $\text{Gal}(\mathbb{F}_{q^n}|\mathbb{F}_q)$ , obtenim que  $\mathbb{F}_{q^n}^{\text{Gal}(\mathbb{F}_{q^n}|\mathbb{F}_q)} = \mathbb{F}_q$  (cf. el punt **3.10.6**). Aquest fet no és aïllat. Comencem per destacar un parell de propietats generals, que se satisfan per definició de cos fix per un subgrup d'automorfismes.

**Proposició 5.1.1.** *Sigui  $L|k$  una extensió algebraica qualsevol de cossos.*

(a) *Per a tot subgrup  $H \subseteq \text{Gal}(L|k)$ , és  $H \subseteq \text{Gal}(L|L^H)$ .*

(b)  $\text{Gal}(L|L^{\text{Gal}(L|k)}) = \text{Gal}(L|k)$ .  $\square$

**5.1.2. La correspondència fonamental de la teoria de Galois.** Considerem una extensió algebraica qualsevol de cossos,  $L|k$ , el seu grup de Galois,  $G := \text{Gal}(L|k)$ , i siguin  $\mathcal{S}(L|k)$  el conjunt de tots els subgrups de  $G$ , i  $\mathcal{E}(L|k)$  el conjunt de totes les subextensions  $K|k$  de  $L|k$ .

Per a cada subgrup  $H \subseteq G$ , podem considerar el cos  $L^H$ , i es tenen les incusions  $k \subseteq L^H \subseteq L$ , de manera que  $L^H|k$  pertany a  $\mathcal{E}(L|k)$ . Així, l'assignació  $H \mapsto L^H|k$  defineix una aplicació  $\mathcal{S}(L|k) \rightarrow \mathcal{E}(L|k)$ . Aquesta aplicació inverteix l'ordre donat per la inclusió; és a dir, si  $H_1 \subseteq H_2$ , llavors  $L^{H_2}|k$  és una subextensió de  $L^{H_1}|k$ . A més a més, l'extensió assignada al subgrup trivial  $\{\text{Id}\}$  és l'extensió  $L|k$ ; és a dir,  $L^{\{\text{Id}\}} = L$ .

Recíprocament, a tota subextensió  $K|k$  de  $L|k$ , podem assignar-li el grup de Galois  $\text{Gal}(L|K)$ , que és un subgrup de  $\text{Gal}(L|k)$ ; això defineix una aplicació  $\mathcal{E}(L|k) \rightarrow \mathcal{S}(L|k)$ . Aquesta aplicació també inverteix l'ordre donat per inclusió; és a dir, si  $K_1|k$  és una subextensió de  $K_2|k$ , llavors  $\text{Gal}(L|K_1) \supseteq \text{Gal}(L|K_2)$ . I, a més a més, a l'extensió total  $L|k$  li correspon el subgrup trivial  $\text{Gal}(L|L) = \{\text{Id}\}$ .

En el cas d'extensions finites de cossos finits, hem vist que aquestes aplicacions són inverses l'una de l'altra (cf. el teorema **3.10.12**). Aquesta propietat se satisfà per a totes les extensions finites i de Galois. La propietat essencial que resta veure és la següent.

**Proposició 5.1.3.** *Sigui  $L|k$  una extensió de Galois finita. Per a tota subextensió  $K|k$  se satisfà que  $K = L^{\text{Gal}(L|K)}$ .*

DEMOSTRACIÓ: Posem  $H := \text{Gal}(L|K)$  i considerem el subcòs  $L^H \subseteq L$ . Per definició de  $L^H$ , es té que  $K \subseteq L^H$ ; a més a més, les dues extensions  $L|K$  i  $L|L^H$  són de Galois i finites, de manera que el grau de cada una d'elles coincideix amb l'ordre del grup de Galois corresponent; si demostrem que els dos grups de Galois coincideixen, obtindrem la igualtat que desitgem entre els cossos  $K$  i  $L^H$ . Ara, la inclusió  $\text{Gal}(L|L^H) \subseteq H$  s'obté immediatament del fet que  $K \subseteq L^H$ . I l'altra inclusió,  $H \subseteq \text{Gal}(L|L^H)$ , és el contingut de la proposició 5.1.1, (a).  $\square$

Aquest resultat és, efectivament, la base per al teorema fonamental. Comencem per veure que la propietat anterior caracteritza, de fet, les extensions finites de Galois.

**Proposició 5.1.4.** *Una extensió finita  $L|k$  és de Galois si, i només si,  $L^{\text{Gal}(L|k)} = k$ .*

DEMOSTRACIÓ: La proposició 5.1.1 (b) dóna la igualtat  $\text{Gal}(L|L^{\text{Gal}(L|k)}) = \text{Gal}(L|k)$ . Si suposem que l'extensió  $L|k$  és de Galois, se satisfà que l'extensió  $L|L^{\text{Gal}(L|k)}$  també és de Galois; i com que les dues són finites, tenim les igualtats  $\#\text{Gal}(L|k) = [L : k]$  i,  $\#\text{Gal}(L|L^{\text{Gal}(L|k)}) = [L : L^{\text{Gal}(L|k)}]$ . Però, llavors, en la successió  $k \subseteq L^{\text{Gal}(L|k)} \subseteq L$ , les extensions són finites i tals que  $[L : L^{\text{Gal}(L|k)}] = [L : k]$ ; per tant,  $L^{\text{Gal}(L|k)} = k$ . La propietat recíproca, que de fet és la caracterització de les extensions finites que són de Galois, és el cas particular  $G = \text{Gal}(L|k)$  del teorema següent.  $\square$

**Teorema 5.1.5 (Artin).** *Siguin  $L$  un cos qualsevol i  $G$  un grup finit d'automorfismes de  $L$ . L'extensió  $L|L^G$  és finita i de Galois i  $\text{Gal}(L|L^G) = G$ .*

DEMOSTRACIÓ: Comencem per provar que (a): tots els elements de  $L$  són separables sobre  $L^G$  i de grau menor o igual que l'ordre de  $G$ .

Com que  $G$  és finit, per a tot  $\theta \in L$ , el conjunt  $C_\theta := \{\sigma(\theta) : \sigma \in G\}$  és finit i  $\#C_\theta \leq \#G$ ; a més a més, per a tot  $\sigma \in G$ , la restricció de  $\sigma$  a  $C_\theta$  defineix una aplicació injectiva i, per tant, bijectiva,  $\sigma|_{C_\theta} : C_\theta \rightarrow C_\theta$ . Doncs, podem definir el polinomi  $f_\theta(X) := \prod_{\eta \in C_\theta} (X - \eta) \in L[X]$ , i se satisfà que, per a tot  $\sigma \in G$ ,  $\sigma(f_\theta)(X) = f_\theta(X)$ ,

de manera que  $f_\theta(X) \in L^G[X]$ . Llavors, (a) resulta del fet que  $\theta$  és una arrel d'aquest polinomi, totes les arrels del qual són simples. En particular, l'extensió  $L|L^G$  és algebraica i separable.

L'extensió  $L|L^G$  és de Galois, perquè  $L$  és el cos de descomposició sobre  $L^G$  de la família de polinomis  $\{f_\theta(X)\}_{\theta \in L}$ , que pertanyen a  $L^G[X]$  i no tenen arrels múltiples. A més a més, totes les subextensions finites de  $L|L^G$  admeten element primitiu i, com que el grau sobre  $L^G$  de tots els elements de  $L$  és menor o igual que  $\#G$ , són de grau menor o igual que  $\#G$ . Així, obligatòriament, l'extensió  $L|L^G$  és finita i  $[L : L^G] \leq \#G$ .

Ja només resta veure que  $\text{Gal}(L|L^G) = G$ . Per construcció, és clar que  $G \subseteq \text{Gal}(L|L^G)$ ; i, d'altra banda,  $\#\text{Gal}(L|L^G) \leq [L : L^G] \leq \#G$ ; per tant,  $G = \text{Gal}(L|L^G)$ , com volíem.  $\square$

## 5.2 El teorema fonamental de la teoria de Galois

El teorema d'Artin és la peça final de la demostració del teorema fonamental de la teoria de Galois: l'existència d'una correspondència bijectiva entre el conjunt dels subgrups del

grup de Galois d'una extensió de Galois finita, i el conjunt de les subextensions d'aquesta extensió de Galois.

**Teorema 5.2.1.** *Sigui  $L|k$  una extensió finita i de Galois de cossos. Com en 5.1.2, posem  $\mathcal{E}(L|k)$  el conjunt de les subextensions  $K|k$  de  $L|k$  i  $\mathcal{S}(L|k)$  el conjunt dels subgrups de  $\text{Gal}(L|k)$ . Les dues aplicacions  $\mathcal{E}(L|k) \rightarrow \mathcal{S}(L|k)$  i  $\mathcal{S}(L|k) \rightarrow \mathcal{E}(L|k)$ , definides per les assignacions  $K|k \mapsto \text{Gal}(L|K)$  i, respectivament,  $H \mapsto L^H|k$ , són bijectives, inverses l'una de l'altra, i inverteixen l'ordre donat per la inclusió. A més a més, l'extensió  $L^H|k$  és normal si, i només si,  $H \subseteq \text{Gal}(L|k)$  és un subgrup normal.*

DEMOSTRACIÓ: Pràcticament ho hem vist tot, però, per comoditat, repetirem alguns arguments. Com que l'extensió  $L|k$  és finita i de Galois, totes les subextensions  $K|k$  de  $L|k$  són finites i separables, i totes les extensions  $L|K$ , per a  $k \subseteq K \subseteq L$ , són finites i de Galois.

Donat un subgrup qualsevol  $H \subseteq \text{Gal}(L|k)$ , el teorema d'Artin ens diu que se satisfà la igualtat  $\text{Gal}(L|L^H) = H$ ; i recíprocament, donada una subextensió qualsevol  $K|k$  de  $L|k$ , se satisfà que  $L^{\text{Gal}(L|K)} = K$ , perquè  $L|K$  és de Galois. Això prova que les dues aplicacions són bijectives i inverses l'una de l'altra; i ambdues inverteixen l'ordre donat per inclusió.

Resta veure que  $\text{Gal}(L|K) \subseteq \text{Gal}(L|k)$  és un subgrup normal si, i només si, l'extensió  $K|k$  és normal. Però si suposem que l'extensió  $K|k$  és normal, el morfisme donat per restricció  $\text{Gal}(L|k) \rightarrow \text{Gal}(K|k)$  és un morfisme exhaustiu de grups, de nucli  $\text{Gal}(L|K)$  (cf. la proposició 4.12.5); per tant,  $\text{Gal}(L|K)$  és un subgrup normal de  $\text{Gal}(L|k)$ . Recíprocament, suposem que  $\text{Gal}(L|K)$  és un subgrup normal de  $\text{Gal}(L|k)$ . Per a veure que l'extensió  $K|k$  és normal, veurem que per a tota  $k$ -immersió  $\sigma$  de  $K$  en un cos algebraicament tancat que contingui  $L$ , és  $\sigma(K) = K$ , de manera que  $\sigma$  és un automorfisme de  $K$ . Però, com que l'extensió  $L|k$  és normal, una tal  $\sigma$  s'estén a un  $k$ -automorfisme de  $L$  i  $\sigma(K) \subseteq L$ , i podem considerar les dues extensions  $L|K$  i  $L|\sigma(K)$ . És clar que  $\text{Gal}(L|\sigma(K)) = \sigma \text{Gal}(L|K) \sigma^{-1}$ ; i com que  $\text{Gal}(L|K)$  és un subgrup normal de  $\text{Gal}(L|k)$  i  $\sigma \in \text{Gal}(L|k)$ , és  $\sigma \text{Gal}(L|K) \sigma^{-1} = \text{Gal}(L|K)$ , de manera que  $\text{Gal}(L|\sigma(K)) = \text{Gal}(L|K)$ . Com a conseqüència, és  $\sigma(K) = K$ , ja que  $\sigma(K)$  és el cos que correspon al grup  $\text{Gal}(L|\sigma(K))$  i  $K$  el que correspon al grup  $\text{Gal}(L|K)$ .  $\square$

Per a acabar aquesta secció, establim algunes propietats que complementen el teorema fonamental i que són útils per al càlcul efectiu amb extensions de Galois. Comencem per l'estudi dels grups de Galois **sobre** el cos composició o **sobre** el cos intersecció corresponents a dues subextensions qualsevol d'una extensió finita i de Galois. Més endavant ho estudiarem **des** del cos base o **des** del cos intersecció.

**Proposició 5.2.2.** *Siguin  $L|k$  una extensió finita i de Galois i  $K_1|k, K_2|k$ , subextensions qualssevol de  $L|k$ . Llavors, sobre els cossos composició,  $K_1K_2$ , i intersecció,  $K_1 \cap K_2$ , tenim que*

- (a)  $\text{Gal}(L|K_1K_2) = \text{Gal}(L|K_1) \cap \text{Gal}(L|K_2)$ ; i
- (b)  $\text{Gal}(L|K_1 \cap K_2) = \langle \text{Gal}(L|K_1), \text{Gal}(L|K_2) \rangle$ , el subgrup de  $\text{Gal}(L|k)$  generat per la reunió  $\text{Gal}(L|K_1) \cup \text{Gal}(L|K_2)$ .

DEMOSTRACIÓ: La propietat (a) és gairebé immediata a partir de les definicions; provem (b).



Posem  $H = \langle \text{Gal}(L|K_1), \text{Gal}(L|K_2) \rangle$ ; en virtut del teorema fonamental, cal veure que  $L^H = K_1 \cap K_2$ . Com que  $K_1 \cap K_2 \subseteq K_i$ , per a  $i = 1, 2$ , és  $\text{Gal}(L|K_i) \subseteq \text{Gal}(L|K_1 \cap K_2)$ ; per tant,  $H \subseteq \text{Gal}(L|K_1 \cap K_2)$ ; és a dir,  $K_1 \cap K_2 \subseteq L^H$ . Recíprocament, si  $x \in L^H$ , aleshores, per a tot  $\sigma \in H$  és  $\sigma(x) = x$ ; per tant, per a tot  $\sigma \in \text{Gal}(L|K_i)$ ,  $i = 1, 2$ , és  $\sigma(x) = x$ ; és a dir,  $x \in L^{\text{Gal}(L|K_i)} = K_i$ ; això és,  $x \in K_1 \cap K_2$ , de manera que tenim l'altra inclusió,  $L^H \subseteq K_1 \cap K_2$ .  $\square$

**5.2.3.** Aquestes dues propietats es poden resumir en el diagrama següent, on escrivim  $G_i := \text{Gal}(L|K_i)$ ,  $i = 1, 2$ , per als grups de Galois. Notem que les inclusions de cossos i les de subgrups es dibuixen, en els diagrames, en sentits oposats: un subcòs, més avall, i un subgrup, més amunt. Això reflecteix la inversió d'ordre de les aplicacions del teorema fonamental.

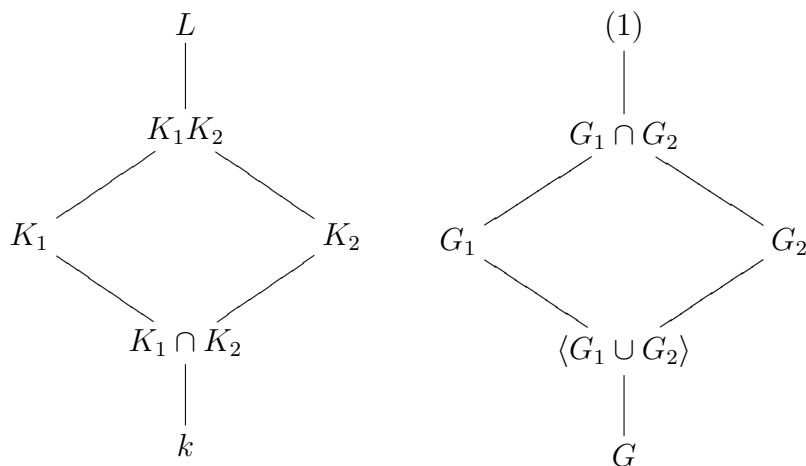


Diagrama 5.1: Grups de Galois sobre la composició o la intersecció

A continuació, estudiem el comportament de les extensions de Galois per canvi de base.

**Proposició 5.2.4.** *Siguin  $k$  un cos,  $L|k$ , una extensió de Galois,  $K|k$  una extensió qualsevol, i suposem que  $L, K \subseteq \bar{k}$ , on  $\bar{k}$  és un cos algebraicament tancat que conté  $k$ . Llavors:*

- (a) *L'extensió  $KL|K$  és de Galois.*
- (b) *L'aplicació de restricció  $\text{Gal}(KL|K) \longrightarrow \text{Gal}(L|k)$ , donada per  $\sigma \mapsto \sigma|_L$ , és un morfisme injectiu de grups.*
- (c) *La imatge del morfisme de restricció és  $\text{Gal}(L|L \cap K)$ . Tot i que aquest resultat és general, només el demostrarem amb la hipòtesi suplementària que l'extensió  $KL|K$  és finita,*
- (d) *Si  $L|k$  és finita, llavors  $KL|K$  és finita i  $[KL : K]$  divideix  $[L : k]$ .*

**DEMOSTRACIÓ:** La propietat (a) és conseqüència immediata dels fets que la separabilitat i la normalitat es conserven per canvi de base (cf. les proposicions **3.9.13** i **4.4.9**). Per a veure (b), adonem-nos que si  $\sigma \in \text{Gal}(KL|K)$ , llavors la restricció  $\sigma|_L$  és un  $k$ -automorfisme de  $L$ , perquè l'extensió  $L|k$  és normal; per tant, l'aplicació de restricció  $\text{Gal}(KL|K) \longrightarrow \text{Gal}(L|k)$  està ben definida i és, evidentment, un morfisme de grups. A

més a més, aquest morfisme és injectiu, perquè si  $\sigma|_L = 1$ , com que  $\sigma|_K = 1$  (perquè  $\sigma \in \text{Gal}(KL|K)$ ), ha de ser  $\sigma = 1$  en  $KL$ .

Per a veure (c), calculem la imatge,  $H$ , del morfisme de restricció. Clarament, com que per a  $\sigma \in \text{Gal}(KL|K)$  és  $\sigma|_K = 1$ , obtenim que  $\sigma|_L$  és la identitat en  $L \cap K$ ; per tant,  $\sigma|_L \in \text{Gal}(L|L \cap K)$ ; és a dir,  $H \subseteq \text{Gal}(L|L \cap K)$ . Recíprocament, si  $\alpha \in L^H$ , és  $\alpha \in L$  i per a tot element  $\sigma \in \text{Gal}(KL|K)$  és  $\sigma|_L(\alpha) = \alpha$ ; o sigui,  $\sigma(\alpha) = \alpha$ , de manera que  $\alpha \in (KL)^{\text{Gal}(KL|K)} = K$ , perquè l'extensió  $KL|K$  és finita i de Galois. Així,  $L^H \subseteq L \cap K$  o, equivalentment,  $\text{Gal}(L|L \cap K) \subseteq H$ , com es volia veure. Finalment, per a veure (d), només cal observar que si  $L|k$  és finita, llavors  $KL|K$  també és finita i  $\text{Gal}(KL|K) \cong \text{Gal}(L|L \cap K) \subseteq \text{Gal}(L|k)$ ; per tant,

$$[KL : K] = \#\text{Gal}(KL|K) \text{ divideix } \#\text{Gal}(L|k) = [L : k],$$

com volíem veure.  $\square$

**5.2.5.** Resumim en un diagrama el comportament de les extensions de Galois per canvi de base.

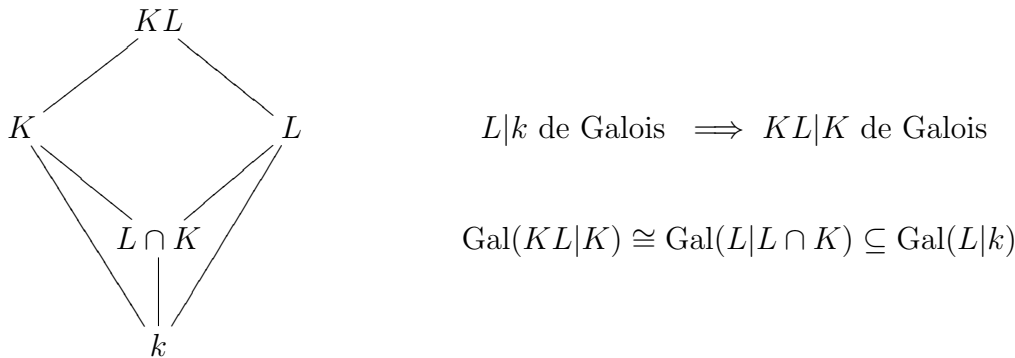


Diagrama 5.2: Comportament del caràcter galoisià per canvi de base

Acabem la secció, amb un estudi bàsic del comportament de les extensions de Galois per composició.

**Proposició 5.2.6.** *Siguin  $\bar{k}$  un cos algebraicament tancat,  $k \subseteq \bar{k}$  un subcòs, i  $K_1|k$  i  $K_2|k$  dues extensions finites i de Galois, i suposem que  $K_1, K_2 \subseteq \bar{k}$ . Llavors:*

- (a) *L'extensió  $K_1K_2|k$  és de Galois.*
- (b) *L'aplicació  $\text{Gal}(K_1K_2|k) \xrightarrow{\varphi} \text{Gal}(K_1|k) \times \text{Gal}(K_2|k)$ , donada per  $\sigma \mapsto (\sigma|_{K_1}, \sigma|_{K_2})$ , és un morfisme injectiu de grups.*
- (c) *Si  $K_1 \cap K_2 = k$ , llavors  $\varphi$  és un isomorfisme.*
- (d) *En general, l'aplicació*

$$\text{Gal}(K_1K_2|K_1 \cap K_2) \longrightarrow \text{Gal}(K_1|K_1 \cap K_2) \times \text{Gal}(K_2|K_1 \cap K_2)$$

*donada per  $\sigma \mapsto (\sigma|_{K_1}, \sigma|_{K_2})$  és un isomorfisme de grups.*

DEMOSTRACIÓ: La composició de dues extensions normals és una extensió normal (cf. la proposició 3.9.14), i la composició de dues extensions separables és una extensió separable (cf. la proposició 4.4.13); per tant, la composició de dues extensions de Galois és una extensió de Galois. Això demostra (a). Per a veure (b), observem que, com que les extensions  $K_1|k$  i  $K_2|k$  són normals, la restricció a  $K_i$  d'un  $k$ -automorfisme de  $K_1K_2$  és un  $k$ -automorfisme de  $K_i$ ; per tant,  $\varphi$  està ben definida i, clarament, és un morfisme de grups. A més a més, si  $\sigma|_{K_1} = 1$  i  $\sigma|_{K_2} = 1$ , llavors  $\sigma$  és la identitat en  $K_1K_2$ ; per tant,  $\varphi$  és injectiu.

Vegem (c). Siguin  $\sigma_1 \in \text{Gal}(K_1|k)$ ,  $\sigma_2 \in \text{Gal}(K_2|k)$ , elements qualssevol; en virtut de la proposició anterior (5.2.4), tenim isomorfismes de grups  $\text{Gal}(K_1K_2|K_2) \rightarrow \text{Gal}(K_1|k)$  i  $\text{Gal}(K_1K_2|K_1) \rightarrow \text{Gal}(K_2|k)$ , donats per restricció, ja que suposem que  $K_1 \cap K_2 = k$ ; per tant, existeixen extensions  $\sigma_1 \in \text{Gal}(K_1K_2|K_2)$ , de  $\sigma_1$ , i  $\sigma_2 \in \text{Gal}(K_1K_2|K_1)$ , de  $\sigma_2$ ; aleshores,  $\sigma_1, \sigma_2$  són  $k$ -automorfismes de  $K_1K_2$ , i té sentit considerar la seva composició  $\sigma := \sigma_2 \circ \sigma_1 \in \text{Gal}(K_1K_2|k)$ . Ara bé, com que  $\sigma_1 \in \text{Gal}(K_1K_2|K_2)$ , és  $\sigma_1|_{K_2} = \text{id}$ , i obtenim que  $\sigma|_{K_2} = \sigma_2|_{K_2} \circ \sigma_1|_{K_2} = \sigma_2$ ; i, anàlogament,  $\sigma_2|_{K_1} = \text{id}$ , i  $\sigma|_{K_1} = \sigma_2|_{K_1} \circ \sigma_1|_{K_1} = \sigma_1$ , de manera que  $\sigma$  és una antiimatge de la parella  $(\sigma_1, \sigma_2)$ . Això demostra que  $\varphi$  és exhaustiu i, en conseqüència, un isomorfisme.

La propietat (d) només és una reformulació de les dues anteriors, ja que si  $K_1|k$  i  $K_2|k$  són extensions de Galois, també ho són les dues extensions  $K_1|K_1 \cap K_2$  i  $K_2|K_1 \cap K_2$ , de manera que podem aplicar els dos resultats (b) i (c), ja demostrats.  $\square$

5.2.7. Resumim en un diagrama el comportament de les extensions de Galois per composició.

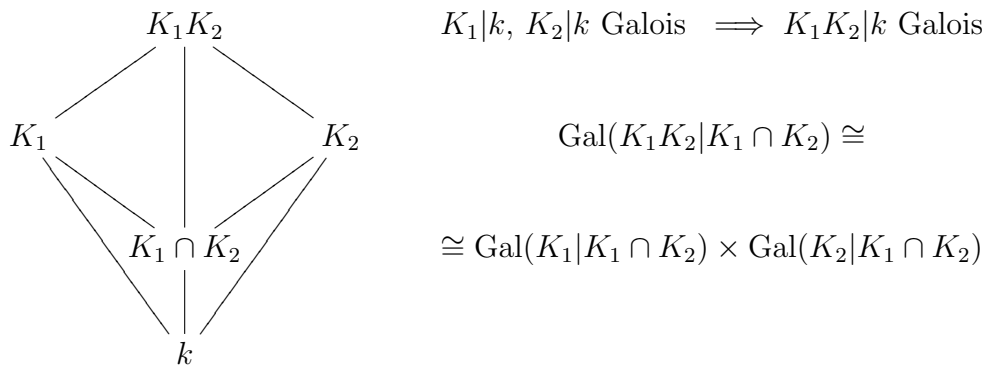


Diagrama 5.3: Comportament del caràcter galoisià per composició

### 5.3 Grups resolubles

En el capítol anterior hem vist que si  $k$  és un cos de característica zero, i si una equació polinòmica  $f(X) = 0$ , on  $f(X) \in k[X]$  és un polinomi no nul, és resoluble per radicals, existeix una extensió normal  $L|k$  que conté el cos de descomposició sobre  $k$  del polinomi  $f(X)$ , i que és tal que el grup de Galois  $G := \text{Gal}(L|k)$  admet una successió de subgrups de la forma  $G_0 := G \supseteq G_1 \supseteq G_2 \supseteq \dots \supseteq G_n = \{\text{Id}\}$ , tal que  $G_i$  és un subgrup normal de  $G_{i-1}$  i el quocient  $G_{i-1}/G_i$  és un grup commutatiu, per a  $1 \leq i \leq n$ . Es tracta de veure que aquesta condició necessària per a la resolubilitat per radicals de l'equació  $f(X) = 0$

també és suficient. Abans de procedir a la demostració d'aquest resultat, convé establir una definició i algun altre resultat previ.

**Definició 5.3.1.** Es diu que un grup  $G$  és *resoluble* si existeix una successió finita de subgrups de  $G$ ,  $G := G_0 \supseteq G_1 \supseteq \dots \supseteq G_n = \{1\}$ , tal que, per a  $1 \leq i \leq n$ ,  $G_i$  és un subgrup normal de  $G_{i-1}$  i el quocient  $G_{i-1}/G_i$  és un grup commutatiu. Una cadena de subgrups d'aquesta forma s'anomena una *resolució* del grup  $G$ .

**Exemples 5.3.2.** (a) Tot grup commutatiu  $G$  és resoluble, perquè la cadena  $G \supseteq \{1\}$  és una resolució de  $G$ .

(b) Si  $k$  és un cos de característica no divisor de  $n$ , el grup de Galois del cos de descomposició sobre  $k$  d'una equació de la forma  $X^n - a \in k[X]$ ,  $a \in k$ , és un grup resoluble. En efecte, si  $K := k(\zeta)$ , on  $\zeta$  és una arrel primitiva  $n$ -èsima de la unitat, i  $L$  és el cos de descomposició sobre  $k$  del polinomi  $X^n - a$ , la cadena de grups de Galois  $\text{Gal}(L|k) \supseteq \text{Gal}(L|K) \supseteq \{1\}$  és una resolució de  $\text{Gal}(L|k)$ , ja que l'extensió  $L|K$  és cíclica i, en conseqüència, abeliana, i l'extensió  $K|k$  és normal i  $\text{Gal}(L|k)/\text{Gal}(L|K) \cong \text{Gal}(K|k)$  és isomorf a un subgrup de  $(\mathbb{Z}/n\mathbb{Z})^*$ .

(c) Sigui  $A$  un anell commutatiu,  $G$  el subgrup de  $\mathbf{GL}(2, A)$  format per les matrius de la forma  $\begin{bmatrix} * & * \\ 0 & * \end{bmatrix}$ ,  $H$  el subgrup de  $G$  format per les matrius de la forma  $\begin{bmatrix} * & * \\ 0 & 1 \end{bmatrix}$ , i  $K$  el subgrup de  $H$  format per les matrius de la forma  $\begin{bmatrix} 1 & * \\ 0 & 1 \end{bmatrix}$ . Llavors,  $G$ ,  $H$  i  $K$  són grups resolubles.

Notem que el conjunt  $K$  és el nucli de la restricció a  $H$  del morfisme determinant,  $\det : H \rightarrow \mathbf{GL}_1(A) = A^*$ ; per tant,  $K$  és un subgrup normal de  $H$ . A més a més, com que aquest morfisme és exhaustiu, el grup quocient  $H/K$  és isomorf a  $\mathbf{GL}_1(A) = A^*$ ; en particular, és un grup commutatiu. D'altra banda,  $K$  és isomorf al grup additiu de  $A$ , perquè l'aplicació  $f : A \rightarrow K$  definida per  $f(x) := \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}$  és un isomorfisme. Per tant,  $K$  és un subgrup commutatiu i, en conseqüència, la cadena de subgrups  $H \supseteq K \supseteq \{1\}$  és una resolució de  $H$ .

Vegem ara que  $G$  és resoluble. El subgrup  $H \subseteq G$  és normal i el grup quocient  $G/H$  és isomorf a  $\mathbf{GL}_1(A)$ , ja que l'aplicació  $g : G \rightarrow \mathbf{GL}_1(A)$  donada per  $\begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \mapsto d$  és un morfisme exhaustiu de grups de nucli  $H$ . Per tant, la cadena  $G \supseteq H \supseteq K \supseteq \{1\}$  és una resolució del grup  $G$ .  $\square$

Per al tractament dels grups resolubles sovint és útil comparar el grup amb els seus subgrups normals i els seus quocients. Recordem el teorema d'isomorfia següent.

**Proposició 5.3.3.** *Sigui  $G$  un grup,  $H \subseteq G$  un subgrup qualsevol, i  $N \subseteq H$  un subgrup normal de  $G$  inclòs en  $H$ . Llavors:*

(a)  $N$  és un subgrup normal de  $H$ .

(b) El quocient  $H/N$  és subgrup de  $G/N$ ;  $i$  és normal si, i només si,  $H \subseteq G$  és normal.

(c) Si  $H \subseteq G$  també és normal, llavors el grup quocient  $G/H$  és isomorf al grup  $\frac{G/N}{H/N}$ .

DEMOSTRACIÓ: La demostració de (a) és immediata i, clarament,  $H/N$  és un subgrup de  $G/N$ . Per a acabar la prova de (b), notem que la projecció canònica  $\psi : G \rightarrow G/N$  ens permet definir una aplicació bijectiva entre el conjunt dels subgrups de  $G$  que contenen  $N$  i el dels subgrups de  $G/N$ , i per la qual subgrups normals es corresponen amb subgrups normals; aquesta aplicació fa correspondre a un subgrup  $\overline{S}$  de  $G/N$  el subgrup  $S := \psi^{-1}(\overline{S})$  de  $G$ , i a un subgrup  $S$  de  $G$  que conté  $N$ , el subgrup  $\overline{S} := \psi(S)$  de  $G/N$ .

Demostrem (c). Considerem la projecció canònica  $\pi : G \rightarrow G/H$ , que és un morfisme exhaustiu de grups; el nucli de  $\pi$  és  $H$  i conté  $N$ , de manera que  $\pi$  factoritza per un morfisme exhaustiu de grups  $\overline{\pi} : G/N \rightarrow G/H$ , el nucli del qual és  $H/N$ ; per tant, el grup quocient  $\frac{G/N}{H/N}$  és isomorf a  $G/H$ , com volíem veure.  $\square$

**Proposició 5.3.4.** *Siguin  $G$  un grup resoluble i  $H$  un subgrup qualsevol de  $G$ . Llavors,  $H$  és resoluble.*

DEMOSTRACIÓ: Sigui  $G_0 := G \supseteq G_1 \supseteq \dots \supseteq G_n = \{1\}$  una resolució de  $G$ ; es tracta de veure que la cadena  $H = H_0 \supseteq H_1 \supseteq \dots \supseteq H_n = \{1\}$ , on  $H_i := H \cap G_i$ , és una resolució de  $H$ . En primer lloc, observem que  $H_i = H \cap G_i \subseteq H \cap G_{i-1} = H_{i-1}$  i que  $H_i$  és normal en  $H_{i-1}$ ; a més a més, el nucli del morfisme de grups  $H_{i-1} = H \cap G_{i-1} \rightarrow G_{i-1} \rightarrow G_{i-1}/G_i$  és, evidentment,  $H_i = H \cap G_i$ ; per tant,  $H_{i-1}/H_i$  s'identifica amb un subgrup de  $G_{i-1}/G_i$  i, per tant, és commutatiu.  $\square$

**Lema 5.3.5.** *Siguin  $G$  un grup, i  $H, K \subseteq G$  subgrups. Suposem que  $H$  està inclòs en el normalitzador de  $K$ ; és a dir, que per a tot element  $h \in H$  i tot element  $k \in K$ , és  $h^{-1}kh \in K$ . Llavors, el subgrup generat per  $H$  i  $K$  en  $G$  és el conjunt  $HK$  format pels productes  $hk$  tals que  $h \in H$  i  $k \in K$ , i coincideix amb el conjunt anàleg  $KH$ .*

DEMOSTRACIÓ: És clar que els conjunts  $HK$  i  $KH$  han d'estar inclosos en el subgrup de  $G$  generat per la reunió  $H \cup K$ . D'altra banda, si  $h \in H$  i  $k \in K$ , és  $h^{-1}kh \in K$  i  $kh = h(h^{-1}kh) \in HK$ , de manera que se satisfà la inclusió  $KH \subseteq HK$ . Anàlogament,  $hk = (hkh^{-1})h \in KH$ , ja que  $hkh^{-1} \in K$ , de manera que  $HK \subseteq KH$ ; d'on  $KH = HK$ . Només resta veure que  $HK$  és un subgrup de  $G$ . Però això és senzill, ja que, per a  $h_1, h_2 \in H$  i  $k_1, k_2 \in K$ , és  $(h_1k_1)(h_2k_2) = h_1h_2h_2^{-1}k_1h_2k_2 = (h_1h_2)(h_2^{-1}k_1h_2)k_2 \in HK$ , perquè  $h_2^{-1}k_1h_2 \in K$ ; això ens diu que el producte de  $G$  és estable en el conjunt  $HK$ ; d'altra banda, com que  $1 \in H$  i  $1 \in K$ , és  $1 = 1 \cdot 1 \in HK$ , i l'element neutre de  $G$  pertany a  $HK$ ; i, finalment, si  $h \in H$  i  $k \in K$ , llavors  $(hk)^{-1} = k^{-1}h^{-1} = h^{-1}(hk^{-1}h^{-1}) \in HK$ , de manera que els inversos dels elements de  $HK$  també pertanyen a  $HK$ ; és a dir,  $HK$  és un subgrup de  $G$ .  $\square$

**Proposició 5.3.6.** *Siguin  $G$  un grup resoluble i  $N$  un subgrup normal de  $G$ . Llavors,  $G/N$  és un grup resoluble.*

DEMOSTRACIÓ: Sigui  $G_0 := G \supseteq G_1 \supseteq \dots \supseteq G_n = \{1\}$  una resolució de  $G$ ; es tracta de veure que la cadena  $G/N = \overline{G} = \overline{G}_0 \supseteq \overline{G}_1 \supseteq \dots \supseteq \overline{G}_n = \{1\}$  és una resolució de  $G/N$ , on posem  $\overline{G}_i := G_iN/N$ , que és el subgrup de  $G/N$  generat per la imatge de  $G_i$  en  $G/N$ .

Com que  $N$  és un subgrup normal de  $G$ , el normalitzador de  $N$  és tot  $G$ ; per tant, per a  $0 \leq i \leq n$ , el subgrup de  $G$  generat per  $G_i$  i  $N$  és  $G_iN$ . A més a més, per ser  $G_i$  un subgrup normal de  $G_{i-1}$ , també  $G_iN$  és un subgrup normal de  $G_{i-1}N$ , i  $\overline{G}_i$  és un subgrup normal de  $\overline{G}_{i-1}$ . Com que  $\overline{G}_0 = G_0N/N = GN/N = G/N$  i  $\overline{G}_n = G_nN/N = N/N = \{1\}$ ,

només resta veure que els grups quocient  $\overline{G}_{i-1}/\overline{G}_i$  són commutatius. Ara bé, el morfisme de grups  $G_{i-1} \xrightarrow{\text{incl}} G_{i-1}N \xrightarrow{\text{proj}} G_{i-1}N/G_iN$  és exhaustiu i el seu nucli conté  $G_i$ ; en conseqüència, tenim un morfisme exhaustiu de grups  $G_{i-1}/G_i \longrightarrow G_{i-1}N/G_iN$ ; com que  $G_{i-1}/G_i$  és commutatiu, també  $G_{i-1}N/G_iN$  és commutatiu; i, com que  $G_{i-1}N/G_iN$  és isomorf a  $\overline{G}_{i-1}/\overline{G}_i$ , aquest darrer grup és commutatiu, com volíem veure.  $\square$

Ara podem establir fàcilment el resultat que relaciona la resolubilitat d'un grup amb la dels seus subgrups i quocients.

**Proposició 5.3.7.** *Siguin  $G$  un grup i  $N \subseteq G$  un subgrup normal de  $G$ . El grup  $G$  és resoluble si, i només si, ho són els grups  $N$  i  $G/N$ .*

DEMOSTRACIÓ: Les dues proposicions anteriors donen una prova de la implicació directa. Recíprocament, suposem que  $N$  i  $G/N$  són resolubles i siguin

$$N_0 := N \supseteq N_1 \supseteq \cdots \supseteq N_r = \{1\}, \quad \overline{G}_0 := G/N \supseteq \overline{G}_1 \supseteq \cdots \supseteq \overline{G}_s = \{1\},$$

resolucions de  $N$  i de  $G/N$ , respectivament. Considerem la projecció  $\pi : G \longrightarrow G/N$ , i siguin  $G_i := \pi^{-1}(\overline{G}_i)$ , per a  $0 \leq i \leq s$ , els grups antiimatge. Com que  $\overline{G}_i$  és un subgrup normal de  $\overline{G}_{i-1}$ , per a  $1 \leq i \leq s$ , obtenim que  $G_i$  és un subgrup normal de  $G_{i-1}$ ; i, a més a més,  $G_{i-1}/G_i$  és isomorf a  $\overline{G}_{i-1}/\overline{G}_i$ ; en particular, els quocients  $G_{i-1}/G_i$  són commutatius. D'altra banda, com que  $\overline{G}_s = \{1\}$ , és  $G_s = N = N_0$ , de manera que la cadena de subgrups de  $G$

$$G := G_0 \supseteq G_1 \supseteq \cdots \supseteq G_s = N = N_0 \supseteq N_1 \supseteq \cdots \supseteq N_r = \{1\}$$

és una resolució de  $G$ .  $\square$

## 5.4 Resolubilitat per radicals

Es tracta de caracteritzar, finalment, les equacions polinòmiques resolubles per radicals. El resultat següent tracta el cas de característica zero.

**Teorema 5.4.1.** *Siguin  $k$  un cos de característica zero,  $\overline{k}$  un cos algebraicament tancat que conté  $k$ , i  $f(X) \in k[X]$  un polinomi no nul qualsevol. Suposem que  $L|k$  és una extensió finita i de Galois tal que  $L$  conté el cos de descomposició sobre  $k$  del polinomi  $f(X)$  i que el grup de Galois  $G := \text{Gal}(L|k)$  és resoluble. Llavors, l'equació  $f(X) = 0$  és resoluble per radicals.*

Abans de procedir a la demostració, establim un resultat que ens ajuda a simplificar-la. Comencem per donar una definició.

**Definició 5.4.2.** Sigui  $G$  un grup resoluble. Una resolució de  $G$ ,

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_r = \{1\},$$

s'anomena una *cadena normal abeliana*; s'anomena *cíclica* si tots els quocients  $G_{i-1}/G_i$  són grups cíclics; i direm que és *cíclica d'índexs primers* si és cíclica i, a més a més, els ordres dels grups quocient  $G_{i-1}/G_i$  són nombres primers.

**Proposició 5.4.3.** *Un grup finit és resoluble si, i només si, admet una resolució cíclica d'índexs primers.*

DEMOSTRACIÓ: Suposem que  $G$  és un grup finit resoluble i que

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_r = \{1\}$$

és una resolució de  $G$ . Cadascun dels grups quocient  $G_{i-1}/G_i$  és un grup finit i commutatiu; i si tenim una resolució cíclica d'índexs primers d'aquest grup quocient, prenent les antiimatges en  $G_{i-1}$  dels subgrups d'aquesta cadena, obtenim una resolució de  $G$  tal que els quocients successius entre els grups  $G_{i-1}$  i  $G_i$  són grups cíclics finits d'ordre primer. I aplicant això a cadascun dels quocients, obtenim una cadena com la desitjada per a  $G$ . Per tant, és suficient demostrar el resultat per als grups finits commutatius. I això és el contingut del resultat següent. La propietat recíproca és evident.  $\square$

**Proposició 5.4.4.** *Tot grup finit, commutatiu, i no trivial admet una resolució cíclica d'índexs primers.*

DEMOSTRACIÓ: Sigui  $G$  un grup finit commutatiu,  $m := \#G$ , l'ordre de  $G$ , i posem  $m = p_1 \cdots p_k$ , on  $p_1, \dots, p_k$  són nombres primers, no necessàriament diferents. Farem la demostració per inducció sobre  $k$ . Si  $k = 1$ , el grup  $G$  és d'ordre primer i, per tant, cíclic, i la cadena  $G \supseteq \{1\}$  és una resolució cíclica d'índexs primers de  $G$ . Suposem, ara, que  $k > 1$  i que el resultat és cert per a tots els grups commutatius l'ordre dels quals sigui un producte de menys de  $k$  nombres primers. Sigui  $g \in G$ ,  $g \neq 1$ , un element diferent del neutre, i  $r > 1$  l'ordre de  $g$ ; aleshores,  $r$  és de la forma  $r = ps$ , on  $p$  és un nombre primer que divideix  $m$  i  $s$  un producte de menys de  $k$  nombres primers. L'element  $g^s \in G$  és d'ordre primer  $p$ , de manera que genera un subgrup cíclic d'ordre primer, posem  $G^1$ , que és normal perquè  $G$  és commutatiu. I el grup quocient  $G/G^1$  és commutatiu i finit, i d'ordre  $s$ . Per hipòtesi d'inducció,  $G/G^1$  admet una resolució cíclica d'índexs primers; les antiimatges en  $G$  dels subgrups d'aquesta resolució formen una cadena cíclica d'índexs primers de  $G$  que s'acaba en  $G^1$ ; però  $G^1$  ja és cíclic d'ordre primer, de manera que la cadena, completada amb el grup trivial  $\{1\}$ , és una resolució cíclica d'índexs primers de  $G$ .  $\square$

Procedim, ara, a la demostració del teorema que hem enunciat en començar aquesta secció.

DEMOSTRACIÓ del teorema **5.4.1**: Per definició d'equació resoluble per radicals, és equivalent veure que l'extensió  $L|k$  és resoluble per radicals. Sigui  $n := \#\text{Gal}(L|k) = [L : k]$  i  $\zeta \in \bar{k}$  una arrel primitiva  $n$ -èsima de la unitat, i considerem l'extensió  $L(\zeta)|k$ , que és de Galois, ja que és la composició de les dues extensions de Galois  $L|k$  i  $k(\zeta)|k$  (cf. la proposició **5.2.6**). Si provem que l'extensió  $L(\zeta)|k$  és radical, ja haurem acabat, perquè  $L|k$  és una subextensió de  $L(\zeta)|k$ .

Sigui  $G_0 := \text{Gal}(L|k) \supseteq G_1 \supseteq \cdots \supseteq G_m = \{1\}$  una resolució cíclica d'índexs primers de  $\text{Gal}(L|k)$ , que existeix perquè  $G$  és un grup resoluble finit. Sigui  $k_i := L^{G_i}$  els cossos fixos,  $0 \leq i \leq m$ ; en virtut del teorema fonamental de la teoria de Galois (cf. el teorema **5.2.1**), tenim la cadena de cossos  $k_0 = k \subseteq k_1 \subseteq k_2 \subseteq \cdots \subseteq k_m = L$ , de manera que les extensions  $k_i|k_{i-1}$  són cícliques de graus primers que divideixen  $n$ , amb grups de Galois  $\text{Gal}(k_i|k_{i-1}) \cong G_{i-1}/G_i$ , per a  $1 \leq i \leq m$ . Com a conseqüència, si afegim  $\zeta$  a tots els cossos i posem  $K_i := k_i(\zeta)$ ,  $0 \leq i \leq m$ , tenim la cadena de cossos  $K_{-1} := k \subseteq K_0 = k(\zeta) \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_m = L(\zeta)$ . Per a  $1 \leq i \leq n$ , les extensions  $K_i|K_{i-1}$ , són trivials o bé cícliques de graus primers que divideixen  $n$ , perquè s'obtenen de les extensions  $k_i|k_{i-1}$  pel canvi de base  $K_{i-1}|k_{i-1}$  i, per tant, tenim morfismes injectius

$\text{Gal}(K_i|K_{i-1}) \longrightarrow \text{Gal}(k_i|k_{i-1}) \cong G_{i-1}/G_i$  dels grups de Galois (cf. la proposició 5.2.4); i, d'altra banda, l'extensió  $K_0|K_{-1}$  és abeliana, amb grup de Galois isomorf a un subgrup de  $(\mathbb{Z}/n\mathbb{Z})^*$ . Finalment, com que  $K_0$  conté les arrels  $n$ -èsimes de la unitat, per a  $1 \leq i \leq m$ ,  $K_{i-1}$  també les conté, de manera que l'extensió  $K_i|K_{i-1}$ , que és cíclica de grau divisor de  $n$ , admet un element primitiu  $\theta_i$  tal que  $\theta_i^{n_i} \in K_{i-1}$ , on  $n_i := [K_i : K_{i-1}]$  (cf. el teorema 4.9.2). Com que  $K_0 = k(\zeta)$  i  $\zeta^n = 1 \in k$ , hem vist que la cadena

$$K_{-1} := k \subseteq K_0 = k(\zeta) \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_m = L(\zeta)$$

és una resolució per radicals de l'extensió  $L(\zeta)|k$ .  $\square$

**5.4.5.** Els teoremes 4.12.7 i 5.4.1, i el fet que un grup és resoluble si, i només si, ho són tots els seus subgrups i els seus quocients (cf. la proposició 5.3.7), proporcionen immediatament la caracterització volguda.

