CURS D'ÀLGEBRA

Artur TRAVESA

Curs 2007-2008

Índex

0.1 Equacions de grau 1 7
0.2 El teorema fonamental de l'àlgebra 8
0.3 Equacions de grau 2 10
0.4 Equacions de grau 3 11

1 Equacions algebraiques **15**
1.1 Polinomis i equacions algebraiques 15
1.2 Divisió de polinomis 19
1.3 Divisibilitat i arrels múltiples 21
1.4 Factorització única a $k[X]$ 24
1.5 Factorització única a $A[X]$ 29
1.6 Criteris d'irreductibilitat de polinomis 33
1.7 Un mètode de factorització en $\mathbb{Z}[X]$ 36

2 El teorema fonamental de l'àlgebra **41**

3 Arrels de la unitat **43**
3.1 Arrels de la unitat 44
3.2 Polinomis ciclotòmics 46
3.3 Elements algebraics i transcendents 51
3.4 Extensions finites de cossos 53
3.5 Cossos ciclotòmics 57

3.6 Cossos quadràtics 60
3.7 Grup de Galois dels cossos ciclotòmics 62
3.8 Grup de Galois d'una extensió algebraica 64
3.9 Extensions normals 68
3.10 Cossos finits 74

4 Radicals **79**
4.1 L'equació $X^n = a$ 80
4.2 Irreductibilitat de $X^{p^r} - a$ 82
4.3 Separabilitat 88
4.4 Extensions separables 92
4.5 El teorema de l'element primitiu 96
4.6 Normes i traces 99
4.7 Separabilitat i traça 103
4.8 El teorema 90 de Hilbert 104
4.9 Extensions cícliques 106
4.10 Teoria de Kummer 109
4.11 Radicals en característica zero 114
4.12 Extensions radicals 117

5 Teorema fonamental i aplicacions **121**
5.1 El teorema d'Artin 122
5.2 El teorema fonamental de la teoria de Galois 124
5.3 Grups resolubles 128
5.4 Resolubilitat per radicals 132
5.5 Equacions ciclotòmiques 136
5.6 Grups de Galois com a grups de permutacions 137
5.7 L'equació general de grau n 141
5.8 L'equació general de grau 3 144

5.9 Les equacions de grau 4 148
5.10 Construccions amb regle i compàs 155
5.11 Seccions del cercle constructibles 162

A Definicions i propietats bàsiques **167**
A.1 Grups 167
A.1.1 Grups 167
A.1.2 Subgrups normals 168
A.2 Anells 168
A.2.1 Anells 168
A.2.2 Morfismes d'anell 169
A.2.3 Subanells 169
A.2.4 Elements invertibles. Cossos 170
A.2.5 Divisors de zero. Dominis d'integritat 170
A.2.6 L'anell producte 172
A.3 Ideals i anells quocient 173
A.3.1 Ideals 173
A.3.2 Anells quocient 174
A.3.3 Dominis d'ideals principals 175
A.3.4 Ideals primers, maximals 175
A.3.5 Característica d'un anell 176

B El lema de Zorn **177**

Introducció

El propòsit principal, encara que no l'únic, d'aquest curs és intentar donar resposta a les qüestions proposades en el problema següent.

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

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 d'*arrels* d'un polinomi.

0.1 Equacions de grau 1

Començarem amb alguns exemples. En primer lloc, convé considerar les equacions més "senzilles"; això és, les de grau 1, o sigui, les de la forma $aX + b = 0$, $a \neq 0$.

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 $a \mid b$. A més a més, en aquest cas, si $c \in \mathbb{Z}$ és tal que $b = ac$, llavors $x = -c$ és l'única solució 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, k, i $a \neq 0$, l'equació $aX + b = 0$ té una única solució, $x = -\dfrac{b}{a} \in k$.

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

És, doncs, evident 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. Podem resumir una solució del problema en l'enunciat següent.

Proposició 0.1.4. *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 $x = -\dfrac{b}{a}$.* □

Observació 0.1.5. 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, $x = -\dfrac{b}{a} \in k$; és a dir, la solució de l'equació en K és la solució de l'equació en k. Dit d'una altra manera, totes les solucions de l'equació pertanyen al cos a què pertanyen els coeficients de l'equació.

0.2 El teorema fonamental de l'àlgebra

En general, per a les equacions de grau més gran que 1 no succeeix el mateix que per a les de grau 1. Per exemple, el polinomi $X^2 + 1$ és de coeficients reals, però les seves arrels, $i, -i$, són nombres complexos no reals.

Amb la finalitat de centrar més el problema, 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 puguem donar una resposta mínimament interessant al problema, restringirem la nostra atenció al cas d'equacions polinòmiques $a_0 + a_1X + \cdots + a_nX^n = 0$, $a_n \neq 0$, de coeficients en un cert cos k. Així, podem enunciar el problema d'una manera més precisa.

Problema. Siguin k un cos i $a_0, a_1, \ldots, a_n \in k$, $n \geq 2$, amb $a_n \neq 0$. Ens preguntem per les solucions de l'equació polinòmica $a_0+a_1X+\cdots+a_nX^n = 0$: En té? Quantes? On? Com són? Es poden calcular? De quina manera?