**Corollari 5.4.6.** *Siguin  $k$  un cos de característica zero,  $f(X) \in k[X]$  un polinomi no nul, i  $L$  el cos de descomposició de  $f(X)$  en un cos algebraicament tancat que conté  $k$ . L'equació polinòmica  $f(X) = 0$  és resoluble per radicals sobre  $k$  si, i només si, el grup de Galois  $\text{Gal}(L|k)$  és resoluble.*  $\square$

**5.4.7.** El punt clau de la caracterització de les equacions polinòmiques resolubles per radicals en el cas de característica zero és el coneixement de les extensions cícliques de grau  $n$  quan el cos base conté les arrels  $n$ -èsimes de la unitat (cf. la proposició 4.10.1, teoria de Kummer). Cadascun dels passos de la demostració que hem fet en el cas de característica zero és vàlid en el cas de característica positiva, sempre que la característica del cos no divideixi el grau de l'extensió cíclica que tractem. I per al cas de grau igual a la característica, el teorema d'Artin-Schreier ens ajuda.

**Definició 5.4.8.** (Cf. la definició 4.11.1.) Siguin  $p$  un nombre primer i  $k$  un cos de característica  $p$ . Anomenarem *extensió radical* de  $k$  tota extensió separable  $K|k$  per a la qual existeix una successió finita de subcossos de la forma

$$k \subseteq k(\theta_1) \subseteq k(\theta_1, \theta_2) \subseteq \cdots \subseteq k(\theta_1, \dots, \theta_m) = K$$

tal que, per a  $1 \leq i \leq m$ , i si posem  $n_i := [k(\theta_1, \dots, \theta_i) : k(\theta_1, \dots, \theta_{i-1})]$ , se satisfà que

- (a)  $\theta_i^{n_i} \in k(\theta_1, \dots, \theta_{i-1})$ , si  $p$  no divideix  $n_i$ ,
- (b) i  $n_i = p$  i  $\theta_i^p - \theta_i \in k(\theta_1, \dots, \theta_{i-1})$ , si  $p$  divideix  $n_i$ .

Anomenarem *extensió resoluble per radicals* tota subextensió  $K|k$  d'una extensió radical, i direm que una equació  $f(X) = 0$ , on  $f(X) \in k[X]$  és un polinomi no nul, és *resoluble per radicals* si el cos de descomposició de  $f(X)$  sobre  $k$  defineix una extensió resoluble per radicals.

Observem que aquestes definicions coincideixen amb les donades en el cas de característica zero, llevat que s'admeten, a més a més, arrels de polinomis de la forma  $X^p - X - a$ , on  $p$  és la característica. Anàlogament al cas de característica zero, se satisfà el teorema següent.

**Teorema 5.4.9.** *Siguin  $p$  un nombre primer,  $k$  un cos de característica  $p$ ,  $f(X) \in k[X]$  un polinomi no nul, i  $L$  el cos de descomposició de  $f(X)$  en un cos algebraicament tancat que conté  $k$ . L'equació polinòmica  $f(X) = 0$  és resoluble per radicals sobre  $k$  si, i només si, el grup de Galois  $\text{Gal}(L|k)$  és resoluble.*



DEMOSTRACIÓ: Aquest teorema es pot demostrar de manera idèntica al cas de característica zero, llevat que en el cas de les extensions cíclics de grau  $p$  cal tenir en compte el teorema d'Artin–Schreier (cf. 4.9.3) i considerar elements primitius  $\theta$  tals que  $\theta^p - \theta$  sigui un element del cos base de l'extensió cíclica corresponent.  $\square$

**Observació 5.4.10.** No caldria considerar polinomis irreductibles sense arrels múltiples. En aquest cas, en la definició del concepte d'extensió radical, no s'exigiria que l'extensió  $K|k$  fos separable, i caldria admetre com a “radicals”, a més a més de les arrels de polinomis de les formes  $X^p - X - a$  i  $X^n - a$ , per a  $n$  no divisible per  $p$ , les arrels dels polinomis de la forma  $X^p - a$ , que donarien compte de les extensions no separables. En aquest cas, caldria formular el teorema exigint la condició que l'extensió  $L|k$  sigui normal en lloc d'exigir que sigui de Galois.

## 5.5 Equacions ciclotòmiques

En aquesta secció, es tracta d'explicar la resolució de les equacions ciclotòmiques i de veure que aquestes equacions són resolubles per radicals en el sentit estricte; és a dir, en el sentit que en la cadena de cossos que donen una extensió radical que conté el cos de descomposició de l'equació ciclotòmica no s'admeten elements primitius que siguin arrels de la unitat.

Siguin  $p$  un nombre primer,  $k$  un cos de característica zero,  $\zeta$  una arrel primitiva  $p$ -èsima de la unitat, i  $K := k(\zeta)$ .

L'extensió  $K|k$  és, llavors, de Galois i el seu grup de Galois és isomorf a un subgrup de  $(\mathbb{Z}/p\mathbb{Z})^*$ ; com que  $\mathbb{Z}/p\mathbb{Z}$  és un cos, el grup  $(\mathbb{Z}/p\mathbb{Z})^*$  és cíclic d'ordre  $p - 1$ , de manera que  $\text{Gal}(K|k)$  és un grup cíclic d'ordre divisor de  $p - 1 < p$ . Així,  $K|k$  és una extensió cíclica de grau divisor de  $p - 1$ ; per tant, si  $\xi$  és una arrel primitiva  $p - 1$ -èsima de la unitat, l'extensió  $K(\xi)|k(\xi)$  admet un element primitiu  $\theta$  tal que  $\theta^{p-1} \in k(\xi)$ ; per tant,  $K = k(\zeta) \subseteq k(\xi, \theta)$ , i  $\xi^{p-1} = 1 \in k$ , i  $\theta^{p-1} \in k(\xi)$ .

Per tant, les arrels primitives  $p$ -èsimes de la unitat es poden expressar per radicals de grau menor o igual que  $p - 1$ ; és a dir, existeix una cadena de cossos de la forma  $k \subseteq k(\theta_1) \subseteq \dots \subseteq k(\theta_1, \dots, \theta_n)$  tal que  $\zeta \in k(\theta_1, \dots, \theta_n)$ , i que  $\theta_i^{n_i} \in k(\theta_1, \dots, \theta_{i-1})$ , amb  $n_i < p$ .

Si algun dels elements  $\theta_i$  és alguna arrel de la unitat, podem substituir l'extensió  $k(\theta_1, \dots, \theta_i)|k(\theta_1, \dots, \theta_{i-1})$  per una cadena com l'anterior, i repetir l'argument inductivament. Així, obtenim el resultat següent.

**Proposició 5.5.1.** *Una extensió de cossos de característica zero  $K|k$  és radical si, i només si, existeix una successió de cossos de la forma*

$$k \subseteq k(\theta_1) \subseteq k(\theta_1, \theta_2) \subseteq \dots \subseteq k(\theta_1, \dots, \theta_m) = K$$

*tal que, per a cada índex  $i$ ,  $1 \leq i \leq m$ , existeix un nombre natural  $n_i \geq 1$  tal que  $\theta_i^{n_i} \in k(\theta_1, \dots, \theta_{i-1})$  i  $X^{n_i} - \theta_i^{n_i} \in k(\theta_1, \dots, \theta_{i-1})[X]$  és irreductible.  $\square$*

Per als cossos de característica positiva se satisfà el resultat anàleg següent.

**Corol·lari 5.5.2.** Una extensió  $K|k$  de cossos de característica  $p > 0$  és radical si, i només si, existeix una successió de cossos de la forma

$$k \subseteq k(\theta_1) \subseteq k(\theta_1, \theta_2) \subseteq \dots \subseteq k(\theta_1, \dots, \theta_m) = K$$

tal que, per a cada índex  $i$ ,  $1 \leq i \leq n$ , existeix un nombre natural  $n_i \geq 1$  tal que

(a)  $\theta_i^{n_i} \in k(\theta_1, \dots, \theta_{i-1})$  i  $X^{n_i} - \theta_i^{n_i} \in k(\theta_1, \dots, \theta_{i-1})[X]$  és irreductible, si  $p$  no divideix  $n_i$ , i

(b)  $n_i = p$ ,  $\theta_i^p - \theta_i \in k(\theta_1, \dots, \theta_{i-1})$ , i  $X^p - X - (\theta_i^p - \theta_i) \in k(\theta_1, \dots, \theta_{i-1})[X]$  és irreductible, si  $p$  divideix  $n_i$ .  $\square$

## 5.6 Grups de Galois com a grups de permutacions

Siguin  $k$  un cos,  $\bar{k}$  un cos algebraicament tancat que conté  $k$ ,  $f(X) \in k[X]$  un polinomi no nul,  $Z_f := \{\theta_1, \dots, \theta_n\} \subseteq \bar{k}$  el conjunt de les arrels de  $f(X)$ , i  $L := k(\theta_1, \dots, \theta_n)$  el cos de descomposició del polinomi  $f(X)$ . Llavors, l'extensió  $L|k$  és normal, i podem considerar el grup de Galois  $\text{Gal}(L|k)$  i una aplicació  $g : \text{Gal}(L|k) \times Z_f \xrightarrow{g} Z_f$  definida per  $(\sigma, \theta) \mapsto \sigma(\theta)$ . Efectivament, donat un  $k$ -automorfisme  $\sigma$  de  $L$  (és a dir, un element de  $\text{Gal}(L|k)$ ), i una arrel  $\theta$  d'un polinomi  $f(X) \in k[X]$ ,  $\sigma(\theta)$  és una altra arrel del mateix polinomi; per tant, l'aplicació està ben definida. És immediat comprovar que se satisfan les propietats següents:

(a) Per a  $\sigma, \tau \in \text{Gal}(L|k)$  i  $\theta \in Z_f$ , és  $(\tau \circ \sigma)(\theta) = \tau(\sigma(\theta))$ .

(b) Per a  $\theta \in Z_f$ ,  $1(\theta) = \theta$ , on 1 és l'element neutre del grup  $\text{Gal}(L|k)$ .

Aquestes propietats per a una aplicació de la forma  $g : G \times C \rightarrow C$ , on  $G$  és un grup qualsevol i  $C$  és un conjunt qualsevol, ja han aparegut (cf. el punt 2.1.1 o la secció A.1.6, de l'apèndix, per a les definicions). En efecte, si  $A$  és un anell commutatiu,  $A[X_1, \dots, X_n]$  és l'anell de polinomis en  $n$  indeterminades i  $S_n$  és el grup de les permutacions de  $\{1, 2, \dots, n\}$ , ja hem vist una aplicació  $S_n \times A[X_1, \dots, X_n] \rightarrow A[X_1, \dots, X_n]$  donada per  $(\sigma, P(X_1, \dots, X_n)) \mapsto P(X_{\sigma(1)}, \dots, X_{\sigma(n)})$ . I que el conjunt dels polinomis  $P(X_1, \dots, X_n) \in A[X_1, \dots, X_n]$  tals que  $P(X_{\sigma(1)}, \dots, X_{\sigma(n)}) = P(X_1, \dots, X_n)$ , per a tot  $\sigma \in S_n$ , és l'anell dels polinomis simètrics. Per comoditat, repetim aquí les definicions i propietats bàsiques.

**Definició 5.6.1.** Siguin  $G$  un grup i  $C$  un conjunt qualssevol. S'anomena *acció per l'esquerra* del grup  $G$  en el conjunt  $C$  tota aplicació  $g : G \times C \rightarrow C$  tal que, si denotem per  $\sigma \cdot x$  la imatge de la parella  $(\sigma, x)$ , se satisfan les dues propietats següents:

(a) per a  $\sigma, \tau \in G$  i  $x \in C$ , és  $(\tau \sigma) \cdot x = \tau \cdot (\sigma \cdot x)$ , i

(b) per a  $x \in C$ ,  $1 \cdot x = x$ , on 1 denota l'element neutre del grup  $G$ .

També es diu que el grup  $G$  actua en el conjunt  $C$ , o que  $C$  és un  $G$ -conjunt.

Així, tenim el resultat següent.

**Corol·lari 5.6.2.** El grup de Galois de l'extensió  $L|k$ , on  $L$  és el cos de descomposició d'un polinomi no nul  $f(X) \in k[X]$ , actua en el conjunt de les arrels de  $f(X)$ .  $\square$

**Observació 5.6.3.** El concepte d'*acció per la dreta* de  $G$  en  $C$  es defineix de manera anàloga; en aquest cas, es tracta d'una aplicació  $G \times C \rightarrow C$  tal que, si denotem per  $x^\sigma$  la imatge de la parella  $(\sigma, x)$ , se satisfan les propietats següents:

- (a) per a  $\sigma, \tau \in G$  i  $x \in C$ , és  $x^{\tau\sigma} = (x^\tau)^\sigma$ , i
- (b) per a  $x \in C$ ,  $x^1 = x$ , on 1 denota l'element neutre del grup  $G$ .

Notem que la diferència està en la propietat (a), perquè per a l'acció per l'esquerra primer actua l'element escrit a la dreta i per a l'acció per la dreta primer actua l'element escrit a l'esquerra.

**5.6.4.** Sigui  $g : G \times C \rightarrow C$  una acció (per l'esquerra) d'un grup  $G$  en un conjunt  $C$ , i sigui  $S(C)$  el grup de les permutacions de  $C$ ; és a dir, el grup de les aplicacions bijectives de  $C$  en  $C$ . L'acció de  $G$  en  $C$  dona lloc a un morfisme de grups  $\psi_g : G \rightarrow S(C)$ . En efecte, donat  $\sigma \in G$ , podem considerar l'aplicació  $g_\sigma : C \rightarrow C$  definida per  $g_\sigma(x) := \sigma \cdot x$ . És immediat comprovar que, per a  $\sigma, \tau \in G$ , és  $g_\sigma \circ g_\tau = g_{\sigma\tau}$  i que  $g_1 = \text{Id}$ , on  $\text{Id}$  és la identitat en el conjunt  $C$ ; en particular,  $g_\sigma$  és bijectiva amb inversa  $g_{\sigma^{-1}}$ , de manera que l'aplicació  $\psi_g : G \rightarrow S(C)$  està ben definida, i, a més a més, és un morfisme de grups. I recíprocament, si  $\psi : G \rightarrow S(C)$  és un morfisme de grups, l'aplicació  $g_\psi : G \times C \rightarrow C$  definida per  $g_\psi(\sigma, x) := \psi(\sigma)(x)$  és una acció per l'esquerra de  $G$  en  $C$ . Dit d'una altra manera, donar una acció per l'esquerra d'un grup  $G$  en un conjunt  $C$  és equivalent a donar un morfisme de grups de  $G$  en el grup  $S(C)$  de les permutacions de  $C$ .

**5.6.5.** Anàlogament, si  $G \times C \rightarrow C$  és una acció per la dreta d'un grup  $G$  en un conjunt  $C$ , l'aplicació  $\psi : G \rightarrow S(C)$  definida per  $\psi(\sigma)(x) := x^{\sigma^{-1}}$  és un morfisme de grups i recíprocament, a tot morfisme de grups  $\psi : G \rightarrow S(C)$  li correspon una acció per la dreta  $(\sigma, x) \mapsto \psi(\sigma^{-1})(x)$ .

**5.6.6.** En el cas que el conjunt  $C$  sigui finit, i si  $n$  designa el seu cardinal, llavors  $S(C)$  és isomorf al grup simètric  $S_n$ . En aquest cas, doncs, donar una acció (per l'esquerra o per la dreta) de  $G$  en  $C$  equival a donar un morfisme de grups  $G \rightarrow S_n$ .

**Definició 5.6.7.** Sigui  $G \times C \rightarrow C$ , o bé, equivalentment,  $G \rightarrow S(C)$ , una acció (per l'esquerra) d'un grup  $G$  en un conjunt  $C$ . Donat un element qualsevol  $x \in C$ , el subconjunt  $G \cdot x := \{\sigma \cdot x : \sigma \in G\} \subseteq C$  s'anomena l'*òrbita* o bé la *trajectòria* de  $x$ . El subconjunt  $G_x := \{\sigma \in G : \sigma \cdot x = x\} \subseteq G$  és un subgrup de  $G$  que s'anomena el *grup d'isotropia*, o també l'*estabilitzador*, de  $x$ . L'acció s'anomena *transitiva* si existeix un element  $x \in C$  tal que  $C = G \cdot x$ ; és a dir, si només hi ha una òrbita.

**Exercici 5.6.8** (cf. **A.1.47**). Sigui  $G \rightarrow S(C)$  una acció d'un grup  $G$  en un conjunt  $C$ . Llavors:

- (a) Dues òrbites que es tallen, coincideixen.
- (b) El conjunt  $C$  és reunió disjunta d'òrbites.
- (c) El cardinal d'una òrbita coincideix amb l'índex del subgrup d'isotropia de qualsevol element de l'òrbita.
- (d) Els grups d'isotropia són conjugats; més concretament, per a tot element  $\sigma \in G$  i tot element  $x \in C$  és  $G_{\sigma \cdot x} = \sigma G_x \sigma^{-1}$ , si l'acció ho és per l'esquerra, i  $G_{x^\sigma} = \sigma^{-1} G_x \sigma$ , si l'acció ho és per la dreta.

(e) Si  $R$  designa un conjunt de representants de les òrbites (és a dir, un conjunt que conté exactament un element de cada òrbita), se satisfà la fórmula de les òrbites:

$$\#C = \sum_{x \in R} [G : G_x],$$

on  $[G : G_x]$  és l'índex del grup d'isotropia de  $x$  en  $G$ .

**5.6.9.** Donat un grup qualsevol  $G$ , podem considerar dues accions per l'esquerra de  $G$  en el conjunt  $G$  dels seus elements. D'una banda, l'acció per translació, donada per la multiplicació; és a dir, l'aplicació  $G \times G \rightarrow G$  donada per  $(x, y) \mapsto xy$ . D'altra banda, l'acció per conjugació; és a dir, l'aplicació  $G \times G \rightarrow G$  donada per  $(x, y) \mapsto xyx^{-1}$ . Les òrbites per l'acció per conjugació s'anomenen les classes de conjugació de  $G$ .

**Observació 5.6.10.** Anàlogament, podem considerar accions per la dreta d'un grup  $G$  en el conjunt dels seus elements; per translació, donada per  $(x, y) \mapsto yx$ , i per conjugació, donada per  $(x, y) \mapsto x^{-1}yx$ . Notem que les òrbites per a les accions per conjugació per la dreta o per l'esquerra són les mateixes.

**Proposició 5.6.11.** *Siguin  $\bar{k}$  un cos algebraicament tancat,  $k \subseteq \bar{k}$  un subcos qualsevol,  $f(X) \in k[X]$  un polinomi no nul,  $Z_f := \{\theta_1, \dots, \theta_n\} \subseteq \bar{k}$  el conjunt de les arrels de  $f(X)$ , i  $L := k(\theta_1, \dots, \theta_n)$  el cos de descomposició del polinomi  $f(X)$ . Llavors, l'acció del grup de Galois  $\text{Gal}(L|k)$  en el conjunt de les arrels de  $f(X)$  identifica  $\text{Gal}(L|k)$  amb un subgrup del grup simètric  $S_n$ .*

DEMOSTRACIÓ: Només cal veure que el morfisme de grups  $\text{Gal}(L|k) \rightarrow S(Z_f) \cong S_n$  donat per l'acció és injectiu. Però això és immediat, ja que si  $\sigma \in \text{Gal}(L|k)$  és tal que  $\sigma(\theta) = \theta$ , per a tota arrel de  $f(X)$ , com que  $\sigma$  és un  $k$ -automorfisme de  $L$  i  $L$  està generat sobre  $k$  per les arrels de  $f(X)$ ,  $\sigma$  és la identitat de  $L$ .  $\square$

Aquest resultat justifica la definició següent.

**Definició 5.6.12.** Sigui  $S_n$  el grup simètric sobre  $\{1, 2, \dots, n\}$ . Un subgrup  $H \subseteq S_n$  s'anomena *transitiu* si l'acció de  $H$  sobre  $\{1, 2, \dots, n\}$  és transitiva; és a dir, si donats  $i, j \in \{1, 2, \dots, n\}$ , existeix  $\sigma \in H$  tal que  $\sigma(i) = j$ .

**Corollari 5.6.13.** *Siguin  $k$  un cos,  $f(X) \in k[X]$  un polinomi irreductible de grau  $n$ , i  $L$  el cos de descomposició de  $f(X)$  sobre  $k$ . El grup de Galois de l'extensió  $L|k$  s'identifica amb un subgrup transitiu del grup simètric  $S_n$ .*

DEMOSTRACIÓ: En efecte, donades dues arrels del polinomi  $f(X)$ ,  $\theta_1, \theta_2$ , existeix una  $k$ -immersió  $\sigma : k(\theta_1) \rightarrow k(\theta_2)$  tal que  $\sigma(\theta_1) = \theta_2$ ; una extensió de  $\sigma$  a un  $k$ -automorfisme de  $L$  dona lloc a una permutació de les arrels de  $f(X)$  tal que  $\sigma(\theta_1) = \theta_2$ . Per tant, el subgrup de  $S_n$  imatge per l'acció és un subgrup transitiu de  $S_n$ .  $\square$

**Exercici 5.6.14.** Sigui  $K|k$  una extensió de Galois finita qualsevol de cossos. El grup de Galois de l'extensió s'identifica amb un subgrup transitiu de  $S_n$ , on  $n := [K : k]$  és el grau de l'extensió.

**Observació 5.6.15.** Donada una extensió finita i de Galois,  $L|k$ , de grau, posem,  $[L:k]=n$ , el grup de Galois  $\text{Gal}(L|k)$  es pot identificar amb un subgrup transitiu del grup simètric  $S_n$ ; ara bé, pot ser que  $L$  sigui el cos de descomposició sobre  $k$  d'un polinomi de grau  $d$  estrictament menor que  $n$ ; en aquest cas, el grup de Galois  $\text{Gal}(L|k)$  també s'identifica amb un subgrup transitiu de  $S_d$ , i no cal cercar-lo dins  $S_n$ .

## 5.7 L'equació general de grau $n$

Ens interessa estudiar qualsevol equació polinòmica. Sigui  $n \geq 2$  un nombre natural i considerem, d'una banda, l'anell de polinomis en  $n + 1$  indeterminades  $A := \mathbb{Z}[a_n, x_1, \dots, x_n]$  i el seu cos de fraccions  $K := \mathbb{Q}(a_n, x_1, \dots, x_n)$ , i, de l'altra, els anells de polinomis en una indeterminada i de coeficients en  $A$ ,  $A[X]$ , o de coeficients en  $K$ ,  $K[X]$ . Recordem la definició del polinomi general (cf. **2.2.4**).

**Definició 5.7.1.** S'anomena *polinomi general* de grau  $n$  el polinomi

$$f(X) := a_n(X - x_1)(X - x_2) \cdots (X - x_n) \in A[X].$$

Observem que el polinomi general de grau  $n$  és un polinomi concret, que pertany a un anell concret, i no qualsevol polinomi de grau  $n$  sobre qualsevol cos.

Els coeficients del polinomi general de grau  $n$ ,  $f(X)$ , són els productes dels polinomis simètrics elementals en  $x_1, \dots, x_n$  per  $a_n$ .

Més concretament, si  $s_1(x_1, \dots, x_n) := x_1 + \cdots + x_n$ ,  $\dots$ ,  $s_n(x_1, \dots, x_n) := x_1 \cdots x_n$  són els polinomis simètrics elementals en  $x_1, \dots, x_n$ , i, si posem

$$a_i := (-1)^{n-i} a_n s_{n-i}(x_1, \dots, x_n),$$

per a  $0 \leq i \leq n - 1$ , el polinomi  $f(X)$  admet l'expressió (cf. les fórmules de Viète **2.2.7**)

$$f(X) = \sum_{i=0}^n a_i X^i \in A[X].$$

Evidentment, el grup simètric  $S_n$  actua de manera natural en  $K$  per permutació de les indeterminades  $x_1, \dots, x_n$ , de manera que aquestes permutacions produeixen automorfismes de  $K$ , per tant, en virtut del teorema d'Artin (cf. **5.1.5**), l'extensió  $K|K^{S_n}$  és una extensió de Galois de grup de Galois isomorf a  $S_n$ . Ara bé,  $K^{S_n} = \mathbb{Q}(a_0, a_1, \dots, a_n)$ ; és a dir,  $K^{S_n}$  és el cos de les funcions racionals simètriques de coeficients en  $\mathbb{Q}(a_n)$  i indeterminades  $x_1, \dots, x_n$ . Aquest cos és isomorf al cos de fraccions racionals en les  $n + 1$  indeterminades  $a_0, a_1, \dots, a_n$  (cf. el teorema **2.3.3**),  $f(X) \in \mathbb{Q}(a_0, a_1, \dots, a_n)[X]$  és irreductible, i el cos de descomposició de  $f(X)$  és  $\mathbb{Q}(a_n, x_1, \dots, x_n) = K$ . En particular, el grup de Galois del cos de descomposició del polinomi  $f(X)$  és isomorf al grup simètric  $S_n$ .

**Teorema 5.7.2.** Si  $n \geq 5$ , l'equació general de grau  $n$  no és resoluble per radicals. Equivalentment, si  $n \geq 5$ , el grup simètric  $S_n$  no és resoluble.

La demostració d'aquest teorema és purament de teoria de grups. La farem per parts.

**Definició 5.7.3.** (cf. **A.1.39**) Sigui  $G$  un grup. S'anomena *subgrup derivat* de  $G$  el subgrup  $DG$  de  $G$  generat per tots els *commutadors*; és a dir, els elements de  $G$  de la forma  $[a, b] := a^{-1}b^{-1}ab$ , per a  $a, b \in G$ .

**Exercici 5.7.4.** (cf. **A.1.40**) Per a tot grup  $G$ , el subgrup derivat de  $G$  és un subgrup normal de  $G$ , el grup quocient  $G/DG$  és commutatiu, i si  $H \subseteq G$  és un subgrup normal de  $G$  tal que  $G/H$  és commutatiu, llavors  $DG \subseteq H$ .

**Lema 5.7.5.** *Per a tot nombre natural  $n \geq 2$ , és  $DS_n = A_n$ . Per a tot nombre natural  $n \geq 5$  és  $DA_n = A_n$ .*

DEMOSTRACIÓ: Clarament, tot commutador  $\tau^{-1}\sigma^{-1}\tau\sigma$  descompon en un nombre parell de transposicions, ja que  $\tau$  i  $\tau^{-1}$  descomponen en el mateix nombre de transposicions, i  $\sigma$  i  $\sigma^{-1}$  també. Per tant, tots els commutadors pertanyen a  $A_n$ ; i això implica que  $DA_n \subseteq DS_n \subseteq A_n$ . Recíprocament, per a  $n \geq 3$ , un 3-cicle qualsevol  $(a, b, c)$  es pot escriure en la forma  $(a, b, c) = (a, b)(a, c)(a, b)(a, c) = (a, b)^{-1}(a, c)^{-1}(a, b)(a, c)$ , de manera que els 3-cicles pertanyen a  $DS_n$ ; com que els 3-cicles generen  $A_n$ , obtenim que, per a  $n \geq 3$ , és  $DS_n = A_n$ . I, per a  $n = 2$ , és immediat que  $DS_2 = A_2 = \{1\}$ . Només resta veure que, per a  $n \geq 5$ , és  $A_n \subseteq DA_n$ . Siguin  $a, b, c, d, e$ , diferents dos a dos; llavors,  $(a, d, b)^{-1}(a, e, c)^{-1}(a, d, b)(a, e, c) = (a, b, c)$ ; així, tot 3-cicle  $(a, b, c)$  pertany a  $DA_n$ ; i això acaba la prova.  $\square$

**Observació 5.7.6.** Per a completar el resultat anterior, observem que és  $DA_4 = V_4 := \{1, (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\}$ , i  $DA_3 = \{1\}$ .

**Corol·lari 5.7.7.** *Per a  $n \geq 5$ ,  $A_n$  no és resoluble.*

DEMOSTRACIÓ: Suposem que  $G$  és un grup resoluble, i que

$$G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_r = \{1\}$$

és una resolució de  $G$ . Llavors,  $G_1$  és un subgrup normal de  $G$  tal que  $G/G_1$  és commutatiu; per tant,  $DG \subseteq G_1$ . Ara bé, com que  $DA_n = A_n$ , per a  $n \geq 5$ , una possible resolució de  $A_n$  no pot començar mai. Per tant,  $A_n$  no admet cap resolució.  $\square$

Com que tot subgrup d'un grup resoluble és resoluble, i com que  $A_n$  no és resoluble, per a  $n \geq 5$ , obtenim immediatament el resultat següent.

**Corol·lari 5.7.8.** *Per a  $n \geq 5$ ,  $S_n$  no és resoluble.*  $\square$

Acabarem aquesta secció amb un resultat que caracteritza les equacions polinòmiques el grup de Galois de les quals està inclòs en el grup alternat.

**Proposició 5.7.9.** *Siguin  $k$  un cos,  $a_0, a_1, \dots, a_n \in k$ ,  $a_n \neq 0$ , elements de  $k$  tals que les arrels del polinomi  $f(X) := a_0 + a_1X + \cdots + a_nX^n \in k[X]$  en un cos algebraicament tancat  $\bar{k}$  que conté  $k$  siguin totes simples,  $\theta_1, \dots, \theta_n \in \bar{k}$  les arrels de  $f(X)$ , i  $L \subseteq \bar{k}$  el cos de descomposició del polinomi. Posem  $\delta := a_n^{n-1} \prod_{i < j} (\theta_i - \theta_j)$ , de manera que el discriminant del polinomi  $f(X)$  és  $\Delta := \delta^2 \in k$ , i sigui  $K := k(\delta)$ . Si identifiquem  $\text{Gal}(L|k)$  amb un subgrup del grup simètric  $S_n$ , aleshores el grup de Galois de l'extensió  $L|K$  és  $\text{Gal}(L|K) = \text{Gal}(L|k) \cap A_n$ .*

DEMOSTRACIÓ: En fer una transposició de dues arrels del polinomi  $f(X)$ , i deixar les altres invariants,  $\delta$  canvia de signe; per tant, en aplicar permutacions parelles,  $\delta$  no varia. Així,  $\delta$  és invariant exactament per les permutacions parelles, de manera que el cos fix per  $\text{Gal}(L|k) \cap A_n$  és  $k(\delta) = K$ .  $\square$

**Corol·lari 5.7.10.** *Amb les mateixes notacions i hipòtesis,  $\text{Gal}(L|k)$  és subgrup de  $A_n$  si, i només si, el discriminant  $\Delta$  és un quadrat de  $k$ ; és a dir, si, i només si,  $k = K$ .*  $\square$

## 5.8 L'equació general de grau 3

**5.8.1.** En aquesta secció es tracta d'explicar la resolució per radicals de l'equació general de grau 3,  $f(X) = 0$ , on

$$f(X) = a(X - x_1)(X - x_2)(X - x_3) = aX^3 + bX^2 + cX + d \\ \in \mathbb{Z}[a, x_1, x_2, x_3][X] \subseteq \mathbb{Q}(a, x_1, x_2, x_3)[X],$$

i en la qual els coeficients són  $a$ , i

$$b := -a(x_1 + x_2 + x_3), \\ c := a(x_1x_2 + x_1x_3 + x_2x_3), \\ d := -ax_1x_2x_3.$$

Com que el grup simètric  $S_3$  és resoluble, i con que el grup de Galois de l'extensió  $\mathbb{Q}(a, x_1, x_2, x_3) | \mathbb{Q}(a, b, c, d)$  és isomorf a  $S_3$ , l'equació  $f(X) = 0$  és resoluble per radicals. Es tracta de veure com es pot obtenir una fórmula per a expressar les arrels de  $f(X)$  per radicals, a partir dels coeficients.

**5.8.2.** L'única resolució possible del grup simètric  $S_3$  és la donada per la cadena de subgrups  $S_3 \supseteq A_3 \supseteq \{1\}$ . El grup  $A_3$  és cíclic d'ordre 3 i el quocient  $S_3/A_3$  és cíclic d'ordre 2. D'acord amb la teoria desenvolupada al final del capítol anterior, i tenint en compte que les arrels quadrades de la unitat ja pertanyen al cos base, serà útil afegir al cos base les arrels cúbiques de la unitat, posem  $1, \rho, \rho^2$ , on  $\rho^3 = 1, \rho \neq 1$ . Doncs, si posem  $k := \mathbb{Q}(\rho)(a, b, c, d)$ , i  $L := \mathbb{Q}(\rho)(a, x_1, x_2, x_3)$ , considerarem l'extensió de Galois  $L|k$ , de grup de Galois  $S_3$ , i el cos  $K := L^{A_3}$ , el cos fix pel grup alternat. Notem que  $K = k(\delta)$ , on  $\delta^2$  és el discriminant del polinomi  $f(X)$  (cf. la proposició **5.7.9**).

**5.8.3.** L'extensió  $L|K$  és cíclica de grau 3 i  $K$  conté les arrels cúbiques de la unitat; per tant, d'acord amb el teorema **4.9.2**, (b), existeix un element primitiu  $\eta$  de  $L|K$  tal que  $\eta^3 \in K$ ; volem determinar un tal element primitiu. Per a això, sigui  $\sigma \in \text{Gal}(L|K)$  el generador del grup de Galois determinat per la permutació  $\sigma(x_1) = x_2, \sigma(x_2) = x_3, \sigma(x_3) = x_1$  de les arrels de  $f(X)$ . A fi de facilitar la notació i els càlculs, considerarem els subíndexs definits en  $\mathbb{Z}/3\mathbb{Z}$ , de manera que serà  $x_0 = x_3, x_4 = x_1, \dots, x_{n+3} = x_n$ , per a tot nombre enter  $n$ .

**5.8.4.** Vegem, primerament, que  $\eta = x_0 + \rho x_1 + \rho^2 x_2$  és un element primitiu de  $L|K$  tal que  $\eta^3 \in K$ .

Per a això, observem que

$$\begin{aligned} \eta &= x_0 + \rho x_1 + \rho^2 x_2, \\ \sigma(\eta) &= \rho^2 x_0 + x_1 + \rho x_2 = \rho^2 \eta, \\ \sigma^2(\eta) &= \rho x_0 + \rho^2 x_1 + x_2 = \rho \eta, \end{aligned}$$

de manera que els tres conjugats de  $\eta$  per  $\text{Gal}(L|K)$  són diferents; és a dir,  $\eta$  és un element de  $L$  de grau 3 sobre  $K$  i, per tant, un element primitiu de l'extensió  $L|K$ .

D'altra banda,  $\sigma(\eta^3) = \sigma(\eta)^3 = \rho^6 \eta^3 = \eta^3$ , de manera que  $\eta^3$  és fix per  $\sigma$  i, en conseqüència,  $\theta := \eta^3 \in L^{(\sigma)} = K$ . Notem que  $\eta, \sigma(\eta), \sigma^2(\eta)$  són les tres arrels cúbiques de  $\theta \in K$ .

Anàlogament,  $\eta' := x_0 + \rho^2 x_1 + \rho x_2$  també és un element primitiu de  $L|K$  tal que  $\eta'^3 \in K$ , ja que

$$\begin{aligned}\eta' &= x_0 + \rho^2 x_1 + \rho x_2, \\ \sigma(\eta') &= \rho x_0 + x_1 + \rho^2 x_2 = \rho \eta', \\ \sigma^2(\eta') &= \rho^2 x_0 + \rho x_1 + x_2 = \rho^2 \eta',\end{aligned}$$

i  $\theta' := \eta'^3 \in L^{(\sigma)} = K$ . Igual que abans,  $\eta'$ ,  $\sigma(\eta')$ ,  $\sigma^2(\eta')$  són les tres arrels cúbiques de  $\theta' \in K$ .

**5.8.5.** Ara, notem que el sistema lineal

$$\begin{aligned}x_0 + x_1 + x_2 &= -\frac{b}{a}, \\ x_0 + \rho x_1 + \rho^2 x_2 &= \eta, \\ x_0 + \rho^2 x_1 + \rho x_2 &= \eta',\end{aligned}$$

té la solució única donada per

$$\begin{aligned}x_0 &= \frac{1}{3} \left( -\frac{b}{a} + \eta + \eta' \right), \\ x_1 &= \frac{1}{3} \left( -\frac{b}{a} + \rho^2 \eta + \rho \eta' \right), \\ x_2 &= \frac{1}{3} \left( -\frac{b}{a} + \rho \eta + \rho^2 \eta' \right),\end{aligned}$$

de manera que disposar d'expressions per radicals de  $x_0$ ,  $x_1$ ,  $x_2$  a partir de  $a$ ,  $b$ ,  $c$  i  $d$  equival a disposar-ne de  $\eta$ ,  $\eta'$  i  $\rho$ ; i, com que  $\rho^2 + \rho + 1 = 0$ ,  $\eta^3 = \theta$  i  $\eta'^3 = \theta'$ , a disposar-ne de  $\theta$  i  $\theta'$ .

**5.8.6.** Es tracta, doncs, d'expressar  $\theta$  i  $\theta'$  per radicals a partir de  $a$ ,  $b$ ,  $c$  i  $d$ . Notem que, si  $\tau \in \text{Gal}(L|k)$  és l'automorfisme determinat per la permutació

$$\tau(x_0) = x_0, \quad \tau(x_1) = x_2, \quad \tau(x_2) = x_1,$$

llavors és  $\eta' = \tau(\eta)$ , de manera que  $\theta' = \tau(\theta)$ . Com a conseqüència, si tenim en compte que  $\tau$  és d'ordre 2, obtenim que els dos elements  $\theta + \theta'$ ,  $\theta\theta'$  són fixos per  $\tau$ , de manera que pertanyen a  $L^{(\tau)} \cap K = k$ . Per tant,  $\theta$  i  $\theta'$  són les dues arrels d'una equació quadràtica sobre  $k$ .

El càlcul explícit proporciona les expressions

$$\begin{aligned}\eta^3 &= x_0^3 + x_1^3 + x_2^3 + 6x_0x_1x_2 \\ &\quad + 3\rho(x_0^2x_1 + x_1^2x_2 + x_2^2x_0) + 3\rho^2(x_0^2x_2 + x_1^2x_0 + x_2^2x_1), \\ \eta'^3 &= x_0^3 + x_1^3 + x_2^3 + 6x_0x_1x_2 \\ &\quad + 3\rho^2(x_0^2x_1 + x_1^2x_2 + x_2^2x_0) + 3\rho(x_0^2x_2 + x_1^2x_0 + x_2^2x_1),\end{aligned}$$

i, en tenir en compte que  $\rho^2 + \rho + 1 = 0$ , les expressions

$$\begin{aligned}\theta + \theta' &= 2(x_0^3 + x_1^3 + x_2^3) + 12x_0x_1x_2 \\ &\quad - 3(x_0^2x_1 + x_1^2x_2 + x_2^2x_0 + x_0^2x_2 + x_1^2x_0 + x_2^2x_1), \\ \theta\theta' &= (x_0^2 + x_1^2 + x_2^2 - x_0x_1 - x_1x_2 - x_2x_0)^3, \\ \eta\eta' &= x_0^2 + x_1^2 + x_2^2 - x_0x_1 - x_1x_2 - x_2x_0.\end{aligned}$$



Aquestes expressions són polinomis simètrics en  $x_0, x_1, x_2$ , i l'aplicació del mètode de Waring produeix les fórmules

$$\begin{aligned}\theta + \theta' &= 2(x_0 + x_1 + x_2)^3 + 27x_0x_1x_2 \\ &\quad - 9(x_0x_1 + x_1x_2 + x_2x_0)(x_0 + x_1 + x_2) \\ &= -2\frac{b^3}{a^3} + 9\frac{bc}{a^2} - 27\frac{d}{a} = -27q, \\ \eta\eta' &= (x_0 + x_1 + x_2)^2 - 3(x_0x_1 + x_1x_2 + x_2x_0) \\ &= \frac{b^2}{a^2} - 3\frac{c}{a} = -3p, \\ \theta\theta' &= \left(\frac{b^2}{a^2} - 3\frac{c}{a}\right)^3 = -27p^3,\end{aligned}$$

on hem posat (cf. la proposició **0.4.1**)

$$p := \frac{c}{a} - \frac{b^2}{3a^2}, \quad q := \frac{d}{a} + \frac{2b^3}{27a^3} - \frac{bc}{3a^2}.$$

Per tant,  $\theta, \theta'$  són les dues solucions de l'equació quadràtica

$$X^2 + 27qX - 27p^3,$$

de discriminant

$$\Delta_2 = 27^2q^2 + 4 \cdot 27p^3 = -27\Delta,$$

on  $\Delta := -4p^3 - 27q^2$ , de manera que, si posem  $\alpha^2 = \Delta$  i  $\beta^2 = -3$ , és

$$\{\theta, \theta'\} = \left\{ \frac{-27q + 3\alpha\beta}{2}, \frac{-27q - 3\alpha\beta}{2} \right\}.$$

Finalment, si tenim en compte que  $\eta\eta' = -3p$ , obtindrem les expressions per radicals de les arrels  $x_0, x_1, x_2$  del polinomi general de grau 3 a partir d'aquestes expressions per radicals de  $\theta, \theta'$ . És a dir, obtindrem el teorema següent.

**Teorema 5.8.7.** *Donat el polinomi general de grau 3,*

$$a(X - x_0)(X - x_1)(X - x_2) = aX^3 + bX^2 + cX + d \in \mathbb{Z}[a, x_0, x_1, x_2][X],$$

posem

$$p := \frac{c}{a} - \frac{b^2}{3a^2}, \quad q := \frac{d}{a} + \frac{2b^3}{27a^3} - \frac{bc}{3a^2}, \quad \Delta := -4p^3 - 27q^2 \in \mathbb{Q}(a, b, c, d),$$

i siguin  $\alpha, \beta, \rho, \theta, \eta$  i  $\eta'$  elements tals que

$$\alpha^2 = \Delta, \quad \beta^2 = -3, \quad \rho = \frac{-1 + \beta}{2}, \quad \theta = \frac{-27q + 3\alpha\beta}{2}, \quad \eta^3 = \theta, \quad \eta' = -\frac{3p}{\eta},$$

en un cos algebraicament tancat que contingui  $\mathbb{Q}(a, x_0, x_1, x_2)$ . Llavors,

$$\frac{1}{3} \left( -\frac{b}{a} + \eta + \eta' \right), \quad \frac{1}{3} \left( -\frac{b}{a} + \rho^2\eta + \rho\eta' \right), \quad \frac{1}{3} \left( -\frac{b}{a} + \rho\eta + \rho^2\eta' \right)$$

són expressions per radicals de les arrels  $x_0, x_1, x_2$  de  $f(X)$ .  $\square$

L'expressió per radicals de les solucions de qualsevol equació de grau 3 sobre un cos de característica diferent de 2 i de 3 s'obtenen immediatament a partir d'aquest teorema (cf. la proposició **0.4.1**).

## 5.9 Les equacions de grau 4

En aquesta secció es tracta d'explicar la resolució per radicals de les equacions de grau 4; comencem per l'equació general.

**5.9.1.** Considerem l'equació general de grau 4,  $f(X) = 0$ , on

$$\begin{aligned} f(X) &= a(X - x_0)(X - x_1)(X - x_2)(X - x_3) \\ &= aX^4 + bX^3 + cX^2 + dX + e \\ &\in \mathbb{Z}[a, x_0, x_1, x_2, x_3][X] \subseteq \mathbb{Q}(a, x_0, x_1, x_2, x_3)[X], \end{aligned}$$

i en la qual els coeficients són  $a$ , i

$$\begin{aligned} b &:= -a(x_0 + x_1 + x_2 + x_3), \\ c &:= a(x_0x_1 + x_0x_2 + x_0x_3 + x_1x_2 + x_1x_3 + x_2x_3), \\ d &:= -a(x_0x_1x_2 + x_0x_1x_3 + x_0x_2x_3 + x_1x_2x_3), \\ e &:= ax_0x_1x_2x_3. \end{aligned}$$

Com que el grup de Galois de l'extensió  $\mathbb{Q}(a, x_0, x_1, x_2, x_3) | \mathbb{Q}(a, b, c, d, e)$  és isomorf al grup simètric  $S_4$ , que és resoluble, l'equació  $f(X) = 0$  és resoluble per radicals. Es tracta de donar una fórmula per a expressar les arrels de  $f(X)$  per radicals, a partir dels coeficients. Posem  $L := \mathbb{Q}(a, x_0, x_1, x_2, x_3)$  i  $k := \mathbb{Q}(a, b, c, d, e)$ .

Notem que considerem  $S_4$  com el grup de permutacions de  $\{x_0, x_1, x_2, x_3\}$ , de manera que serà útil pensar en les permutacions de  $\{0, 1, 2, 3\}$ . Comencem per donar una resolució de  $S_4$ .

**Proposició 5.9.2.** *Siguin  $S_4$  el grup simètric,  $A_4 \subseteq S_4$  el grup alternat,  $V_4 \subseteq A_4$  el grup de Klein,  $V_4 := \{1, (0, 1)(2, 3), (0, 2)(1, 3), (0, 3)(1, 2)\}$ , i  $C := \{1, (0, 1)(2, 3)\}$ . La cadena de subgrups  $S_4 \supseteq A_4 \supseteq V_4 \supseteq C \supseteq \{1\}$  és una resolució del grup simètric  $S_4$ , de quocients cíclics d'ordres primers.*

**DEMOSTRACIÓ:** El morfisme signe,  $S_4 \xrightarrow{\text{sig}} \{\pm 1\}$ , que assigna a cada permutació el seu signe, és exhaustiu; i, per definició de  $A_4$ , el seu nucli és  $A_4$ ; per tant,  $A_4$  és un subgrup normal de  $S_4$  i el quocient és isomorf a  $\{\pm 1\}$ , que és un grup cíclic d'ordre 2.

D'altra banda,  $V_4$  és el grup derivat de  $A_4$ , de manera que és un subgrup normal de  $A_4$ ; com que és d'ordre 4, i  $A_4$  és d'ordre 12, el quocient  $A_4/V_4$  és un grup cíclic d'ordre 3. De fet,  $V_4$  és un subgrup normal de  $S_4$  i el quocient  $S_4/V_4 \cong S_3$ ; i, amb aquesta identificació, és  $A_4/V_4 \cong A_3$ .

Finalment, és clar que  $C$  és un subgrup normal de  $V_4$ , que és cíclic d'ordre 2, i que el quocient  $V_4/C$  també és cíclic d'ordre 2. Això acaba la prova.  $\square$

**Observació 5.9.3.** En lloc de  $C$ , podríem haver considerat qualsevol dels altres dos subgrups de  $V_4$  d'ordre 2; per qüestions de notació, escriurem  $C_1 := C := \{1, (0, 1)(2, 3)\}$ ,  $C_2 := \{1, (0, 2)(1, 3)\}$ ,  $C_3 := \{1, (0, 3)(1, 2)\}$ .

Per a la resolució de l'equació  $f(X) = 0$ , serà útil considerar la part del reticle de subcossos de  $L$  donat per la correspondència de Galois entre subextensions de  $L|k$  i els subgrups de  $S_4$  que correspon als subgrups de la resolució de  $S_4$ . I també serà útil considerar un resolvent cúbic de  $f(X)$ .

**Definició 5.9.4.** Amb les notacions anteriors, posem

$$y_1 := x_0x_1 + x_2x_3, \quad y_2 := x_0x_2 + x_1x_3, \quad y_3 := x_0x_3 + x_1x_2,$$

i sigui  $g(X) := a^3(X - y_1)(X - y_2)(X - y_3) \in L[X]$ . El polinomi  $g(X)$  s'anomena un *resolvent cúbic* de  $f(X)$ .

**Lema 5.9.5.** *Se satisfan les propietats següents.*

- (a)  $g(X) = a^3X^3 - a^2cX^2 + (abd - 4a^2e)X - (ad^2 + b^2e - 4ace) \in k[X]$ .
- (b)  $\Delta_g = a^6\Delta_f$ , on  $\Delta_f$ ,  $\Delta_g$  denoten, respectivament, els discriminants dels polinomis  $f(X)$ ,  $g(X)$ .

**DEMOSTRACIÓ:** Si pensem  $g(X)$ , com a polinomi en les indeterminades  $x_0, x_1, x_2, x_3$  i de coeficients en l'anell  $\mathbb{Q}(a)[X]$ , resulta que és un polinomi simètric; l'expressió de (a) s'obté en aplicar el mètode de Waring per a expressar els coeficients en funció dels polinomis simètrics elementals en les indeterminades  $x_0, x_1, x_2, x_3$ . I, anàlogament, es fa el mateix per als discriminants.  $\square$

També podem escriure elements primitius per als subcossos de  $L$  fixos pels subgrups  $C_i \subseteq V_4 \subseteq A_4 \subseteq S_4$ .

**Definició 5.9.6.** Posem  $K := L^{V_4}$ , i  $K_i := L^{C_i}$ , per a  $1 \leq i \leq 3$ , els cossos fixos pels subgrups  $V_4$ ,  $C_1$ ,  $C_2$ , i  $C_3$ , respectivament.

**Proposició 5.9.7.** *Se satisfan les propietats següents.*

- (a)  $K = k(y_1, y_2, y_3)$ , el cos de descomposició del polinomi  $g(X)$  sobre  $k$ .
- (b) Posem  $\{0, 1, 2, 3\} = \{0, i, j, k\}$ , com a conjunts. Llavors, se satisfan les igualtats  $K_i = K(x_0 + x_i) = K(x_0x_i) = K(x_j + x_k) = K(x_jx_k)$ .
- (c)  $L = K(x_0) = K(x_1) = K(x_2) = K(x_3)$ .
- (d) El polinomi  $f(X)$  és irreductible en  $K[X]$ .

**DEMOSTRACIÓ:** (a) Sigui  $\sigma \in V_4$ ; llavors,  $\sigma(y_i) = y_i$ , per a  $1 \leq i \leq 3$ . I recíprocament, si  $\sigma \in S_4$ , però  $\sigma \notin V_4$ , llavors existeix  $i$ ,  $1 \leq i \leq 3$ , tal que  $\sigma(y_i) \neq y_i$ . Per tant, el subgrup de  $S_4$  que deixa fixos  $y_1, y_2, y_3$  és exactament  $V_4$ ; és a dir,  $\text{Gal}(L|k(y_1, y_2, y_3)) = V_4$ , d'on  $L^{V_4} = k(y_1, y_2, y_3)$ , com volíem veure.

(b) Anàlogament, la identitat i  $(0, i)(j, k)$  són els únics elements de  $V_4$  que deixen fixos els elements  $x_0 + x_i$ ,  $x_0x_i$ ,  $x_j + x_k$ ,  $x_jx_k$ ; com que  $\text{Gal}(L|K) = V_4$ , obtenim que  $L^{C_i} = K(x_0 + x_i) = K(x_0x_i) = K(x_j + x_k) = K(x_jx_k)$ .

(c) De la mateixa manera, cap element de  $V_4$  diferent de la identitat no deixa fixos cap dels elements  $x_0, x_1, x_2$ , ni  $x_3$ ; per tant, cap d'aquests elements no està en cap subextensió pròpia de  $L|K$ ; és a dir,  $L = K(x_i)$ , per a  $0 \leq i \leq 3$ .

(d) Finalment, com que  $[L : K] = \#\text{Gal}(L|K) = \#V_4 = 4$ , i com que  $x_0$  és un element primitiu, resulta que  $\text{Irr}(x_0, K)(X) \in K[X]$  és un polinomi de grau 4 que divideix  $f(X) \in k[X] \subseteq K[X]$ ; i com que  $f(X)$  és de grau 4,  $f(X)$  és irreductible en  $K[X]$ .  $\square$

**5.9.8.** La pregunta que ens hem formulat és: com podem resoldre per radicals l'equació  $f(X) = 0$ ? La proposició anterior ens ensenya, en particular, que el polinomi  $f(X)$  encara és irreductible com a polinomi de  $K[X]$ , i que  $K$  és el cos de descomposició sobre  $k$  del polinomi  $g(X)$ ; i, com que el polinomi  $g(X)$  és de grau 3, ja el sabem resoldre per radicals. Per tant, el problema és resoldre per radicals el polinomi  $f(X)$  sobre el cos  $K$ ; és a dir, recuperar  $x_0, x_1, x_2, x_3$  a partir de  $y_1 = x_0x_1 + x_2x_3$ ,  $y_2 = x_0x_2 + x_1x_3$ ,  $y_3 = x_0x_3 + x_1x_2$ , i fer-ho per radicals.

Considerem, doncs, una de les arrels del polinomi  $g(X)$ , expressada per radicals a partir dels seus coeficients; això és, considerem una arrel de  $g(X)$  expressada per radicals a partir de  $a, b, c, d, e$ . Sigui  $y_1$  aquesta arrel. Com que  $x_0$  (i anàlogament  $x_1, x_2, x_3$ ) és un element primitiu de l'extensió  $L|K_1$ , el polinomi irreductible de  $x_0$  sobre  $K_1$  és  $(X - x_0)(X - \sigma(x_0))$ , on  $\sigma \in C_1$ ,  $\sigma \neq 1$ ; per tant,

$$\text{Irr}(x_0, K_1)(X) = (X - x_0)(X - x_1) = X^2 - (x_0 + x_1)X + x_0x_1;$$

i, anàlogament,

$$\text{Irr}(x_2, K_1)(X) = (X - x_2)(X - x_3) = X^2 - (x_2 + x_3)X + x_2x_3.$$

Per tant,  $x_0, x_1, x_2, x_3$  es poden expressar per radicals a partir dels coeficients d'aquests dos polinomis; així, cal expressar per radicals els elements

$$x_0 + x_1, \quad x_2 + x_3, \quad x_0x_1, \quad x_2x_3.$$

Cadascun d'aquests elements és un element primitiu de l'extensió  $K_1|K$ , de manera que satisfà una equació de grau 2 sobre  $K$ ; més concretament, com que hi ha un isomorfisme  $\text{Gal}(K_1|K) = \text{Gal}(L|K)/\text{Gal}(L|K_1) \cong \{1, (0, 2)(1, 3)\}$ , obtenim que

$$\begin{aligned} \text{Irr}(x_0 + x_1, K)(X) &= (X - (x_0 + x_1))(X - (x_2 + x_3)) \\ &= X^2 - (x_0 + x_1 + x_2 + x_3)X + (x_0 + x_1)(x_2 + x_3) \\ &= X^2 + \frac{b}{a}X + \frac{c}{a} - y_1, \\ \text{Irr}(x_0x_1, K)(X) &= (X - x_0x_1)(X - x_2x_3) = \\ &= X^2 - (x_0x_1 + x_2x_3)X + x_0x_1x_2x_3 = \\ &= X^2 - y_1X + \frac{e}{a}. \end{aligned}$$

Per tant,  $x_0 + x_1, x_2 + x_3, x_0x_1, x_2x_3$  s'expressen per radicals a partir dels coeficients dels polinomis  $X^2 + \frac{b}{a}X + \frac{c}{a} - y_1$  i  $X^2 - y_1X + \frac{e}{a}$ ; és a dir, per radicals a partir de  $a, b, c, d, e$ , ja que  $y_1$  s'expressa per radicals a partir de  $a, b, c, d, e$ .

Els discriminants d'aquests polinomis de grau 2 són quadrats d'elements primitius de l'extensió  $K_1|K$ ; per tant, un d'ells s'obté de l'altre en multiplicar pel quadrat d'un element de  $K$ ; més concretament, el càlcul del seu producte es pot fer explícitament i, en tenir en compte que  $y_1$  és arrel de  $g(X)$ , proporciona la igualtat

$$\begin{aligned} \left(\frac{b^2}{a^2} - 4\frac{c}{a} + 4y_1\right) \left(y_1^2 - 4\frac{e}{a}\right) &= \frac{1}{a^3} \left(4g(y_1) + ab^2y_1^2 + 4ad^2 - 4abdy_1\right) \\ &= \left(\frac{by_1 - 2d}{a}\right)^2. \end{aligned}$$

Així, si  $\alpha$  és tal que  $\alpha^2 = y_1^2 - 4\frac{e}{a}$ , llavors  $\frac{b^2}{a^2} - 4\frac{c}{a} + 4y_1 = \left(\frac{by_1 - 2d}{a\alpha}\right)^2$ . Per tant, els conjunts de les arrels dels dos polinomis  $X^2 - y_1X + \frac{e}{a} = 0$  i  $X^2 + \frac{b}{a}X + \frac{c}{a} - y_1 = 0$  són

$$\begin{aligned}\{x_0x_1, x_2x_3\} &= \left\{ \frac{y_1 + \alpha}{2}, \frac{y_1 - \alpha}{2} \right\}, \\ \{x_0 + x_1, x_2 + x_3\} &= \left\{ \frac{-b\alpha + by_1 - 2d}{2a\alpha}, \frac{-b\alpha - by_1 + 2d}{2a\alpha} \right\}.\end{aligned}$$

Si posem  $x_0x_1 = \frac{y_1 + \alpha}{2}$ , llavors és  $x_2x_3 = \frac{y_1 - \alpha}{2}$ ; però: quin dels dos elements  $\frac{-b\alpha + by_1 - 2d}{2a\alpha}$ ,  $\frac{-b\alpha - by_1 + 2d}{2a\alpha}$  és, llavors,  $x_0 + x_1$ ? Com que

$$\begin{aligned}a(X^2 - (x_0 + x_1)X + x_0x_1)(X^2 - (x_2 + x_3)X + x_2x_3) = \\ a(X - x_0)(X - x_1)(X - x_2)(X - x_3) = f(X),\end{aligned}$$

hauria de ser

$$a\left(X^2 - (x_0 + x_1)X + \frac{y_1 + \alpha}{2}\right)\left(X^2 - (x_2 + x_3)X + \frac{y_1 - \alpha}{2}\right) = f(X).$$

Si poséssim  $\frac{-b\alpha + by_1 - 2d}{2a\alpha}$  en lloc de  $x_0 + x_1$ , tindríem que

$$x_2 + x_3 = \frac{-b\alpha - by_1 + 2d}{2a\alpha};$$

però, fent els càlculs, resulta que

$$\begin{aligned}a\left(X^2 - \frac{-b\alpha + by_1 - 2d}{2a\alpha}X + \frac{y_1 + \alpha}{2}\right)\left(X^2 - \frac{-b\alpha - by_1 + 2d}{2a\alpha}X + \frac{y_1 - \alpha}{2}\right) \\ = aX^4 + bX^3 + cX^2 + (by_1 - d)X + e,\end{aligned}$$

que no és el polinomi  $f(X)$ . Per tant, ha de ser  $x_0 + x_1 = \frac{-b\alpha - by_1 + 2d}{2a\alpha}$ , i, en conseqüència,  $x_2 + x_3 = \frac{-b\alpha + by_1 - 2d}{2a\alpha}$ .

Això ens diu que  $x_0x_1 = \frac{y_1 + \alpha}{2}$  i  $x_0 + x_1 = \frac{-b\alpha - by_1 + 2d}{2a\alpha}$ ; per tant,  $x_0, x_1$  són les arrels de  $X^2 - \frac{-b\alpha - by_1 + 2d}{2a\alpha}X + \frac{y_1 + \alpha}{2}$ ; i, anàlogament,  $x_2, x_3$  són les arrels de  $X^2 - \frac{-b\alpha + by_1 - 2d}{2a\alpha}X + \frac{y_1 - \alpha}{2}$ .

Dit d'una altra manera, si  $\beta$  i  $\gamma$  són tals que

$$\beta^2 = \left(\frac{-b\alpha - by_1 + 2d}{2a\alpha}\right)^2 - 4\frac{y_1 + \alpha}{2}, \quad \gamma^2 = \left(\frac{-b\alpha + by_1 - 2d}{2a\alpha}\right)^2 - 4\frac{y_1 - \alpha}{2},$$

és a dir,  $\beta^2$  i  $\gamma^2$  són els discriminants dels polinomis

$$X^2 - \frac{-b\alpha - by_1 + 2d}{2a\alpha}X + \frac{y_1 + \alpha}{2}, \quad X^2 - \frac{-b\alpha + by_1 - 2d}{2a\alpha}X + \frac{y_1 - \alpha}{2},$$

respectivament, obtenim, finalment, que les arrels de  $f(X)$  s'expressen per radicals a partir de  $a, b, c, d, e$ , de la manera següent:

$$\begin{aligned} \{x_0, x_1\} &= \left\{ \frac{-b\alpha - by_1 + 2d + 2a\alpha\beta}{4a\alpha}, \frac{-b\alpha - by_1 + 2d - 2a\alpha\beta}{4a\alpha} \right\}, \\ \{x_2, x_3\} &= \left\{ \frac{-b\alpha + by_1 - 2d + 2a\alpha\gamma}{4a\alpha}, \frac{-b\alpha + by_1 - 2d - 2a\alpha\gamma}{4a\alpha} \right\}. \end{aligned}$$

En resum, hem provat el resultat següent.

**Teorema 5.9.9.** *Siguin  $y_1$  una arrel del resolvent cúbic  $g(X)$ , que podem suposar expressada per radicals a partir de  $a, b, c, d, e$ , i  $\alpha, \beta, \gamma$  tals que*

$$\begin{aligned} \alpha^2 &= y_1^2 - 4\frac{e}{a}, \\ \beta^2 &= \left( \frac{-b\alpha - by_1 + 2d}{2a\alpha} \right)^2 - 4\frac{y_1 + \alpha}{2}, \\ \gamma^2 &= \left( \frac{-b\alpha + by_1 - 2d}{2a\alpha} \right)^2 - 4\frac{y_1 - \alpha}{2}. \end{aligned}$$

Llavors, les arrels  $x_0, x_1, x_2, x_3$  del polinomi general  $aX^4 + bX^3 + cX^2 + dX + e$  són

$$\begin{aligned} &\frac{-b\alpha - by_1 + 2d + 2a\alpha\beta}{4a\alpha}, \quad \frac{-b\alpha - by_1 + 2d - 2a\alpha\beta}{4a\alpha}, \\ &\frac{-b\alpha + by_1 - 2d + 2a\alpha\gamma}{4a\alpha}, \quad \frac{-b\alpha + by_1 - 2d - 2a\alpha\gamma}{4a\alpha}. \quad \square \end{aligned}$$

**Corollari 5.9.10.** *Siguin  $k$  un cos qualsevol de característica diferent de 2 i de 3, considerem un polinomi  $f(X) := aX^4 + bX^3 + cX^2 + dX + e \in k[X]$ , amb  $a, b, c, d, e \in k$ ,  $a \neq 0$ , i posem*

$$g(X) = a^3X^3 - a^2cX^2 + (abd - 4a^2e)X - (ad^2 + b^2e - 4ace) \in k[X].$$

*Si existeix alguna arrel  $y_1$  de  $g(X)$  tal que  $y_1^2 \neq 4\frac{e}{a}$ , siguin  $\alpha, \beta, \gamma$  tals que*

$$\begin{aligned} \alpha^2 = y_1^2 - 4\frac{e}{a} \neq 0, \quad \beta^2 &= \left( \frac{-b\alpha - by_1 + 2d}{2a\alpha} \right)^2 - 4\frac{y_1 + \alpha}{2}, \\ \gamma^2 &= \left( \frac{-b\alpha + by_1 - 2d}{2a\alpha} \right)^2 - 4\frac{y_1 - \alpha}{2}. \end{aligned}$$

Llavors, les arrels del polinomi  $f(X)$  són

$$\begin{aligned} &\frac{-b\alpha - by_1 + 2d + 2a\alpha\beta}{4a\alpha}, \quad \frac{-b\alpha - by_1 + 2d - 2a\alpha\beta}{4a\alpha}, \\ &\frac{-b\alpha + by_1 - 2d + 2a\alpha\gamma}{4a\alpha}, \quad \frac{-b\alpha + by_1 - 2d - 2a\alpha\gamma}{4a\alpha}. \end{aligned}$$

*En el cas que les tres arrels de  $g(X)$  satisfacin  $y_1^2 = 4\frac{e}{a}$ , siguin  $\delta, \varepsilon, \eta$  tals que*

$$\delta^2 = b^2 - 4ac + 4a^2y_1, \quad \varepsilon^2 = \left( \frac{-b + \delta}{2a} \right)^2 - 2y_1, \quad \eta^2 = \left( \frac{-b - \delta}{2a} \right)^2 - 2y_1.$$

Llavors, les arrels de  $f(X)$  són

$$\frac{-b + \delta + 2a\varepsilon}{4a}, \quad \frac{-b + \delta - 2a\varepsilon}{4a}, \quad \frac{-b - \delta + 2a\eta}{4a}, \quad \frac{-b - \delta - 2a\eta}{4a},$$

*i els dos polinomis  $f(X)$  i  $g(X)$  tenen arrels múltiples.*

DEMOSTRACIÓ: Siguin  $\alpha_0, \alpha_1, \alpha_2, \alpha_3$  les arrels de  $f(X)$  i considerem l'únic morfisme d'anells  $\mathbb{Z}[a, x_0, x_1, x_2, x_3] \rightarrow k(\alpha_0, \alpha_1, \alpha_2, \alpha_3)$  que envia la indeterminada  $a$  a l'element  $a \in k$ , i les indeterminades  $x_i$  als elements  $\alpha_i$ . Els coeficients del polinomi  $f(X)$  són els polinomis simètrics elementals, multiplicats per  $a$ , dels  $\alpha_0, \alpha_1, \alpha_2, \alpha_3$ ; per tant, si alguna de les arrels  $y_1$  del polinomi  $g(X)$  satisfà la condició  $y_1^2 \neq 4\frac{e}{a}$ , podem aplicar el teorema anterior en la imatge del morfisme, de manera que el polinomi  $f(X)$  té les arrels descrites en l'enunciat.

Suposem, contràriament, que totes les arrels  $y_1$  de  $g(X)$  satisfan la condició  $y_1^2 = 4\frac{e}{a}$ ; com que també satisfan  $g(y_1) = 0$ , totes satisfan també la igualtat  $abdy_1 = ad^2 + b^2e$ ; per tant,  $(by_1 - 2d)^2 = b^2y_1^2 - 4bdy_1 + 4d^2 = 0$ , d'on  $by_1 = 2d$ . Si, ara, calculem els polinomis simètrics elementals en les expressions donades en l'enunciat, i les multipliquem per  $a$ , obtindrem que les expressions de l'enunciat són expressions radicals de les arrels de  $f(X)$ , com volem demostrar. La justificació del fet que  $f(X)$  i  $g(X)$  tenen arrels múltiples és senzilla, perquè les tres arrels de  $g(X)$  són arrels del polinomi  $aX^2 - 4e$ , que és de grau 2 i, per tant,  $g(X)$  té alguna arrel múltiple. En particular, el discriminant de  $g(X)$  i el de  $f(X)$  són zero.  $\square$

## 5.10 Construccions amb regla i compàs

Sovint se sent a parlar de, o se sent anomenar, algun dels tres problemes clàssics següents.

**5.10.1. La duplicació del cub.** Donat un cub, construir un cub de volum doble.

**5.10.2. La trisecció de l'angle.** Donat un angle, construir l'angle d'obertura la tercera part del donat.

**5.10.3. La quadratura del cercle.** Donat un cercle, construir un quadrat d'àrea igual a la del cercle.

Perquè aquests problemes puguin ésser considerats ben formulats des del punt de vista matemàtic, cal dir què s'entén per construir, i cal tenir conceptes adequats per a poder mesurar angles, àrees i volums. I, encara, si tenim en compte que, per als clàssics, construir volia dir construir amb regla i compàs, encara cal precisar què vol dir "construir amb regla i compàs".

**5.10.4.** Considerem el model euclidià del pla, donat pel cos  $\mathbb{C}$  dels nombres complexos. Així, un punt del pla s'identifica, en un sistema de coordenades cartesianes, amb una parella ordenada de nombres reals,  $(x, y)$ , i, aquesta parella, amb el nombre complex  $x + iy$ . En particular, en el pla euclidià disposem dels conceptes habituals de mesura per a angles i superfícies. El problema que ens plantegem, en aquest model, és: donat un conjunt de punts del pla, quins altres punts es poden construir a partir d'aquests només amb l'ús d'un regla (sense distàncies marcades en ell) i un compàs?

Cal definir acuradament què entendrem per construir un punt amb regla i compàs a partir d'uns quants punts donats; és a dir, què entendrem per *usar el regla* i què per *usar el compàs*.

(a) *Usar el regla.* Donats dos punts diferents, usar el regla a partir d'aquests punts vol dir dibuixar qualsevol *segment rectilini* de longitud finita que contingui els dos punts. Notem

que si identifiquem els punts amb les parelles  $(x_0, y_0)$ ,  $(x_1, y_1)$ , diferents, entenem que els punts de la recta que els conté són els punts de la forma  $(\lambda x_1 + (1 - \lambda)x_0, \lambda y_1 + (1 - \lambda)y_0)$ , per a  $\lambda \in \mathbb{R}$ ; per tant, *usar el regle* vol dir considerar els punts d'aquesta forma, amb  $\lambda$  en un interval tancat qualsevol que contingui l'interval  $[0, 1]$ .

(b) *Usar el compàs*. Donats tres punts, dos d'ells, com a mínim, diferents, usar el compàs a partir d'aquests punts vol dir dibuixar una *circumferència*, o un *arc de circumferència*, de centre en un d'ells i radi la distància entre dos diferents dels tres punts. Notem que si identifiquem els tres punts amb les parelles  $(x_0, y_0)$ ,  $(x_1, y_1)$ ,  $(x_2, y_2)$ , on  $(x_2, y_2) \neq (x_1, y_1)$ , entenem que els punts de la *circumferència* de centre en  $(x_0, y_0)$  i radi la distància  $r$  entre els altres dos, de manera que  $r^2 = (x_2 - x_1)^2 + (y_2 - y_1)^2$ , són els punts  $(x, y)$  per als quals se satisfà la igualtat  $(x - x_0)^2 + (y - y_0)^2 = r^2$ ; per tant, *usar el compàs* vol dir considerar els punts  $(x, y)$  d'aquesta forma.

Amb aquestes definicions sobre què és, en el nostre model, usar el regle i què és usar el compàs, podem dir què entenem per construir (formalment) un nou punt o, per a ser més precisos, quins són els punts construïbles amb regle i compàs a partir de punts ja construïts. Notem que per a usar el regle o per a usar el compàs necessitem un mínim de dos punts diferents. Això fa raonable suposar que el conjunt  $C_0$  de la definició següent sigui de cardinal com a mínim 2.

**Definició 5.10.5.** Sigui  $C_0 \subseteq \mathbb{C}$  un conjunt qualsevol de punts del pla, amb l'única restricció que sigui de cardinal  $\#C_0 \geq 2$ . Per a tot nombre natural  $n \geq 0$ , definim inductivament el conjunt  $C_{n+1}$  a partir de  $C_n$ , i l'anomenem el *conjunt dels punts que es construeixen amb regle i compàs en un pas* a partir de  $C_n$ , com el conjunt format pels punts que són:

- (a) els punts de  $C_n$ ;
- (b) el punt intersecció de dos segments rectilinis no paral·lels dibuixats, cadascun d'ells, a partir de dos punts diferents de  $C_n$ ;
- (c) els dos punts intersecció de dues circumferències no tangents dibuixades, cadascuna d'elles, a partir de dos o tres punts diferents de  $C_n$ ; i
- (d) els punts intersecció d'un segment rectilini amb un arc de circumferència dibuixats, cadascun d'ells, a partir de punts diferents de  $C_n$ , i de manera que el segment i l'arc no siguin tangents.

Direm que un punt  $P$  del pla és *construïble amb regle i compàs* a partir d'un conjunt  $C_0$  si existeix  $n \in \mathbb{N}$  tal que  $P \in C_n$ ; és a dir, el conjunt de punts construïbles amb regle i compàs a partir de  $C_0$  és  $\bigcup_{n \in \mathbb{N}} C_n$ .

**Observació 5.10.6.** En aquesta definició s'utilitza el concepte de segments no paral·lels en el sentit habitual de la geometria euclidiana plana; és a dir, dues rectes del pla són paral·leles si coincideixen o bé si no es tallen. Anàlogament, una recta i una circumferència en el pla, o bé dues circumferències en el pla, si es tallen, ho fan en dos punts diferents (i això equival a dir que no són tangents) o bé en un sol punt (i això equival a dir que són tangents).



**Exercici 5.10.7.** A partir de punts i de segments ja construïts, és possible, amb regla i compàs: (a) doblar un segment donat; (b) bisecar un segment donat; (c) construir un segment perpendicular a un segment donat per un punt donat del segment; (d) construir un segment perpendicular a un segment donat per un punt exterior al segment; i (e) construir un segment paral·lel a un segment donat que contingui un punt donat exterior al segment.

**Observació 5.10.8.** Les condicions de no tangència es poden suprimir de les definicions, en el sentit que el punt de tangència es pot construir, potser en més passos, sense usar punts de tangència; així, els punts construïbles usant punts de tangència també ho són sense usar-ne. En efecte, el punt d'intersecció de dues circumferències tangents en un punt és el punt d'intersecció de cadascuna d'elles amb el segment que uneix els dos centres (cf. la figura 5.1); i el punt d'intersecció d'una circumferència i una recta tangent a aquesta és el punt d'intersecció de la circumferència amb la perpendicular a la recta que conté el centre de la circumferència (cf. la figura 5.2).

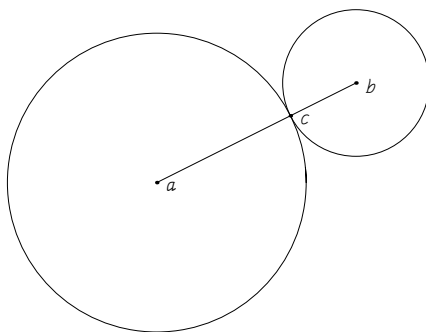


Figura 5.1: Punt de tangència de dues circumferències

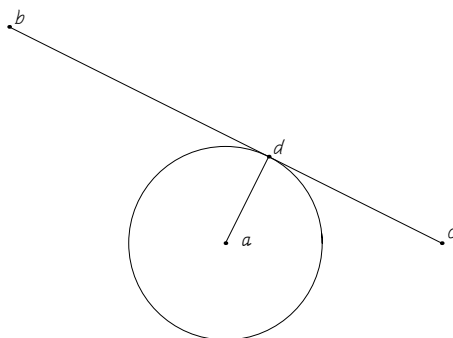


Figura 5.2: Punt de tangència d'una circumferència i un segment

**5.10.9 (Angles).** Podem entendre un *angle* com dos segments que es tallen; per tant, disposar d'un angle equival a disposar de dos punts en una circumferència de centre en el punt d'intersecció dels dos segments i radi la distància entre dos punts construïts qualssevol; per exemple, entre 0 i 1. És a dir, disposar d'un angle equival a disposar de dos punts d'una circumferència de radi 1 i centre en el punt intersecció dels dos segments que el formen.

**Exercici 5.10.10.** A partir d'angles ja construïts, és possible, amb regla i compàs: (a) transportar un angle donat i fer-lo adjacent a un segment donat; (b) bisecar un angle donat; i (c) sumar i restar angles donats.

**Proposició 5.10.11.** *Sigui  $C_0$  un conjunt no buit de punts del pla que contingui, com a mínim, dos punts diferents, i identifiquem dos d'aquests punts amb  $0, 1 \in \mathbb{C}$ . El conjunt  $C$  dels punts del pla construïbles amb regla i compàs a partir de  $C_0$  és un subcòs de  $\mathbb{C}$  que conté  $C_0$  i  $\mathbb{Q}$ , i que és tancat per arrels quadrades; és a dir, tal que si  $a \in C$ , i  $\alpha \in \mathbb{C}$  és tal que  $\alpha^2 = a$ , llavors  $\pm\alpha \in C$ .*

**DEMOSTRACIÓ:** Donats dos punts en el pla, és a dir, dos nombres complexos (que suposem construïts amb regla i compàs a partir de  $C_0$ ), la regla del paral·lelogram ens permet construir la seva suma (exercici); i, donat un punt del pla (que també suposem construït amb regla i compàs a partir de  $C_0$ ), podem construir el seu oposat respecte de l'origen (immediat); per tant, el conjunt dels punts del pla que són construïbles amb regla i compàs a partir de  $C_0$  és tancat per la suma i l'oposat; és a dir, és un subgrup additiu de  $\mathbb{C}$ .

D'altra banda, la possibilitat de construir rectes paral·leles amb regla i compàs, i les propietats dels triangles semblants, ens permeten obtenir el producte de dos nombres reals positius i el quocient d'un nombre real positiu per un altre nombre real positiu no nul (cf. la figura 5.3).

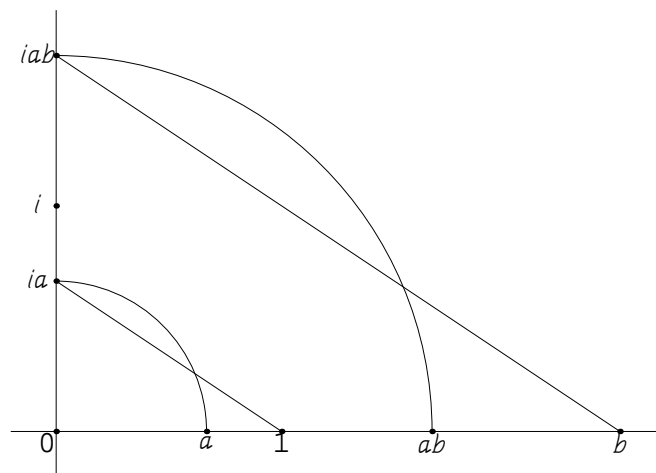


Figura 5.3: Producte de nombres reals positius

En efecte, coneguts 1 i  $a$ , la construcció de la recta paral·lela a la recta determinada per 1 i  $ia$  que conté  $b$  (o que conté  $iab$ ) proporciona  $iab$  (o  $b$ ). Per tant, obtenim el producte  $ab$  o el quocient  $b$  entre  $ab$  i  $a$ .

I, finalment, la possibilitat de sumar i restar angles amb regla i compàs ens permet construir el producte i el quocient de dos nombres complexos qualssevol, el segon dels quals sigui no nul en el cas del quocient. Per a això, només cal tenir present la forma polar dels nombres complexos (exercici). Per tant, el conjunt dels punts del pla construïbles amb regla i compàs a partir de  $C_0$  és tancat per productes i per quocients; és a dir, és un subcòs de  $\mathbb{C}$ .

Aquest cos conté, òbviament,  $\mathbb{Q}$  (ja que és un cos i conté  $0, 1$ ), i també conté  $C_0$  (per hipòtesi); per tant, conté el cos generat sobre  $\mathbb{Q}$  per  $C_0$ .

Només resta demostrar que  $C$  és tancat per arrels quadrades. Com que la bisecció d'angles és possible amb regla i compàs, només cal veure que podem construir les arrels quadrades dels nombres reals positius; i això es pot fer de la manera següent.

Sigui  $d$  el nombre, real i positiu, del qual volem construir la seva arrel quadrada amb regla i compàs. Podem fer la construcció d'una circumferència de diàmetre  $d + 1$  i, a continuació, la d'una perpendicular a un diàmetre sobre un dels dos punts del diàmetre que estan a distància 1 de la circumferència. Llavors, el segment determinat pel peu de la perpendicular i la circumferència té longitud l'arrel quadrada positiva de  $d$  (cf. la figura 5.4).

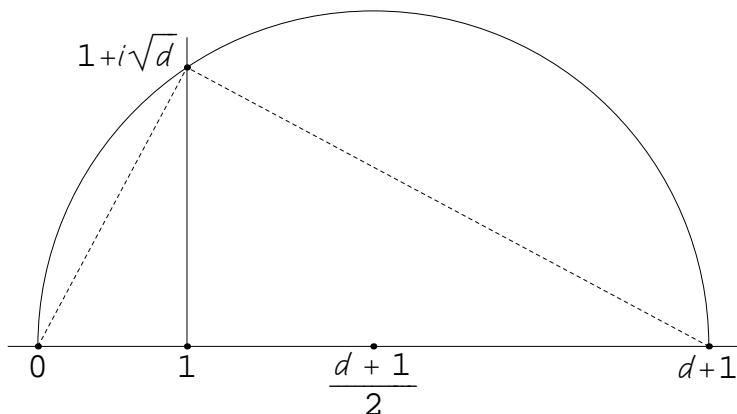


Figura 5.4: Arrel quadrada d'un nombre real positiu

Efectivament, si  $h$  és l'altura d'aquest segment perpendicular, llavors tenim que  $\frac{1}{h} = \frac{h}{d}$ , de manera que  $h = \sqrt{d}$ , com calia veure.  $\square$

**Teorema 5.10.12.** *Sigui  $C_0$  un conjunt no buit de punts del pla que contingui, com a mínim, dos punts diferents. Prenem dos punts diferents de  $C_0$  i identifiquem-los amb  $0, 1 \in \mathbb{C}$ , i sigui  $C := \bigcup_{i \in \mathbb{N}} C_i$  el cos dels nombres construïbles amb regla i compàs a partir de  $C_0$ . Sigui  $k := \mathbb{Q}(C_0) \subseteq \mathbb{C}$  el cos generat sobre  $\mathbb{Q}$  per  $C_0$ . Llavors, si  $\alpha$  és un punt qualsevol de  $C$ , l'extensió  $k(\alpha)|k$  és de grau una potència de 2; a més a més, l'extensió  $k(\alpha)|k$  és radical i admet una cadena de subcossos de la forma*

$$k \subseteq k(\theta_1) \subseteq k(\theta_1, \theta_2) \subseteq \dots \subseteq k(\theta_1, \dots, \theta_m) = k(\alpha)$$

*tal que  $\theta_i^2 \in k(\theta_1, \dots, \theta_{i-1})$ . I recíprocament, si  $\alpha \in \mathbb{C}$  és un nombre complex tal que el cos  $k(\alpha) \subseteq \mathbb{C}$  admet una cadena com aquesta, llavors  $\alpha$  és construïble amb regla i compàs a partir de  $C_0$ .*

**DEMOSTRACIÓ:** Sigui  $\alpha \in C$ ; per definició, existeix  $i \in \mathbb{N}$  tal que  $\alpha \in C_i$ ; això ens diu que  $\alpha$  es construeix a partir d'una quantitat finita de punts de  $C_0$  en un nombre finit de passos. Ara bé, a cada pas, es produeix un nou punt com a intersecció de dues rectes (i, en aquest cas, el punt construït pertany al mateix cos que els punts a partir dels quals es construeix), o bé d'una recta i una circumferència (i, en aquest cas, el punt construït pertany a un cos extensió quadràtica del cos que conté els punts a partir dels quals es construeix, ja que la intersecció d'una recta i una circumferència és donada per les arrels

d'una equació quadràtica), o bé de dues circumferències (i, en aquest cas, el punt construït pertany a un cos extensió quadràtica del cos que conté els punts a partir dels quals es construeix, ja que la intersecció de dues circumferències també és donada per les arrels d'una equació quadràtica). Per tant, la successió de punts que construeixen  $\alpha$  a partir de  $C_0$  dóna una successió d'elements de  $\mathbb{C}$  tal com la  $\theta_1, \dots, \theta_m$ , si tenim en compte de canviar l'element primitiu de cada extensió quadràtica pel discriminant del polinomi de grau 2 que la defineix.

I el recíproc també és senzill; com que l'extracció d'arrels quadrades és una operació que es pot realitzar amb regla i compàs, tots els elements de  $k(\theta_1, \dots, \theta_m)$  es poden construir amb regla i compàs a partir de  $k$ , és a dir, a partir de  $C_0$ .  $\square$

Ja només amb aquest resultat, podem demostrar la impossibilitat de la construcció amb regla i compàs de molts nombres complexos. Per exemple:

**5.10.13. Impossibilitat de la duplicació del cub.** Donar un cub, equival a donar la seva aresta; per tant, a donar dos punts diferents del pla. L'aplicació del teorema ens diu que si un punt del pla,  $\alpha$ , és construïble amb regla i compàs a partir d'aquests dos, el grau  $[\mathbb{Q}(\alpha) : \mathbb{Q}]$  ha de ser una potència de 2. Ara bé, l'aresta d'un cub de volum doble que el volum del cub unitat és l'arrel real, posem  $\alpha$ , del polinomi  $X^3 - 2$ , que és irreductible en  $\mathbb{Q}[X]$ ; per tant, el grau  $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$  no és una potència de 2, de manera que  $\alpha$ , és a dir, el cub de volum 2, no és construïble amb regla i compàs a partir del cub d'aresta unitat.

**5.10.14. Impossibilitat de la trisecció de l'angle.** En general, hi ha alguns angles que es poden trisecar; per exemple, podem construir amb regla i compàs l'angle d'un sisè de volta (o l'angle d'un terç de volta). Però aquests dos angles no poden ser trisecats amb regla i compàs. En efecte, donar l'angle d'un terç de volta equival a donar una arrel cúbica primitiva de la unitat, posem  $\rho$ . Per tant, el problema de la trisecció d'aquest angle equival al de la construcció amb regla i compàs d'una arrel novena primitiva de la unitat, posem  $\zeta$ , a partir de  $0, 1, \rho$ . Ara bé,  $[\mathbb{Q}(\zeta) : \mathbb{Q}(\rho)] = \frac{[\mathbb{Q}(\zeta) : \mathbb{Q}]}{[\mathbb{Q}(\rho) : \mathbb{Q}]} = \frac{\varphi(9)}{\varphi(3)} = \frac{6}{2} = 3$ , que no és una potència de 2.

Més generalment, si  $\alpha$  és un angle qualsevol, construir  $\alpha$  amb regla i compàs equival a construir  $\cos(\alpha)$  amb regla i compàs. La relació algebraica entre el cosinus de l'angle  $\alpha$  i el cosinus de l'angle  $\alpha/3$  és

$$4 \cos^3(\alpha/3) - 3 \cos(\alpha/3) - \cos(\alpha) = 0,$$

de manera que  $\cos(\alpha/3)$  és arrel d'un polinomi de grau 3 de coeficients en  $\mathbb{Q}(\cos(\alpha))$  i, en conseqüència, l'angle  $\alpha$  es podrà trisecar amb regla i compàs si, i només si, l'extensió  $\mathbb{Q}(\cos(\alpha/3))|\mathbb{Q}(\cos(\alpha))$  és trivial o bé quadràtica.

**Observació 5.10.15.** El polinomi  $4X^3 - 3X - \cos(\alpha) \in \mathbb{Q}(\cos(\alpha))[X]$  és, genèricament, irreductible; en aquest cas,  $\alpha$  no es podrà trisecar amb regla i compàs. Per exemple, si  $\cos(\alpha)$  és un nombre transcendent, el polinomi  $4X^3 - 3X - \cos(\alpha) \in \mathbb{Q}(\cos(\alpha))[X]$  és irreductible, perquè és de grau 1 en  $\cos(\alpha)$ . Però el polinomi és irreductible per a la majoria dels nombres  $\alpha$ , encara que  $\cos(\alpha)$  sigui un nombre algebraic.

**5.10.16. Impossibilitat de la quadratura del cercle.** Aquest problema equival a construir amb regla i compàs, a partir del cercle de radi 1, això és, a partir de  $0, 1$ , l'aresta d'un quadrat d'àrea  $\pi$ ; és a dir, a construir amb regla i compàs, a partir de  $0, 1$ , el nombre  $\sqrt{\pi}$ . Ara bé, aquest nombre no és ni tan sols algebraic sobre  $\mathbb{Q}$  (cf. la secció 5.12). Per tant, no pot ser de grau potència de 2 sobre  $\mathbb{Q}$ .

## 5.11 Seccions construïbles del cercle

Una altra pregunta, també clàssica, a la qual respongué Gauss, és quines seccions circulars són construïbles amb regla i compàs; és a dir, quines arrels de la unitat són construïbles amb regla i compàs.

Per a respondre aquesta qüestió, és útil caracteritzar els nombres construïbles amb regla i compàs d'una altra manera. Recordem que hem vist (cf. el teorema 5.10.12) que, donat un nombre  $\alpha \in \mathbb{C}$ , i si posem  $k := \mathbb{Q}(C_0)$ , el nombre  $\alpha$  és construïble amb regla i compàs a partir de  $C_0$  si, i només si, l'extensió  $k(\alpha)|k$  és radical i admet una cadena de subcossos de la forma

$$k \subseteq k(\theta_1) \subseteq k(\theta_1, \theta_2) \subseteq \cdots \subseteq k(\theta_1, \dots, \theta_m) = k(\alpha)$$

tal que, per a  $1 \leq i \leq m$ , és  $\theta_i^2 \in k(\theta_1, \dots, \theta_{i-1})$ . Podem caracteritzar aquest fet d'una altra manera més convenient per als nostres propòsits actuals.

**Teorema 5.11.1.** *Sigui  $C_0$  un conjunt no buit de punts del pla que contingui, com a mínim, dos punts diferents. Identifiquem dos punts diferents de  $C_0$  amb  $0, 1 \in \mathbb{C}$ , i sigui  $k := \mathbb{Q}(C_0)$ . Llavors, un nombre  $\alpha \in \mathbb{C}$  és construïble amb regla i compàs a partir de  $C_0$  si, i només si, la clausura normal de l'extensió  $k(\alpha)|k$  és de grau una potència de 2.*

**DEMOSTRACIÓ:** Suposem que  $\alpha$  és construïble amb regla i compàs a partir de  $C_0$ , i sigui  $k \subseteq k(\theta_1) \subseteq k(\theta_1, \theta_2) \subseteq \cdots \subseteq k(\theta_1, \dots, \theta_m) = k(\alpha)$  una cadena radical de manera que  $\theta_i^2 \in k(\theta_1, \dots, \theta_{i-1})$ , per a  $1 \leq i \leq m$ . Si  $L|k$  és la clausura normal de l'extensió  $k(\alpha)|k$ , llavors  $L = \bigcup_{\sigma} \sigma(k(\alpha)) = \bigcup_{\sigma} k(\sigma(\alpha))$ , quan  $\sigma$  recorre  $\text{Gal}(L|k)$ . Ara bé, per a tot  $\sigma \in \text{Gal}(L|k)$ , resulta que és  $\sigma(\theta_i)^2 \in k(\sigma(\theta_1), \dots, \sigma(\theta_{i-1}))$ , de manera que podem construir una cadena radical per a l'extensió  $L|k$  afegint, successivament, els elements  $\sigma(\theta_i)$ , per a  $1 \leq i \leq m$  i per a  $\sigma \in \text{Gal}(L|k)$ ; així, obtenim una cadena radical d'extensions quadràtiques per a  $L|k$ , de manera que el grau  $[L : k]$  és una potència de 2.

Suposem, recíprocament, que la clausura normal  $L|k$  de l'extensió  $k(\alpha)|k$  és de grau potència de 2. Si provem que el grup de Galois  $\text{Gal}(L|k)$  és resoluble, llavors existeix una resolució de  $\text{Gal}(L|k)$  per una cadena de subgrups tals que els quocients successius siguin d'ordre 2, de manera que l'extensió  $L|k$  admet una cadena radical formada per extensions quadràtiques, com cal provar. I el fet que  $\text{Gal}(L|k)$  és un grup resoluble és un cas particular del resultat següent de teoria de grups.  $\square$

**Definició 5.11.2.** Sigui  $p$  un nombre primer. Un grup finit  $G$  s'anomena un  $p$ -grup si, i només si, l'ordre de  $G$  és una potència de  $p$ .

**Teorema 5.11.3.** *Siguin  $p$  un nombre primer i  $G$  un  $p$ -grup. Llavors,  $G$  és resoluble.*

I aquest teorema és una conseqüència immediata del resultat següent.

**Lema 5.11.4.** *Siguin  $p$  un nombre primer i  $G$  un  $p$ -grup no trivial. Llavors, el centre de  $G$ , definit com  $C(G) := \{g \in G : gh = hg, \text{ per a tot } h \in G\}$ , és un subgrup no trivial de  $G$ ; és a dir,  $C(G) \neq \{1\}$ .*

**DEMOSTRACIÓ:** Considerem l'acció per conjugació de  $G$  en  $G$ ; un element  $g \in G$  és fix per l'acció de  $G$  si, i només si,  $g \in C(G)$ ; és a dir,  $[G : G_g] = 1$  si, i només si,  $g \in C(G)$ .

Per tant, la fórmula d'òrbites (cf. l'exercici 5.6.8),  $\#G = \sum_{g \in R} [G : G_g]$ , on  $R$  és un conjunt de representants de les classes de conjugació d'elements de  $G$ , es pot llegir en la forma  $\#G = \#C(G) + \sum_{g \in R'} [G : G_g]$ , on  $R'$  és un conjunt de representants de les classes de conjugació d'elements de  $G$  que tenen més d'un element. Ara bé, com que  $G$  és un  $p$ -grup, tots els sumands de  $\sum_{g \in R'} [G : G_g]$  són múltiples de  $p$ , i  $\#G$  també; per tant,  $\#C(G)$  és un múltiple de  $p$ , que no pot ser 0, ja que  $1 \in C(G)$ . Així,  $C(G) \neq \{1\}$ , com volíem veure.  $\square$

Ara, la demostració del teorema és senzilla.

**DEMOSTRACIÓ:** Sigui  $G_0 := G$ , i  $G_1 := C(G)$ ; llavors,  $C(G)$  és un subgrup normal i commutatiu de  $G$  i  $G/C(G)$  és un  $p$ -grup d'ordre estrictament menor que  $p$ . Podem usar inducció sobre l'exponent de  $p$  en l'ordre del grup, i obtenim que  $G/C(G)$  és resoluble. Per tant,  $G$  és resoluble, ja que  $C(G)$  és un subgrup normal de  $G$  tal que  $C(G)$  i  $G/C(G)$  són resolubles.  $\square$

Amb la caracterització que hem fet dels nombres construïbles amb regla i compàs, podem fer la caracterització dels  $n$ -àgons regulars construïbles amb regla i compàs; és a dir, de les arrels de la unitat construïbles amb regla i compàs, o, si es vol, de les seccions circulars construïbles amb regla i compàs.

**Corol·lari 5.11.5.** *Sigui  $n \geq 3$  un nombre natural. Un  $n$ -àgon regular és construïble amb regla i compàs si, i només si,  $\varphi(n)$  és una potència de 2.*

**DEMOSTRACIÓ:** Un  $n$ -àgon regular és construïble amb regla i compàs si, i només si, ho és una arrel  $n$ -èsima primitiva de la unitat; és a dir, si, i només si, el grau  $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$  és una potència de 2.  $\square$

**Corol·lari 5.11.6.** *Els  $n$ -àgons regulars construïbles amb regla i compàs són els que corresponen als valors de  $n$  de la forma  $n = 2^a p_1 \cdots p_m$ , on  $a \geq 0$ , i  $p_1, \dots, p_m$  són nombres primers diferents i de la forma  $p_i = 2^{2^{n_i}} + 1$ .*

**DEMOSTRACIÓ:** Només cal calcular els nombres naturals  $n$  tals que  $\varphi(n)$  és una potència de 2. Com que un nombre primer  $p$  divideix  $\varphi(p^2)$ , l'únic nombre primer tal que el seu quadrat pot dividir  $n$  és  $p = 2$ ; així,  $n$  ha de ser de la forma  $n = 2^a p_1 \cdots p_m$ , per a nombres primers senars  $p_1, \dots, p_m$  tals que  $\varphi(p_i) = p_i - 1$  sigui una potència de 2; ara bé, si un nombre de la forma  $2^b + 1$  és primer, llavors  $b$  és una potència de 2, ja que, si  $b = 2^c s$ , amb  $s > 1$  senar, llavors  $2^b + 1 = 2^{2^c s} + 1$  és divisible per  $2^{2^c} + 1$ . El recíproc és immediat, com ho demostra el càlcul del valor de la funció d'Euler en els nombres de la forma donada.  $\square$

**Observació 5.11.7.** Recordem que els *nombres de Fermat* són els nombres de la successió  $F_k := 2^{2^k} + 1$ ,  $k \geq 0$ . Se sap que  $F_0 = 3$ ,  $F_1 = 5$ ,  $F_2 = 17$ ,  $F_3 = 257$  i  $F_4 = 65537$  són primers, i no se n'ha trobat cap més de primer. El teorema que s'acaba de provar diu que un  $n$ -àgon regular és construïble amb regla i compàs si, i només si,  $n$  és el producte d'una potència de 2 per alguns nombres primers, diferents, de Fermat,

**Observació 5.11.8.** No és cert que si un element  $\alpha \in \mathbb{C}$  és tal que  $[\mathbb{Q}(\alpha) : \mathbb{Q}]$  és una potència de 2, llavors  $\alpha$  sigui construïble amb regla i compàs sobre  $\mathbb{Q}$ . Cal que la clausura normal de l'extensió sigui de grau potència de 2.

Per exemple, si  $\alpha$  és una arrel del polinomi  $f(X) = X^4 + 2X + 2$ , que és un polinomi irreductible de  $\mathbb{Q}[X]$ , i si  $L$  és el cos de descomposició de  $f(X)$  sobre  $\mathbb{Q}$ , se satisfà que  $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$ , però  $[L : \mathbb{Q}] = 24$ , ja que  $\text{Gal}(L|\mathbb{Q}) \cong S_4$ .

D'acord amb la definició 5.9.4, el resovent cúbic de  $f(X)$  és  $g(X) = X^3 - 8X - 4$ , el discriminant del qual és  $\Delta = -4 \cdot (-8)^3 - 27 \cdot (-4)^2 = 1616 = 2^4 \cdot 101$ , que no és un quadrat de  $\mathbb{Q}$ ; a més a més,  $g(X)$  és irreductible en  $\mathbb{Q}[X]$  (per exemple, perquè és irreductible en  $\mathbb{Z}/5\mathbb{Z}[X]$ , o bé perquè és de grau 3 i no té arrels en  $\mathbb{Q}$ ); per tant, el grup de Galois del cos de descomposició de  $g(X)$  és isomorf al grup simètric  $S_3$  (ja que no està inclòs en  $A_3$  i és d'ordre divisible per 3). Ara bé, aquest cos és subcòs de  $L$ , de manera que el grau  $[L : \mathbb{Q}]$  és divisible per 6, i  $\text{Gal}(L|\mathbb{Q})$  no està inclòs en  $A_4$  (ja que el discriminant de  $f(X)$  no és un quadrat de  $\mathbb{Q}$ ). Així, el grup de Galois de l'extensió  $L|\mathbb{Q}$  és isomorf a un subgrup transitiu de  $S_4$  no inclòs en  $A_4$ , i d'ordre divisible per 6 (i que admet per quocient un grup isomorf a  $S_3$ ); l'únic tal subgrup és  $S_4$ .

**Exercici 5.11.9.** L'únic subgrup transitiu de  $S_4$  que admet per quocient un grup isomorf a  $S_3$  és el propi  $S_4$ .

Acabem aquesta secció amb un estudi que ens explica quins poden ser els grups de Galois dels cossos de descomposició de les equacions donades per polinomis irreductibles de la forma  $X^4 + cX^2 + e \in k[X]$ , on  $c, e \in k$ , i  $k$  un cos de característica diferent de 2 i de 3.

**Proposició 5.11.10.** *Siguin  $k$  un cos de característica diferent de 2 i de 3,  $c, e \in k$  elements tals que el polinomi  $f(X) := X^4 + cX^2 + e \in k[X]$  sigui irreductible, i  $L$  el cos de descomposició sobre  $k$  del polinomi  $f(X)$ . Llavors,  $\text{Gal}(L|k)$  és isomorf a un dels tres grups  $V_4$ , de Klein,  $C_4$ , cíclic d'ordre 4, o bé  $D_{2,4}$ , diedral d'ordre 8.*

**Observació 5.11.11.** Els models dins del grup  $S_4$  d'aquests subgrups són els següents: el grup de Klein

$$V_4 = \{1, (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\},$$

que és un subgrup normal de  $S_4$ ; el grup

$$C_4 = \{1, (1, 2, 3, 4), (1, 3)(2, 4), (1, 4, 3, 2)\},$$

que és cíclic, i els seus subgrups conjugats

$$\{1, (1, 2, 4, 3), (1, 4)(2, 3), (1, 3, 4, 2)\},$$

i

$$\{1, (1, 3, 2, 4), (1, 2)(3, 4), (1, 4, 2, 3)\};$$

i el grup diedral

$$D_{2,4} = V_4 \cup \{(1, 2, 3, 4), (1, 4, 3, 2), (1, 3), (2, 4)\}$$

i els seus conjugats

$$V_4 \cup \{(1, 2, 4, 3), (1, 3, 4, 2), (1, 4), (2, 3)\},$$

$$V_4 \cup \{(1, 3, 2, 4), (1, 4, 2, 3), (1, 2), (3, 4)\}.$$

**DEMOSTRACIÓ:** Podem usar el fet, trivial, que el polinomi  $f(X)$  és resoluble per radicals quadràtics; per tant,  $\text{Gal}(L|k)$  és un subgrup transitiu de  $S_4$  d'ordre potència de 2. I els subgrups transitius de  $S_4$  d'ordre potència de 2 són els enunciats.  $\square$

**Exercici 5.11.12.** Els subgrups transitius de  $S_4$  d'ordre potència de 2, són isomorfs als subgrups  $V_4$ ,  $C_4$ , o bé  $D_{2,4}$  explicitats en l'observació anterior.

**Exercici 5.11.13.** Sigui  $L|k$  una extensió de Galois de cossos de característica diferent de 2 i de 3 i tal que el grup de Galois  $\text{Gal}(L|k)$  sigui isomorf a un dels grups  $V_4$ , de Klein,  $C_4$ , cíclic d'ordre 4, o bé  $D_{2,4}$ , diedral d'ordre 8. Llavors,  $L$  és el cos de descomposició sobre  $k$  d'un polinomi irreductible  $f(X) \in k[X]$  de la forma  $f(X) = X^4 + cX^2 + e$ , amb  $c, e \in k$ .

## 5.12 La transcendència de $\pi$

L'objectiu d'aquesta secció és provar que la quadratura del cercle no és possible només amb regle i compàs.

La solució d'aquest problema clàssic es dedueix immediatament del teorema següent, que fou provat per primer cop per Lindemann, l'any 1882.

**Teorema 5.12.1.** *El nombre  $\pi$  és transcendent.*

DEMOSTRACIÓ: Qui és el nombre  $\pi$ ? Òbviament, necessitem una definició que ens permeti treballar-hi. Una de les definicions equivalents del nombre  $\pi$ , de la qual partirem, és la donada per la igualtat d'Euler,

$$e^{i\pi} + 1 = 0.$$

De fet, ni tan sols cal la definició precisa de  $\pi$  com el menor nombre real positiu per al qual se satisfà aquesta igualtat; és suficient que per al nombre  $\pi$  se satisfaci la igualtat. Per a provar la transcendència de  $\pi$  veurem, equivalentment ja que  $i$  és algebraic, que  $i\pi$  és transcendent. I ho farem per reducció a l'absurd.

Sigui  $\overline{\mathbb{Q}} \subseteq \mathbb{C}$  la clausura algebraica de  $\mathbb{Q}$  en  $\mathbb{C}$ . Si fos que  $i\pi \in \overline{\mathbb{Q}}$ , podríem considerar el polinomi minimal de  $i\pi$  sobre  $\mathbb{Q}$ ,

$$(0) \quad f(X) := \text{Irr}(i\pi, \mathbb{Q})(X) = \sum_{i=0}^n a_i X^i \in \mathbb{Z}[X], \quad a_i \in \mathbb{Z}, \quad a := a_n > 0,$$

que hem multiplicat pel denominador comú positiu dels coeficients a fi de poder-lo considerar de coeficients enters i primitiu, de manera que tindríem que  $\text{mcd}(a_0, \dots, a_n) = 1$ , encara que aquesta propietat no farà falta.

Siguin  $\theta_1 := i\pi$ ,  $\theta_2, \dots, \theta_n$  els  $n$  conjugats de  $i\pi$ ; és a dir, les  $n$  arrels (diferents) de  $f(X)$ . Com que  $e^{\theta_1} + 1 = 0$ , tenim, trivialment, que

$$(1 + e^{\theta_1})(1 + e^{\theta_2}) \cdots (1 + e^{\theta_n}) = 0.$$

El desenvolupament del producte és la suma dels  $2^n$  nombres  $e^{\eta(\varepsilon_1, \dots, \varepsilon_n)}$  que corresponen a les  $2^n$  expressions

$$\eta(\varepsilon_1, \dots, \varepsilon_n) := \varepsilon_1 \theta_1 + \cdots + \varepsilon_n \theta_n, \quad \varepsilon_1, \dots, \varepsilon_n \in \{0, 1\};$$

per tant, podem reescriure el producte en la forma

$$(1) \quad \ell + e^{\alpha_1} + \cdots + e^{\alpha_r} = 0,$$



on  $\alpha_1, \dots, \alpha_r$  són totes les expressions  $\eta(\varepsilon_1, \dots, \varepsilon_n)$  no nul·les i  $\ell = 2^n - r$ , que corresponen a la suma d'una unitat per a cadascuna de les expressions  $\eta(\varepsilon_1, \dots, \varepsilon_n)$  que siguin nul·les. Obtenim, doncs, una certa combinació lineal, de coeficients enters, de valors de la funció exponencial; d'aquesta relació de dependència lineal n'obtidrem una contradicció. Notem que alguna de les expressions ha de ser no nul·la, i això implica que  $r \geq 1$  (per exemple,  $\eta(1, 0, \dots, 0) = \theta_1 = i\pi \neq 0$ ). I, d'altra banda, com que el producte dels primers factors del producte (que correspon a  $\varepsilon_1 = \dots = \varepsilon_n = 0$ ) és 1, ha de ser  $r \neq 2^n$ , de manera que  $\ell \neq 0$ .

Definim el polinomi

$$(2) \quad g_0(X) := a^r (X - \alpha_1) \cdots (X - \alpha_r) =: \sum_{i=0}^r d_i X^i \in \mathbb{C}[X], \quad d_i \in \mathbb{C},$$

i veiem que  $g_0(X) \in \mathbb{Z}[X]$ ; és a dir, que  $d_i \in \mathbb{Z}$ .

Notem que, de la definició de  $g_0(X)$  s'obté té que  $d_r = a^r$  i  $d_0 = (-1)^r a^r \alpha_1 \cdots \alpha_r \neq 0$ , on  $a = a_n \in \mathbb{Z}$  és el coeficient dominant de  $f(X)$ ; a més a més, per a  $1 \leq i \leq r$ , és  $d_{r-i} = (-1)^i a^r s_i(\alpha_1, \dots, \alpha_r) = (-1)^i a^{r-i} s_i(a\alpha_1, \dots, a\alpha_r)$ , on els  $s_i(\alpha_1, \dots, \alpha_r)$  són els polinomis simètrics elementals (cf. la definició **2.2.6**); així, tenim que (cf. el teorema **2.3.1**)

$$(3) \quad g_0(X) \in \mathbb{Z}[as_1(\alpha_1, \dots, \alpha_r), \dots, a^r s_r(\alpha_1, \dots, \alpha_r)][X].$$

Ara bé, per a  $1 \leq i \leq r$ , és  $s_i(\eta_1, \dots, \eta_{2^n}) = s_i(\alpha_1, \dots, \alpha_r)$ , mentre que per a  $i > r$  és  $s_i(\eta_1, \dots, \eta_{2^n}) = 0$ ; per tant, la propietat (3) implica que

$$(4) \quad g_0(X) \in \mathbb{Z}[as_1(\eta_1, \dots, \eta_{2^n}), \dots, a^r s_r(\eta_1, \dots, \eta_{2^n}), \dots, a^{2^n} s_{2^n}(\eta_1, \dots, \eta_{2^n})][X].$$

Ara, notem que una permutació qualsevol de  $\theta_1, \dots, \theta_n$  produeix una permutació de les  $2^n$  expressions  $\eta_1, \dots, \eta_{2^n}$ , de manera que els polinomis simètrics elementals  $s_i(\eta_1, \dots, \eta_{2^n})$  són fixos per l'acció del grup simètric  $S_n$ ; és a dir, obtenim que, per a  $1 \leq i \leq 2^n$ , és

$$(5) \quad s_i(\eta_1, \dots, \eta_{2^n}) \in \mathbb{Z}[\theta_1, \dots, \theta_n]^{S_n} = \mathbb{Z}[s_1(\theta_1, \dots, \theta_n), \dots, s_n(\theta_1, \dots, \theta_n)].$$

En repartir la potència de  $a$  entre els diferents monomis, i com que  $a \in \mathbb{Z}$ , obtenim que

$$\begin{aligned} a^i s_i(\eta_1, \dots, \eta_{2^n}) &\in \mathbb{Z}[as_1(\theta_1, \dots, \theta_n), \dots, a^n s_n(\theta_1, \dots, \theta_n)] \\ &\subseteq \mathbb{Z}[as_1(\theta_1, \dots, \theta_n), \dots, as_n(\theta_1, \dots, \theta_n)] \\ &= \mathbb{Z}[a_{n-1}, \dots, a_0] = \mathbb{Z}; \end{aligned}$$

i això ens diu que

$$g_0(X) \in \mathbb{Z}[X],$$

com volíem veure.

Ara, un cop vist que  $g_0(X) \in \mathbb{Z}[X]$ , considerem, també, el polinomi que se n'obté en prendre el valor absolut dels seus coeficients,

$$(6) \quad h_0(X) := \sum_{i=0}^r |d_i| X^i \in \mathbb{N}[X] \subseteq \mathbb{Z}[X].$$

Així, per a tot nombre complex  $t$ , es disposa d'una fita

$$(7) \quad |g_0(t)| \leq \sum_{i=0}^r |d_i| |t|^i = h_0(|t|).$$

Ara, per a tot nombre natural  $p$  (que més endavant triarem primer i prou gran, però que per ara pot ser qualsevol), considerem els polinomis

$$(8) \quad g_p(X) := X^{p-1}g_0(X)^p =: \sum_{i=p-1}^{p-1+rp} b_i X^i \in \mathbb{Z}[X], \quad b_i \in \mathbb{Z},$$

i, anàlogament,

$$(9) \quad h_p(X) := X^{p-1}h_0(X)^p \in \mathbb{N}[X];$$

també definim les integrals

$$(10) \quad I_p(t) := \int_0^t e^{t-z} g_p(z) dz = \int_0^1 e^{t(1-x)} g_p(tx) t dx, \quad t \in \mathbb{C};$$

i considerem el nombre complex

$$(11) \quad J(p) := \sum_{k=1}^r I_p(\alpha_k) \in \mathbb{C}.$$

Podem fitar els valors absoluts de les integrals  $I_p(t)$  com segueix. Per a tot nombre real  $x$ ,  $0 \leq x \leq 1$ , i com que els coeficients de  $h_0(X)$  són no negatius, obtenim que

$$(12) \quad h_0(|tx|) \leq h_0(|t|);$$

per tant,

$$(13) \quad \begin{aligned} |I_p(t)| &\leq \int_0^1 |e^{t(1-x)}| |g_p(tx)| |t| dx && (|e^{t(1-x)}| \leq e^{|t(1-x)|}) \\ &\leq \int_0^1 e^{|t(1-x)|} |g_p(tx)| |t| dx && (8) \\ &= \int_0^1 e^{|t(1-x)|} |tx|^{p-1} |g_0(tx)|^p |t| dx && (|x| \leq 1, |1-x| \leq 1) \\ &\leq \int_0^1 e^{|t|} |t|^p |g_0(tx)|^p dx && (7) \\ &\leq \int_0^1 e^{|t|} |t|^p h_0(|tx|)^p dx && (12) \\ &\leq \int_0^1 e^{|t|} |t|^p h_0(|t|)^p dx && (9) \\ &\leq \int_0^1 e^{|t|} |t| h_p(|t|) dx && (\int_0^1 dx = 1) \\ &= |t| e^{|t|} h_p(|t|). \end{aligned}$$

Com a conseqüència, obtenim una fita per a  $|J(p)|$  en la forma

$$(14) \quad |J(p)| \leq \sum_{k=1}^r |I_p(\alpha_k)| \leq \sum_{k=1}^r |\alpha_k| e^{|\alpha_k|} h_p(|\alpha_k|) = \sum_{k=1}^r e^{|\alpha_k|} (|\alpha_k| h_0(|\alpha_k|))^p;$$

i, si posem  $c_k := |\alpha_k| h_0(|\alpha_k|)$ , i  $c := \max\{e^{|\alpha_k|}, c_k : 1 \leq k \leq r\}$ , obtenim que, per a alguna constant  $C$ , independent de  $p$ , per exemple,  $C = rc^2$ , és

$$(15) \quad |J(p)| \leq rc^{p+1} \leq C^p.$$

Així, la funció complexa  $J(p)$  presenta un creixement que és, avaluada en els nombres naturals, com a màxim exponencial. Ara es tracta de veure que el creixement de  $J(p)$  per a  $p$  primer és més gran que el factorial de  $p - 1$ , de manera que les desigualtats

$$(16) \quad (p - 1)! \leq |J(p)| \leq C^p$$

són contradictòries per a  $p$  primer prou gran.

Una successió d'integracions per parts, tantes com el grau  $m = p - 1 + rp$  del polinomi  $g_p(X)$ , ens permet obtenir la igualtat, que farem servir més endavant,

$$(17) \quad I_p(t) = e^t \sum_{j=0}^{p-1+rp} g_p^{(j)}(0) - \sum_{j=0}^{p-1+rp} g_p^{(j)}(t).$$

En efecte, notem que

$$\begin{aligned} \int_0^1 e^{t(1-x)} g_p^{(j)}(tx) t dx &= -e^{t(1-x)} g_p^{(j)}(tx) \Big|_0^1 + \int_0^1 e^{t(1-x)} g_p^{(j+1)}(tx) t dx \\ &= e^t g_p^{(j)}(0) - g_p^{(j)}(t) + \int_0^1 e^{t(1-x)} g_p^{(j+1)}(tx) t dx, \end{aligned}$$

i que les derivades  $g_p^{(j+1)}(tx)$  són nul·les més enllà del grau,  $j = p - 1 + rp$ , del polinomi  $g_p(X)$ .

A fi d'obtenir la fita  $(p - 1)! \leq |J(p)|$  de (16), ens cal avaluar les derivades  $g_p^{(j)}(0)$  i  $g_p^{(j)}(\alpha_k)$ , per a tot  $j$  i tot  $k$ ,  $1 \leq k \leq r$ . Comencem per les primeres.

A partir de la definició, (8), del polinomi  $g_p(X)$ , tenim que, per a tot  $j \geq 0$ , és  $g_p^{(j)}(0) = j! b_j$ ; en particular,

$$(18) \quad \begin{aligned} g_p^{(j)}(0) &= 0 \in p! \mathbb{Z}, & j < p - 1, \\ g_p^{(j)}(0) &\in p! \mathbb{Z}, & j > p - 1, \\ g_p^{(p-1)}(0) &= (p - 1)! b_{p-1}, & j = p - 1. \end{aligned}$$

Ara bé, tenim que  $b_{p-1} = d_0^p$ , amb  $d_0 \neq 0$ , de manera que

$$(19) \quad g_p^{(p-1)}(0) = (p - 1)! d_0^p \in (p - 1)! \mathbb{Z}.$$

A partir d'ara, restringim  $p$  al conjunt dels nombres primers que no divideixen el nombre natural  $\ell d_0 = (2^n - r) d_0$ , de manera que només n'excloem una quantitat finita; llavors,

$$(20) \quad g_p^{(p-1)}(0) \notin p! \mathbb{Z}.$$

Avaluem, ara, les derivades  $g_p^{(j)}(\alpha_k)$ . Per a això, definim els polinomis  $g_{p,k}(X)$  per les igualtats

$$(21) \quad g_p(X) = (X - \alpha_k)^p g_{p,k}(X)$$

i derivem per la fórmula de Leibniz. Obtenim la igualtat

$$(22) \quad g_p^{(j)}(X) = \sum_{i=0}^j \binom{j}{i} (D^{j-i} (X - \alpha_k)^p) g_{p,k}^{(i)}(X).$$

Per a  $j - i < p$ , el valor en  $\alpha_k$  del derivat  $(j - i)$ -èsim del factor  $(X - \alpha_k)^p$  és zero, perquè  $\alpha_k$  és una arrel de multiplicitat  $p > j - i$  del polinomi; per a  $j - i > p$ , el derivat  $(j - i)$ -èsim del polinomi  $(X - \alpha_k)^p$ , de grau  $p$ , també és zero; i per a  $j - i = p$ , el derivat  $p$ -èsim del polinomi  $(X - \alpha_k)^p$ , és exactament  $p!$ . Per tant, tenim que

$$(23) \quad g_p^{(j)}(\alpha_k) = \binom{j}{j-p} p! g_{p,k}^{(j-p)}(\alpha_k) = \binom{j}{p} p! g_{p,k}^{(j-p)}(\alpha_k);$$

en particular,  $g_p^{(j)}(\alpha_k) = 0$ , si  $j < p$ .

D'altra banda, l'expressió

$$(24) \quad \sum_{k=1}^r \sum_{j=0}^{p-1+rp} \binom{j}{p} g_{p,k}^{(j-p)}(\alpha_k),$$

polinòmica de coeficients enters en  $a\alpha_1, \dots, a\alpha_r$ , és invariant per les permutacions dels  $\alpha_1, \dots, \alpha_r$ ; per tant, de nou pel teorema de Waring (cf. **2.3.1**), obtenim que

$$(25) \quad \sum_{k=1}^r \sum_{j=0}^{p-1+rp} g_p^{(j)}(\alpha_k) = p! \sum_{k=1}^r \sum_{j=0}^{p-1+rp} \binom{j}{p} g_{p,k}^{(j-p)}(\alpha_k) \in p!\mathbb{Z}.$$

Ja només resta posar junta tota la informació obtinguda fins ara. De la definició, (11), de  $J(p)$ , i en tenir en compte (17) i que

$$(1) \quad \sum_{k=1}^r e^{\alpha_k} = -\ell = r - 2^n,$$

tenim que

$$(26) \quad \begin{aligned} -J(p) &= \ell \sum_{j=0}^{p-1+rp} g_p^{(j)}(0) + \sum_{k=1}^r \sum_{j=0}^{p-1+rp} g_p^{(j)}(\alpha_k) \\ &= \ell g_p^{(p-1)}(0) + \ell \sum_{j=0, j \neq p-1}^{p-1+rp} g_p^{(j)}(0) + \sum_{k=1}^r \sum_{j=0}^{p-1+rp} g_p^{(j)}(\alpha_k); \end{aligned}$$

a més a més, com que, per (18) i (25) és

$$(27) \quad \ell \sum_{j=0, j \neq p-1}^{p-1+rp} g_p^{(j)}(0) + \sum_{k=1}^r \sum_{j=0}^{p-1+rp} g_p^{(j)}(\alpha_k) \in p!\mathbb{Z},$$

resulta que

$$(28) \quad -J(p) = \ell(p-1)!A + p!B,$$

on  $A, B \in \mathbb{Z}$ ,  $A = d_0^p \neq 0$  (cf. (19)).

Finalment, com que  $p$  no divideix  $\ell A$ , resulta que  $0 \neq -J(p) \in (p-1)!\mathbb{Z}$  i, en conseqüència,

$$|J(p)| \geq (p-1)!,$$

com calia veure.  $\square$

## 5.13 Exercicis

**Exercici 5.13.1.** Siguin  $p$  un nombre natural primer senar, i  $\zeta \in \mathbb{C}$  una arrel primitiva  $p$ -èsima de la unitat. Definim la suma de Gauss per al caràcter de Legendre per la fórmula

$$g(\zeta) := \sum_{a \pmod{p}} \left(\frac{a}{p}\right) \zeta^a. \text{ Llavors, } g(\zeta)^2 = \left(\frac{-1}{p}\right) p.$$

**Exercici 5.13.2** (Kronecker-Weber, cas quadràtic). Es tracta de provar que si  $K|\mathbb{Q}$  és una extensió quadràtica qualsevol, llavors existeix un nombre natural  $n \geq 1$  tal que  $K \subseteq \mathbb{Q}(\zeta_n)$ , on  $\zeta_n$  designa una arrel primitiva  $n$ -èsima de la unitat.

- Per a tot nombre natural primer senar,  $p$ , posem  $p^* := \left(\frac{-1}{p}\right) p$ . Llavors l'únic subcòs quadràtic de  $\mathbb{Q}(\zeta_p)$  és  $\mathbb{Q}(\sqrt{p^*})$ .
- Per a tot nombre natural primer senar,  $p$ , se satisfà que  $\mathbb{Q}(\sqrt{p}) \subseteq \mathbb{Q}(\zeta_{4p})$ .
- Se satisfà que  $\mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{-2}) \subseteq \mathbb{Q}(\zeta_8)$ .
- Per a tot nombre enter  $n$ , lliure de quadrats,  $\mathbb{Q}(\sqrt{n}) \subseteq \mathbb{Q}(\zeta_{4n})$ .
- En quins casos  $4n$  no és òptim (és a dir, es pot canviar per un divisor propi)?

Aquest resultat és un cas particular del teorema de Kronecker-Weber, que afirma que per a tot cos  $K$  tal que l'extensió  $K|\mathbb{Q}$  és abeliana i finita, existeix una arrel de la unitat,  $\zeta$ , tal que  $K \subseteq \mathbb{Q}(\zeta)$ ; és a dir, que tota extensió abeliana de  $\mathbb{Q}$  és ciclotòmica.

**Exercici 5.13.3** (Períodes de Gauss). Siguin  $p$  un nombre natural primer senar i  $\zeta$  una arrel primitiva  $p$ -èsima de la unitat. El grup de Galois  $\text{Gal}\mathbb{Q}(\zeta)|\mathbb{Q}$  és cíclic d'ordre  $p-1$ , de manera que hi ha una correspondència bijectiva entre el conjunt de les subextensions de l'extensió ciclotòmica  $\mathbb{Q}(\zeta)|\mathbb{Q}$  i el conjunt dels divisors positius  $d$  de  $p-1$ . L'objectiu de l'exercici és donar un element primitiu per a cada un dels subcossos de  $\mathbb{Q}(\zeta)$ ; és a dir, donar-ne un generador sobre  $\mathbb{Q}$ .

Sigui  $g$  un generador del grup multiplicatiu  $(\mathbb{Z}/p\mathbb{Z})^*$ . Aleshores, l'automorfisme  $\sigma$  de  $\mathbb{Q}(\zeta)$  definit per la fórmula  $\sigma(\zeta) := \zeta^g$  és un generador del grup  $\text{Gal}\mathbb{Q}(\zeta)|\mathbb{Q}$ . Per a tot nombre enter  $i$  escrivim  $\zeta_i := \zeta^{g^i}$ .

- Per a  $i, j$  nombres enters qualssevol, és  $\zeta_i = \zeta_j$  si, i només si,  $i \equiv j \pmod{p-1}$ .
- Per a  $i, j$  nombres enters qualssevol, és  $\sigma^j(\zeta_i) = \zeta_{i+j}$ .

**Definició 5.13.4.** Sigui  $n$  un divisor qualsevol de  $p-1$  i  $d := \frac{p-1}{n}$ . Per a tot nombre enter  $i$ ,  $0 \leq i \leq n-1$ , anomenarem  $i$ -èsim  $n$ -període de  $\zeta$  relatiu a  $g$  l'element

$$\eta_i := \sum_{j=0}^{d-1} \sigma^{jn}(\zeta_i) = \sum_{j=0}^{d-1} \zeta_{i+jn} \in \mathbb{Q}(\zeta).$$

- El conjunt  $\{\eta_0, \eta_1, \dots, \eta_{n-1}\}$  no depèn ni de l'elecció del generador  $g$  de  $(\mathbb{Z}/p\mathbb{Z})^*$  ni de l'elecció de l'arrel primitiva  $p$ -èsima de la unitat  $\zeta$ . A més a més, el període  $\eta_0$  no depèn de l'elecció de  $g$ , i els diferents  $\eta_i$  són els  $n$ -períodes  $\eta'_0$  associats a les diferents arrels primitives  $p$ -èsimes de la unitat  $\zeta'$ .

- (d) Siguin  $K \subseteq \mathbb{Q}(\zeta)$  un subcòs qualsevol i  $n := [K : \mathbb{Q}]$  el grau. Aleshores, per a tot nombre enter  $i$ ,  $0 \leq i \leq n - 1$ , podem escriure  $K = \mathbb{Q}(\eta_i)$ , on  $\eta_i$  denota el  $i$ -èsim  $n$ -període de  $\zeta$  relatiu a qualsevol generador del grup  $(\mathbb{Z}/p\mathbb{Z})^*$ .

# Apèndix A

## Definicions i propietats bàsiques

En aquest apèndix, es tracta de fer una recopilació d'algunes definicions i resultats elementals sobre les estructures algebraiques bàsiques que intervenen en el desenvolupament del text principal; estructures que, sovint, poden haver estat objecte d'estudi previ. A més a més, aquest recull també ha de servir per a establir les notacions i les convencions que s'utilitzen en el text principal.

Per a fer un estudi formal acurat de les estructures algebraiques més bàsiques que hem utilitzat, com, per exemple, les de grup o d'anell, convindria donar una visió general del concepte d'operació. En particular, s'hauria de parlar d'operacions binàries (o sigui, aplicacions del tipus  $A \times A \rightarrow A$ ), d'operacions 0-àries (aplicacions del tipus  $\{0\} \rightarrow A$ ), i d'operacions 1-àries (aplicacions del tipus  $A \rightarrow A$ ). I per a l'estudi d'estructures com la de mòdul o la d'àlgebra, caldria fer-ho també d'accions (aplicacions del tipus  $K \times A \rightarrow A$ ). Ens limitarem a fer un estudi rigorós, però d'una manera menys formal i, alhora, més habitual en moltes referències bàsiques.

### A.1 Grups

Aquesta secció es dedica a l'estructura de grup. Els grups apareixen de manera natural en totes les branques de les matemàtiques. Usualment, les transformacions dels objectes per a les quals es pot fer una altra transformació que retorna a la situació inicial solen proporcionar estructures de grup; molt sovint es parla dels *grups d'automorfismes* dels objectes considerats. Per exemple, el grup de les transformacions lineals invertibles d'un espai vectorial, o el grup dels desplaçaments del pla euclidià, o el grup de les afinitats invertibles d'un espai afí, són exemples que s'estudien en un curs bàsic de geometria lineal.

En el text principal, l'estructura de grup que apareix de manera destacada ho fa com a grup d'automorfismes: és l'anomenat grup de Galois d'una extensió algebraica de cossos (cf. **3.8.10**, o bé **3.7.4**) o d'una equació algebraica. I una gran part de la teoria necessària de grups es desenvolupa, paral·lelament a la seva aplicació, en el text principal. Aquest apèndix es limita a exposar-ne les beceroles.

### A.1.1 Grups

**Definició A.1.1.** Un *grup*  $G$  és un conjunt amb una operació binària, que usualment notarem en forma de producte, per a la qual se satisfà la propietat associativa, que conté un element neutre, i tal que cada element té un invers. Si, a més a més, l'operació és commutativa, es parla d'un *grup abelià* o d'un *grup commutatiu*.

**A.1.2.** Així, un grup és un conjunt no buit (conté l'element neutre) amb una operació per a la qual se satisfan les propietats següents.

- (a) Associativa: per a tot  $a, b, c \in G$  és  $a(bc) = (ab)c$ .
- (b) Existència d'element neutre: existeix  $1 \in G$  tal que per a tot  $a \in G$  és  $a1 = a = 1a$ ; l'element  $1$  és únic i s'anomena *l'element neutre* de  $G$ ; també se l'anomena *l'element*  $u$  de  $G$ .
- (c) Tot element té invers: per a tot  $a \in G$  existeix  $b \in G$  tal que  $ab = 1 = ba$ . Per a cada element  $a \in G$ , aquest element  $b$  és únic, s'anomena *l'element invers de  $a$* , i s'escriu  $b =: a^{-1}$ .

I els grups abelians (o, també, commutatius) són els grups per als quals se satisfà, a més a més, la propietat

- (d) Commutativa: per a tot  $a, b \in G$  és  $ab = ba$ .

En el cas dels grups abelians, a més a més de fer-se servir la notació multiplicativa, també s'utilitza sovint la notació additiva; en aquest cas, les propietats s'escriuen en la forma

- (a) associativa: per a tot  $a, b, c \in G$  és  $a + (b + c) = (a + b) + c$ ;
- (b) existència d'element neutre: existeix  $0 \in G$  tal que per a tot  $a \in G$  és  $a+0 = a = 0+a$ ; aquest element neutre se sol anomenar *l'element zero*;
- (c) tot element té invers: per a tot  $a \in G$  existeix  $b \in G$  tal que  $a + b = 0 = b + a$ ; aquest element  $b$  és únic, s'anomena *l'element oposat de  $a$* , i s'escriu  $b =: -a$ ;
- (d) commutativa: per a tot  $a, b \in G$  és  $a + b = b + a$ .

**Observació A.1.3.** Formalment, podríem definir un grup com un conjunt amb una operació binària,  $\cdot$ , una 0-ària,  $1$ , i una 1-ària,  $( )^{-1}$ , de manera que se satisfacin els axiomes anteriors. En particular, l'existència d'operacions 0-àries ja implica que el conjunt és no buit. En aquest apèndix no tractarem els grups des d'un punt de vista formal, i serà suficient el tractament donat a partir de la definició anterior.

**A.1.4.** En un grup se satisfan les *lleis de simplificació*:  $ab = ac \implies b = c$ , i  $ac = bc \implies a = b$ , ja que podem multiplicar la primera a l'esquerra per l'invers de  $a$ , i la segona a la dreta per l'invers de  $c$ .

**A.1.5.** Notem que  $(ab)^{-1} = b^{-1}a^{-1}$ , i que, si  $a, b$  commuten entre ells, llavors també  $(ab)^{-1} = a^{-1}b^{-1}$ . Notem, també, que  $(ab)^2 = abab$ , i que això només coincideix amb  $a^2b^2$  si  $a, b$  commuten entre ells. En general, doncs, no és cert que  $(ab)^n$  coincideixi amb  $a^n b^n$ , per a  $n \neq 1$ . Però si el grup és commutatiu, llavors per a tot  $a, b \in G$  i tot  $n \in \mathbb{Z}$  és  $(ab)^n = a^n b^n$ .



### A.1.2 Morfismes de grups

**Definició A.1.6.** Siguin  $G, H$  grups. Un *morfisme de grups* de  $G$  en  $H$  és una aplicació  $f : G \rightarrow H$  tal que per a tot  $a, b \in G$  és  $f(ab) = f(a)f(b)$ . Un morfisme de grups  $f : G \rightarrow G$  s'anomena un *endomorfisme*.

**A.1.7.** Si  $f : G \rightarrow H$  és un morfisme de grups, llavors  $f(1) = 1$  i, per a tot  $a \in G$ ,  $f(a^{-1}) = (f(a))^{-1}$ .

**Definició A.1.8.** Per a tot grup  $G$ , l'aplicació identitat de  $G$ ,  $\text{id} : G \rightarrow G$ , donada per  $a \mapsto a$ , és un morfisme de grups; s'anomena el *morfisme identitat* de  $G$ .

**A.1.9.** La composició de morfismes de grups és un morfisme de grups; és a dir, si  $G, G'$  i  $G''$  són grups, i  $f : G' \rightarrow G, g : G \rightarrow G''$  són morfismes de grups, llavors l'aplicació composició  $g \circ f : G' \rightarrow G''$ , donada per l'assignació  $a \mapsto g(f(a))$ , és un morfisme de grups. S'anomena el *morfisme composició* de  $f$  i  $g$ .

**Definició A.1.10.** Un morfisme de grups  $f : G \rightarrow H$  és un *isomorfisme* si, i només si, existeix un morfisme invers de grups; és a dir, si existeix un morfisme de grups  $g : H \rightarrow G$  tal que les composicions  $g \circ f = \text{id}_G$  i  $f \circ g = \text{id}_H$ , són les identitats respectives en  $G$  i  $H$ . Un isomorfisme de grups  $f : G \rightarrow G$  s'anomena un *automorfisme*.

**A.1.11.** Per a tot grup  $G$ , la identitat de  $G$ ,  $\text{id} : G \rightarrow G$ , és un automorfisme de grups.

**A.1.12.** La composició d'isomorfismes de grups és un isomorfisme de grups; és a dir, si  $G, G'$  i  $G''$  són grups, i  $f : G' \rightarrow G, g : G \rightarrow G''$  són isomorfismes de grups, llavors l'aplicació composició  $g \circ f : G' \rightarrow G''$  és un isomorfisme de grups.

**Proposició A.1.13.** Els isomorfismes de grups coincideixen amb els morfismes de grups que, com a aplicacions entre conjunts, són aplicacions bijectives.  $\square$

**Definició A.1.14.** El conjunt dels automorfismes d'un grup  $G$ , amb la composició com a operació binària i la identitat com a element neutre, és un grup: el *grup dels automorfismes* de  $G$ ; s'escriu  $\text{Aut}(G)$ .

### A.1.3 Producte de grups

**Definició A.1.15** (El grup producte cartesià). Sigui  $\{G_i\}_{i \in I}$  una família no buida de grups. Existeix un grup  $G$  i una família de morfismes de grups  $\pi_i : G \rightarrow G_i, i \in I$ , de manera que per a tot grup  $H$  i tota família de morfismes de grups  $\{\varphi_i : H \rightarrow G_i\}_{i \in I}$  existeix un únic morfisme de grups  $\varphi : H \rightarrow G$  tal que, per a tot  $i \in I$ , és  $\pi_i \circ \varphi = \varphi_i$ . El grup  $G$  és únic llevat d'un únic isomorfisme que commuta amb els morfismes  $\pi_i$  i s'anomena el *grup producte* de la família  $\{G_i\}_{i \in I}$ ; els morfismes  $\pi_i$  s'anomenen les *projeccions* de  $G$  en  $G_i$ . S'acostuma a escriure  $G =: \prod_{i \in I} G_i$ .

**Observació A.1.16.** Per a provar l'existència del grup producte es pot prendre com a  $G$  el producte cartesià dels conjunts de la família  $\{G_i\}_{i \in I}$ , definir les operacions de grup component a component, i definir els morfismes  $\pi_i : G \rightarrow G_i$  com les projeccions de  $G$  en els factors  $G_i$ . Notem que la universal del producte es pot llegir com que *donar un morfisme d'un grup en un grup producte equival a donar les seves projeccions*, i es pot resumir en el diagrama

$$\forall \{\varphi_i\}_{i \in I} \exists! \varphi \forall i \in I$$

Diagrama A.1: Propietat universal del producte de grups

### A.1.4 Subgrups

**Definició A.1.17.** Sigui  $G$  un grup. Un *subgrup*  $H \subseteq G$  és un subconjunt al qual es poden restringir *totes* les operacions del grup; és a dir, és un subconjunt tal que  $1 \in H$ , per a tot  $a, b \in H$  és  $ab \in H$ , i per a tot  $a \in H$ , és  $a^{-1} \in H$ .

**A.1.18.** En particular, si  $H \subseteq G$  és un subgrup, llavors  $H$  és un grup amb les restriccions de les operacions de  $G$ .

**A.1.19.**  $\{1\} \subseteq G$  i  $G \subseteq G$  són subgrups de  $G$ . El subgrup  $\{1\}$  s'anomena el subgrup *trivial* de  $G$ . I el subgrup  $G$  s'anomena el subgrup *total* de  $G$ .

**A.1.20.** Siguin  $G$  un grup i  $\{H_i\}_{i \in I}$  una família no buida de subgrups de  $G$ ; és a dir,  $I$  és un conjunt no buit i, per a tot  $i \in I$ ,  $H_i \subseteq G$  és un subgrup. Llavors, la intersecció,  $\bigcap_{i \in I} H_i \subseteq G$ , és un subgrup de  $G$ .

**A.1.21.** Si  $H \subseteq G$  és un subgrup d'un grup  $G$ , l'aplicació d'inclusió  $H \rightarrow G$ , donada per  $a \mapsto a$ , és un morfisme injectiu de grups.

**Definició A.1.22.** Si  $f : G \rightarrow H$  és un morfisme de grups, llavors el *nucli* de  $f$ ,  $\ker f := \{a \in G : f(a) = 1\}$ , és un subgrup de  $G$ . I la *imatge* de  $f$ ,  $\text{im} f := f(G)$ , és un subgrup de  $H$ .

**A.1.23.** Més generalment, si  $f : G \rightarrow H$  és un morfisme de grups, i  $G' \subseteq G$  és un subgrup de  $G$ , llavors  $f(G') \subseteq H$  és un subgrup de  $H$ . I si  $H' \subseteq H$  és un subgrup de  $H$ , llavors  $f^{-1}(H') := \{a \in G : f(a) \in H'\} \subseteq G$  és un subgrup de  $G$ .

**A.1.24.** Sigui  $f : G \rightarrow H$  és un morfisme de grups. Es té que  $f$  és injectiu si, i només si,  $\ker f = \{1\}$ ; és a dir, si, i només si,  $\ker f$  és el subgrup trivial de  $G$ . I, òbviament,  $f$  és exhaustiu si, i només si,  $\text{im} f = H$ ; és a dir, si, i només si,  $\text{im} f$  és el subgrup total de  $H$ .

### A.1.5 Subgrups normals i grups quocient

En general, no tots els subgrups d'un grup poden ser nuclis de morfismes de grups. Els que ho són tenen propietats especials que convé destacar.

**Observació A.1.25.** El nom de subgrup normal que es dona als subgrups normals no és arbitrari; la seva definició prové d'abstraure les propietats dels subgrups que es corresponen amb les extensions normals de cossos.

**Definició A.1.26.** Sigui  $G$  un grup. Un subgrup  $N \subseteq G$  es diu que és un subgrup *normal* de  $G$  si, i només si, existeix un grup  $H$  i un morfisme de grups  $f : G \rightarrow H$  tals que  $N = \ker f$ .

**A.1.27.** Sigui  $G$  un grup. Aleshores, els subgrups trivial i total,  $\{1\}$ ,  $G$ , són subgrups normals de  $G$ . I la intersecció d'una família no buida de subgrups normals és un subgrup normal.

**Proposició A.1.28.** *Siguin  $G$  un grup i  $N \subseteq G$  un subgrup de  $G$ . Llavors, les propietats següents són equivalents.*

- (a)  $N \subseteq G$  és un subgrup normal.
- (b) Per a tot  $a \in G$ , els conjunts  $aN := \{ax : x \in N\}$  i  $Na := \{xa : x \in N\}$  coincideixen.
- (c) Per a tot  $a \in G$ ,  $aN \subseteq Na$ .
- (d) Per a tot  $a \in G$ ,  $aNa^{-1} \subseteq N$ .
- (e) Per a tot  $a \in G$ ,  $aNa^{-1} = N$ .
- (f) Els conjunts  $G/N := \{aN : a \in G\}$  i  $N \backslash G := \{Na : a \in G\}$  coincideixen.
- (g) El conjunt  $G/N$  és un grup i l'aplicació  $\pi : G \rightarrow G/N$  donada per l'assignació  $a \mapsto aN$  és un morfisme de grups.  $\square$

**A.1.29.** En particular, si  $G$  és un grup commutatiu, llavors tot subgrup  $H \subseteq G$  és normal.

**Definició A.1.30.** Sigui  $G$  un grup i  $N \subseteq G$  un subgrup normal de  $G$ . El grup  $G/N$  s'anomena el *grup quocient* de  $G$  mòdul  $N$ ; i el morfisme de grups  $\pi : G \rightarrow G/N$  s'anomena la *projecció canònica* de  $G$  en  $G/N$ .

**Proposició A.1.31** (Primer teorema d'isomorfia de grups). *Siguin  $G, H$ , grups qualssevol i  $f : G \rightarrow H$  un morfisme de grups. L'aplicació  $\bar{f} : G/\ker f \rightarrow \text{im} f$  donada per l'assignació  $a \cdot \ker f \mapsto f(a)$  està ben definida i és un isomorfisme de grups.  $\square$*

**A.1.32.** Sigui  $f : G \rightarrow H$  un morfisme de grups. Per definició, el nucli de  $f$ ,  $\ker f \subseteq G$ , és un subgrup normal de  $G$ . D'altra banda, si  $N \subseteq H$  és un subgrup normal de  $H$ , aleshores  $f^{-1}(N) \subseteq G$  és un subgrup normal de  $G$ . I si  $N \subseteq G$  és un subgrup normal de  $G$ , llavors  $f(N) \subseteq \text{im} f$  és un subgrup normal de  $\text{im} f$ ; però, en general,  $f(N) \subseteq H$  no és subgrup normal de  $H$ .

**A.1.33.** Sigui  $G$  un grup i  $N \subseteq H \subseteq G$  subgrups. Si  $N \subseteq G$  és subgrup normal de  $G$ , llavors  $N \subseteq H$  és subgrup normal de  $H$ . Però pot ser que  $N \subseteq H$  sigui subgrup normal de  $H$  i  $H \subseteq G$  sigui subgrup normal de  $G$  i, en canvi,  $N \subseteq G$  no sigui subgrup normal de  $G$ .

**Proposició A.1.34.** *Siguin  $G, H$ , grups,  $N \subseteq G$  un subgrup normal,  $\pi : G \rightarrow G/N$  la projecció canònica, i  $f : G \rightarrow H$  un morfisme qualsevol. Condició necessària i suficient perquè existeixi un morfisme de grups  $\bar{f} : G/N \rightarrow H$  tal que  $f = \bar{f} \circ \pi$  és que  $N \subseteq \text{Ker}(f)$ . A més a més, en aquest cas,  $\bar{f}$  és exhaustiu si, i només si, ho és  $f$ .  $\square$*

**Proposició A.1.35** (Segon teorema d'isomorfia de grups). *Siguin  $N \subseteq H \subseteq G$  subgrups normals d'un grup  $G$ . Llavors,  $N$  és un subgrup normal de  $H$ ,  $H/N \subseteq G/N$  és un subgrup normal de  $G/N$  i es té un isomorfisme canònic  $(G/N)/(H/N) \cong G/H$ .  $\square$*

**A.1.36.** Siguin  $G$  un grup i  $H, K \subseteq G$  subconjunts qualssevol. Es defineix el conjunt  $H \cdot K := \{h \cdot k : h \in H, k \in K\}$ . En general, encara que  $H$  i  $K$  siguin subgrups de  $G$ , el conjunt  $H \cdot K$  no és un subgrup de  $G$ . Però si  $H, K \subseteq G$  són subgrups i algun dels dos subgrups és normal, llavors  $H \cdot K = K \cdot H$  i és un subgrup de  $G$ ; i si tots dos són subgrups normals, llavors  $H \cdot K$  és un subgrup normal.

**Proposició A.1.37** (Tercer teorema d'isomorfia de grups). *Siguin  $G$  un grup,  $H, N \subseteq G$  subgrups de  $G$ , i suposem que  $N$  és un subgrup normal de  $G$ . Llavors,  $H \cdot N = N \cdot H \subseteq G$  és un subgrup,  $N \subseteq H \cdot N$  és un subgrup normal,  $N \cap H \subseteq H$  és un subgrup normal, i es té un isomorfisme canònic  $H \cdot N/N \cong H/(N \cap H)$ .  $\square$*

**Definició A.1.38.** Sigui  $G$  un grup qualsevol. Es defineix el *centre* de  $G$  com el subconjunt  $Z(G) := \{x \in G : \text{per a tot } y \in G \ xy = yx\}$ , dels elements que commuten amb tots els elements de  $G$ . És un subgrup normal de  $G$ .

**Definició A.1.39.** Sigui  $G$  un grup qualsevol. El *derivat* de  $G$  és el subgrup  $D(G) \subseteq G$  generat pels commutadors,  $[x, y] := xyx^{-1}y^{-1}$ ,  $x, y \in G$ .

**Proposició A.1.40.** *Per a tot grup  $G$ , el subgrup derivat de  $G$  és un subgrup normal de  $G$ , el grup quocient  $G/D(G)$  és commutatiu, i si  $H \subseteq G$  és un subgrup normal de  $G$  tal que  $G/H$  és commutatiu, llavors  $D(G) \subseteq H$ .  $\square$*

## A.1.6 Accions de grups en conjunts

**Definició A.1.41.** Siguin  $G$  un grup, que notem multiplicativament, i  $X$  un conjunt, qualssevol. Una *acció per l'esquerra* de  $G$  en  $X$  és una aplicació  $G \times X \rightarrow X$ , que denotem per  $(g, x) \mapsto gx$ , o per  $(g, x) \mapsto g \cdot x$ , per a la qual se satisfan les dues propietats següents.

- (a) Per a tot  $x \in X$  és  $1 \cdot x = x$ ;
- (b) Per a tot  $g, h \in G$  i tot  $x \in X$ , és  $g \cdot (h \cdot x) = (gh) \cdot x$ .

També es diu que  $G$  *opera per l'esquerra* en  $X$ , o que  $X$  és un  $G$ -*conjunt per l'esquerra*.

Una *acció per la dreta* de  $G$  en  $X$  és una aplicació  $G \times X \rightarrow X$ , que denotem per  $(g, x) \mapsto x^g$ , o per  $(g, x) \mapsto x \cdot g$ , per a la qual se satisfan les dues propietats següents.

- (a) Per a tot  $x \in X$  és  $x^1 = x$ ;
- (b) Per a tot  $g, h \in G$  i tot  $x \in X$ , és  $x^{gh} = (x^g)^h$ .

També es diu que  $G$  *opera per la dreta* en  $X$ , o que  $X$  és un  $G$ -*conjunt per la dreta*.

**Observació A.1.42.** Notem la diferència entre les dues nocions: quan un producte  $gh$ ,  $g, h \in G$ , actua per l'esquerra, primer ho fa  $h$  i després ho fa  $g$ ; mentre que si l'acció és per la dreta, primer actua  $g$  i després actua  $h$ .

**Exemple A.1.43.** Sigui  $X = \{x_1, \dots, x_n\}$  un conjunt finit de cardinal  $n$ . El grup simètric  $S_n$ , de les permutacions de  $\{1, \dots, n\}$ , actua (per l'esquerra) de manera natural en  $X$  per  $(\sigma, x_k) \mapsto x_{\sigma(k)}$ .

**A.1.44** (Morfisme associat a una acció). Siguin  $G$  un grup,  $X$  un conjunt, qualssevol, i  $G \times X \rightarrow X$  una acció per l'esquerra de  $G$  en  $X$ . Denotem per  $S_X$  el grup de les permutacions de  $X$ ; és a dir, el grup de les aplicacions bijectives de  $X$  en  $X$ .

Podem associar a l'acció una aplicació  $\sigma : G \rightarrow S_X$  de manera que a cada  $g \in G$  li fem correspondre l'aplicació  $\sigma_g : X \rightarrow X$  donada per  $x \mapsto g \cdot x$ . Llavors,  $\sigma$  és un morfisme de grups.

Recíprocament, si  $\sigma : G \rightarrow S_X$  és un morfisme de grups, l'aplicació  $G \times X \rightarrow X$  donada per  $(g, x) \mapsto \sigma(g)(x)$ , és una acció de  $G$  en  $X$ .

A més a més, el morfisme es recupera a partir de l'acció, i recíprocament; així, és equivalent parlar d'accions per l'esquerra de  $G$  en  $X$  o de morfismes de grups de  $G$  en  $S_X$ .

**A.1.45.** Si volem fer el mateix amb accions per la dreta, l'aplicació  $g \mapsto \sigma_g$ , on  $\sigma_g(x) := x^g$ , no seria un morfisme de grups, sinó un antimorfisme. Ara bé, podem considerar l'aplicació definida per  $\sigma_g(x) := x^{g^{-1}}$ , i llavors tenim un morfisme de grups.

En particular, donada una acció per l'esquerra  $(g, x) \mapsto g \cdot x$ , l'aplicació donada per  $(g, x) \mapsto g^{-1} \cdot x$  és una acció per la dreta. I, recíprocament, donada una acció per la dreta  $(g, x) \mapsto x^g$ , l'aplicació donada per  $(g, x) \mapsto x^{g^{-1}}$  és una acció per l'esquerra. Per tant, l'estudi de les accions per la dreta és equivalent a l'estudi de les accions per l'esquerra.

**Definició A.1.46.** Siguin  $G$  un grup i  $X$  un conjunt, qualssevol. Una acció  $G \times X \rightarrow X$  s'anomena *fidel*, o bé es diu que  $G$  actua *fidelment* en  $X$  si el morfisme associat de grups  $G \rightarrow S_X$  és injectiu.

**Proposició A.1.47.** *Sigui  $G \rightarrow S(C)$  una acció d'un grup  $G$  en un conjunt  $C$ . Llavors (cf. la definició 5.6.7):*

- Dues òrbites que es tallen, coincideixen.*
- El conjunt  $C$  és reunió disjunta d'òrbites.*
- El cardinal d'una òrbita coincideix amb l'índex del subgrup d'isotropia de qualsevol element de l'òrbita.*
- Els grups d'isotropia són conjugats; més concretament, per a tot element  $\sigma \in G$  i tot element  $x \in C$  és  $G_{\sigma \cdot x} = \sigma G_x \sigma^{-1}$ , si l'acció ho és per l'esquerra, i  $G_{x^\sigma} = \sigma^{-1} G_x \sigma$ , si l'acció ho és per la dreta.*
- Si  $R$  designa un conjunt de representants de les òrbites (és a dir, un conjunt que conté exactament un element de cada òrbita), se satisfà la fórmula de les òrbites:*

$$\#C = \sum_{x \in R} [G : G_x],$$

on  $[G : G_x]$  és l'índex del grup d'isotropia de  $x$  en  $G$ .  $\square$

## A.2 Anells

### A.2.1 Anells

**Definició A.2.1.** Un *anell*  $A$  és un conjunt amb dues operacions, suma i producte, de manera que  $(A, +)$  és un grup commutatiu, l'element neutre del qual designem per  $0$ , i el

producte és associatiu, té neutre, anomenat unitat i que designem per 1, i és distributiu respecte de la suma. Si, a més a més, el producte és commutatiu, es parla d'un *anell commutatiu*.

**A.2.2.** Així, un anell és un conjunt no buit  $A$  (conté elements neutres), amb dues operacions per a les quals se satisfan les propietats següents.

- (a) Associativa de la suma: per a tot  $a, b, c \in A$  és  $a + (b + c) = (a + b) + c$ .
- (b) Existència d'element neutre per a la suma: existeix  $0 \in A$  tal que per a tot  $a \in A$  és  $a + 0 = a = 0 + a$ ; l'element 0 és únic i s'anomena *l'element zero* de  $A$ .
- (c) Tot element té invers per a la suma: per a tot element  $a \in A$  existeix  $b \in A$  tal que  $a + b = 0 = b + a$ . Per a cada element  $a \in A$ , aquest element  $b$  és únic, s'anomena *l'element oposat de  $a$* , i s'escriu  $b =: -a$ .
- (d) Commutativa de la suma: per a tot  $a, b \in A$  és  $a + b = b + a$ .
- (e) Associativa del producte: per a tot  $a, b, c \in A$  és  $a(bc) = (ab)c$ .
- (f) Existència d'element neutre per al producte: existeix  $1 \in A$  tal que per a tot  $a \in A$  és  $a1 = a = 1a$ ; l'element 1 és únic i s'anomena *l'element unitat* de  $A$ .
- (g) Distributives: per a tot  $a, b, c \in A$ , és  $a(b + c) = ab + ac$  i  $(a + b)c = ac + bc$ .

Un anell es diu que és *commutatiu* si, a més a més, se satisfà la propietat

- (h) Commutativa del producte: per a tot  $a, b \in A$  és  $ab = ba$ .

**Observació A.2.3.** Formalment, i de manera similar al cas dels grups, podríem haver definit un anell com un conjunt amb dues operacions binàries,  $+$  i  $\cdot$ , dues 0-àries, 0 i 1, i una 1-ària,  $-$ , de manera que se satisfacin els axiomes anteriors. En particular, l'existència d'operacions 0-àries ja implica que el conjunt és no buit.

**A.2.4.** En particular, un anell és un conjunt no buit (conté els elements neutres per a la suma i el producte), però pot ésser reduït al conjunt  $\{0\}$ ; en efecte, en un conjunt d'un sol element només podem definir les operacions d'una manera, se satisfan els axiomes d'anell (commutatiu), i  $1 = 0$ . Aquest anell s'anomena *l'anell zero* o *anell trivial*.

**A.2.5.** Notem que si  $A$  és un anell i  $a \in A$ , llavors  $a0 + a0 = a(0 + 0) = a0 = a0 + 0$ , de manera que  $a0 = 0$ . Anàlogament, per a tot  $a \in A$ , és  $0a = 0$ .

**A.2.6.** I si en un anell  $A$  és  $1 = 0$ , llavors  $A$  és l'anell  $A = \{0\}$ . En efecte, per a tot  $a \in A$  és  $a = 1a = 0a = 0$ .

**A.2.7.** Com a exemples bàsics d'anells, podem considerar l'anell dels nombres enters,  $\mathbb{Z}$ , els anells de classes de residus,  $\mathbb{Z}/n\mathbb{Z}$  (cf. **A.3.12** per a la definició de l'anell quocient en general), que són commutatius, i els anells de matrius de coeficients enters, racionals, reals o complexos,  $\mathbf{M}(n, \mathbb{Z})$ ,  $\mathbf{M}(n, \mathbb{Q})$ ,  $\mathbf{M}(n, \mathbb{R})$ ,  $\mathbf{M}(n, \mathbb{C})$ , que no són commutatius per a  $n \geq 2$ . Notem que  $\mathbb{Z}/1\mathbb{Z}$  és l'anell  $\{0\}$ .

## A.2.2 Morfismes d'anell

**Definició A.2.8.** Donats anells  $A, B$ , un *morfisme d'anells* de  $A$  en  $B$  és una aplicació  $f : A \rightarrow B$  tal que per a tota parella d'elements  $a, b \in A$ ,  $f(a + b) = f(a) + f(b)$ ,  $f(ab) = f(a)f(b)$ , i  $f(1) = 1$ .

**A.2.9.** En particular, un morfisme d'anells és un morfisme de grups entre els grups abelians additius corresponents. En particular, les condicions  $f(0) = 0$  i  $f(-a) = -f(a)$  es dedueixen de la primera i dels axiomes d'anell. Però no succeeix el mateix per a la condició  $f(1) = 1$ ; cal imposar-la.

**A.2.10.** Per a tot anell  $A$ , l'aplicació identitat de  $A$ ,  $\text{id}_A : A \rightarrow A$ , donada per  $a \mapsto a$ , és un morfisme d'anells; s'anomena el *morfisme identitat* de  $A$ .

**A.2.11.** La composició de morfismes d'anells és un morfisme d'anells; és a dir, si  $A, A'$  i  $A''$  són anells, i  $f : A' \rightarrow A$ ,  $g : A \rightarrow A''$  són morfismes d'anells, llavors l'aplicació composició  $g \circ f : A' \rightarrow A''$ , donada per l'assignació  $a \mapsto g(f(a))$ , és un morfisme d'anells. S'anomena el *morfisme composició* de  $f$  i  $g$ .

**Definició A.2.12.** Un morfisme d'anells  $A \xrightarrow{f} B$  és un *isomorfisme* si, i només si, admet un morfisme invers; és a dir, si existeix un morfisme d'anells  $B \xrightarrow{g} A$  tal que  $g \circ f = \text{id}_A$  i  $f \circ g = \text{id}_B$ . Un isomorfisme d'anells  $f : A \rightarrow A$  s'anomena un *automorfisme*.

**A.2.13.** Per a tot anell  $A$ , la identitat de  $A$ ,  $\text{id} : A \rightarrow A$ , és un automorfisme d'anells.

**A.2.14.** La composició d'isomorfismes d'anells és un isomorfisme d'anells; és a dir, si  $A, A'$  i  $A''$  són anells, i  $f : A' \rightarrow A$ ,  $g : A \rightarrow A''$  són isomorfismes d'anells, llavors l'aplicació composició  $g \circ f : A' \rightarrow A''$  és un isomorfisme d'anells.

**Proposició A.2.15.** *Els isomorfismes d'anells coincideixen amb els morfismes d'anells que, com a aplicacions entre conjunts, són aplicacions bijectives.*  $\square$

**Definició A.2.16.** El conjunt dels automorfismes d'un anell  $A$ , amb la composició com a operació binària i la identitat com a element neutre, és un grup: el *grup dels automorfismes* de  $A$ ; s'escriu  $\text{Aut}(A)$ .

## A.2.3 Subanells

**Definició A.2.17.** Sigui  $A$  un anell. Un *subanell* de  $A$  és un subconjunt  $B \subseteq A$  al qual es poden restringir *totes* les operacions de l'anell; és a dir, és un subconjunt tal que  $0, 1 \in B$ , per a tot  $a, b \in B$  és  $a + b \in B$  i  $ab \in B$ , i per a tot  $a \in B$  és  $-a \in B$ .

**A.2.18.** Aquestes condicions impliquen que les operacions de  $A$  es poden restringir a  $B$ ; llavors, els axiomes d'anell se satisfan immediatament, perquè imposen que  $1 \in B$ . Així,  $B$  també és un anell. I si  $A$  és commutatiu, llavors  $B$  és commutatiu; però  $B$  pot ésser commutatiu sense que  $A$  ho sigui.

**A.2.19.** En particular,  $A$  és un subanell de  $A$ ; però si  $A \neq \{0\}$ , llavors  $\{0\}$  no és un subanell de  $A$ .

**A.2.20.** Els subanells d'un anell  $A$  són exactament les imatges dels morfismes d'anells  $B \rightarrow A$ , per a tots els anells  $B$  per als quals n'existeixi algun.

**A.2.21.** Si  $A$  és un anell i  $\{B_i\}_{i \in I}$  és una família no buida de subanells  $B_i \subseteq A$ , la intersecció  $\bigcap_{i \in I} B_i \subseteq A$  és un subanell de  $A$ .

**Definició A.2.22.** Si  $A$  és un anell qualsevol, el *centre* de  $A$  és el subanell format per tots els elements  $a \in A$  tals que per a tot element  $b \in A$  és  $ab = ba$ .

**A.2.23.** Si  $B \subseteq A$  és un subanell d'un anell  $A$ , l'aplicació d'inclusió  $B \rightarrow A$ , donada per  $a \mapsto a$ , és un morfisme injectiu d'anells.

**Observació A.2.24.** Si  $f : A \rightarrow B$  és un morfisme d'anells, llavors el *nucli* de  $f$ ,  $\ker f := \{a \in A : f(a) = 0\}$ , és un subgrup additiu de  $A$ , però, si  $A \neq \{0\}$ , no és pas un subanell, llevat que sigui  $B = \{0\}$ , en què  $\ker f = A$ . En canvi, la *imatge* de  $f$ ,  $\operatorname{im} f := f(A)$ , és un subanell de  $B$ , llevat que siguin  $A = \{0\}$  i  $B \neq \{0\}$ .

**A.2.25.** Més generalment, si  $f : A \rightarrow B$  és un morfisme d'anells, i  $A' \subseteq A$  és un subanell de  $A$ , llavors  $f(A') \subseteq B$  és un subanell de  $B$ . I si  $B' \subseteq B$  és un subanell de  $B$ , llavors  $f^{-1}(B') \subseteq A$  és un subanell de  $A$ .

**A.2.26.** Sigui  $f : A \rightarrow B$  és un morfisme d'anells. Es té que  $f$  és injectiu si, i només si,  $\ker f = \{0\}$ ; és a dir, si, i només si,  $\ker f$  és el subgrup (additiu) trivial de  $A$ . I, òbviament,  $f$  és exhaustiu si, i només si,  $\operatorname{im} f = B$ ; és a dir, si, i només si,  $\operatorname{im} f$  és el subanell total de  $B$ .

## A.2.4 Elements invertibles. Cossos

**Definició A.2.27.** Donat un anell  $A$ , un element  $a \in A$  s'anomena *invertible*, o també es diu que  $a$  és una *unitat* de  $A$ , si existeix un element  $b \in A$  tal que  $ab = ba = 1$ .

**Definició A.2.28.** Un anell commutatiu  $k$  s'anomena un *cos* si  $0 \neq 1$  i tot element no nul de  $k$  és invertible.

**Observació A.2.29.** Notem que a la definició de cos demanem que l'anell sigui commutatiu; si no se satisfà la commutativitat, parlem d'*àlgebres de divisió* o de *cossos no-commutatius*.

**A.2.30.** Com a exemples bàsics de cossos, podem considerar, per exemple, els cossos dels nombres racionals,  $\mathbb{Q}$ , dels nombres reals,  $\mathbb{R}$ , dels nombres complexos,  $\mathbb{C}$ , i els cossos  $\mathbb{Z}/p\mathbb{Z}$ , on  $p$  és un nombre enter primer qualsevol.

## A.2.5 Divisors de zero. Dominis d'integritat

**Definició A.2.31.** Sigui  $k$  un anell commutatiu. Un element  $a \in k$  s'anomena un *divisor de zero* si existeix un element  $b \in k$ ,  $b \neq 0$ , tal que  $ab = 0$ .

**A.2.32.** Si l'anell  $k$  és diferent de l'anell  $\{0\}$ , l'element  $0$  és un divisor de zero.

**Definició A.2.33.** Un *domini d'integritat* és un anell commutatiu  $k$  tal que  $1 \neq 0$  i que no té cap més divisor de zero que  $0$ .



**A.2.34.** L'anell  $\mathbb{Z}$  dels nombres enters és un domini d'integritat; en efecte, si  $m, n$  són nombres enters diferents de zero, el seu producte és un nombre enter diferent de zero; per tant, l'únic nombre enter divisor de zero és 0.

**A.2.35.** D'altra banda, per a un nombre enter  $n \geq 2$ , l'anell quocient  $\mathbb{Z}/n\mathbb{Z}$  (cf. **A.3.12**, més endavant, per a la definició de l'anell quocient) admet divisors de zero si, i només si,  $n$  és un nombre enter compost. En efecte, si  $n = ab$  és una descomposició de  $n$  com a producte de dos nombres enters  $a, b \notin \{0, 1, -1\}$ , llavors  $a$  i  $b$  són divisors de zero en  $\mathbb{Z}/n\mathbb{Z}$ . Amb tota generalitat, la classe mòdul  $n$  d'un nombre enter  $a$  és un divisor de zero en  $\mathbb{Z}/n\mathbb{Z}$  si, i només si,  $\text{mcd}(n, a) \neq 1$ .

**A.2.36.** Tot cos  $k$  és un domini d'integritat; en efecte, si  $a \in k$ ,  $a \neq 0$ , podem considerar l'invers  $b \in k$  de  $a$ , de manera que  $ab = 1$ . Ara, si per a un element  $z \in k$  és  $za = 0$ , tenim que  $0 = 0 \cdot b = zab = z \cdot 1 = z$ ; per tant, l'únic divisor de zero de  $k$  és 0.

**A.2.37.** Com a conseqüència, tot subanell d'un cos o d'un domini d'integritat és un domini d'integritat.

**A.2.38.** Recíprocament, tot domini d'integritat és subanell d'algun cos. En efecte, la construcció següent proporciona el *cos de fraccions d'un domini d'integritat*.

**A.2.39.** Sigui  $k$  un domini d'integritat. En el conjunt producte cartesià  $k \times (k - \{0\})$ , definim la relació

$$(a, b) \sim (c, d) \Leftrightarrow ad - cb = 0.$$

(a) La relació  $\sim$  és una relació d'equivalència per a la qual se satisfan les propietats

$$\begin{aligned} (a, b) \sim (a', b'), \quad (c, d) \sim (c', d') &\implies (ad + cb, bd) \sim (a'd' + c'b', b'd'), \\ (a, b) \sim (a', b'), \quad (c, d) \sim (c', d') &\implies (ac, bd) \sim (a'c', b'd'). \end{aligned}$$

Denotem per  $\frac{a}{b}$  la classe d'equivalència de la parella  $(a, b)$  i per  $K$  el conjunt de totes les classes d'equivalència. En  $K$ , podem definir les operacions suma i producte, per a  $a, b, c, d \in k$ ,  $b, d \neq 0$ , per les fórmules

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + cb}{bd}, \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd},$$

(b) El conjunt  $K$  amb aquestes operacions és un cos. El cos  $K$  s'anomena el *cos de fraccions* de  $k$ .

(c) L'aplicació  $k \rightarrow K$  definida per l'assignació  $a \mapsto \frac{a}{1}$  és un morfisme injectiu d'anells, de manera que podem identificar cada element  $a \in k$  amb la classe  $\frac{a}{1} \in K$  i l'anell  $k$  amb un subanell del cos  $K$ .

(d) Si  $f : k \rightarrow A$  és un morfisme d'anells tal que per a tot  $a \in k - \{0\}$  l'element  $f(a) \in A$  és invertible, llavors  $f$  s'estén de manera única a un morfisme d'anells  $K \rightarrow A$ , que és injectiu si  $A \neq \{0\}$ . Com a conseqüència,  $K$  és el més petit de tots els cossos que contenen  $k$  com a subanell.

## A.2.6 L'anell producte

**Definició A.2.40.** Sigui  $\{A_i\}_{i \in I}$  una família no buida d'anells. En el conjunt producte cartesià

$$A := \prod_{i \in I} A_i,$$

es defineixen la suma i el producte component a component; és a dir, per a elements  $\alpha := \{a_i\}_{i \in I}$ ,  $\beta := \{b_i\}_{i \in I} \in A$ , es defineix  $\alpha + \beta := \{a_i + b_i\}_{i \in I}$  i  $\alpha\beta := \{a_i b_i\}_{i \in I}$ . Llavors,  $A$  és un anell, l'element neutre del qual és la família  $0 = \{0\}_{i \in I}$  en què cada component és l'element neutre del grup commutatiu  $A_i$  corresponent, i l'element unitat del qual és la família  $1 = \{1\}_{i \in I}$  en què cada component és l'element unitat de l'anell  $A_i$  corresponent. L'anell  $A$  s'anomena l'*anell producte (cartesià)* de la família d'anells  $\{A_i\}_{i \in I}$ . Si tots els anells  $A_i$  són commutatius, llavors  $A$  és commutatiu. Si la família és finita; és a dir, si el conjunt  $I$  és finit, posem  $I = \{1, 2, \dots, n\}$ , s'escriu  $A = \prod_{i=1}^n A_i = A_1 \times A_2 \times \dots \times A_n$ .

**A.2.41.** Notem que si  $A, B$  són anells diferents de  $\{0\}$ , llavors  $A \times B$  no és un domini d'integritat. En efecte, els elements  $(1, 0), (0, 1) \in A \times B$  són diferents de 0 i el seu producte és 0. Més generalment, l'anell producte només és un domini d'integritat en el cas en què un dels anells  $A_i$  és un domini d'integritat i per a tot  $j \neq i$  és  $A_j = \{0\}$ .

**A.2.42.** Podem considerar les aplicacions naturals d'inclusió  $A_j \xrightarrow{\psi_j} \prod_{i \in I} A_i$ , definides per a  $j \in I$  per  $a_j \mapsto \{a_i\}_{i \in I}$ , on  $a_i = 0$  per a  $i \neq j$ . Les aplicacions  $\psi_j$ , encara que sempre són morfismes dels grups commutatius additius corresponents, només són morfismes d'anells en el cas en què tots els anells  $A_i$  o tots menys un són l'anell  $\{0\}$ . En general, doncs, no permeten identificar l'anell  $A_j$  amb cap subanell de l'anell producte.

**A.2.43.** Si, per a tot  $i \in I$ , és  $A_i = A$ , un anell donat, llavors s'escriu  $A^I := \prod_{i \in I} A$ . Podem considerar l'aplicació  $\psi : A \rightarrow A^I$  definida per  $a \mapsto \{a_i\}_{i \in I}$ , on  $a_i := a$ , per a tot  $i \in I$ . Llavors,  $\psi$  és un morfisme d'anells; s'anomena la inclusió diagonal de  $A$  en  $A^I$ .

## A.3 Ideals i anells quocient

### A.3.1 Ideals

**Definició A.3.1.** Un *ideal per l'esquerra* d'un anell  $A$  és un subgrup  $(\mathfrak{a}, +)$  tal que per a tot  $a \in \mathfrak{a}$  i tot  $\lambda \in A$  és  $\lambda a \in \mathfrak{a}$ . Un *ideal per la dreta* d'un anell  $A$  és un subgrup  $(\mathfrak{a}, +)$  tal que per a tot  $a \in \mathfrak{a}$  i tot  $\lambda \in A$  és  $a \lambda \in \mathfrak{a}$ . Un *ideal bilateral* d'un anell  $A$  és un subgrup  $(\mathfrak{a}, +)$  que és alhora un ideal per l'esquerra i un ideal per la dreta. S'anomenen *ideals* els ideals per l'esquerra, els ideals per la dreta i els ideals bilaterals.

**A.3.2.** Notem que si l'anell  $A$  és commutatiu, els conceptes d'ideal per l'esquerra i d'ideal per la dreta coincideixen, de manera que tots els ideals són ideals bilaterals.

**A.3.3.** Els *ideals trivials* d'un anell  $A$  són l'ideal total,  $A$ , i l'ideal nul,  $\{0\}$ ; són ideals bilaterals.

**A.3.4.** Sigui  $f : A \rightarrow B$  un morfisme qualsevol d'anells; llavors, el seu *nucli* és l'ideal bilateral de  $A$  definit per  $\ker(f) := \{a \in A : f(a) = 0\}$ .

**A.3.5.** Més generalment, si  $f : A \rightarrow B$  és un morfisme d'anells, i  $\mathfrak{b} \subseteq B$  és un ideal (per l'esquerra, per la dreta, o bilateral) de  $B$ , llavors  $f^{-1}(\mathfrak{b}) \subseteq A$  és un ideal (per l'esquerra, per la dreta, o bilateral, respectivament) de  $A$ . I si  $\mathfrak{a} \subseteq A$  és un ideal (per l'esquerra, per la dreta, o bilateral) de  $A$ , llavors  $f(\mathfrak{a}) \subseteq f(A)$  és un ideal (per l'esquerra, per la dreta, o bilateral, respectivament) de l'anell imatge, però no necessàriament un ideal de  $B$ .

**A.3.6.** Un anell commutatiu  $A$  és un cos si, i només si, els únics ideals de  $A$  són els trivials.

**A.3.7.** Si  $k$  és un cos i  $A$  és un anell diferent de  $\{0\}$ , tot morfisme d'anells  $k \rightarrow A$  és injectiu.

**A.3.8.** Si  $A$  és un anell i  $\{\mathfrak{a}_i\}_{i \in I}$  és una família no buida d'ideals (per l'esquerra, per la dreta, bilaterals)  $\mathfrak{a}_i \subseteq A$ , la intersecció  $\bigcap_{i \in I} \mathfrak{a}_i \subseteq A$  és un ideal (per l'esquerra, per la dreta, bilateral, respectivament) de  $A$ .

**Definició A.3.9.** Siguin  $A$  un anell i  $C \subseteq A$  un subconjunt qualsevol. L'*ideal* (per l'esquerra, per la dreta, bilateral) generat per  $C$  és la intersecció de tots els ideals (per l'esquerra, per la dreta, bilaterals, respectivament) de  $A$  que contenen el conjunt  $C$ .

**A.3.10.** Si  $C = \{a\}$ ,  $a \in A$ , és un conjunt d'un sol element, l'ideal per l'esquerra generat per  $C$  és l'ideal principal per l'esquerra  $Aa := \{\lambda a : \lambda \in A\}$ ; i l'ideal per la dreta generat per  $C$  és l'ideal principal per la dreta  $aA := \{a\lambda : \lambda \in A\}$ . L'ideal bilateral generat per  $C$  és el conjunt format pels elements de la forma  $\sum_{\lambda, \mu \in A} \lambda a \mu$ , on tots els elements  $\lambda, \mu \in A$ ,

llevat d'una quantitat finita, són 0.

**A.3.11.** Més generalment, per a un subconjunt qualsevol  $C \subseteq A$ , l'ideal per l'esquerra generat per  $C$  és el conjunt dels elements de la forma  $\sum_{c \in C} \lambda_c c$ , on  $\lambda_c \in A$  són tots 0, llevat d'una quantitat finita. Anàlogament, l'ideal per la dreta generat per  $C$  és el conjunt dels elements de la forma  $\sum_{c \in C} c \lambda_c$ , on  $\lambda_c \in A$  són tots 0, llevat d'una quantitat finita.

## A.3.2 Anells quotient

**Definició A.3.12.** Siguin  $A$  un anell i  $\mathfrak{a} \subseteq A$  un subgrup additiu. La condició que s'imposa a  $\mathfrak{a}$  perquè aquest subgrup sigui un ideal (bilateral) de  $A$  és exactament la condició que es necessita a fi que el grup abelià quotient  $(A/\mathfrak{a}, +)$  sigui un anell i el morfisme de projecció  $A \rightarrow A/\mathfrak{a}$ , donat per  $a \mapsto a + \mathfrak{a}$ , sigui un morfisme d'anells. D'aquesta manera s'obté l'*anell quotient* de  $A$  per l'ideal  $\mathfrak{a}$ . Si l'anell  $A$  és commutatiu, llavors l'anell quotient  $A/\mathfrak{a}$  també és commutatiu.

**A.3.13.** El morfisme de projecció  $A \rightarrow A/\mathfrak{a}$  permet definir una bijecció que respecta l'ordre donat per la inclusió d'ideals entre el conjunt dels ideals (per l'esquerra, per la dreta, bilaterals) de l'anell quotient  $A/\mathfrak{a}$  i el conjunt dels ideals (per l'esquerra, per la dreta, bilaterals, respectivament) de  $A$  que contenen  $\mathfrak{a}$ .

**A.3.14.** També se satisfà el *teorema d'isomorfia*: si  $f : A \rightarrow B$  és un morfisme d'anells, llavors l'assignació  $a + \ker f \mapsto f(a)$  defineix un isomorfisme entre l'anell quocient  $A/\ker(f)$  i l'anell imatge  $f(A)$ .

**A.3.15.** La bijecció entre el conjunt d'ideals de  $A/\mathfrak{a}$  i el conjunt d'ideals de  $A$  que contenen  $\mathfrak{a}$  que proporciona el morfisme de projecció  $A \rightarrow A/\mathfrak{a}$  respecta ideals primers i ideals maximals. És a dir, els ideals primers de  $A/\mathfrak{a}$  es corresponen amb els ideals primers de  $A$  que contenen  $\mathfrak{a}$ ; i el mateix fet succeeix per als ideals maximals (cf. **A.3.20** i **A.3.21** per a les definicions d'ideal primer i d'ideal maximal).

### A.3.3 Dominis d'ideals principals

**Definició A.3.16.** Sigui  $A$  un anell commutatiu. Per a tot element  $a \in A$ , el conjunt  $(a) := aA = Aa := \{\lambda a : \lambda \in A\}$  és un ideal de  $A$ ; s'anomena l'*ideal principal* generat per  $a$ .

**A.3.17.** Com que  $\{0\} = 0A$  i  $A = 1A$ , els ideals trivials són principals.

**Definició A.3.18.** Un *domini d'ideals principals*, o *domini principal*, és un domini d'integritat tal que tots els seus ideals són principals.

**Observació A.3.19.** No és cert que tot subanell d'un domini d'ideals principals sigui un domini d'ideals principals. Per exemple, l'anell de polinomis de coeficients racionals,  $\mathbb{Q}[X]$ , és un domini d'ideals principals, perquè  $\mathbb{Q}$  és un cos, mentre que l'anell de polinomis de coeficients enters,  $\mathbb{Z}[X]$ , que és un subanell de  $\mathbb{Q}[X]$ , no és un domini d'ideals principals; per exemple, perquè l'ideal format pels polinomis de terme constant parell, que es pot generar per  $2$  i  $X$ , no és principal.

### A.3.4 Ideals primers, maximals

**Definició A.3.20.** Sigui  $A$  un anell commutatiu. Un ideal  $\mathfrak{p} \subseteq A$  s'anomena *primer* si, i només si,  $\mathfrak{p} \neq A$  i per a  $a, b \in A$ ,  $a, b \notin \mathfrak{p}$  és  $ab \notin \mathfrak{p}$ .

**Definició A.3.21.** Sigui  $A$  un anell commutatiu. Un ideal  $\mathfrak{m} \subseteq A$  s'anomena *maximal* si, i només si,  $\mathfrak{m} \neq A$  i per a tot ideal  $I \subsetneq A$  tal que  $\mathfrak{m} \subseteq I$  és  $\mathfrak{m} = I$ .

**Exercici A.3.22.** Siguin  $A$  un anell commutatiu i  $\mathfrak{p} \subseteq A$  un ideal. Llavors:

- (a) L'ideal  $\mathfrak{p}$  és primer si, i només si, l'anell quocient  $A/\mathfrak{p}$  és un domini d'integritat.
- (b) L'ideal  $\mathfrak{p}$  és maximal si, i només si, l'anell quocient  $A/\mathfrak{p}$  és un cos.
- (c) Tot ideal maximal de  $A$  és un ideal primer.

### A.3.5 Característica d'un anell

**Observació A.3.23.** Sigui  $A$  un anell; llavors, existeix un únic morfisme d'anells  $\mathbb{Z} \rightarrow A$ .

En efecte, la imatge de  $1 \in \mathbb{Z}$  ha d'ésser  $1 \in A$  i, en conseqüència, la imatge de  $n = \overbrace{1 + \dots + 1}^n \in \mathbb{N}$  en  $A$  ha d'ésser  $n := \overbrace{1 + \dots + 1}^n \in A$  i la de  $-n$ ,  $n \in \mathbb{N}$ , ha d'ésser  $-n \in A$ . Així, només cal comprovar que les assignacions  $n \mapsto n \in A$ ,  $-n \mapsto -n \in A$ , per a  $n \in \mathbb{N}$ , defineixen un morfisme d'anells; i aquesta comprovació és rutinària.

**Definició A.3.24.** Sigui  $A$  qualsevol anell. El nucli de l'únic morfisme d'anells  $\mathbb{Z} \rightarrow A$  és un ideal de  $\mathbb{Z}$  que, com que  $\mathbb{Z}$  és un domini d'ideals principals, és de la forma  $c\mathbb{Z}$ , per a un nombre enter  $c \in \mathbb{Z}$ , que podem triar de manera que sigui  $c \geq 0$  i que, llavors, és únic. Aquest nombre enter  $c$  s'anomena la *característica* de l'anell  $A$ ; s'acostuma a escriure  $c := \text{car}(A)$ . O sigui, la característica d'un anell  $A$  és el generador no negatiu del nucli de l'únic morfisme d'anells de  $\mathbb{Z}$  en  $A$ .

**A.3.25.** En particular, els anells de característica 0 són els anells que contenen un subanell isomorf a  $\mathbb{Z}$ . En general, el teorema d'isomorfia ens assegura que  $A$  conté un subanell isomorf a  $\mathbb{Z}/c\mathbb{Z}$ , on  $c$  és la característica de  $A$ .

**A.3.26.** Sigui  $A$  un anell de característica  $c > 0$ . Llavors,  $c$  és el menor nombre natural no nul tal que  $c := \overbrace{1 + \dots + 1}^c = 0$  en  $A$ . Si  $A$  és de característica 0, llavors per a tot nombre natural  $c > 0$  és  $c := \overbrace{1 + \dots + 1}^c \neq 0$  en  $A$ .

**A.3.27.** Notem que si la característica d'un anell és un nombre compost  $c = mn$ , amb  $m, n \in \mathbb{N}$ ,  $m, n > 1$ , els elements  $m, n \in A$  són divisors de zero diferents de zero. Per tant, recíprocament, si  $A$  és un domini d'integritat, la seva característica és, o bé 0 o bé un nombre primer  $p$ .

**A.3.28.** Si  $B \subseteq A$  és un subanell, llavors  $\text{car}(B) = \text{car}(A)$ .

**A.3.29.** Si  $f : A \rightarrow B$  és un morfisme d'anells, llavors  $\text{car}(A)$  és un múltiple de  $\text{car}(B)$ .

**A.3.30.** Per a un producte,  $A = \prod_{i \in I} A_i$ , d'una família no buida d'anells,  $\{A_i\}_{i \in I}$ ,  $I \neq \emptyset$ , es té que  $\text{car}(A) = \text{mcm}\{\text{car}(A_i) : i \in I\}$ , el mínim comú múltiple de les característiques dels anells factors.

## A.4 Mòduls i àlgebres

### A.4.1 Mòduls

Tot i que la teoria de mòduls es pot fer sobre anells no commutatius, i el seu estudi és important en diferents branques de la matemàtica, ens limitarem a fer un resum de la teoria bàsica de mòduls sobre anells commutatius. Això ens evitarà la necessitat de parlar de mòduls per l'esquerra, o de mòduls per la dreta, o de mòduls bilaterals, o de bimòduls, i serà suficient per als propòsits del text principal.

**Definició A.4.1.** Sigui  $k$  un anell commutatiu. Un *k-mòdul* és un grup abelià  $M$  per al qual hi ha una acció  $k \times M \rightarrow M$ , que escriurem per juxtaposició,  $(\lambda, x) \mapsto \lambda x$ , tal que per a tot  $\lambda, \mu \in k$  i tot  $x, y \in M$  és

- (a)  $\lambda(x + y) = \lambda x + \lambda y$ ,
- (b)  $(\lambda + \mu)x = \lambda x + \mu x$ ,
- (c)  $(\lambda \cdot \mu)x = \lambda(\mu x)$ ,
- (d)  $1x = x$ ,

on 1 és l'element unitat de l'anell  $k$ . En particular, com que  $M$  conté un element neutre per a la suma,  $M \neq \emptyset$ . Si  $k$  és un cos, els  $k$ -mòduls s'acostumen a anomenar *espais vectorials sobre  $k$* , o també  *$k$ -espais vectorials*.

**A.4.2.** És una conseqüència immediata dels axiomes anteriors que per a tot  $\lambda \in k$  i tot  $x \in M$  és  $\lambda 0 = 0$ ,  $\lambda(-x) = -\lambda x$ ,  $0x = 0$ ,  $(-\lambda)x = -\lambda x$ . Notem que, en aquestes propietats, 0 pot ser l'element neutre de la suma de  $M$  o l'element neutre de la suma de  $k$ , i que el signe  $-$  serveix per a indicar els oposats per a les sumes, tant de  $M$  com de  $k$ . El context permet, en cada moment, distingir-los. Per exemple, en la igualtat  $0x = 0$ , l'element 0 que actua sobre  $x \in M$  només pot ser l'element neutre de la suma de  $k$ , mentre que l'element 0 del costat dret de la igualtat només pot ser l'element neutre de la suma de  $M$ .

**Definició A.4.3.** Siguin  $k$  un anell commutatiu i  $M$  un  $k$ -mòdul. Un  *$k$ -submòdul* de  $M$  (o, també, un *sub- $k$ -mòdul* de  $M$ ) és un subgrup  $N \subseteq M$  al qual restringeix l'acció de  $k$ ; és a dir, un subgrup tal que per a tot  $\lambda \in k$  i tot  $x \in N$  és  $\lambda x \in N$ . En aquesta situació, se satisfan els axiomes anteriors, de manera que  $N$  és un  $k$ -mòdul.

**Observació A.4.4.** En particular, el mateix anell  $k$  és, de manera natural, un  $k$ -mòdul; els ideals de  $k$  són exactament els  $k$ -submòduls de  $k$ .

**Definició A.4.5.** Siguin  $k$  un anell commutatiu i considerem  $k$ -mòduls  $M, N$ . Un *morfisme de  $k$ -mòduls*, o també una *aplicació  $k$ -lineal*, de  $M$  en  $N$  és una aplicació  $f : M \rightarrow N$  tal que per a tot  $\lambda, \mu \in k$  i tot  $x, y \in M$  és  $f(\lambda x + \mu y) = \lambda f(x) + \mu f(y)$ . De fet, això és equivalent a dir que és un morfisme de grups abelians ( $f(x + y) = f(x) + f(y)$ ) que respecta l'acció de l'anell  $k$  ( $f(\lambda x) = \lambda f(x)$ ).

**Definició A.4.6.** Si  $N \subseteq M$  és un  $k$ -submòdul, en particular també és un subgrup del grup abelià  $M$ ; per tant, té sentit considerar el grup abelià quocient  $M/N$ . I el fet que  $N$  sigui un  $k$ -submòdul fa que l'acció de  $k$  sigui compatible amb aquest pas al quocient; és a dir, que si, per a  $x, y \in M$ , és  $x + N = y + N$ , llavors per a tot  $\lambda \in k$  és  $\lambda x + N = \lambda y + N$ . Per tant, de manera natural,  $M/N$  esdevé un  $k$ -mòdul. S'anomena el  *$k$ -mòdul quocient* de  $M$  per  $N$ . La *projeció canònica*,  $\pi : M \rightarrow M/N$ , donada per  $\pi(x) := x + N$ , és una aplicació lineal.

**A.4.7.** Si  $f : M \rightarrow N$  és una aplicació lineal entre  $k$ -mòduls, en particular és un morfisme de grups abelians, de manera que té sentit parlar del nucli de  $f$  i de la imatge de  $f$ . Es té  $\ker f \subseteq M$ , és un  $k$ -submòdul de  $M$  i que  $\operatorname{im} f = f(M) \subseteq N$ , és un  $k$ -submòdul de  $N$ .

**Proposició A.4.8** (Primer teorema d'isomorfia per a  $k$ -mòduls). *Siguin  $k$  un anell commutatiu i  $f : M \rightarrow N$  una aplicació lineal entre  $k$ -mòduls. L'isomorfisme canònic de grups abelians  $\bar{f} : M/\ker f \rightarrow \operatorname{im} f$ , donat per l'assignació  $x + \ker f \mapsto f(x)$ , també ho és*

de  $k$ -mòduls, i la descomposició canònica del morfisme  $f$  com a composició de morfismes de grups abelians,

$$\begin{array}{ccc} M & \xrightarrow{f} & N \\ \pi \downarrow & & \uparrow \text{inc} \\ M/\ker f & \xrightarrow{\bar{f}} & \text{im } f. \end{array}$$

ho és com a morfismes de  $k$ -mòduls.

### A.4.2 Àlgebres

**Definició A.4.9.** Sigui  $k$  un anell commutatiu. Una  $k$ -àlgebra (associativa) és un  $k$ -mòdul  $A$  per al qual hi ha un producte  $\circ : A \times A \rightarrow A$ , associatiu, distributiu respecte de la suma de  $A$ , i tal que per a tot  $\lambda \in k$  i tota parella d'elements  $x, y \in A$  se satisfà que  $(\lambda x) \circ y = \lambda(x \circ y) = x \circ (\lambda y)$ . Si, a més a més,  $A$  conté un element neutre,  $1$ , per a aquest producte, parlem d'una  $k$ -àlgebra unitària; i si el producte és commutatiu, parlem d'una  $k$ -àlgebra commutativa.

**Observació A.4.10.** El concepte general de  $k$ -àlgebra és més ampli, i aquí ens limitem al de  $k$ -àlgebra associativa; a més a més, només considerarem  $k$ -àlgebres unitàries i, sovint, commutatives. En general, però, i per a la persona interessada en el tema, diguem que una  $k$ -àlgebra és un  $k$ -mòdul,  $A$ , amb un producte  $k$ -bilineal,  $\circ : A \times A \rightarrow A$ . La  $k$ -bilinealitat del producte és la compatibilitat que es demana amb l'estructura de  $k$ -mòdul.

**A.4.11.** Com a exemples importants de  $k$ -àlgebres, mencionem la  $k$ -àlgebra  $k[X]$  dels polinomis en una indeterminada i coeficients en  $k$  (cf. **1.1.6**), o la  $k$ -àlgebra  $\mathbf{M}(n, k)$  de les matrius  $n \times n$  de coeficients en  $k$ , o la  $k$ -àlgebra  $\text{End}_k(E)$  dels endomorfismes d'un  $k$ -mòdul  $E$ . En general, donada una extensió qualsevol de cossos,  $K|k$  (cf. **3.4.2**), el cos  $K$  és, de manera natural, una  $k$ -àlgebra (associativa, commutativa i unitària). I, més generalment, encara, tot anell  $A$  és una  $\mathbb{Z}$ -àlgebra associativa i unitària, que és commutativa si  $A$  és un anell commutatiu.

**A.4.12.** Sigui  $k$  un anell commutatiu i considerem  $k$ -àlgebres  $A, B$ . Un morfisme de  $k$ -àlgebres és una aplicació  $f : A \rightarrow B$  que és  $k$ -lineal i que és morfisme per al producte; és a dir, tal que per a tot  $a, b \in A$ , i tot  $\lambda, \mu \in k$ , és  $f(\lambda a + \mu b) = \lambda f(a) + \mu f(b)$ , i  $f(a \circ b) = f(a) \circ f(b)$ .

Si  $A, B$  són  $k$ -àlgebres unitàries, un morfisme de  $k$ -àlgebres unitàries és un morfisme de  $k$ -àlgebres tal que  $f(1) = 1$ .

**Definició A.4.13.** Sigui  $k$  un anell commutatiu i  $A$  una  $k$ -àlgebra. Una  $k$ -subàlgebra de  $A$  és un  $k$ -submòdul  $B \subseteq A$  tal que per a tot  $a, b \in B$  és  $a \circ b \in B$ ; és a dir, un  $k$ -submòdul estable pel producte bilineal. Si  $A$  és unitària, una  $k$ -subàlgebra unitària és una  $k$ -subàlgebra que conté l'element unitat de  $A$ .

**Observació A.4.14.** Si  $k$  és un anell commutatiu, sovint considerem  $k$ -àlgebres associatives, unitàries i commutatives. Això és dir  $k$ -mòduls que, alhora, són anells, i que les estructures són compatibles. En particular, si tenim morfismes de  $k$ -àlgebres associatives i unitàries, tenim morfismes de  $k$ -mòduls i, alhora, d'anells. Per tant, els nuclis són  $k$ -submòduls i, alhora, ideals, de manera que el  $k$ -mòdul quocient també és un anell i podem parlar de la  $k$ -àlgebra quocient. I se satisfà el primer teorema d'isomorfia per a l'estructura de  $k$ -àlgebra associativa i unitària. No ens entretenim en els detalls.

**Observació A.4.15.** Siguin  $k$  un anell commutatiu i  $A$  una  $k$ -àlgebra associativa i unitària. Existeix un únic morfisme de  $k$ -àlgebres  $f : k \rightarrow A$ , ja que la imatge de  $1 \in k$  ha de ser  $1 \in A$  i, per a tot  $\lambda \in k$ , la imatge de  $\lambda = \lambda \cdot 1$  ha de ser  $f(\lambda) = \lambda f(1)$ , de manera que és determinada unívocament. Llavors, la imatge d'aquest morfisme,  $f(k)$ , és un subanell del centre de  $A$  que, alhora, és un  $k$ -mòdul (i una  $k$ -àlgebra). En particular, tenim que  $A$  és una  $f(k)$ -àlgebra associativa i unitària, i que  $f(k) \subseteq A$ . En particular, podem pensar tota àlgebra associativa i unitària com una àlgebra sobre un subanell del seu centre.

**Observació A.4.16.** Si  $k$  és un anell commutatiu i  $A$  és una  $k$ -àlgebra associativa i unitària, podem parlar del grup dels automorfismes de  $A$  com a  $k$ -àlgebra. Sovint s'anomenen *k-automorfismes*. Notem que són els automorfismes,  $\sigma$ , de  $A$  tals que per a tot  $\lambda \in k$  és  $\sigma(\lambda) = \lambda 1$ . i si  $k \subseteq A$ ,  $\lambda 1 = \lambda$ , de manera que són els automorfismes,  $\sigma$ , de  $A$  tals que per a tot  $\lambda \in k$  és  $\sigma(\lambda) = \lambda$ ; si es vol, els automorfismes de  $A$  que, restringits a  $k \cdot 1 \subseteq A$  són la identitat.



# Apèndix B

## El lema de Zorn

Algunes vegades, els axiomes usuals de la teoria de conjunts (per exemple, els axiomes de Zermelo–Fraenkel) no són suficients per a explicar propietats interessants de les diferents teories; cal usar un altre axioma: l'axioma de l'elecció.

Aquest axioma **sembla** tan evident que, molt sovint, pot passar desapercebut. Una de les maneres equivalents de formular-lo és la següent.

**B.0.17 (Axioma de l'elecció).** El producte cartesià d'una família no buida de conjunts no buits és un conjunt no buit.

**Observació B.0.18.** Així, donada una família no buida de conjunts no buits, podem considerar alhora un element de cadascun dels conjunts. En efecte, un element del producte cartesià és una família d'elements, un de cadascun dels conjunts de la família. Per això se l'anomena una *funció d'elecció*.

Formulat d'aquesta manera, sembla que, efectivament, aquest axioma hauria d'ésser acceptat sense discussió. (Podem estar segurs que no l'hem usat implícitament alguna vegada?) En canvi, és equivalent, per exemple, a la propietat següent, no tan evident.

**B.0.19 (Teorema de Zermelo).** Sigui  $C$  un conjunt no buit qualsevol. Existeix en  $C$  una relació de bon ordre.

**Observació B.0.20.** Donat un conjunt qualsevol,  $C$ , una relació d'ordre  $\leq$  en  $C$  es diu que és un *bon ordre* si, i només si, tot subconjunt no buit de  $C$  té un *primer element*; és a dir, si per a tot subconjunt  $D \subseteq C$ ,  $D \neq \emptyset$ , existeix un element  $a \in D$  tal que  $a \leq b$ , per a tot  $b \in D$ .

A primer cop d'ull, la formulació del teorema de Zermelo també pot semblar evident; però hom pot pensar en l'exemple següent. Donat un conjunt infinit no numerable  $C$ , sigui  $\leq$  un bon ordre en  $C$ . Sigui  $a_1 \in C$  el primer element de  $C_1 := C$  i  $C_2 := C - \{a_1\}$ . A continuació, prenem  $a_2$  el primer element de  $C_2$  i sigui  $C_3 := C_2 - \{a_2\}$ . I així, successivament. Podem procedir d'aquesta manera i formar una successió (numerable) d'elements de  $C$ . Ara bé, què succeeix amb els elements que “continuen” després de la successió? Com els podem veure ordenats? Quin és el primer element “després” de la successió? Ja no sembla tan clar.

**Observació B.0.21.** Les preguntes anteriors es poden contestar, d'una manera completament satisfactòria però que ens portaria massa lluny per als objectius d'aquest text expositori, amb la teoria dels ordinals i dels cardinals, i l'ús de l'axioma de l'elecció!

No és el nostre objectiu provar, en aquest curs, l'equivalència de l'axioma de l'elecció i el teorema de Zermelo. Ni, tampoc, la seva equivalència amb el lema de Zorn que, de fet, serà la formulació equivalent de l'axioma de l'elecció que més utilitzarem en el curs. Comencem amb algunes definicions prèvies.

**Definició B.0.22.** Sigui  $C$  un conjunt ordenat per una relació d'ordre  $\leq$ ; és a dir, una relació reflexiva, transitiva i antisimètrica. Es diu que l'ordre de  $C$  és *inductiu* si, i només si, tot subconjunt totalment ordenat  $D \subseteq C$  té una fita superior (en  $C$ ); és a dir, per a tot subconjunt  $D \subseteq C$  per al qual se satisfà la condició d'ordre total (donats  $a, b \in D$ , és  $a \leq b$  o bé  $b \leq a$ ), existeix un element  $c \in C$  tal que  $a \leq c$ , per a tot  $a \in D$ .

**B.0.23 (Lema de Zorn).** Sigui  $C$  un conjunt ordenat per un ordre  $\leq$ . Si l'ordre de  $C$  és inductiu,  $C$  conté elements maximals.

Conseqüències importants del lema de Zorn (moltes d'elles, de fet, li són equivalents) són, entre d'altres, les següents.

**B.0.24 (Teorema de Tykhonov).** Sigui  $\{X_i\}_{i \in I}$  una família no buida d'espais topològics compactes. Llavors, l'espai topològic producte és compacte (i no buit).

**B.0.25.** Tot espai vectorial té una base.

**B.0.26.** Tot anell commutatiu té un ideal maximal.

**B.0.27.** Tot anell té un ideal maximal per l'esquerra, un ideal maximal per la dreta, i un ideal maximal.

**B.0.28.** Tot cos és subcòs d'un cos algebraicament tancat.

**B.0.29.** Tot cos admet una clausura algebraica; és a dir, tot cos  $k$  és subcòs d'un cos algebraicament tancat  $k^a$  tal que l'extensió  $k^a|k$  és algebraica.

Algun altre resultat que es deriva del lema de Zorn ja ha estat vist en el curs; per exemple, l'extensió algebraica de morfismes de cossos (cf. **3.8.8**). Demostrem ara, i a tall d'exemple, que tot espai vectorial diferent de  $(0)$  té una base; aquest resultat l'usem en el curs per a definir el grau d'una extensió qualsevol de cossos (cf. **3.4.4**).

**DEMOSTRACIÓ de B.0.25:** Siguin  $K$  un cos qualsevol i  $E$  un  $K$ -espai vectorial no nul. Considerem el conjunt  $\mathcal{C}$  format per tots els subconjunts de  $E$  que són  $K$ -linealment independents, i, en  $\mathcal{C}$ , la relació d'ordre donada per la inclusió de subconjunts; és a dir, donats dos subconjunts  $A, B \subseteq E$  que siguin  $K$ -linealment independents, direm que  $A \leq B$  si, i només si,  $A \subseteq B$ .

Provem que l'ordre de  $\mathcal{C}$  és inductiu. Considerem, doncs, un subconjunt no buit i totalment ordenat  $\mathcal{D} \subseteq \mathcal{C}$  i sigui  $F$  la reunió de tots els elements de  $\mathcal{D}$  (que són subconjunts  $K$ -linealment independents de  $E$ ). Clarament,  $F$  conté tots els elements de  $\mathcal{D}$ , de manera que, si  $F$  és  $K$ -linealment independent, és  $F \in \mathcal{C}$  i, com a conseqüència,  $\mathcal{D}$  té una fita superior en  $\mathcal{C}$ , com cal demostrar. Ara bé, qualsevol combinació lineal no trivial entre elements de  $F$  contindria una quantitat finita de vectors de  $E$ ; aquests vectors estarien, cadascun, en algun element del conjunt  $\mathcal{D}$ ; la finitud de la quantitat d'aquests vectors i el fet que  $\mathcal{D}$  és totalment ordenat ens permeten assegurar que tots ells pertanyerien a un mateix conjunt de  $\mathcal{D}$ , de manera que  $\mathcal{D}$  contindria un conjunt  $K$ -linealment dependent, fet

contrari a la definició de  $\mathcal{D}$  com a subconjunt de  $\mathcal{C}$ . Per tant,  $F$  és un conjunt  $K$ -linealment independent i l'ordre de  $\mathcal{C}$  és inductiu.

Apliquem, ara, el lema de Zorn. Obtenim que  $\mathcal{C}$  té un element maximal. Sigui  $B \in \mathcal{C}$  un element maximal de  $\mathcal{C}$ . Si veiem que  $B$  és un conjunt de generadors de  $E$  com a  $K$ -espai vectorial, obtenim que  $B$  és una base de  $E$ , de manera que el resultat està provat. Ara bé, si  $B$  no generés  $E$  com a  $K$ -espai vectorial, existiria un vector  $v \in E$  que no seria combinació lineal d'elements de  $B$ , de manera que  $B' := B \cup \{v\}$  seria un subconjunt  $K$ -linealment independent de  $E$ ; i això contradiria la maximalitat de  $B$  en  $\mathcal{C}$ , ja que seria  $B' \in \mathcal{C}$  i  $B < B'$ . Per tant,  $B$  és una base de  $E$ .  $\square$

**B.0.30.** Finalment, demostrem el teorema **B.0.28**: tot cos és subcòs d'un cos algebraicament tancat.

DEMOSTRACIÓ: Sigui  $k$  un cos qualsevol. Considerem el conjunt  $\mathcal{C}$  format per les parelles  $(K, i_K : k \hookrightarrow K)$  tals que  $K|k$  és una extensió algebraica; i ordenem el conjunt  $\mathcal{C}$  per la relació d'inclusió entre els cossos. Com que la reunió dels cossos d'una cadena és un cos, i tots els elements de la reunió pertanyen a algun dels cossos de la cadena, tots els elements de la reunió d'una cadena de cossos que són extensions algebraiques de  $k$  són algebraics sobre  $k$ ; és a dir, la reunió d'una cadena de  $\mathcal{C}$  és una fita superior de  $\mathcal{C}$ . Així, l'ordre és inductiu i el lema de Zorn ens permet assegurar que en  $\mathcal{C}$  hi ha elements maximals. Només cal observar que un tal element maximal, posem  $K$ , que és un cos extensió algebraica de  $k$ , és algebraicament tancat. En efecte, si un polinomi irreductible i no constant,  $f(X) \in K[X]$ , no tingués totes les seves arrels en  $K$ , el cos  $L := K[X]/(f(X))$  seria un cos extensió algebraica de  $K$  i, per tant, de  $k$ , i seria  $K \subsetneq L$ , de manera que  $K$  no seria maximal.  $\square$



# Apèndix C

## Solucions d'alguns exercicis

En aquest apèndix, indiquem solucions per a alguns exercicis seleccionats del text principal. En alguns casos, les solucions escrites aquí són, essencialment, completes. En altres casos, les solucions proposades només contenen el resultat que es tracta de calcular, sense indicacions de com fer-ho. En altres casos, les solucions no són completes, però contenen indicacions que esperem que puguin ésser útils en cas que qui llegeix desitgi ajuda per a la resolució d'alguns dels exercicis proposats. Finalment, en alguns casos, les solucions proposades només tenen la pretensió que puguin ésser usades com a recordatori o com a formulari.

### C.0 Exercicis de la Introducció

En la descripció d'aquestes solucions, utilitzem notacions que encara no s'han introduït en el text principal, però que o bé són usuals o bé són introduïdes més endavant. Per exemple, utilitzem la notació  $A[X]$  per a l'anell de polinomis de coeficients en  $A$ , o bé  $\mathbb{Q}(\sqrt{3})$  per a designar el mínim subcòs de  $\mathbb{C}$  que conté  $\sqrt{3}$ , o bé  $\mathbb{Z}[\sqrt{3}]$  per a designar el mínim subanell de  $\mathbb{Q}(\sqrt{3})$  que conté  $\sqrt{3}$ . Desitgem que aquest fet no representi cap problema (si de cas, potser un estímul) per a qui llegeix.

D'altra banda, i si no diem res que ho contradigui i tractem el cas de característica zero, sovint suposarem que treballem dins el cos  $\mathbb{C}$  dels nombres complexos, amb la convenció habitual  $i := \sqrt{-1}$ .

**Solució C.0.1** (de l'exercici 0.5.2). Sigui  $\omega := \frac{-1 + \sqrt{3}i}{2}$ .

(a) Per al polinomi  $f(X) := X^3 - 6X - 6 \in \mathbb{Z}[X]$ , l'aplicació de les fórmules de Cardano de 0.4.1 o de 0.5.1 proporciona les expressions, per a les arrels complexes de  $f(X)$ ,

$$\omega^k \sqrt[3]{3 - \sqrt{\frac{27 \cdot 6^2 - 4 \cdot 6^3}{108}}} + \frac{2\omega^{-k}}{\sqrt[3]{3 - \sqrt{\frac{27 \cdot 6^2 - 4 \cdot 6^3}{108}}}} = \omega^k \sqrt[3]{2} + \omega^{-k} \sqrt[3]{4}, \quad k = 0, 1, 2.$$

Notem que podem escriure aquestes arrels en la forma

$$\sqrt[3]{2} + \sqrt[3]{4}, \quad -\frac{\sqrt[3]{2} + \sqrt[3]{4}}{2} + \frac{\sqrt{3}(\sqrt[3]{2} - \sqrt[3]{4})}{2}i, \quad -\frac{\sqrt[3]{2} + \sqrt[3]{4}}{2} - \frac{\sqrt{3}(\sqrt[3]{2} - \sqrt[3]{4})}{2}i.$$

- (b) Sigui  $f(X) := X^3 - 6X - 4 \in \mathbb{Z}[X]$ . Com que, en  $\mathbb{Q}[X]$ , se satisfà que  $f(X) = (X + 2)(X^2 - 2X - 2)$ , resulta que les arrels de  $f(X)$ , en  $\mathbb{C}$ , són els nombres  $-2$ ,  $1 + \sqrt{3}$ ,  $1 - \sqrt{3}$ ; les dues darreres obtingudes per aplicació de la fórmula usual per a la resolució de les equacions quadràtiques.

En canvi, l'aplicació de les fórmules de Cardano proporciona, per a les arrels complexes de  $f(X)$ , les expressions

$$\omega^k \sqrt[3]{2 + 2i} + \frac{2}{\omega^k \sqrt[3]{2 + 2i}}, \quad k = 0, 1, 2.$$

Notem, però, que  $2 + 2i = (-1 + i)^3$  i que  $\frac{2}{-1 + i} = -1 - i$ , de manera que les solucions es poden escriure com

$$(-1 + i)\omega^k + (-1 - i)\omega^{-k}, \quad k = 0, 1, 2.$$

- (c) Sigui  $f(X) := X^3 - 2X + 1 \in \mathbb{Z}[X]$ . Com que, en  $\mathbb{Q}[X]$ , se satisfà que  $f(X) = (X - 1)(X^2 + X - 1)$ , resulta que les arrels de  $f(X)$  en  $\mathbb{C}$  són els nombres reals  $1$ ,  $\frac{-1 + \sqrt{5}}{2}$ ,  $\frac{-1 - \sqrt{5}}{2}$ .

En canvi, l'aplicació de les fórmules de Cardano proporciona, per a les arrels complexes de  $f(X)$ , les expressions

$$\omega^k \sqrt[3]{-\frac{1}{2} + \sqrt{\frac{-5}{108}}} + \frac{2}{3\omega^k \sqrt[3]{-\frac{1}{2} + \sqrt{\frac{-5}{108}}}}, \quad k = 0, 1, 2.$$

**Observació:** Per a simplificar les expressions, podem observar que

$$-\frac{1}{2} + \sqrt{\frac{-5}{108}} = \frac{1}{\sqrt{3}^3} \frac{\sqrt{5}i - 3\sqrt{3}}{2} = \left( \frac{\sqrt{3} + \sqrt{5}i}{2\sqrt{3}} \right)^3;$$

per tant, podem escriure les arrels dels polinomis en la forma

$$\omega^k \frac{\sqrt{3} + \sqrt{5}i}{2\sqrt{3}} + \frac{2}{3\omega^k \frac{\sqrt{3} + \sqrt{5}i}{2\sqrt{3}}} = \omega^k \frac{\sqrt{3} + \sqrt{5}i}{2\sqrt{3}} + \omega^{-k} \frac{\sqrt{3} - \sqrt{5}i}{2\sqrt{3}},$$

$k = 0, 1, 2$ ; o sigui, el doble de la part real dels nombres complexos

$$\omega^k \frac{\sqrt{3} + \sqrt{5}i}{2\sqrt{3}}, \quad k = 0, 1, 2.$$

Aquests nombres són, respectivament,  $1$ ,  $\frac{-1 - \sqrt{5}}{2}$ ,  $\frac{-1 + \sqrt{5}}{2}$ .

- (d) Sigui  $f(X) := X^3 - \sqrt{3}X^2 - 2X + 2\sqrt{3} \in \mathbb{Z}[\sqrt{3}][X]$ . Com que, en  $\mathbb{Q}(\sqrt{3})[X]$ , se satisfà que  $f(X) = (X - \sqrt{3})(X^2 - 2)$ , resulta que les arrels de  $f(X)$  en  $\mathbb{C}$  són els nombres  $\sqrt{3}$ ,  $\sqrt{2}$ ,  $-\sqrt{2}$ .

En canvi, l'aplicació de les fórmules de Cardano proporciona, per a les arrels complexes de  $f(X)$ , les expressions

$$\frac{1}{\sqrt{3}} + \frac{3}{\sqrt[3]{\frac{1}{2}(-30\sqrt{3} + 6i\sqrt{6})}} + \frac{1}{3}\sqrt[3]{\frac{1}{2}(-30\sqrt{3} + 6i\sqrt{6})},$$

$$\frac{1}{\sqrt{3}} - \frac{1}{6}(1 - i\sqrt{3})\sqrt[3]{\frac{1}{2}(-30\sqrt{3} + 6i\sqrt{6})} - \frac{3(1 + i\sqrt{3})}{2^{2/3}\sqrt[3]{-30\sqrt{3} + 6i\sqrt{6}}},$$

$$\frac{1}{\sqrt{3}} - \frac{1}{6}(1 + i\sqrt{3})\sqrt[3]{\frac{1}{2}(-30\sqrt{3} + 6i\sqrt{6})} - \frac{3(1 - i\sqrt{3})}{2^{2/3}\sqrt[3]{-30\sqrt{3} + 6i\sqrt{6}}}.$$

**Observació:** Podem simplificar les expressions de la manera següent. Comencem per veure que

$$\frac{1}{2}(-30\sqrt{3} + 6i\sqrt{6}) = \sqrt{3}^3(1 + \sqrt{2}i)^3;$$

això proporciona una expressió més senzilla per a les arrels cúbiques, de manera que podem escriure les expressions anteriors en la forma

$$\frac{1}{\sqrt{3}} + \frac{3}{\sqrt{3}(1 + \sqrt{2}i)} + \frac{1}{3}\sqrt{3}(1 + \sqrt{2}i) = \sqrt{3},$$

$$\frac{1}{\sqrt{3}} - \frac{1}{6}(1 - i\sqrt{3})\sqrt{3}(1 + \sqrt{2}i) - \frac{3(1 + i\sqrt{3})}{2\sqrt{3}(1 + \sqrt{2}i)} = -\sqrt{2},$$

$$\frac{1}{\sqrt{3}} - \frac{1}{6}(1 + i\sqrt{3})\sqrt{3}(1 + \sqrt{2}i) - \frac{3(1 - i\sqrt{3})}{2\sqrt{3}(1 + \sqrt{2}i)} = \sqrt{2}.$$

## C.1 Exercicis del capítol 1

**Solució C.1.1** (de l'exercici 1.1.16). A més a més de les matrius  $1_2$  i  $-1_2$ , les altres han de tenir polinomi característic  $X^2 - 1$ ; per tant, són les matrius  $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ ,  $\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$ , i totes les matrius de la forma  $\begin{bmatrix} a & b \\ c & -a \end{bmatrix}$ , per a  $a, b, c \in \mathbb{Q}$  tals que  $a^2 + bc = 1$ .

**Solució C.1.2** (de l'exercici 1.1.17). Efectivament, les solucions són les successions  $u = \{u_n\}_{n \in \mathbb{N}} \in A$  tals que  $u_n = \pm 1$ , per a tot  $n \in \mathbb{N}$ . I, clarament, aquestes successions es poden interpretar com a funcions característiques dels subconjunts de  $\mathbb{N}$  (de valors 1 i  $-1$ , en lloc de 0 i 1). Per tant, l'equació  $X^2 = 1$  té tantes solucions en  $A$  com subconjunts té el conjunt  $\mathbb{N}$ .

**Solució C.1.3** (de l'exercici 1.8.1). (a2) Sigui  $f(X) := X^4 + 1 \in \mathbb{Z}[X]$ . Com que  $f(X)$  és mònic i el terme constant és 1, les úniques arrels racionals possibles de  $f(X)$  són  $\pm 1$ ; però cap d'aquests nombres és arrel de  $f(X)$ , ja que  $f(-1) = f(1) = 2 \neq 0$ . Per tant, el polinomi  $f(X)$  no té factors de grau 1 ni en  $\mathbb{Z}[X]$  ni en  $\mathbb{Q}[X]$ .

Suposem que tingués algun factor de grau 2 en  $\mathbb{Q}[X]$ , que podem suposar mònic; com que  $f(X)$  és primitiu, també tindria un factor mònic de grau 2 en  $\mathbb{Z}[X]$  (cf. el lema de Gauss **1.5.13**) i obtindríem una descomposició de la forma

$$X^4 + 1 = f(X) = (X^2 + aX + b)(X^2 + cX + d), \quad a, b, c, d \in \mathbb{Z}.$$

En multiplicar i igualar els coeficients, obtindríem que els nombres enters  $a, b, c, d$  són solució del sistema d'equacions

$$\begin{aligned} a + c &= 0, & c &= -a, \\ b + d + ac &= 0, & a^2 &= b + d, & a^2 &= \pm 2, \\ ad + bc &= 0, & a(d - b) &= 0, \\ bd &= 1; & b = d &= \pm 1; \end{aligned}$$

que no té solucions enteres.

- (b2) Per a  $p = 2$ , tenim que  $f(X) = X^4 + 1 \equiv (X + 1)^4 \pmod{2}$ ; és a dir,  $f(X)$  no és irreductible en  $(\mathbb{Z}/2\mathbb{Z})[X]$  (i descompon en factors lineals).

Si  $p \equiv 1 \pmod{8}$ , llavors existeix  $\alpha \in (\mathbb{Z}/p\mathbb{Z})^*$  d'ordre 8, perquè aquest grup és cíclic d'ordre  $p - 1$ , múltiple de 8; i per a aquest element se satisfà que  $\alpha^4 = -1$  i, llavors,

$$X^4 + 1 \equiv (X - \alpha)(X - \alpha^3)(X - \alpha^5)(X - \alpha^7) \pmod{p},$$

de manera que  $f(X)$  descompon en factors lineals en  $(\mathbb{Z}/p\mathbb{Z})[X]$ .

Si  $p \equiv 5 \pmod{8}$ , llavors existeix  $\alpha \in (\mathbb{Z}/p\mathbb{Z})^*$  tal que  $\alpha^2 = -1$  i, llavors,

$$X^4 + 1 \equiv (X^2 - \alpha)(X^2 + \alpha) \pmod{p},$$

de manera que  $f(X)$  és el producte de dos polinomis (irreductibles, perquè en  $(\mathbb{Z}/p\mathbb{Z})^*$  no hi ha elements d'ordre 8) de grau 2 en  $(\mathbb{Z}/p\mathbb{Z})[X]$ .

Si  $p \equiv 7 \pmod{8}$ , llavors existeix  $\alpha \in (\mathbb{Z}/p\mathbb{Z})^*$  tal que  $\alpha^2 = 2$  i, llavors,

$$(X^2 + \alpha X + 1)(X^2 - \alpha X + 1) = X^4 + (2 - \alpha^2)X^2 + 1 \equiv X^4 + 1 \pmod{p},$$

de manera que  $f(X)$  és el producte de dos polinomis (irreductibles) de grau 2 en  $\mathbb{Z}/p\mathbb{Z}[X]$ .

I, finalment, si  $p \equiv 3 \pmod{8}$ , llavors existeix  $\alpha \in (\mathbb{Z}/p\mathbb{Z})^*$  tal que  $\alpha^2 = -2$  i, llavors,

$$(X^2 + \alpha X - 1)(X^2 - \alpha X - 1) = X^4 + (-2 - \alpha^2)X^2 + 1 \equiv X^4 + 1 \pmod{p},$$

de manera que  $f(X)$  és el producte de dos polinomis (irreductibles) de grau 2 en  $(\mathbb{Z}/p\mathbb{Z})[X]$ .

- (a1) Per al polinomi  $f(X) := X^4 - 10X^2 + 1 \in \mathbb{Z}[X]$  es pot utilitzar un argument semblant al del cas anterior. Com que  $f(X)$  és mònic i el terme constant és 1, les úniques arrels racionals possibles de  $f(X)$  són  $\pm 1$ ; però cap d'aquests nombres és arrel de  $f(X)$ , ja que  $f(-1) = f(1) = -8 \neq 0$ . Per tant, el polinomi  $f(X)$  no té factors de grau 1 ni en  $\mathbb{Z}[X]$  ni en  $\mathbb{Q}[X]$ .



Suposem que tinguéis algun factor de grau 2 en  $\mathbb{Q}[X]$ , que podem suposar mònic; com que  $f(X)$  és primitiu, també tindria un factor mònic de grau 2 en  $\mathbb{Z}[X]$  i obtindríem una descomposició de la forma

$$X^4 + 1 = f(X) = (X^2 + aX + b)(X^2 + cX + d), \quad a, b, c, d \in \mathbb{Z}.$$

En multiplicar i igualar els coeficients, obtindríem que els nombres enters  $a, b, c, d$  són solució del sistema d'equacions

$$\begin{aligned} a + c &= 0, & c &= -a, \\ b + d + ac &= -10, & a^2 &= b + d + 10, & a^2 &= 10 \pm 2, \\ ad + bc &= 0, & a(d - b) &= 0, \\ bd &= 1; & b = d &= \pm 1; \end{aligned}$$

que no té solucions enteres, perquè ni 12 ni 8 són quadrats en  $\mathbb{Z}$ .

(b1) Per a  $p = 2$ , tenim que  $f(X) \equiv X^4 + 1 \equiv (X + 1)^4 \pmod{2}$ ; és a dir,  $f(X)$  no és irreductible en  $(\mathbb{Z}/2\mathbb{Z})[X]$  (i descompon en factors lineals).

Per a  $p = 3$ , tenim que  $f(X) \equiv X^4 + 2X^2 + 1 \equiv (X^2 + 1)^2 \pmod{3}$ ; és a dir,  $f(X)$  no és irreductible en  $(\mathbb{Z}/3\mathbb{Z})[X]$ ; és el quadrat d'un polinomi (irreductible) de grau 2.

Ara, si  $p$  és un nombre primer diferent de 2 i de 3, ha de ser  $p \equiv \pm 1, \pm 5, \pm 7, \pm 11 \pmod{24}$ .

Si  $p \equiv \pm 5 \pmod{24}$ , llavors existeix  $\alpha \in (\mathbb{Z}/p\mathbb{Z})^*$  tal que  $\alpha^2 = 6$  (i no existeixen arrels quadrades ni de 2 ni de 3); i, llavors, mòdul  $p$ , és

$$(X^2 - (5 + 2\alpha))(X^2 - (5 - 2\alpha)) = X^4 - 10X^2 + (5^2 - 4\alpha^2) \equiv X^4 - 10X^2 + 1,$$

de manera que  $f(X)$  és el producte de dos polinomis (irreductibles) de grau 2 en  $(\mathbb{Z}/p\mathbb{Z})[X]$ .

Si  $p \equiv \pm 7 \pmod{24}$ , llavors existeix  $\alpha \in (\mathbb{Z}/p\mathbb{Z})^*$  tal que  $\alpha^2 = 2$  (i no existeixen arrels quadrades ni de 3 ni de 6); i, llavors, mòdul  $p$ , és

$$(X^2 + 2\alpha X - 1)(X^2 - 2\alpha X - 1) = X^4 + (-2 - 4\alpha^2)X^2 + 1 \equiv X^4 - 10X^2 + 1,$$

de manera que  $f(X)$  és el producte de dos polinomis (irreductibles) de grau 2 en  $(\mathbb{Z}/p\mathbb{Z})[X]$ .

Si  $p \equiv \pm 11 \pmod{24}$ , llavors existeix  $\alpha \in (\mathbb{Z}/p\mathbb{Z})^*$  tal que  $\alpha^2 = 3$  (i no existeixen arrels quadrades ni de 2 ni de 6); i, llavors, mòdul  $p$ , és

$$(X^2 + 2\alpha X + 1)(X^2 - 2\alpha X + 1) = X^4 + (2 - 4\alpha^2)X^2 + 1 \equiv X^4 - 10X^2 + 1,$$

de manera que  $f(X)$  és el producte de dos polinomis (irreductibles) de grau 2 en  $(\mathbb{Z}/p\mathbb{Z})[X]$ .

Finalment, Si  $p \equiv \pm 1 \pmod{24}$ , llavors existeixen  $\alpha, \beta \in (\mathbb{Z}/p\mathbb{Z})^*$  tals que  $\alpha^2 = 2$  i  $\beta^2 = 3$ , i és  $(\alpha\beta)^2 = 6$ . Llavors, mòdul  $p$ , és

$$\begin{aligned} & (X - (\alpha + \beta))(X - (\alpha - \beta))(X + (\alpha + \beta))(X + (\alpha - \beta)) \\ & \equiv (X^2 - (\alpha + \beta)^2)(X^2 - (\alpha - \beta)^2) \\ & \equiv X^4 - ((\alpha + \beta)^2 + (\alpha - \beta)^2)X^2 + (\alpha + \beta)^2(\alpha - \beta)^2 \\ & = X^4 - 2(\alpha^2 + \beta^2)X^2 + (\alpha^2 - \beta^2)^2 \\ & \equiv X^4 - 10X^2 + 1, \end{aligned}$$

de manera que  $f(X)$  és el producte de quatre polinomis de grau 1 en  $(\mathbb{Z}/p\mathbb{Z})[X]$ .

**Observació.** No cal descriure amb detall les classes mòdul 24 dels nombres primers diferents de 2 i de 3. De fet, si per al símbol de Legendre se satisfà que  $\left(\frac{2}{p}\right) = 1$ , hi ha una arrel quadrada de 2 mòdul  $p$  i val la descomposició escrita en el cas  $p \equiv \pm 7 \pmod{24}$ , encara que els factors potser no són irreductibles; si per al símbol de Legendre se satisfà que  $\left(\frac{3}{p}\right) = 1$ , hi ha una arrel quadrada de 3 mòdul  $p$  i val la descomposició escrita en el cas  $p \equiv \pm 11 \pmod{24}$ , encara que els factors potser no són irreductibles; i si per als símbols de Legendre se satisfà que  $\left(\frac{2}{p}\right) = \left(\frac{3}{p}\right) = -1$ , llavors és  $\left(\frac{6}{p}\right) = 1$ , i val la descomposició escrita en el cas  $p \equiv \pm 5 \pmod{24}$ . I el cas  $p \equiv \pm 1 \pmod{24}$  correspon al fet que  $\left(\frac{2}{p}\right) = \left(\frac{3}{p}\right) = \left(\frac{6}{p}\right) = 1$ , i valen les tres descomposicions, de les quals es pot deduir fàcilment la descomposició en factors lineals.

**Solució C.1.4** (de l'exercici 1.8.3).

- (a)  $X^4 - 2X^3 + 2X^2 + X + 4 = (X^2 - 3X + 4)(X^2 + X + 1)$ ; com que els dos polinomis de grau 2 no tenen arrels racionals (i són de grau més petit o igual que 3), són irreductibles en  $\mathbb{Q}[X]$ .
- (b)  $X^4 - 5X^3 + 3X - 2 \equiv X(X^3 + X^2 + 1) \pmod{2}$ , i  $X^3 + X^2 + 1$  és irreductible mòdul 2; per tant, si el polinomi redueix en  $\mathbb{Q}[X]$ , llavors ho fa en  $\mathbb{Z}[X]$  i la reducció mòdul 2 d'aquesta descomposició ha de ser compatible amb el factor  $X$  i un factor irreductible de grau 3; per tant, resulta que si el polinomi redueix en  $\mathbb{Q}[X]$ , llavors té una arrel en  $\mathbb{Q}$  (i en  $\mathbb{Z}$ ). Però cap dels nombres  $\pm 1$  ni  $\pm 2$  no en són arrels; per tant, el polinomi és irreductible.
- (c) El polinomi  $3X^5 - 4X^3 - 6X^2 + 6$  és 2-Eisenstein i, per tant, irreductible en  $\mathbb{Q}[X]$ , i també en  $\mathbb{Z}[X]$ , perquè és primitiu.
- (d) El polinomi  $5X^5 - 6X^4 - 3X^2 + 9X - 15$  és 3-Eisenstein i, per tant, irreductible en  $\mathbb{Q}[X]$ , i també en  $\mathbb{Z}[X]$ , perquè és primitiu.
- (e) Sigui  $f(X) := X^6 + 12X^5 + 49X^4 + 96X^3 + 99X^2 + 54X + 15$ ; llavors,  $f(X - 1) = X^6 + 6X^5 + 4X^4 + 2X + 2$  és 2-Eisenstein i, per tant, irreductible en  $\mathbb{Q}[X]$ . Per tant,  $f(X)$  és irreductible en  $\mathbb{Q}[X]$  i també en  $\mathbb{Z}[X]$ , perquè és primitiu.
- (f) Sigui  $f(X) := X^5 + X^4 + 2X^3 + 2X^2 + 2X + 3$ . En primer lloc, tenim que  $f(X) \equiv X(X^4 + X^3 - X^2 - X - 1) \pmod{3}$ ; i el polinomi  $X^4 + X^3 - X^2 - X - 1$  és irreductible mòdul 3. (Efectivament, no té arrels ni és divisible per cap dels polinomis mònics irreductibles de grau 2 de  $(\mathbb{Z}/3\mathbb{Z})[X]$ , que són els polinomis  $X^2 + 1$ ,  $X^2 + X - 1$ , i  $X^2 - X - 1$ .) Així, si  $f(X)$  fos reductible en  $\mathbb{Q}[X]$ , com que és mònic, també ho seria en  $\mathbb{Z}[X]$  i tindria una arrel en  $\mathbb{Z}$ .

Però resulta que  $f(X) \equiv (X^2 + X + 1)(X^3 + X + 1) \pmod{2}$ , i els dos polinomis són irreductibles mòdul 2. Com que una arrel de  $f(X)$  en  $\mathbb{Z}$  donaria lloc a una arrel en

$\mathbb{Z}/2\mathbb{Z}$ , resulta que  $f(X)$  no pot tenir arrels en  $\mathbb{Z}$ . Com que hem vist que si redueix, llavors té una arrel, resulta que  $f(X)$  és irreductible.

- Solució C.1.5** (de l'exercici 1.8.5). (a) Les arrels del polinomi són les 9 classes 1, 2, 3, 5, 6, 7, 9, 10, 11 (mod 12). Notem, però, que el polinomi és de grau 3.
- (b) El polinomi descompon en la forma  $3(X-2)(X^2-X+1) \pmod{5}$ , i  $X^2-X+1$  no té arrels mòdul 5. Per tant, l'única arrel del polinomi és 2 (mod 5), i és simple.
- (c) El polinomi descompon en la forma  $5(X-3)(X-4)(X^2+1) \pmod{7}$ , i  $X^2+1$  no té arrels mòdul 7, de manera que les arrels són 3, 4 (mod 7), i són simples.
- (d) El polinomi  $X^3+X+1$  no té arrels mòdul 2; és irreductible.

## C.2 Exercicis del capítol 2

**Solució C.2.1** (de l'exercici 2.6.1). (a) La fórmula de derivació d'un producte ens diu que el derivat del producte  $\prod_{i=1}^n (T - X_i)$  és la suma, sobre l'índex  $i$ , del derivat del factor  $T - X_i$ , que és 1, pel producte dels altres factors, que és exactament el polinomi  $g_i(T)$ . Això és la fórmula demanada,  $D(f, T) = \sum_{i=1}^n g_i(T)$ .

- (b) Comencem per observar que  $f(T) = \sum_{k=0}^n (-1)^k s_k(X_1, \dots, X_n) T^{n-k}$ , de manera que

$$0 = f(X_i) = \sum_{k=0}^n (-1)^k s_k(X_1, \dots, X_n) X_i^{n-k}.$$

A més a més, per a  $k \geq 1$ , és (divisió pel mètode de Ruffini)

$$\frac{T^k - X_i^k}{T - X_i} = \sum_{r=0}^{k-1} X_i^{k-1-r} T^r,$$

per tant, podem escriure

$$\begin{aligned} g_i(T) &= \frac{f(T)}{T - X_i} = \frac{f(T) - f(X_i)}{T - X_i} \\ &= \frac{\sum_{k=0}^n (-1)^k s_k(X_1, \dots, X_n) (T^{n-k} - X_i^{n-k})}{T - X_i} \\ &= \sum_{k=0}^{n-1} (-1)^k s_k(X_1, \dots, X_n) \frac{(T^{n-k} - X_i^{n-k})}{T - X_i} \\ &= \sum_{k=0}^{n-1} (-1)^k s_k(X_1, \dots, X_n) \sum_{r=0}^{n-k-1} X_i^{n-k-1-r} T^r \\ &= \sum_{r=0}^{n-1} \left( \sum_{k=0}^{n-r-1} (-1)^k s_k(X_1, \dots, X_n) X_i^{n-k-1-r} \right) T^r; \end{aligned}$$

és a dir, per a  $0 \leq r \leq n-1$  i  $1 \leq i \leq n$ , el coeficient de  $T^r$  de  $g_i(T)$ , és donat per l'expressió

$$\sum_{k=0}^{n-r-1} (-1)^k s_k(X_1, \dots, X_n) X_i^{n-k-1-r}.$$

- (c) El càlcul del derivat del polinomi  $f(T)$ , expressat com la suma dels polinomis  $g_i(T)$ , proporciona la igualtat

$$D(f, T) = \sum_{r=0}^{n-1} \left( \sum_{k=0}^{n-r-1} (-1)^k s_k(X_1, \dots, X_n) t_{n-k-1-r}(X_1, \dots, X_n) \right) T^r,$$

mentre que el càlcul directe proporciona la igualtat

$$\begin{aligned} D(f, T) &= \sum_{k=0}^{n-1} (-1)^k s_k(X_1, \dots, X_n) (n-k) T^{n-k-1} \\ &= \sum_{r=0}^{n-1} (-1)^{n-1-r} s_{n-1-r}(X_1, \dots, X_n) (r+1) T^r. \end{aligned}$$

Per tant, en igualar els coeficients per a  $0 \leq r \leq n-1$ , obtenim que

$$\begin{aligned} \sum_{k=0}^{n-1-r} (-1)^k s_k(X_1, \dots, X_n) t_{n-k-1-r}(X_1, \dots, X_n) \\ = (-1)^{n-1-r} s_{n-1-r}(X_1, \dots, X_n) (r+1). \end{aligned}$$

I si posem  $m := n-1-r$  i ho passem tot al primer terme, obtenim que, per a  $0 \leq m \leq n-1$ , és

$$\sum_{k=0}^{m-1} (-1)^k s_k(X_1, \dots, X_n) t_{m-k}(X_1, \dots, X_n) + (-1)^m m s_m(X_1, \dots, X_n) = 0,$$

com calia demostrar, ja que  $t_0(X_1, \dots, X_n) - r - 1 = n - r - 1 = m$ .

- (d) Per a  $m \geq n$ , podem sumar les igualtats

$$0 = f(X_i) X_i^{m-n} = \sum_{k=0}^n (-1)^k s_k(X_1, \dots, X_n) X_i^{m-k}$$

per a  $1 \leq i \leq n$ ; s'obtenen immediatament les fórmules

$$\sum_{k=0}^n (-1)^k s_k(X_1, \dots, X_n) t_{m-k}(X_1, \dots, X_n) = 0$$

que, multiplicades per  $(-1)^m$ , són les que cal demostrar.

- (e) El resultat és una conseqüència del fet que, si  $k$  és de característica 0 o més gran estrictament que  $n$ , llavors, en  $k$ , podem dividir per tots els nombres naturals entre 1 i  $n$ ; per tant, per inducció sobre  $m \leq n$  i tenint en compte les fórmules de Newton

per a  $m \leq n$  i, en particular, que  $s_1(X_1, \dots, X_n) = t_1(X_1, \dots, X_n)$ , obtenim que, per a  $1 \leq m \leq n$ , és

$$k[s_1(X_1, \dots, X_n), \dots, s_m(X_1, \dots, X_n)] = k[t_1(X_1, \dots, X_n), \dots, t_m(X_1, \dots, X_n)].$$

Ara, només cal notar que

$$k[X_1, \dots, X_n]^{S_n} = k[s_1(X_1, \dots, X_n), \dots, s_n(X_1, \dots, X_n)]$$

i tenir en compte que si un polinomi simètric és de grau total  $m < n$ , en l'expressió polinòmica en  $s_1(X_1, \dots, X_n), \dots, s_n(X_1, \dots, X_n)$  no hi pot aparèixer cap dels polinomis  $s_{m+1}(X_1, \dots, X_n), \dots, s_n(X_1, \dots, X_n)$ , que són de grau més gran.

**Solució C.2.2** (de l'exercici 2.6.3). (a) Sigui

$$f(X) := aX^3 + bX^2 + cX + d = a(X - x_1)(X - x_2)(X - x_3);$$

llavors, si posem

$$s_1 = x_1 + x_2 + x_3, \quad s_2 = x_1x_2 + x_1x_3 + x_2x_3, \quad s_3 = x_1x_2x_3,$$

tenim que

$$b = -as_1, \quad c = as_2, \quad d = -as_3,$$

i el discriminant és donat per

$$a^4(x_1 - x_2)^2(x_1 - x_3)^2(x_2 - x_3)^2.$$

Podem aplicar el mètode de Waring a aquest polinomi simètric. El polinomi és homogeni de grau total 6, de manera que l'expressió com a polinomi en els polinomis simètrics elementals ha de ser una combinació lineal dels productes

$$s_1^6, \quad s_1^4s_2, \quad s_1^3s_3, \quad s_1^2s_2^2, \quad s_1s_2s_3, \quad s_2^3, \quad s_3^2.$$

A més a més, d'acord amb l'ordre definit a la demostració del teorema de Waring, el monomi no nul més gran del desenvolupament del discriminant és  $x_1^4x_2^2$ . D'aquest fet en treiem dues conseqüències: d'una banda, que el producte de polinomis simètrics elementals que correspon a aquest sumand és  $s_1^2s_2^2$ ; de l'altra, en tenir en compte que els monomis més grans dels productes de polinomis simètrics de més amunt són, respectivament,

$$x_1^6, \quad x_1^5x_2, \quad x_1^4x_2x_3, \quad x_1^4x_2^2, \quad x_1^3x_2^2x_3, \quad x_1^3x_2^3, \quad x_1^2x_2^2x_3^2,$$

obtenim que, en el desenvolupament del discriminant, només hi poden aparèixer els productes

$$s_1^3s_3, \quad s_1^2s_2^2, \quad s_1s_2s_3, \quad s_2^3, \quad s_3^2.$$

Posem, doncs,

$$\Delta = a^4(x_1 - x_2)^2(x_1 - x_3)^2(x_2 - x_3)^2 = \alpha s_1^3s_3 + \beta s_1^2s_2^2 + \gamma s_1s_2s_3 + \delta s_2^3 + \varepsilon s_3^2,$$

amb coeficients indeterminats  $\alpha, \beta, \gamma, \delta, \varepsilon$ . Com que l'expressió que resulti del discriminant expressat com a producte dels polinomis simètrics elementals ha de ser vàlida per a tots els polinomis, podem prendre polinomis particulars per a calcular els valors dels coeficients indeterminats  $\alpha, \beta, \gamma, \delta, \varepsilon$ .

Posem en una taula els valors triats per a les arrels del polinomi, els valors que resulten per a  $s_1 = x_1 + x_2 + x_3$ ,  $s_2 = x_1x_2 + x_1x_3 + x_2x_3$ ,  $s_3 = x_1x_2x_3$ ,  $\Delta = a^4 \prod_{1 \leq i < j \leq 3} (x_i - x_j)^2$ ,

i la combinació lineal

$$\alpha s_1^3 s_3 + \beta s_1^2 s_2^2 + \gamma s_1 s_2 s_3 + \delta s_2^3 + \varepsilon s_3^2$$

que resulta d'aquests valors:

$x_1$	$x_2$	$x_3$	$s_1$	$s_2$	$s_3$	$\Delta$	
1	-1	0	0	-1	0	$4a^4$	$-\delta$
1	1	0	2	1	0	0	$4\beta + \delta$
1	1	-1	1	-1	-1	0	$-\alpha + \beta + \gamma - \delta + \varepsilon$
1	1	1	3	3	1	0	$27\alpha + 81\beta + 9\gamma + 27\delta + \varepsilon$
1	-1	2	2	-1	-2	$36a^4$	$-16\alpha + 4\beta + 4\gamma - \delta + 4\varepsilon$

Això produeix el sistema d'equacions lineals

$$\begin{aligned} -\delta &= 4a^4, \\ 4\beta + \delta &= 0, \\ -\alpha + \beta + \gamma - \delta + \varepsilon &= 0, \\ 27\alpha + 81\beta + 9\gamma + 27\delta + \varepsilon &= 0, \\ -16\alpha + 4\beta + 4\gamma - \delta + 4\varepsilon &= 36a^4, \end{aligned}$$

que té solució

$$\alpha = -4a^4, \quad \beta = a^4, \quad \gamma = 18a^4, \quad \delta = -4a^4, \quad \varepsilon = -27a^4.$$

Així, obtenim l'expressió per al discriminant del polinomi  $aX^3 + bX^2 + cX + d$ :

$$\Delta = -4a^4 s_1^3 s_3 + a^4 s_1^2 s_2^2 + 18a^4 s_1 s_2 s_3 - 4a^4 s_2^3 - 27a^4 s_3^2$$

que, tenint en compte que  $as_1 = -b$ ,  $as_2 = c$  i  $as_3 = -d$ , proporciona la fórmula

$$\Delta(aX^3 + bX^2 + cX + d) = -4b^3d + b^2c^2 + 18abcd - 4ac^3 - 27a^2d^2.$$

(b) Només cal fer la substitució  $a = 1$ ,  $b = 0$ ,  $c = p$ ,  $d = q$ , i s'obté que

$$\Delta(X^3 + pX + q) = -4p^3 - 27q^2.$$

**Solució C.2.3** (de l'exercici 2.6.4). Posem  $f(X) := X^n + a$ ,  $\alpha$  una arrel del polinomi, de manera que  $\alpha^n = -a$ , i  $\zeta := \zeta_n$  una arrel  $n$ -èsima primitiva de la unitat. Llavors, les arrels del polinomi  $f(X)$  són els  $n$  nombres  $\alpha\zeta^i$ ,  $0 \leq i \leq n-1$ , i el discriminant es pot escriure com

$$\begin{aligned} \Delta(X^n + a) &= \prod_{0 \leq i < j \leq n-1} (\zeta^i \alpha - \zeta^j \alpha)^2 \\ &= (-1)^{n(n-1)/2} \prod_{i,j;j \neq i} \alpha \zeta^i (1 - \zeta^{j-i}) \\ &= (-1)^{n(n-1)/2} \alpha^{n(n-1)} \prod_{i,j;j \neq i} \zeta^i (1 - \zeta^{j-i}) \\ &= (-1)^{n(n-1)/2} (-a)^{n-1} \prod_{i,j;j \neq i} \zeta^i (1 - \zeta^{j-i}). \end{aligned}$$

Ara bé, resulta que, fixat un índex  $i$ ,

$$\prod_{j:j \neq i} (X - \zeta^{j-i}) = \frac{X^n - 1}{X - 1} = 1 + X + \cdots + X^{n-1},$$

de manera que  $\prod_{j:j \neq i} (1 - \zeta^{j-i}) = n$ ; per tant,

$$\begin{aligned} \Delta(X^n + a) &= (-1)^{n(n-1)/2} (-a)^{n-1} \prod_{0 \leq i \leq n-1} n \zeta^i \\ &= (-1)^{n(n-1)/2} (-a)^{n-1} n^n \zeta^{\sum_{0 \leq i \leq n-1} i} \\ &= (-1)^{n(n-1)/2} (-a)^{n-1} n^n \zeta^{n(n-1)/2}. \end{aligned}$$

Finalment, notem que si  $n$  és senar, llavors  $n - 1$  és parell i  $\zeta^n = 1$ , de manera que  $\zeta^{n(n-1)/2} = 1 = (-1)^{n-1}$ ; i si  $n$  és parell, llavors  $\zeta^{n/2} = -1$ , de manera que, també,  $\zeta^{n(n-1)/2} = (-1)^{n-1}$ ; per tant,

$$\Delta(X^n + a) = (-1)^{n(n-1)/2} (-a)^{n-1} n^n (-1)^{n-1} = (-1)^{n(n-1)/2} n^n a^{n-1}.$$

**Solució C.2.4** (dels exercicis 2.6.5 i 2.6.6). Les propietats (b), (c), (d) són immediates a partir de la definició i les propietats bàsiques dels determinants. Ens ocuparem, doncs, de la propietat (a).

Siguin  $C_1, \dots, C_{n+m} \in A^{n+m}$  els vectors columna del determinant de Sylvester. Llavors,  $R(f(X), g(X)) = \det(C_1, \dots, C_{n+m})$ .

Podem calcular aquest determinant sobre qualsevol anell que contingui  $A$  com a subanell; en particular, sobre l'anell de polinomis  $A[X]$ , o bé sobre un cos algebraicament tancat,  $k$ , que contingui el cos de fraccions de  $A$ .

Si suposem que  $f(X)$  i  $g(X)$  tenen una arrel comuna,  $\alpha \in K$ , podem escriure

$$\det(C_1, \dots, C_{n+m}) = \det(C_1, \dots, C_{n+m-1}, C),$$

on  $C = C_{n+m} + C_{n+m-1}\alpha + C_{n+m-2}\alpha^2 + \cdots + C_1\alpha^{n+m-1}$ . Aquest vector columna és el vector

$$(\alpha^{m-1}f(\alpha), \dots, \alpha f(\alpha), f(\alpha), \alpha^{n-1}g(\alpha), \dots, \alpha g(\alpha), g(\alpha))^t,$$

i és el vector nul perquè  $f(\alpha) = g(\alpha) = 0$ ; per tant, el determinant és

$$R(f(X), g(X)) = \det(C_1, \dots, C_{n+m-1}, C) = \det(C_1, \dots, C_{n+m-1}, 0) = 0.$$

Per a la prova del recíproc, treballem anàlogament en  $A[X]$  i considerem  $\alpha := X$ . El càlcul anterior del determinant permet desenvolupar-lo per la darrera columna, i obtenim que  $\det(C_1, \dots, C_{n+m-1}, C)$  és de la forma  $f(X)\psi(X) + g(X)\varphi(X)$ , per a certs polinomis  $\psi(X), \varphi(X) \in A[X]$ , els coeficients dels quals s'obtenen dels menors complementaris corresponents a cadascun dels components del vector  $C$ . Notem que també és  $\text{gr}(\varphi(X)) < \text{gr}(f(X))$  i  $\text{gr}(\psi(X)) < \text{gr}(g(X))$ . Si suposem que el determinant és nul, obtenim que  $f(X)\psi(X) + g(X)\varphi(X) = 0$  i això implica que  $f(X)$  i  $g(X)$  tenen un factor comú no trivial sobre el cos de fraccions de  $A$ . En efecte, no pot ser que  $f(X)$  divideixi  $\varphi(X)$ , perquè els graus no ho permeten; per tant, algun factor irreductible de  $f(X)$  ha de dividir  $g(X)$ . I això implica que  $f(X)$  i  $g(X)$  tenen una arrel comuna.

Notem que aquest càlcul també demostra l'existència de l'afirmació de l'exercici **2.6.6**. La unicitat d'aquest enunciat s'obté per divisió euclidiana, perquè si  $R(f(X), g(X)) \neq 0$ , llavors  $f(X)$  i  $g(X)$  són coprimers.

**Solució C.2.5** (de l'exercici **2.6.7**). Treballem en l'anell de polinomis en  $n + m + 3$  indeterminades  $A := \mathbb{Z}[a_n, b_m, \alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_m][X]$ .

Posem  $f(X) := a_n(X - \alpha_1) \cdots (X - \alpha_n)$ , i  $g(X) := b_m(X - \beta_1) \cdots (X - \beta_m)$ . Llavors, les fórmules de Viète ens donen les fórmules per als coeficients,

$$a_k = (-1)^{n-k} \cdot a_n \cdot s_{n-k}(\alpha_1, \dots, \alpha_n), \quad 0 \leq k \leq n-1,$$

$$b_r = (-1)^{m-r} \cdot b_m \cdot s_{m-r}(\beta_1, \dots, \beta_m). \quad 0 \leq r \leq m-1.$$

En substituir en el determinant de Sylvester, obtenim que  $R(f(X), g(X))$  és el producte de  $a_n^m \cdot b_m^n$  per un polinomi en  $\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_m$ , i coeficients enters; posem  $R(f(X), g(X)) =: a_n^m \cdot b_m^n h(\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_m)$ .

En virtut de l'exercici **2.6.5**, aquest polinomi és divisible per tots els polinomis  $\alpha_i - \beta_j$ ,  $1 \leq i \leq n$ ,  $1 \leq j \leq m$ , perquè si algun  $\alpha_i$  coincideix amb algun  $\beta_j$ , el resultant s'anul·la. I com que tots aquests polinomis són primers entre si, el polinomi  $h(\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_m)$  és divisible pel producte

$$R := \prod_{i=1}^n \prod_{j=1}^m (\alpha_i - \beta_j).$$

Així, el polinomi

$$S := a_n^m \cdot b_m^n \prod_{i=1}^n \prod_{j=1}^m (\alpha_i - \beta_j)$$

divideix  $R(f(X), g(X))$ . Ara bé, podem calcular  $S$  de la manera següent:

$$S = a_n^m \prod_{i=1}^n \left( b_m \prod_{j=1}^m (\alpha_i - \beta_j) \right) = a_n^m \prod_{i=1}^n g(\alpha_i);$$

i, per tant,  $S$  és homogeni de grau  $n$  en  $b_0, \dots, b_m$ . De manera similar,

$$S = b_m^n \prod_{j=1}^m \left( a_n \prod_{i=1}^n (\alpha_i - \beta_j) \right) = (-1)^{nm} b_m^n \prod_{j=1}^m f(\beta_j);$$

i, per tant,  $S$  és homogeni de grau  $m$  en  $a_0, \dots, a_n$ .

Així, tant el resultant,  $R(f(X), g(X))$ , com el polinomi  $S$ , són homogenis del mateix grau en les  $a_i$  i en les  $b_j$ , i  $S$  divideix  $R$ . Per tant,  $R(f(X), g(X)) = uS$ , per a alguna constant  $u$ . Però com que tots dos polinomis contenen el monomi  $a_n^m b_m^n$ , aquesta constant ha de ser 1. I això acaba la prova.

**Solució C.2.6** (de l'exercici **2.6.8**). Amb les notacions de la resolució l'exercici anterior, **C.2.5**, si posem  $g(X) := D(f, X)$ , el polinomi derivat de  $f(X)$ , tenim que

$$R(f(X), D(f, X)) = a_n^{n-1} \prod_{i=1}^n D(f, \alpha_i),$$



on  $\alpha_1, \dots, \alpha_n$  són les arrels de  $f(X)$ . La derivació de  $f(X)$  a partir de la fórmula de derivació d'un producte proporciona la igualtat

$$D(f, \alpha_i) = a_n \sum_{j=1}^n (\alpha_i - \alpha_1) \cdots (\alpha_i - \alpha_{j-1}) \cdot (\alpha_i - \alpha_{j+1}) \cdots (\alpha_i - \alpha_n);$$

o sigui,

$$D(f, \alpha_i) = a_n (\alpha_i - \alpha_1) \cdots (\alpha_i - \alpha_{i-1}) \cdot (\alpha_i - \alpha_{i+1}) \cdots (\alpha_i - \alpha_n).$$

Per tant, en substituir, tenim que

$$R(f(X), D(f, X)) = a_n^{2n-1} \prod_{i=1}^n \prod_{j \neq i} (\alpha_i - \alpha_j).$$

D'altra banda, d'acord amb el corol·lari 2.4.4, tenim que

$$\Delta(f(X)) = (-1)^{n(n-1)/2} a_n^{2n-2} \prod_{i=1}^n \prod_{j \neq i} (\alpha_i - \alpha_j).$$

I això proporciona la igualtat que se cerca.

**Solució C.2.7** (de l'exercici 2.6.9). El càlcul de  $R(f(X), D(f, X))$  a partir del determinant de Sylvester és senzill, i proporciona, en tenir el compte l'exercici anterior, 2.6.8, la igualtat

$$\Delta(X^n + aX + b) = (-1)^{n(n-1)/2} (n^n b^{n-1} + (1-n)^{n-1} a^n).$$

## C.3 Exercicis del capítol 3

**Solució C.3.1** (de l'exercici 3.11.2). Com que  $\text{mcd}(r, s) = d$ , podem escriure  $r = dv$ ,  $s = du$ , amb  $v, u \in \mathbb{Z}$  i  $\text{mcd}(v, u) = 1$ , i llavors és  $m = \frac{rs}{d} = duv = ru = sv$ ; a més a més, existeixen nombres enters  $x, y$  tals que  $1 = xu + yv$ .

Ara, observem que la potència  $u$ -èsima de  $\zeta_m$  és una arrel  $r$ -èsima primitiva de la unitat (l'ordre de  $\zeta_m^u$  és  $m/u = r$ ); com que  $\zeta_r$  també és una arrel  $r$ -èsima primitiva de la unitat, existeix un nombre enter  $a$ ,  $1 \leq a \leq r$  i  $\text{mcd}(a, r) = 1$ , tal que  $\zeta_m^u = \zeta_r^a$ . En particular, això fa explícita la inclusió  $\mathbb{Q}(\zeta_r) = \mathbb{Q}(\zeta_r^a) \subseteq \mathbb{Q}(\zeta_m)$ .

Anàlogament,  $\zeta_m^v = \zeta_s^b$ , per a un cert nombre enter  $b$ ,  $1 \leq b \leq s$  tal que  $\text{mcd}(b, s) = 1$ , i també  $\mathbb{Q}(\zeta_s) \subseteq \mathbb{Q}(\zeta_m)$ . En particular, obtenim la inclusió  $\mathbb{Q}(\zeta_r, \zeta_s) \subseteq \mathbb{Q}(\zeta_m)$ .

A més a més, de la igualtat  $1 = xu + yv$ , tenim que  $\zeta_r^{ax} \cdot \zeta_s^{by} = \zeta_m^{ux+vy} = \zeta_m$ ; per tant,  $\zeta_m \in \mathbb{Q}(\zeta_r, \zeta_s)$ . i, en conseqüència, obtenim l'altra inclusió,  $\mathbb{Q}(\zeta_m) \subseteq \mathbb{Q}(\zeta_r, \zeta_s)$ .

Per a la segona part, és clar que  $\zeta_d \in \mathbb{Q}(\zeta_r) \cap \mathbb{Q}(\zeta_s)$ , de manera que té sentit considerar les extensions  $\mathbb{Q}(\zeta_r)|\mathbb{Q}(\zeta_d)$  i  $\mathbb{Q}(\zeta_s)|\mathbb{Q}(\zeta_d)$ , i la seva composició  $\mathbb{Q}(\zeta_m)|\mathbb{Q}(\zeta_d)$ . Els graus respectius d'aquestes extensions són  $\frac{\varphi(r)}{\varphi(d)}$ ,  $\frac{\varphi(s)}{\varphi(d)}$  i  $\frac{\varphi(m)}{\varphi(d)}$ ; i, com que  $\varphi(m)\varphi(d) = \varphi(r)\varphi(s)$ , tenim que el grau de la composició és el producte de graus; per tant, la intersecció de les dues extensions és l'extensió trivial; és a dir,  $\mathbb{Q}(\zeta_r) \cap \mathbb{Q}(\zeta_s) = \mathbb{Q}(\zeta_d)$ , com calia veure.

Els càlculs corresponen al diagrama

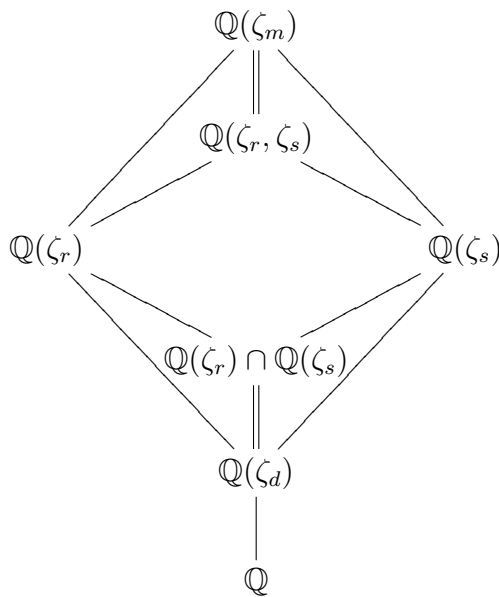


Diagrama C.1: Composició de cossos ciclotòmics, general

**Solució C.3.2** (de l'exercici 3.11.3). (a) Sigui  $f(X) := \Phi_{np}(X^{p^{r-1}})$ ; els dos polinomis  $\Phi_{np^r}(X)$  i  $f(X)$  són mònic, de coeficients enters i del mateix grau:

$$\text{gr}(f(X)) = p^{r-1} \text{gr}(\Phi_{np}(X)) = p^{r-1} \varphi(np) = \varphi(np^r) = \text{gr}(\Phi_{np^r}(X)).$$

Com que totes les arrels del polinomi  $\Phi_{np^r}(X)$  són simples, per a comprovar la igualtat  $\Phi_{np^r}(X) = f(X)$  és suficient veure que cadascuna de les arrels de  $\Phi_{np^r}(X)$  és una arrel del polinomi  $f(X)$ . I això és senzill; si  $\zeta$  és una arrel de  $\Phi_{np^r}(X)$ , llavors és un element d'ordre  $np^r$  del grup  $\mathbb{C}^*$ ; per tant,  $\zeta^{p^{r-1}}$  és un element d'ordre  $np$ , és a dir, una arrel de  $\Phi_{np}(X)$ ; o sigui,  $\zeta$  és una arrel de  $f(X)$ .

(b) El cas particular  $n = 1$  proporciona la igualtat  $\Phi_{p^r}(X) = \Phi_p(X^{p^{r-1}})$ ; com que

$$\Phi_p(X) = \frac{X^p - 1}{X - 1} = \sum_{i=0}^{p-1} X^i,$$

obtemin el resultat que volem en substituir  $X$  per  $X^{p^{r-1}}$ .

(c) Un nombre complex no nul,  $\zeta$ , és d'ordre  $2n$ , amb  $n \geq 1$  senar, si, i només si,  $-\zeta$  és d'ordre  $n$ ; per tant,  $\zeta$  és una arrel de  $\Phi_{2n}(X)$  si, i només si,  $-\zeta$  és una arrel de  $\Phi_n(X)$ ; i això equival a dir que  $\zeta$  és una arrel de  $\Phi_n(-X)$ . Ara bé, com que tots dos són polinomis mònic (aquí cal fer servir que  $n \geq 3$ , de manera que  $\text{gr}(\Phi_n(X)) = \varphi(n)$  és parell i, en conseqüència,  $\Phi_n(-X)$  també és mònic) i les seves arrels són simples, els polinomis coincideixen.

Notem que en el cas  $n = 1$ , tenim que  $\Phi_2(X) = X + 1 = -(-X - 1) = -\Phi_1(-X)$ .

(d) Demostrem la igualtat en la forma

$$\Phi_{np}(X)\Phi_n(X) = \Phi_n(X^p);$$

posem  $f(X) := \Phi_{np}(X)\Phi_n(X)$ . Notem que els dos polinomis  $f(X)$  i  $g(X) := \Phi_n(X^p)$  són mònicos i del mateix grau

$$\varphi(np) + \varphi(n) = \varphi(n)(\varphi(p) + 1) = \varphi(n)p.$$

A més a més, totes les arrels de  $f(X)$  són simples; per tant, és suficient veure que totes les arrels de  $f(X)$  són arrels de  $\Phi_n(X^p)$ .

Ara, si  $\zeta$  és una arrel de  $f(X)$ , pot ser-ho de  $\Phi_{np}(X)$  o bé de  $\Phi_n(X)$ ; això és dir que  $\zeta$  és un element de  $\mathbb{C}^*$  d'ordre exactament  $np$  o bé  $n$ ; en tots dos casos,  $\zeta^p$  és un element d'ordre  $n$ , és a dir, una arrel de  $\Phi_n(X)$ ; equivalentment,  $\zeta$  és una arrel de  $\Phi_n(X^p)$ .

**Solució C.3.3** (de l'exercici 3.11.4). Suposem que podem escriure un nombre natural  $n$  en la forma  $n = n'p^r$ , on  $p$  és un nombre primer,  $r > 1$ , i  $n'$  no és divisible per  $p$ . Com que per als polinomis ciclotòmics se satisfà la igualtat  $\Phi_n(X) = \Phi_{n'p}(X^{p^{r-1}})$ , si el polinomi  $\Phi_n(X)$  tingués algun coeficient diferent de  $-1, 0$  i  $1$ , llavors  $\Phi_{n'p}(X)$  també en tindria.

Podem aplicar aquest resultat reiteradament a tots els factors primers que divideixen  $n$  amb exponent estrictament més gran que 1; això implica que el menor  $n$  per al qual algun dels coeficients de  $\Phi_n(X)$  és diferent de  $-1, 0$  i  $1$  és un nombre natural lliure de quadrats.

D'altra banda, si  $n = 2n'$ , amb  $n'$  senar, la igualtat de polinomis  $\Phi_n(X) = \Phi_{n'}(-X)$  ens diu que si algun dels coeficients de  $\Phi_n(X)$  fos diferent de  $-1, 0$  i  $1$ , llavors també ho seria el coeficient corresponent de  $\Phi_{n'}(X)$  (potser canviat de signe). Per tant, si  $n$  és el menor nombre tal que algun dels coeficients del polinomi  $\Phi_n(X)$  és diferent de  $-1, 0$  o  $1$ , llavors  $n$  és senar (i lliure de quadrats).

A més a més, per a tot nombre primer senar  $p$ , és  $\Phi_p(X) = 1 + X + X^2 + \dots + X^{p-1}$ , de manera que els seus primers  $p$  coeficients són iguals a 1, i tots els posteriors, a 0. Com a conseqüència, el menor nombre natural  $n$  (si existeix) tal que algun dels coeficients del polinomi ciclotòmic  $\Phi_n(X)$  és diferent de  $-1, 0$  i  $1$  és un nombre senar, compost i lliure de quadrats.

Ara, notem que  $105 = 3 \cdot 5 \cdot 7$  és el menor nombre natural senar, compost, lliure de quadrats, i que és el producte de tres o més nombres primers diferents. I el polinomi ciclotòmic 105-èsim és

$$\begin{aligned} \Phi_{105}(X) = & X^{48} + X^{47} + X^{46} - X^{43} - X^{42} - 2X^{41} \\ & - X^{40} - X^{39} + X^{36} + X^{35} + X^{34} \\ & + X^{33} + X^{32} + X^{31} - X^{28} - X^{26} - X^{24} \\ & - X^{22} - X^{20} + X^{17} + X^{16} + X^{15} \\ & + X^{14} + X^{13} + X^{12} - X^9 - X^8 \\ & - 2X^7 - X^6 - X^5 + X^2 + X + 1; \end{aligned}$$

els coeficients de  $X^7$  i de  $X^{41}$  del qual són iguals a  $-2$ . Així,  $n = 105$  és un exemple d'allò que demana l'enunciat.

Per a provar que  $n = 105$  és el menor, només resta veure que per a tota parella de nombres primers senars diferents,  $p, q$ , tals que  $pq < 105$ , tots els coeficients del polinomi  $\Phi_{pq}(X)$  pertanyen al conjunt  $\{-1, 0, 1\}$ . I un simple càlcul (per exemple, hom pot usar algun manipulador algebraic) acaba la demostració.

**Observació:** Es pot demostrar (ho fem de seguida) que si  $p, q$  són dos nombres primers diferents qualssevol, no necessàriament tals que  $pq < 105$ , llavors tots els coeficients del

polinomi ciclotòmic  $\Phi_{pq}(X)$  pertanyen al conjunt  $\{-1, 0, 1\}$ . Això fa que el menor possible nombre natural  $n$  per al qual el polinomi ciclotòmic  $\Phi_n(X)$  té algun coeficient diferent de  $-1, 0$  i  $1$  sigui  $3 \cdot 5 \cdot 7 = 105$ , i no cal fer cap recerca exhaustiva entre els nombres menors que  $105$  que són producte de dos nombres primers diferents.

El recíproc d'aquest resultat és fals. Per exemple, per a  $n = 651 = 3 \cdot 7 \cdot 31$ , tots els coeficients del polinomi ciclotòmic són  $-1, 0$  o  $1$ , com posa de manifest la taula següent, que conté els coeficients d'aquest polinomi.

1, 1, 1, 0, 0,	0, 0, -1, -1, -1,	0, 0, 0, 0, 0,	0, 0, 0, 0, 0,
0, 1, 1, 1, 0,	0, 0, 0, -1, -1,	-1, -1, -1, -1, 0,	0, 0, 0, 1, 1,
1, 0, 1, 1, 1,	0, 0, 0, 0, -1,	-1, -1, -1, -1, -1,	0, 0, 0, 0, 1,
1, 1, 0, 1, 1,	1, 0, 0, 0, 0,	-1, -1, -1, -1, -1,	-1, 0, 0, 0, 0,
1, 1, 1, 0, 1,	1, 1, 0, 0, 0,	0, -1, -1, 0, 0,	0, -1, 0, 0, 0,
-1, 0, 0, 1, 0,	1, 1, 1, 0, 0,	0, 0, -1, -1, 0,	0, 0, -1, 0, 0,
0, -1, 0, 0, 0,	-1, 0, 1, 1, 0,	0, 1, 1, 0, -1,	0, 0, 0, -1, 0,
0, 0, -1, 0, 0,	0, -1, 0, 1, 1,	0, 0, 1, 1, 0,	-1, 0, 0, 0, -1,
0, 0, 0, -1, 0,	0, 0, -1, 0, 1,	1, 0, 0, 1, 1,	0, -1, 0, 0, 0,
-1, 0, 0, 0, -1,	0, 1, 1, 0, 0,	1, 1, 0, -1, 0,	0, 0, -1, 0, 0,
0, -1, 0, 0, 0,	-1, 0, 1, 1, 0,	0, 1, 1, 0, -1,	0, 0, 0, -1, 0,
0, 0, -1, 0, 0,	0, -1, 0, 1, 1,	0, 0, 1, 1, 0,	-1, 0, 0, 0, -1,
0, 0, 0, -1, 0,	0, 0, -1, -1, 0,	0, 0, 0, 1, 1,	1, 0, 1, 0, 0,
-1, 0, 0, 0, -1,	0, 0, 0, -1, -1,	0, 0, 0, 0, 1,	1, 1, 0, 1, 1,
1, 0, 0, 0, 0,	-1, -1, -1, -1, -1,	-1, 0, 0, 0, 0,	1, 1, 1, 0, 1,
1, 1, 0, 0, 0,	0, -1, -1, -1, -1,	-1, -1, 0, 0, 0,	0, 1, 1, 1, 0,
1, 1, 1, 0, 0,	0, 0, -1, -1, -1,	-1, -1, -1, 0, 0,	0, 0, 1, 1, 1,
0, 0, 0, 0, 0,	0, 0, 0, 0, 0,	0, -1, -1, -1, 0,	0, 0, 0, 1, 1,

1

Demostrem, doncs, que si  $p, q$  són nombres primers senars diferents, llavors tots els coeficients de  $\Phi_{pq}(X)$  pertanyen al conjunt  $\{-1, 0, 1\}$ .

Per a això, comencem per adonar-nos del fet que podem escriure  $\Phi_p(X^q)$  en la forma

$$\Phi_p(X^q) = \sum_{i=0}^{p-1} X^{pe_i} X^i,$$

per a certs exponents  $e_i \geq 0$  escaients.

En efecte, a partir de la igualtat  $\Phi_p(X^q) = \sum_{j=0}^{p-1} X^{qj}$ , i si fem la divisió entera de cada exponent  $qj$  entre  $p$ , obtenim igualtats  $qj = pd_j + r_j$ , amb  $0 \leq r_j \leq p-1$ , i  $d_j \geq 0$ . Ara bé, com que  $q \neq p$ ,  $q$  és invertible mòdul  $p$  i el conjunt de nombres  $\{qj : 0 \leq j \leq p-1\}$  és un conjunt complet de representants de les classes mòdul  $p$ ; per tant, el conjunt format pels residus  $r_j$ ,  $0 \leq j \leq p-1$ , coincideix amb el conjunt  $\{0, 1, \dots, p-1\}$ . O sigui, la successió  $r_0, r_1, \dots, r_{p-1}$  és una reordenació de la successió  $0, 1, \dots, p-1$ . Així, l'escriptura

$$\Phi_p(X^q) = \sum_{j=0}^{p-1} X^{qj} = \sum_{i=0}^{p-1} X^{pe_i} X^i,$$

on  $e_i = d_j$ , si  $i = r_j$ , només és una reordenació dels sumands, d'acord amb la classe residual mòdul  $p$  de l'exponent  $qj$ .

Anàlogament, en multiplicar per  $X$  i restar, podem escriure

$$\Phi_p(X^q)(X - 1) = \sum_{i=0}^{p-1} ((X^p)^{a_i} - (X^p)^{e_i})X^i,$$

per a certs nombres enters  $a_i, e_i \geq 0$ .

Fins aquí no hem fet servir per a res que  $q$  sigui un nombre primer; només, que no és divisible per  $p$ , de manera que és invertible mòdul  $p$ . Ara ens restringirem al cas en què  $q$  és primer per a calcular explícitament el polinomi ciclotòmic  $\Phi_{pq}(X)$ .

Com que  $q$  és primer i no divideix  $p$ ; podem aplicar la fórmula

$$\Phi_{pq}(X) = \frac{\Phi_p(X^q)}{\Phi_p(X)},$$

de manera que obtenim l'expressió

$$\begin{aligned} \Phi_{pq}(X) &= \frac{\Phi_p(X^q)}{\Phi_p(X)} = \frac{\Phi_p(X^q)(X - 1)}{\Phi_p(X)(X - 1)} = \frac{\Phi_p(X^q)(X - 1)}{X^p - 1} \\ &= \sum_{i=0}^{p-1} \frac{(X^p)^{a_i} - (X^p)^{e_i}}{X^p - 1} X^i. \end{aligned}$$

Ara bé, els polinomis  $(X^p)^{a_i} - (X^p)^{e_i}$ , són polinomis en  $X^p$ , i divisibles per  $X^p - 1$ , de manera que, per a obtenir els coeficients de tots els monomis de grau  $\equiv i \pmod{p}$  del polinomi  $\Phi_{pq}(X)$ , només hem de dividir els polinomis  $(X^p)^{a_i} - (X^p)^{e_i}$  per  $X^p - 1$ . Com que la divisió proporciona les igualtats

$$\frac{(X^p)^{a_i} - (X^p)^{e_i}}{X^p - 1} = \begin{cases} -X^{pa_i} \sum_{j=0}^{e_i - a_i - 1} (X^p)^j, & \text{si } a_i < e_i \\ 0, & \text{si } a_i = e_i \\ X^{pe_i} \sum_{j=0}^{a_i - e_i - 1} (X^p)^j, & \text{si } a_i > e_i \end{cases}$$

(tots els coeficients,  $-1$ ),  
(tots els coeficients,  $0$ ),  
(tots els coeficients,  $1$ ),

resulta que tots els coeficients pertanyen al conjunt  $\{-1, 0, 1\}$ , com calia provar.

**Solució C.3.4** (de l'exercici 3.11.5). (a) Com que el polinomi  $\Phi_n(X)$  divideix  $X^n - 1$  en  $\mathbb{Z}[X]$ , existeix un polinomi  $f(X) \in \mathbb{Z}[X]$  tal que  $X^n - 1 = \Phi_n(X)f(X)$ ; llavors, per a tot nombre enter  $m$ , és  $m^n - 1 = \Phi_n(m)f(m)$ , de manera que el nombre  $m^n - 1$  és múltiple enter de  $\Phi_n(m)$ ; en particular, si aquest darrer és múltiple d'un nombre primer  $p$ , tenim que  $m^n - 1$  també és múltiple de  $p$ .

- (b) Ara, si  $d$  és l'ordre (multiplicatiu) de  $m$  mòdul  $p$ , tenim que  $d$  divideix  $n$  (perquè  $m^n \equiv 1 \pmod{p}$ ); i que  $p \equiv 1 \pmod{d}$  (perquè  $m^{p-1} \equiv 1 \pmod{p}$ , pel petit teorema de Fermat).

Si fos  $e := n/d > 1$ , el polinomi  $\frac{X^n - 1}{X^d - 1} = \sum_{i=0}^{e-1} X^{di}$  seria múltiple, en  $\mathbb{Z}[X]$ , del polinomi  $\Phi_n(X)$ . En efecte, això s'obté de les igualtats

$$X^k - 1 = \prod_{\delta|k} \Phi_\delta(X),$$

per a  $k = n$  i  $k = d < n$ ; el quocient corresponent és el producte de  $\Phi_n(X)$  pels polinomis ciclotòmics  $\Phi_\delta(X)$  en els casos  $\delta|n$ ,  $\delta \nmid d$ ,  $\delta < n$ .

Ara, del fet que  $p$  divideix  $\Phi_n(m)$ , obtenim que  $p$  divideix la suma  $\sum_{i=0}^{e-1} m^{di}$  i, com que

$$\sum_{i=0}^{e-1} m^{di} \equiv \sum_{i=0}^{e-1} 1 = e \pmod{p},$$

tenim que  $p$  divideix  $e$ ; per tant,  $p$  divideix  $n = de$ .

- (c) Així, si  $p$  no divideix  $n$ , no pot ser  $e > 1$ , de manera que  $d = n$  és l'ordre de  $m$  mòdul  $p$ , que divideix  $p - 1$ ; és a dir,  $p \equiv 1 \pmod{n}$ , com volíem veure.

Finalment, notem que si  $p$  divideix  $\Phi_n(n)$ , llavors  $p \nmid n$ , per la primera part, i  $p \equiv 1 \pmod{n}$ , per la segona.

- (d) Per a qualsevol nombre real  $x > 1$ , la distància entre  $x$  i qualsevol de les  $\varphi(n)$  arrels  $n$ -èsimes primitives de la unitat és estrictament més gran que la seva distància a 1; i, si  $x \geq 2$ , aquesta és més gran o igual que 1; per tant,

$$|\Phi_n(x)| = \prod_{\zeta \in \mu_n(\mathbb{C}), \zeta \text{ primitiva}} |x - \zeta| > |x - 1|^{\varphi(n)} \geq x - 1,$$

perquè  $n > 1$  i  $x \geq 2$ .

- (e) D'entrada, podem suposar que  $n \geq 2$  (i, si es vol, que  $n \geq 3$ , ja que tots els nombres primers, excepte  $p = 2$ , són senars i, per tant, congrus a 1 mòdul 2). D'acord amb la indicació, considerem la successió formada pels nombres enters  $kn$ , per a  $k \geq 1$ . Per a cadascun d'aquests valors, i pel resultat de l'apartat (d), tenim un nombre enter  $\Phi_{kn}(kn)$  tal que  $|\Phi_{kn}(kn)| > 1$ , de manera que és divisible per algun nombre primer  $p_k$ . Per l'apartat (c), obtenim que  $p_k \equiv 1 \pmod{kn}$ ; d'on  $p_k \equiv 1 \pmod{n}$ , i  $p_k > kn > k$ .

Així, hem provat que, per a tot nombre natural  $k$ , existeix un nombre primer més gran que  $k$  i que és congru a 1 modul  $n$ ; d'aquí es dedueix l'existència d'una infinitat de nombres primers  $p \equiv 1 \pmod{n}$ .

**Solució C.3.5** (de l'exercici 3.11.6). Notem que el producte de Dirichlet es pot escriure en la forma

$$(f * g)(n) = \sum_{de=n} f(d)g(e),$$

expressió a partir de la qual és més còmoda la demostració de la propietat associativa de la convolució:

$$\begin{aligned} ((f * g) * h)(n) &= \sum_{de=n} (f * g)(d)h(e) = \sum_{de=n} \sum_{\delta\varepsilon=d} f(\delta)g(\varepsilon)h(e) \\ &= \sum_{\delta\varepsilon e=n} f(\delta)g(\varepsilon)h(e), \end{aligned}$$

$$\begin{aligned} (f * (g * h))(n) &= \sum_{\delta d=n} f(\delta)(g * h)(d) = \sum_{\delta d=n} f(\delta) \sum_{\varepsilon e=d} g(\varepsilon)h(e) \\ &= \sum_{\delta\varepsilon e=n} f(\delta)g(\varepsilon)h(e); \end{aligned}$$

la resta de les propietats d'anell es demostren de manera immediata, sense cap dificultat. En particular, si l'anell  $A$  és commutatiu, el producte de Dirichlet també ho és, i l'anell de les funcions aritmètiques amb el producte de Dirichlet és un anell commutatiu. Per exemple, les igualtats

$$(f * \delta)(n) = \sum_{de=n} f(d)\delta(e) = f(n)\delta(1) + \sum_{de=n, e>1} f(d)\delta(e) = f(n) + 0 = f(n)$$

ens ensenyen que la funció  $\delta$  és l'element unitat (per la dreta) de l'anell.

Ara, notem que, amb les notacions de l'enunciat, tenim que  $\mu * u = u * \mu$ , perquè  $\mu$  i  $u$  només prenen valors en el centre de  $A$ , i que

$$(\mu * u)(n) = \sum_{d|n} \mu(d)u(n/e) = \sum_{d|n} \mu(d) = \delta(n),$$

de manera que, efectivament, la funció  $u$  és invertible i la seva inversa és la funció  $\mu$ ; és a dir, que  $\mu * u = u * \mu = \delta$ . En efecte, repetim la demostració de la proposició **3.2.16**. Per a  $n = 1$ , és clar que  $\sum_{d|1} \mu(d) = \mu(1) = 1 = \delta(1)$ . I per a  $n > 1$ , comencem per considerar

la descomposició de  $n$  com a producte de nombres primers,

$$n = p_1^{a_1} \cdots p_r^{a_r}, \quad r \geq 1, \quad a_1, \dots, a_r \geq 1,$$

on  $p_1, \dots, p_r$  designen nombres naturals primers diferents dos a dos. Llavors, els divisors naturals de  $n$  són els nombres

$$d = p_1^{b_1} \cdots p_r^{b_r}, \quad b_1, \dots, b_r \geq 0,$$

de manera que  $\mu(d) = 0$  per a tots els divisors  $d$  per als quals algun dels exponents  $b_i$  es tingui que  $b_i \geq 2$ . Així,

$$\sum_{d|n} \mu(d) = \sum_{b_1, \dots, b_r \in \{0,1\}} \mu(p_1^{b_1} \cdots p_r^{b_r}) = \sum_{k=0}^r \binom{r}{k} (-1)^k = (1-1)^r = 0 = \delta(n),$$

com calia provar.

Això ja ens dona immediatament la propietat de l'enunciat, ja que aquesta es pot escriure en la forma

$$f * u = g \quad \Leftrightarrow \quad f = g * \mu,$$

i només cal multiplicar per  $\mu$  la primera igualtat per a obtenir la segona i, a l'inrevés, multiplicar per  $u$  la segona per a obtenir la primera.

**Solució C.3.6** (de l'exercici 3.11.7). Recordem que el cos  $\mathbb{F}_{q^d}$  és subcòs de  $\mathbb{F}_{q^n}$  si, i només si,  $d$  divideix  $n$ , i que  $\mathbb{F}_{q^n}$  és el cos de descomposició del polinomi  $X^{q^n} - X \in \mathbb{F}_q[X]$ .

- (a,b) Com a conseqüència, els elements de  $\mathbb{F}_{q^n}$  són les arrels dels polinomis irreductibles que divideixen  $X^{q^n} - X$ ; i, d'altra banda, són els elements que generen els subcossos de  $\mathbb{F}_{q^n}$ , és a dir, els cossos  $\mathbb{F}_{q^d}$ , per a  $d$  divisor de  $n$ .

Així, els dos polinomis

$$X^{q^n} - X, \quad \prod_{d|n} \prod_{f_d} f_d(X),$$

són mòncics, tenen les mateixes arrels, i cap d'ells no té factors múltiples; per tant, coincideixen.

- (c) La igualtat desitjada s'obté en escriure els graus dels polinomis a la igualtat anterior:

$$q^n = \sum_{d|n} \sum_{f_d} \text{gr}(f_d) = \sum_{d|n} \sum_{f_d} d = \sum_{d|n} d\psi_q(d).$$

- (d) Només cal aplicar la fórmula d'inversió de Möbius a la igualtat de (c) i, després, dividir per  $n$ .
- (e) Notem que el nombre enter  $\sum_{d|n} \mu(d)q^{n/d}$  és múltiple de  $q$ , ja que ho són tots els sumands; com que el quocient d'aquest nombre per  $n$  és el nombre natural  $\psi_q(n)$ , si  $\text{mcd}(n, q) = 1$ , no es pot simplificar cap factor de  $q$ ; és a dir, si  $\text{mcd}(n, q) = 1$ , llavors  $\psi_q(n)$  és múltiple enter de  $q$ .

## C.4 Exercicis del capítol 4

**Solució C.4.1** (de l'exercici 4.13.1). (a) Tenim la cadena d'extensions

$$k = \mathbb{F}_p(t^p, u^p) \subsetneq \mathbb{F}_p(t^p, u) \subsetneq \mathbb{F}_p(t, u) = L,$$

i cadascuna és de grau  $p$ . En efecte, el polinomi  $X^p - u^p \in \mathbb{F}_p(t^p)[u^p][X]$  és mònic i irreductible (per exemple, perquè és de grau 1 en  $u^p$ ), i admet  $u$  com a arrel; per tant,  $[\mathbb{F}_p(t^p, u) : \mathbb{F}_p(t^p, u^p)] = p$ . I anàlogament per a l'altra extensió: el polinomi  $X^p - t^p \in \mathbb{F}_p(u)[t^p][X]$  és mònic i irreductible i admet  $t$  com a arrel; per tant, també  $[\mathbb{F}_p(t, u) : \mathbb{F}_p(t^p, u)] = p$ .

- (b) Clarament, si  $\alpha \in L$ , llavors  $\alpha = \alpha(t, u)$  és un quocient de polinomis en  $t, u$ , i coeficients en  $\mathbb{F}_p$ . Com que el cos és de característica  $p$  i per als coeficients és  $c^p = c$ , resulta que  $\alpha(t, u)^p = \alpha(t^p, u^p) \in \mathbb{F}_p(t^p, u^p) = k$ ; és a dir,  $\alpha$  és arrel del polinomi  $X^p - \alpha^p \in k[X]$ , de grau  $p$ ; per tant, el grau de  $k(\alpha)$  sobre  $k$  és menor o igual que  $p$ .

A més a més, el grau és un divisor de  $p^2$ ; per tant, el grau és  $p$  o bé 1; i només és 1 si  $\alpha \in k$ .

- (c) Com que l'extensió  $L|k$  no admet element primitiu i és finita, hi ha d'haver una infinitat de cossos intermedis.



- (d) Per a cada element  $f(t^p, u^p) \in \mathbb{F}_p(t^p, u^p) = k$ , i n'hi ha una infinitat, podem considerar l'extensió  $K_f := k(uf(t^p, u^p) + t) | k$  (cf. la demostració de la proposició 4.5.3). I totes són diferents.

En efecte, notem que per a  $f_1(t^p, u^p) \neq f_2(t^p, u^p)$ , podem escriure

$$u = \frac{(uf_1(t^p, u^p) + t) - (uf_2(t^p, u^p) + t)}{f_1(t^p, u^p) - f_2(t^p, u^p)},$$

de manera que si  $K_{f_1} = K_{f_2} =: K$ , llavors  $u \in K$  i, per tant, també  $t \in K$ , de manera que  $K = L$ ; i això és una contradicció amb el fet que  $L | k$  no admet element primitiu.

**Solució C.4.2** (de l'exercici 4.13.2). Sigui  $\sigma \in \text{Gal}(\mathbb{Q}(\alpha_1, \alpha_2) | \mathbb{Q}(\alpha_1 \cdot \alpha_2))$ ; llavors,  $\sigma(\alpha_1) \cdot \sigma(\alpha_2) = \sigma(\alpha_1 \cdot \alpha_2) = \alpha_1 \cdot \alpha_2$ , i podem definir

$$q := \frac{\sigma(\alpha_1)}{\alpha_1} = \frac{\alpha_2}{\sigma(\alpha_2)}.$$

Com que les extensions  $\mathbb{Q}(\alpha_i) | \mathbb{Q}$  són normals, la restricció de  $\sigma$  a  $\mathbb{Q}(\alpha_i)$  és un automorfisme de  $\mathbb{Q}(\alpha_i)$  i, per tant,

$$q = \frac{\sigma(\alpha_1)}{\alpha_1} = \frac{\alpha_2}{\sigma(\alpha_2)} \in \mathbb{Q}(\alpha_1) \cap \mathbb{Q}(\alpha_2) = \mathbb{Q}.$$

Això ens diu que  $\sigma(\alpha_1) = q\alpha_1$ ; i, en conseqüència, per a tot nombre natural  $n$  es té que  $\sigma^n(\alpha_1) = q^n \alpha_1$ . Si tenim en compte que la restricció de  $\sigma$  a  $\mathbb{Q}(\alpha_1)$  és d'ordre finit i divisor del grau  $[\mathbb{Q}(\alpha_1) : \mathbb{Q}] = \#\text{Gal}(\mathbb{Q}(\alpha_1) | \mathbb{Q})$ , per al valor de  $n$  igual a l'ordre d'aquesta restricció de  $\sigma$  resulta que és  $q^n = 1$ . Així,  $q$  és una arrel de la unitat de  $\mathbb{Q}$  i, per tant,  $q = 1$  o bé  $q = -1$ . I la segona possibilitat només es pot donar si el grau  $[\mathbb{Q}(\alpha_1) : \mathbb{Q}]$  és parell.

En conseqüència, si els dos graus  $[\mathbb{Q}(\alpha_i) : \mathbb{Q}]$ ,  $i = 1, 2$ , són senars, resulta que  $q = 1$  i llavors  $\sigma(\alpha_i) = \alpha_i$ ,  $i = 1, 2$ , de manera que  $\sigma$  és la identitat en  $\mathbb{Q}(\alpha_1, \alpha_2)$ . Això diu que el grup de Galois  $\text{Gal}(\mathbb{Q}(\alpha_1, \alpha_2) | \mathbb{Q}(\alpha_1 \cdot \alpha_2))$  és trivial i, per tant, que  $\mathbb{Q}(\alpha_1, \alpha_2) = \mathbb{Q}(\alpha_1 \cdot \alpha_2)$ , com volíem provar.

## C.5 Exercicis del capítol 5

**Solució C.5.1** (de l'exercici 5.6.14). L'extensió és separable, de manera que admet un element primitiu,  $\alpha$ . I per a cada arrel  $\beta$  del polinomi  $\text{Irr}(\alpha, k)(X) \in k[X]$  existeix un  $k$ -automorfisme  $\sigma$  de  $K$  tal que  $\sigma(\alpha) = \beta$ . Així, per a cada parella d'arrels del polinomi  $\text{Irr}(\alpha, k)(X)$  hi ha un element del grup de Galois  $\text{Gal}(K | k)$  que transforma l'una en l'altra; és a dir,  $\text{Gal}(K | k)$  actua transitivament en el conjunt de les arrels de  $\text{Irr}(\alpha, k)(X)$ , com calia veure.

**Solució C.5.2** (de l'exercici 5.13.1). Calculem  $g(\zeta)^2$  en la forma  $g(\zeta)^2 =$

$$\sum_{a \neq 0 \pmod{p}} \left(\frac{a}{p}\right) \zeta^a \sum_{b \neq 0 \pmod{p}} \left(\frac{b}{p}\right) \zeta^b = \sum_{a \neq 0 \pmod{p}} \sum_{b \neq 0 \pmod{p}} \left(\frac{ab}{p}\right) \zeta^{a+b}.$$

Ara, per a  $a \not\equiv 0 \pmod{p}$ , podem escriure  $b = ac$ , amb  $c \not\equiv 0 \pmod{p}$ , de manera bijectiva, perquè  $a$  és invertible; per tant, i perquè  $\left(\frac{a^2}{p}\right) = 1$ , podem escriure la nova expressió  $g(\zeta)^2 =$

$$\sum_{c \not\equiv 0 \pmod{p}} \sum_{a \not\equiv 0 \pmod{p}} \left(\frac{a^2 c}{p}\right) \zeta^{(1+c)a} = \sum_{c \not\equiv 0 \pmod{p}} \left(\frac{c}{p}\right) \sum_{a \not\equiv 0 \pmod{p}} \zeta^{(1+c)a}.$$

Si  $c \not\equiv -1 \pmod{p}$ , llavors  $\zeta^{1+c}$  és una arrel primitiva  $p$ -èsima de la unitat, de manera que  $\sum_{a \not\equiv 0 \pmod{p}} \zeta^{(1+c)a} = -1$ . I si  $c \equiv -1 \pmod{p}$ , llavors  $\zeta^{c+1} = 1$ , de manera que

$$\sum_{a \not\equiv 0 \pmod{p}} \zeta^{(1+c)a} = p - 1. \text{ Això proporciona l'expressió}$$

$$g(\zeta)^2 = \sum_{c \not\equiv 0, -1 \pmod{p}} \left(\frac{c}{p}\right) (-1) + \left(\frac{-1}{p}\right) (p - 1) = \left(\frac{-1}{p}\right) p,$$

perquè

$$\sum_c \left(\frac{c}{p}\right) = 0.$$

**Solució C.5.3** (de l'exercici 5.13.2). (a) L'exercici anterior, (5.13.1), ens permet dir que  $\mathbb{Q}(\sqrt{p^*}) \subseteq \mathbb{Q}(\zeta_p)$ . A més a més, l'extensió  $\mathbb{Q}(\zeta_p)|\mathbb{Q}$  és cíclica de grau parell, per tant, admet una única subextensió de grau 2.

(b) És clar que  $\mathbb{Q}(\sqrt{-1}) = \mathbb{Q}(\zeta_4)$ ; per tant,  $\mathbb{Q}(\sqrt{p}) \subseteq \mathbb{Q}(\sqrt{p^*}, \sqrt{-1}) \subseteq \mathbb{Q}(\zeta_p, \zeta_4) = \mathbb{Q}(\zeta_{4p})$ . A més a més, notem que si  $p \equiv 1 \pmod{4}$ , llavors  $p = p^*$ , de manera que  $4p$  no és òptim; en aquest cas,  $\mathbb{Q}(\sqrt{p}) \subseteq \mathbb{Q}(\zeta_p)$ , i  $p$  és òptim.

(c) Notem que  $\mathbb{Q}(\zeta_8) = \mathbb{Q}(\sqrt{2}, \zeta_4)$ ; per tant, també  $\mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{-2}) \subseteq \mathbb{Q}(\zeta_8)$ . Notem que, en aquest cas, si posem  $p = 2$ , és  $\mathbb{Q}(\sqrt{p}), \mathbb{Q}(\sqrt{-p}) \subseteq \mathbb{Q}(\zeta_{4p})$ .

(d) De nou, per composició, si  $n = \pm p_1 \cdots p_r$ , amb  $p_1, \dots, p_r$  nombres naturals primers diferents (entre els quals pot haver-hi el 2), llavors es té que  $\mathbb{Q}(\sqrt{n}) \subseteq \mathbb{Q}(\zeta_{4n})$  (aquí cal entendre, òbviament,  $\zeta_{-m} = \zeta_m$ ).

(e) Si  $n \in \mathbb{Z}$ , i  $n \equiv 1 \pmod{4}$ , llavors  $\mathbb{Q}(\sqrt{n}) \subseteq \mathbb{Q}(\zeta_n)$ ; però si  $n \not\equiv 1 \pmod{4}$ , llavors  $4n$  és òptim.

**Solució C.5.4** (de l'exercici 5.13.3). Les propietats (a) i (b) són simples comprovacions; no ens hi entretenim.

(c) Es pot argumentar que els exponents de  $\zeta$  en els períodes són les classes laterals del subgrup format pels exponents del període  $\eta_0$ ; i aquest subgrup no depèn del generador; ni les classes laterals tampoc. A més a més, si canviem  $\zeta$  per una altra arrel primitiva  $p$ -èsima de la unitat  $\zeta'$ , podem escriure  $\zeta' = \zeta^{g^\alpha}$  per a un cert nombre enter  $\alpha$ ; aleshores, per a tot nombre nombre enter  $i$ ,  $0 \leq i \leq n - 1$ , és

$$\eta'_i = \sum_{j=0}^{d-1} \zeta'_{i+jn} = \sum_{j=0}^{d-1} \zeta_{\alpha+i+jn} = \eta_{\alpha+i}.$$

Per tant, els períodes  $\eta_i$  es poden obtenir com els períodes  $\eta_0$  associats a les diferents arrels primitives  $p$ -èsimes de la unitat.

- (d) Sigui, ara,  $K|\mathbb{Q}$  una subextensió de  $\mathbb{Q}(\zeta)|\mathbb{Q}$ . El grau  $n := [K : \mathbb{Q}]$  és un divisor de  $p-1$  i  $K$  és el cos fix per l'únic subgrup  $H \subseteq \text{Gal}\mathbb{Q}(\zeta)|\mathbb{Q}$  d'índex  $n$ . Per tant, el cos  $K$  és generat sobre  $\mathbb{Q}$  pels coeficients del polinomi irreductible de  $\zeta$  sobre el cos  $K$ . Ara bé,  $H$  és el grup  $\langle \sigma^n \rangle$ , de manera que

$$\text{Irr}(\zeta, K)(X) = \prod_{\tau \in H} (X - \tau(\zeta)) = \prod_{j=0}^{d-1} (X - \sigma^{jn}(\zeta)),$$

on  $d := \frac{p-1}{n}$ ; els coeficients d'aquest polinomi són els polinomis simètrics elementals  $s_k := s_k(x_0, x_1, \dots, x_{d-1})$ ,  $1 \leq k \leq d$ , dels elements  $x_j := \sigma^{jn}(\zeta) = \zeta_{jn}$ ,  $0 \leq j \leq d-1$ . El cos generat sobre  $\mathbb{Q}$  pels polinomis simètrics elementals  $s_k(x_0, x_1, \dots, x_{d-1})$  és el mateix que el generat pels polinomis de Newton  $t_k := t_k(x_0, x_1, \dots, x_{d-1}) := \sum_{j=0}^{d-1} x_j^k$  (cf. l'exercici **2.6.1**). Aquests darrers són exactament

els  $n$ -períodes de  $\zeta$  relatius a un cert generador  $g'$  de  $(\mathbb{Z}/p\mathbb{Z})^*$ : en efecte, com que  $1 \leq k < p$ , el nombre enter  $k$  és una unitat de  $(\mathbb{Z}/p\mathbb{Z})^*$  i es pot escriure en la forma  $k = g^i$  per a un cert nombre enter  $i$ ; aleshores,  $t_k = \eta_i$ . Per tant,  $K \subseteq \mathbb{Q}(\eta_0, \eta_1, \dots, \eta_{n-1})$ . D'altra banda, de la definició dels períodes és clar que  $\sigma^n(\eta_i) = \eta_i$ , de manera que  $\eta_i \in K$ , ja que  $K$  és el cos fix per  $\langle \sigma^n \rangle$ . Això demostra la igualtat  $K = \mathbb{Q}(\eta_0, \eta_1, \dots, \eta_{n-1})$ .

Finalment, se satisfà la igualtat  $\sigma^j(\eta_i) = \eta_{i+j}$ , per a tota parella de nombres enters  $i, j$ ; per tant, els períodes  $\eta_i$  són tots conjugats; com que  $\mathbb{Q}(\eta_i) \subseteq \mathbb{Q}(\zeta)$ , l'extensió  $\mathbb{Q}(\eta_i)|\mathbb{Q}$  és de Galois (i abeliana), de manera que  $K = \mathbb{Q}(\eta_i)$ , com volem veure.



# Apèndix D

## Cronologia

Destinem aquest apèndix a presentar un llistat, ordenat cronològicament, de les persones que, d'una manera o altra, apareixen en el text i de les quals coneixem el lloc o la data de naixement.

### **Euclides**

(*Εὐκλείδης*) Euclides d'Alexandria

(Alexandria, Egipte, aprox. 323 a.C.; Alexandria, Egipte, aprox. 285 a.C.)

### Scipione **del Ferro**

(Bolonya, Estats Pontificis; 6 de febrer de 1465, Bolonya, Estats Pontificis, 20 de novembre de 1526)

### Nicolò Fontana, **Tartaglia**

(Brescia, República de Venècia, aprox. 1499; Venècia, República de Venècia, 13 de desembre de 1557)

### Girolamo **Cardano**

Hieronimus Cardanus

(Pavia, Ducat de Milà, Sacre Imperi, 24 de setembre de 1501; Roma, Estats Pontificis, 21 de setembre de 1576)

### Lodovico **Ferrari**

(Bolonya, Estats Pontificis, 2 de febrer de 1522; Bolonya, Estats Pontificis, 5 d'octubre de 1565)

### François **Viète**

(Fontenay-le-Comte, Poitou—ara Vendée, França, 1540; París, França, 13 de desembre de 1603)

### René **Descartes**

(La Haye en Touraine, actualment Descartes, França, 31 de març de 1596; Estocolm, Suècia, 11 de febrer de 1650)

### Pierre de **Fermat**

(Beaumont de Lomagne, França, 17 d'agost de 1601; Castres, França, 12 de gener de 1665)

### Isaac **Newton**

(Woolfsthorpe by Colsterworth, Anglaterra, 25 de desembre de 1642 (Ju), 4 de gener de 1643 (Gr); Kensington, Anglaterra, 20 de març de 1717 (Ju), 31 de març de 1717 (Gr))

Gottfried Wilhelm von **Leibniz**:

(Leipzig, Saxònia, Sacre Imperi, 1 de juliol de 1646; Hannover, Baixa Saxònia, Sacre Imperi, 14 de novembre de 1716).

Abraham **de Moivre**

(Vitry-le-François, Xampanya, França, 26 de maig de 1667; Londres, Anglaterra, 27 de novembre de 1754)

Gabriel **Cramer**

(Ginebra, Suïssa, 31 de juliol de 1704; Banhòus-de-Céser, França, 4 de gener de 1752)

Leonhard **Euler**

(Basilea, Suïssa, 15 d'abril de 1707; Sant Petersburg, Rússia, 7 de setembre de 1783 (Ju), 18 de setembre de 1783 (Gr))

Étienne **Bézout**

(Nemours, França, 31 de març de 1730; Basses-Loges, Avon, Sena i Marne, França, 27 de setembre 1783)

Edward **Waring**

(Old Heath, Shrewsbury, Shropshire, Anglaterra, 1734; Pontesbury, Shropshire, Anglaterra, 15 d'agost de 1798)

Alexandre Théophile **Vandermonde**

(París, França, 28 de febrer de 1735; París, França, 1 de gener de 1796)

Joseph Louis **Lagrange**

Giuseppe Lodovico Lagrangia, o bé Giuseppe Luigi Lagrangia

(Torí, Regne de Sardenya, 25 de gener de 1736; París, França, 10 d'abril de 1813)

Adrien Marie **Legendre**

(París, França, 18 de setembre de 1752; París, França, 10 de gener de 1833)

Johann Carl Friedrich **Gauss**

(Brunsvic, Baixa Saxònia, Sacre Imperi, 30 d'abril de 1777; Göttingen, Baixa Saxònia, Prússia, 23 de febrer de 1855)

Bernard Placidus Johann Nepomuk **Bolzano**

(Praga, Bohèmia, Imperi Austro-Húngar (ara República Txeca), 5 d'octubre de 1781; Praga, Bohèmia, Imperi Austro-Húngar (ara República Txeca) 18 de desembre de 1848)

August Ferdinand **Möbius**

(Schulpforta, Saxònia, 17 de novembre de 1790; Leipzig, Alemanya, 26 de setembre de 1868)

Niels Henrik **Abel**

(Frindøe, Noruega, 5 d'agost de 1802; Froland, Noruega, 6 d'abril de 1829)

William Rowan **Hamilton**

(Dublín, Irlanda, 4 d'agost de 1805; Dublín, Irlanda, 2 de setembre de 1865)

Ernst Eduard **Kummer**

(Sorau, Brandenburg, Prússia, 29 de gener de 1810; Berlín, Prússia, Imperi Alemany, 14 de maig de 1893)

Évariste **Galois**

(Bourg la Reine, París, França, 25 d'octubre de 1811; París, França, 31 de maig de 1832)

James Joseph **Sylvester**

(Londres, Anglaterra, 3 de setembre de 1814; Londres, Anglaterra, 15 de març de 1897)

Arthur **Cayley**

(Richmond, Surrey, Anglaterra, 16 d'agost de 1821; Cambridge, Anglaterra, 26 de gener de 1895)

Ferdinand Gotthold Max **Eisenstein**

(Berlín, Prússia, 16 d'abril de 1823; Berlín, Prússia, 11 d'octubre de 1852)

Leopold **Kronecker**

(Liegnitz, Silèsia, Prússia, 7 de desembre de 1823; Berlín, Prússia, Imperi Alemany, 29 de desembre de 1891)

Julius Wilhelm Richard **Dedekind**

(Brunsvic, Baixa Saxònia, Prússia, 6 d'octubre de 1831; Brunsvic, Baixa Saxònia, Imperi Alemany, 12 de febrer de 1916)

Heinrich Martin **Weber**

(Heidelberg, Baden Württemberg, Confederació Germànica, 5 de maig de 1842; Estrasburg, Imperi Alemany, 17 de maig de 1913)

Georg Ferdinand Ludwig Philipp **Cantor**

(Sant Petersburg, Rússia, 3 de març de 1845; Halle, Saxònia Anhalt, Imperi Alemany, 6 de gener de 1918)

Felix Christian **Klein**

(Düsseldorf, Prússia, 25 d'abril de 1849; Göttingen, Alemanya, 22 de juny de 1925)

Ferdinand Georg **Frobenius**

(Berlín-Charlottenburg, Prússia, 26 d'octubre de 1849; Berlín, Prússia, Imperi Alemany, 3 d'agost de 1917)

Carl Louis Ferdinand von **Lindemann**

(Hannover, 12 d'abril de 1852; Munic, Baviera, Alemanya, 6 de març de 1939)

Giuseppe **Peano**

(Cuneo, Regne de Sardenya, ara Itàlia, 27 d'agost de 1858; Torí, Itàlia, 20 d'abril de 1932)

David **Hilbert**

(Königsberg, Prússia, 23 de gener de 1862; Göttingen, Baixa Saxònia, Alemanya, 14 de febrer de 1943)

Ernst Friedrich Ferdinand **Zermelo**

(Berlín, Alemanya, 27 de juliol de 1871; Friburg, Alemanya, 21 de maig de 1953)

Adolf Abraham Halevi **Fraenkel**

(Munic, Alemanya, 17 de febrer de 1891; Jerusalem, Israel, 15 d'octubre de 1965)

Emil **Artin**

(Viena, Àustria, Imperi Austrohongarès, 3 de març de 1898; Hamburg, Alemanya, 20 de desembre de 1962)

Otto **Schreier**

(Viena, Àustria, 3 de març de 1901; Hamburg, Alemanya, 2 de juny de 1929)

Bartel Leendert van der **Waerden**

(Amsterdam, Holanda, 2 de febrer de 1903; Zuric, Suïssa, 12 de gener de 1996)

Max August **Zorn**

(Krefeld, Alemanya, 6 de juny de 1906; Bloomington, Indiana, Estats Units, 9 de març de 1993)

Andrey Nikolayevich **Tykhonov**

(Gzhatska, Smolensk, Imperi rus, 17 d'octubre de 1906 (Ju), 30 d'octubre de 1906 (Gr); Moscow, Rússia, 7 d'octubre de 1993)

Nathan **Jacobson** (nascut Nachman **Arbiser**)

(Varsòvia, Polònia, Imperi rus, 23 de setembre de 1910 (Ju), 5 d'octubre de 1910 (Gr); Hamden, Connecticut, Estats Units, 5 de desembre de 1999)

Serge **Lang**

(Saint Germain en Laye, París, 19 de maig de 1927; Berkeley, Califòrnia, Estats Units, 12 de setembre de 2005)



# Referències

- [Ar 1991] Artin, Michael: *Algebra*. Prentice Hall, New Jersey, USA, 1991. ISBN: 0-13-004763-5.
- [Ga 1801] Gauss, C. F.: *Disquisicions Aritmètiques*. Traducció i pròleg de Griselda Pascual Xufre. Institut d'Estudis Catalans, Barcelona, 1996. ISBN: 84-7283-313-5.
- [Hi 1897] Hilbert, D.: *The theory of algebraic number fields. (Zahlbericht)* Traducció de l'alemany a l'anglès d'Iain T. Adamson. Amb una introducció de Franz Lemmermeyer i Norbert Schappacher. Springer Verlag, Berlin, Heidelberg, 1998. ISBN: 3-540-62779-0.
- [Ja 1974] Jacobson, Nathan: *Basic Algebra, I*. W. H. Freeman and Company, San Francisco, California, USA, 1974. ISBN: 0-7167-0453-6.
- [Ja 1980] Jacobson, Nathan: *Basic Algebra, II*. W. H. Freeman and Company, San Francisco, California, USA, 1980. ISBN: 0-7167-1079-X.
- [La 1971] Lang, Serge: *Álgebra*. Aguilar, Madrid, 1971. Traducció: Milagros Ancochea. ISBN: 84-03-20216-4. Versió original, *Algebra* (second printing). Addison Wesley Publishing Company, Reading, Massachussets, USA, 1965.
- [La 1984] Lang, Serge: *Algebra*, Second Edition. Addison Wesley Publishing Company, Reading, Massachussets, USA, 1984. ISBN: 0-201-05487-6.
- [MacTutor] O'Connor, John J.; Robertson, Edmund F.: *MacTutor History of Mathematics archive*, University of Saint Andrews, Scotland, UK. URL: [www-history.mcs.st-andrews.ac.uk](http://www-history.mcs.st-andrews.ac.uk)
- [vW 1970] van der Waerden, Bartel Leendert: *Algebra*, vol. 1. Traducció a l'anglès de la setena edició alemanya per Fred Blum i John R. Schulenberger. Frederick Ungar Publishing Company, New York, USA, 1970. SBN (Standard Book Number): 8044-4950-3.
- [vW 1970] van der Waerden, Bartel Leendert: *Algebra*, vol. 2. Traducció a l'anglès de la cinquena edició alemanya per John R. Schulenberger. Frederick Ungar Publishing Company, New York, USA, 1970. SBN (Standard Book Number): 8044-4951-1.



# Índex de figures

5.1	Punt de tangència de dues circumferències . . . . .	137
5.2	Punt de tangència d'una circumferència i un segment . . . . .	137
5.3	Producte de nombres reals positius . . . . .	138
5.4	Arrel quadrada d'un nombre real positiu . . . . .	139



# Índex de diagrames

3.1	Comportament del grau per canvi de base . . . . .	55
3.2	Comportament del grau per composició . . . . .	55
3.3	Composició de cossos ciclotòmics . . . . .	56
3.4	Comportament de la normalitat per canvi de base . . . . .	67
3.5	Comportament de la normalitat per composició . . . . .	67
4.1	Cos de descomposició de $X^p - a$ . . . . .	78
4.2	Comportament de la separabilitat per canvi de base . . . . .	87
4.3	Comportament de la separabilitat per a torres d'extensions . . . . .	87
4.4	Comportament de la separabilitat per composició . . . . .	88
4.5	Clausura normal d'una extensió separable . . . . .	88
5.1	Grups de Galois sobre la composició o la intersecció . . . . .	113
5.2	Comportament del caràcter galoisià per canvi de base . . . . .	114
5.3	Comportament del caràcter galoisià per composició . . . . .	115
A.1	Propietat universal del producte de grups . . . . .	154
C.1	Composició de cossos ciclotòmics, general . . . . .	186



# Índex terminològic

- $G$ -conjunt, 122
  - per l'esquerra, 156
  - per la dreta, 156
- $[K : k]_s$ , 83
- $\mathbb{C}$ , 1
- $\text{Gal}(K|k)$ , 62
- $\text{Gal}(\mathbb{Q}(\zeta_n)|\mathbb{Q})$ , 60
- $\text{Irr}(\theta, k)(X)$ , 51
- $\Phi_n(X)$ , 47
- $\mathbb{Q}$ , 1
- $\mathbb{R}$ , 1
- $\mathbb{Z}$ , 1
- $\text{gr}(f(X))$ , 10
- $\pi$ , 140, 144
- $k$ -àlgebra, 9, 32, 91, 151, 167
  - associativa, 167
  - commutativa, 167
  - quocient, 167
  - unitària, 167
- $k$ -automorfisme, 32, 62, 64, 66, 79, 97, 168
- $k$ -espai vectorial, 166
- $k$ -immersió, 61, 63, 64, 79, 92, 112
- $k$ -isomorfisme, 61
- $k$ -mòdul, 151, 165
  - quocient, 166
- $k$ -subàlgebra, 167
  - unitària, 167
- $k$ -submòdul, 166
- $k(\theta)$ , 51
- $k[\theta]$ , 51
- $n$ -àgon regular, 142
- $p$ -grup, 110, 141
- àlgebra de divisió, 160
- òrbita, 123
  
- Abel, iii, iv, 103, 198
- acció, 31, 122, 151, 165
  - d'un grup en un conjunt, 122
  - fidel, 32, 157
  - per conjugació, 124, 141
  - per l'esquerra, 31, 156
    - d'un grup en un conjunt, 122
  - per la dreta, 156
    - d'un grup en un conjunt, 123
    - per translació, 124
    - transitiva, 123, 124
- algoritme d'Euclides, 21, 26
- anell, 2, 9, 151, 158, 162–164
  - commutatiu, 9, 25, 116, 158, 164–167, 170
  - de polinomis, 11, 20, 22, 23, 31
  - no commutatiu, 165
  - producte, 12, 162, 165
  - quocient, 161, 163
  - trivial, 158
  - zero, 158
- angle, 135, 137
- aplicació
  - bijectiva, 153, 157, 159
  - identitat, 153, 159
  - lineal, 166
  - polinòmica, 12
- arc de circumferència, 136
- arrel
  - $n$ -èsima de la unitat, 46
  - cúbica, 7
  - d'un polinomi, 1, 3, 12
  - de la unitat, iv, 45–47, 70, 75, 95, 104
  - doble, 15
  - múltiple, 15, 16
  - primitiva  $n$ -èsima de la unitat, 47
  - primitiva de la unitat, 45, 59, 63, 80, 89, 99
  - quadrada, 4
  - simple, 15
  - triple, 15
- Artin, iii, 75, 98, 101, 102, 110–112, 120, 121, 125, 199
- automorfisme, 32, 60, 70, 151, 153, 159
  - d'anells, 159
  - de Frobenius, 45, 70, 110
  - de grups, 153
- axioma de l'elecció, 3, 169, 170
- axiomes de Zermelo-Fraenkel, 169
  
- Bézout, 198
- base, 170

- bimòdul, 165
- bisecció
  - d'un angle, 138
  - d'un segment, 137
- Bolzano, 198
- bon ordre, 169
- cadena, 117–119, 171
  - cíclica, 118
    - d'índexs primers, 118
  - normal, 118
    - abeliana, 118
  - radical, 141
- Cantor, iii, 199
- canvi de base, 55, 67, 75, 87, 104, 109, 114, 119
- caràcter
  - ciclotòmic, 45, 60, 62, 70, 80
  - de Legendre, 149
- característica, 15, 39, 41, 42, 58, 165, 173, 180
  - d'un anell, 165
- Cardano, iii, 197
- cardinal, 2, 68, 136, 169
- Cayley, 92, 199
- centre
  - d'un anell, 11
  - d'un grup, 141, 156
  - d'una circumferència, 136
- circumferència, 136
  - unitat, 12
- circumferències tangents, 136
- classe
  - d'equivalència, 18, 161
  - de conjugació, 124, 142
- clausura
  - algebraica, 144, 170
  - normal, 67, 75, 82, 83, 88, 93, 105, 141
  - separable, 88
- coeficient
  - d'un polinomi, 10, 11
  - dominant d'un polinomi, 10, 25
  - principal d'un polinomi, 10
- commutador, 125
- compàs, 109, 135, 141, 144
- composició, 55, 67, 88, 109, 115
  - d'extensions, 75
- conjugació complexa, 39
- conjunt, 156
  - numerable, 51
  - ordenat, 169
    - inductiu, 170
  - totalment ordenat, 170
- construcció amb regle i compàs, 109
- contingut, 22
  - d'un polinomi, 21–23, 26
- coordenades cartesianes, 135
- correspondència bijectiva, 111
- cos, 2, 160, 161, 164, 166
  - algebraicament tancat, 3, 39, 53, 62, 170, 171
  - ciclotòmic, 45, 56, 59, 186
  - composició, 55, 77, 104, 112
  - compost, 55
  - de característica zero, 82
  - de descomposició, 54, 58, 64, 71, 77, 78, 80, 111
  - de fraccions, 22, 23, 25, 39, 161
  - finit, 45, 46, 68, 82
  - fix, 110
  - infinit, 89
  - intersecció, 112
  - no-commutatiu, 160
  - numerable, 51
  - perfecte, 86
  - quadràtic, 58
- Cramer, 27, 198
- creixement exponencial, 147
- criteri
  - d'Eisenstein, 23
  - de reducció, 25
- de Moivre, 47, 198
- Dedekind, iii, 199
- del Ferro, iii, 197
- derivat d'un grup, 156
- Descartes, 135, 197
- descomposició canònica d'un morfisme, 167
- determinant de Vandermonde, 27
- dimensió, 9
- discriminant, 38, 39, 43, 129, 131, 143
  - d'un polinomi, 31
- Disquisitiones Arithmeticae, iii
- dividend, 13
- divisió de polinomis, 9, 13, 21
- divisibilitat, 14
- divisor, 13, 14
  - de zero, 160, 161, 165
- doblar un segment, 137
- domini
  - d'ideals principals, 18, 19, 51, 164, 165
  - d'integritat, 11, 12, 16–20, 24, 25, 39, 160–162, 164, 165
  - de factorització única, 9, 16, 18–23, 31
  - principal, 14, 164
- duplicació del cub, iv, 109, 135, 140



- Eisenstein, 23, 199
- element
- algebraic, 10, 51, 52, 55, 82
  - conjugat, 144, 195
  - fix, 71
    - per una acció, 32
  - invariant per una acció, 32
  - invers, 117, 152
  - invertible, 11, 13, 17, 18, 22, 25, 160
  - irreductible, 17, 18, 20, 22–24
  - maximal, 170, 171
  - neutre, 117, 152, 166, 167
  - oposat, 152, 158
  - primer, 17, 18, 20
  - primitiu, 75, 89, 90, 95, 97–100, 111, 121, 127, 131, 149
  - quadrat, 4
  - separable, 75, 82, 85, 111
  - transcendent, 51
  - u, 152
  - unitat, 158, 166
  - zero, 152, 158
- elements associats, 18, 20
- endomorfisme, 9, 153
- de grups, 153
- enter
- de Gauss, 17
  - lliure de quadrats, 24, 59
- equació
- algebraica, iii, 12, 151
  - cúbica, 5, 7, 12, 109
  - ciclotòmica, 103, 109, 121
  - general, 109
    - de grau 3, 127
    - de grau 4, 130
  - lineal, 4, 12, 27
  - polinòmica, 1, 9, 12, 115
  - quàrtica, 109
  - quadràtica, 4, 12, 140
  - resoluble
    - per radicals, 103, 104, 118
  - resoluble per radicals, 106, 107, 109, 115, 120, 121, 130
- espai
- topològic
    - compacte, 170
    - producte, 170
    - vectorial, 9, 166, 170
- estabilitzador, 123
- Euclides, 135, 197
- Euler, iii, 48, 56, 144, 198
- extensió
- abeliana, 95, 116, 120, 149
  - algebraica, iii, 53, 54, 75, 95, 110, 111, 151, 170, 171
    - de morfismes, 45, 64, 83, 106
  - cíclica, 45, 75, 95, 97–100, 116, 119, 121, 127
  - ciclotòmica, 45, 149
  - de cossos, 45, 167
  - de Galois, 95, 98, 109, 111, 112, 114, 115, 118, 119, 125
  - finita, 45, 53, 54, 95, 112, 118
  - inseparable, 94
  - nilpotent, 95
  - normal, 45, 66–68, 79, 83, 95, 112, 115, 116, 122, 154
  - quadràtica, 45, 100, 139
  - radical, 75, 104, 105, 119–121, 141
  - resoluble, iv, 95
    - per radicals, 75, 104, 105, 119, 120, 127
  - separable, 75, 85, 87, 88, 94, 95, 111, 115, 120
  - transcendent, 53
- fórmula
- d'òrbites, 124, 142, 157
  - de Leibniz, 147
  - de Newton, 41, 181
  - del binomi, 47
- fórmules
- de Cardano, 5, 7
  - de de Moivre, 47
  - de Newton, 31
  - de Viète, 31, 35, 37, 38, 125
- família, 154
- Fermat, 47, 142, 197
- Ferrari, iii, 197
- fita superior, 170
- forma bilineal
- no degenerada, 94
  - simètrica, 94
- Fraenkel, 169, 199
- Frobenius, 45, 70, 110, 199
- funció
- $\mu$  de Möbius, 49
  - $\varphi$  d'Euler, 48, 56
  - característica, 2
  - d'elecció, 169
  - d'Euler, 48
  - de Möbius, 49
  - polinòmica, 9, 12
  - racional, 103

- Galois, iii, iv, 45, 60, 62, 68–71, 75, 77, 80, 83, 95, 97, 98, 109–112, 114–116, 118, 119, 122, 125, 143, 149, 198  
 Gauss, iii, iv, 21, 103, 104, 109, 141, 149, 194, 198  
 grau, 55, 170  
   d'inseparabilitat, 86, 92  
   d'un polinomi, 3, 10, 16  
   d'una extensió, 53  
   de separabilitat, 75, 83, 85, 90, 92  
   total, 35, 41, 181  
 grup, 122, 151, 152, 156  
   abelià, 152, 165, 166  
   quocient, 166  
   additiu, 116  
   alternat, 130  
   cíclic, 45, 70, 97, 143, 149  
   commutatiu, 116, 152  
   d'isotropia, 123  
   de Galois, 45, 60–62, 69–71, 77, 80, 83, 95, 97, 100, 110, 112, 115, 116, 119, 122, 125, 143, 149, 151  
   de Klein, 130, 143  
   diedral, 143  
   nilpotent, 95  
   producte, 153  
   quocient, 155, 163  
   resoluble, 95, 107, 109, 115–119, 126, 127, 130, 141  
   simètric, 31, 109, 123, 130, 143  
 Hamilton, 92, 198  
 Hilbert, 75, 95, 97, 98, 199  
 ideal, 162, 164–166  
   bilateral, 162, 163  
   maximal, 17, 18, 51, 164, 170  
   nul, 162  
   per l'esquerra, 162  
   per la dreta, 162  
   primer, 17, 18, 164  
   principal, 9, 14, 51, 163, 164  
   total, 162  
   trivial, 162, 164  
 igualtat  
   d'Euler, 144  
   de Bézout, 21  
 imatge, 154, 160  
   d'una aplicació lineal, 166  
 immersió de cossos, 45  
 inclusió diagonal, 162  
 indeterminada, 9, 11, 34, 35, 38  
 interval tancat, 136  
 isomorfisme, 24, 25, 153  
   canònic, 166  
   d'anells, 159, 164  
   d'extensions, 61  
   de grups, 153  
 Jacobson, 200  
 Klein, 130, 143, 199  
 Kronecker, iii, 149, 199  
 Kummer, 45, 75, 99, 120, 198  
 Lagrange, iii, 198  
 Lang, 200  
 Legendre, iii, 149, 198  
 Leibniz, 147, 198  
 lema  
   de Gauss, 21–24  
   de Zorn, 3, 169–171  
 Lindemann, iv, 144, 199  
 lleis de simplificació, 152  
 longitud, 135  
 Möbius, 49, 198  
 múltiple, 1, 14  
 màxim comú divisor, 20, 21, 26  
 mètode  
   de Ruffini, 41, 179  
   de Waring, 35, 131  
 mòdul, 165  
   bilateral, 165  
   lliure, 11  
   per l'esquerra, 165  
   per la dreta, 165  
   quocient, 166  
 matriu, 27  
   de Sylvester, 42  
 monomi, 3, 5, 10, 35  
   principal, 25  
 morfisme  
   composició, 153, 159  
   d'anells, 10, 11, 25, 32, 37, 160, 161, 163–165  
   d'extensions, 61  
   de  $k$ -àlgebres, 167  
   de  $k$ -mòduls, 166  
   de grups, 32, 153, 154, 166  
   de mòduls, 166  
   determinant, 116  
   extensió, 11  
   identitat, 153, 159  
   injectiu

- d'anells, 160
  - de grups, 154
  - invers, 153
  - projecció, 153
- multiplicitat, 14, 16, 26
  - d'una arrel, 9, 15
  - d'una arrel d'un polinomi, 3
- Newton, 41, 195, 197
- nombre
  - $\pi$ , 140
  - algebraic, 45, 51, 140, 144
  - combinatori, 25
  - construïble amb regla i compàs, 139
  - de Fermat, 142
  - natural, 180
  - positiu, 144
  - primer, 24, 25
  - racional, 45
  - real, 144
  - senar, 25
  - transcendent, 140, 144
- norma, 75, 91
  - d'un element algebraic, 10
- normalitzador, 117
- nucli, 154, 155, 160, 165
  - d'una aplicació lineal, 166
- operació, 151, 152, 158
  - 0-ària, 151, 152, 158
  - 1-ària, 151, 152, 158
  - associativa, 152
  - binària, 151, 152, 158
  - commutativa, 152
- ordinal, 169
- ordre, 169
  - inductiu, 170, 171
  - total, 35, 170
- partició, 18
- Peano, 199
- període de Gauss, 149, 194
- permutació, 38, 157
- perpendicular
  - en un punt, 137
  - per un punt exterior, 137
- pla euclidià, 135
- polígon regular construïble, 109, 110
- polinomi, 1, 9, 10, 38, 39
  - característic, 91, 92
  - ciclotòmic, 25, 29, 45, 47, 49, 50, 52
  - constant, 10
  - d'Eisenstein, 24, 25
  - de Newton, 31, 41, 195
  - derivat, 15, 26, 41, 43, 179
  - general, 34, 35, 38, 125
    - de grau  $n$ , 125
  - homogeni, 42
  - irreductible, 9, 17, 22–25, 171
  - mònic, 11, 13
  - mínim, 10
  - minimal, 10, 51, 55, 62, 65, 97
  - no constant, 24, 171
  - primitiu, 21–26, 144
  - resultant, 31
  - simètric, 9, 31–33, 35, 36, 38, 41, 131, 181, 195
    - elemental, 31, 34, 35, 38, 40, 41, 125, 145, 195
- primer
  - element, 169
  - teorema d'isomorfia, 164, 166
    - d'anells, 164
    - de  $k$ -mòduls, 166
    - de grups, 155
- primitiu, 21
- producte cartesià, 162
- projecció, 153, 163
  - canònica, 155, 166
- propietat
  - associativa, 152, 158
  - commutativa, 152, 158
  - distributiva, 158
  - universal del producte, 153
- punt
  - construïble amb regla i compàs, 136
  - d'una varietat afí, 12
  - de tangència, 137
- quadratura del cercle, iv, 109, 110, 135, 140, 144
- quocient, 13
- radi d'una circumferència, 136
- radical, iv, 75, 103, 109
- recta tangent a una circumferència, 136
- rectes paral·leles, 136
- regla
  - de Ruffini, 15
  - del paral·lel·lògram, 138
- regla, 109, 135, 141, 144
- regla i compàs, iv
- relació d'equivalència, 18, 161
- Renaixement, 103

- residu, 13
- resolubilitat per radicals, iii
- resolució, 116–118, 126, 127, 130
  - cíclica, 118
  - d'índexs primers, 118, 119, 130
  - dun cos, 104
- resolvent cúbic, 130, 131, 143
- resta d'angles, 138
- resultant, 31, 42
- reticle, iv, 130
  - de subcossos, 130
- Ruffini, iii, 15, 26, 41, 179
  
- Schreier, 75, 98, 101, 102, 120, 121, 199
- secció
  - construïble del cercle, iv, 109, 141
  - del cercle, 109
- segment
  - paral·lel, 137
  - rectilini, 135
- segon teorema d'isomorfia de grups, 155
- signe d'una permutació, 130
- sistema, 27
  - de Cramer, 27
- solució
  - d'una equació, 1
  - d'una equació algebraica, 12
- sub- $k$ -mòdul, 166
- subanell, 10, 159, 161, 165
  - total, 160
- subcòs, 2
- subextensió, iv, 112
- subgrup, 112, 154
  - derivat, 125, 130, 156
  - intersecció, 154
  - normal, 112, 116, 117, 130, 154–156
  - total, 154, 155
  - transitiu, 124, 143
  - trivial, 154, 155, 160
- submòdul, 166
- suma
  - d'angles, 138
  - de Gauss, 149
- superfície, 135
- Sylvester, 199
  
- Tartaglia, iii, 197
- teorema
  - 90 de Hilbert, 75, 95, 97, 98
  - d'Artin, 109–112, 125
  - d'Artin-Schreier, 75, 98, 101, 102, 120, 121
  - d'independència lineal de caràcters, 75, 94, 96
  - d'isomorfia, 164, 166
  - d'anells, 164, 165
  - de  $k$ -mòduls, 166
  - de grups, 155
  - de Bolzano, 39
  - de Cayley-Hamilton, 10, 92
  - de Kronecker-Weber, 149
  - de l'element primitiu, 75, 90
  - de Tykhonov, 170
  - de Waring, 31, 148
  - de Zermelo, 169, 170
  - del residu, 15
  - fonamental
    - de l'Àlgebra, 3, 31, 39, 40
    - de l'Aritmètica, 46
    - de la teoria de Galois, 45, 68, 75, 109, 111, 119
  - petit de Fermat, 47
  - xinès del residu, 56
- teoria
  - de conjunts, iii
  - de Galois, iii, 1, 68, 70, 75, 109, 111, 119
  - de grups, iii
  - de Kummer, 45, 75, 99, 120
  - de nombres cardinals, 53
- tercer teorema d'isomorfia de grups, 156
- torre d'extensions, 75, 87, 104
- traça, 75, 91, 94
  - d'un element algebraic, 10
- trajectòria, 123
- transcendència de  $\pi$ , 110
- transport d'angles, 138
- transposició, 38, 126
- trisecció de l'angle, iv, 109, 135, 140
- Tykhonov, 170, 200
  
- unitat, 160
- usar
  - el compàs, 136
  - el regle, 136
  
- Vandermonde, 27, 198
- Viète, 31, 35, 125, 197
  
- Waerden, 200
- Waring, 35, 131, 148, 198
- Weber, iii, 149, 199
  
- Zermelo, 169, 199
- zero d'una funció polinòmica, 12
- Zorn, 169, 170, 200