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 0.2.1. (Teorema fonamental de l'àlgebra) *Tot polinomi no nul de coeficients complexos té tantes arrels en $\mathbb{C}$ com indica el grau del polinomi, si comptem cadascuna amb la seva multiplicitat.* □

Corol·lari 0.2.2. *Siguin $k \subseteq \mathbb{C}$ un subcòs i $f(X) \in k[X]$ un polinomi no nul. El polinomi $f(X)$ té tantes arrels en $\mathbb{C}$ com indica el seu grau, si comptem cadascuna amb la seva multiplicitat.* □

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 seran objecte d'un estudi més detallat més endavant. D'altra banda, una demostració del teorema fonamental de l'àlgebra també es farà més endavant.

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

Definició 0.2.4. Sigui k un cos. Es diu que k és un cos algebraicament tancat si, i només si, tot polinomi no nul de coeficients en k té tantes arrels en k com indica el grau del polinomi, si comptem cadascuna amb la seva multiplicitat.

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 cos sobre el qual considerem el polinomi.

Observació 0.2.5. Encara que ho pugui semblar, aquest resultat no és gens restrictiu. En efecte, se satisfà la proposició següent, una demostració de la qual, que usa l'axioma de l'elecció en la forma del lema de Zorn, es dóna en un apèndix.

Teorema 0.2.6. *Tot cos és subcòs d'un cos algebraicament tancat.* □

Aquests preliminars ens permeten donar una resposta a les tres primeres qüestions plantejades. Si k és un subcòs d'un cos algebraicament tancat, $\overline{k}$, tot polinomi no nul de coeficients en k té tantes arrels en $\overline{k}$ 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 $f(X) \in k[X]$, 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.

0.3 Equacions de grau 2

Després 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.

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

(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 $\alpha \in \overline{k}$ tal que $\alpha^2 = b^2 - 4ac$; és a dir, sigui α una arrel en $\overline{k}$ del polinomi $X^2 - (b^2 - 4ac)$. Les solucions en $\overline{k}$ de l'equació $aX^2 + bX + c = 0$ són $x_1 = \dfrac{-b+\alpha}{2a}$, $x_2 = \dfrac{-b-\alpha}{2a}$. En particular, $x_1 \in k$ si, i només si, $\alpha \in k$, si, i només si, $x_2 \in k$.*

(c) *Se satisfà la igualtat $aX^2 + bX + c = a(X - x_1)(X - x_2)$, en $\overline{k}[X]$.*

Demostració: En primer lloc, observem que per a tot $x \in \overline{k}$ és $ax^2 + bx + c = 0$ 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 $x \in \overline{k}$ és una solució de $aX^2 + bX + c = 0$, per a $\alpha := 2ax + b \in \overline{k}$ és $\alpha^2 = b^2 - 4ac$. Recíprocament, si $\alpha \in \overline{k}$ és tal que $\alpha^2 = b^2 - 4ac$, per a $x = \dfrac{-b+\alpha}{2a}$, i per a $x = \dfrac{-b-\alpha}{2a}$, és $ax^2 + bx + c = 0$. A més a més, la

relació entre α 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 $x_1+x_2 = \frac{-b+\alpha}{2a} + \frac{-b-\alpha}{2a} = \frac{-b}{a}$, i $x_1x_2 = \frac{-b+\alpha}{2a}\frac{-b-\alpha}{2a} = \frac{b^2-\alpha^2}{4a^2} = \frac{c}{a}$, on $\alpha^2 = b^2 - 4ac$. Per tant, $a(X-x_1)(X-x_2) = aX^2 + bX + c$. □

Resta estudiar el cas en què $2 = 0$.

Proposició 0.3.2. *Siguin k un subcòs d'un cos algebraicament tancat, $\overline{k}$, i $a, b, c \in k$, $a \neq 0$. Suposem que $2 = 0$ en k. Si $x_1 \in \overline{k}$ és una solució de l'equació $aX^2 + bX + c = 0$, l'altra és $x_2 = x_1 + \frac{b}{a}$. En particular, $x_1 \in k$ 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 $x_2 := x_1 + \frac{b}{a}$, se satisfà que $ax_2^2 + bx_2 + c = a\big(x_1^2 + \frac{b^2}{a^2}\big) + bx_1 + \frac{b^2}{a} + c = ax_1^2 + bx_1 + c = 0$; per tant, si x_1 és solució de $aX^2 + bX + c = 0$, x_2 també ho és.

D'altra banda, $x_1 + x_2 = \frac{b}{a}$ i $x_1x_2 = x_1(x_1 + \frac{b}{a}) = x_1^2 + \frac{b}{a}x_1 = -\frac{c}{a} = \frac{c}{a}$, de manera que $a(X - x_1)(X - x_2) = a(X + x_1)(X + x_2) = a(X^2 + (x_1 + x_2)X + x_1x_2) = aX^2 + bX + c$. Per tant, les úniques solucions possibles de $aX^2 + bX + c = 0$ són x_1 i x_2. □

Notem que, en aquest cas, no donem cap manera explícita de càlcul de les solucions.

Exemple 0.3.3. 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, alhora, la seva "arrel quadrada"). Succeeix alguna cosa estranya?

0.4 Equacions de grau 3

A continuació, i per a acabar els exemples preliminars, donarem les solucions de les equacions cúbiques (o sigui, les de grau 3). Per a simplificar, suposarem

que $2 \neq 0$ i que $3 \neq 0$ en el cos. En el cas d'equacions de coeficients reals i solucions reals, la solució del problema ja era coneguda pels matemàtics italians del Renaixement; les fórmules que expressen les solucions s'anomenen fórmules de Cardano.

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

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

Siguin $\alpha, \beta \in \overline{k}$ tals que $\alpha^2 = \Delta$, i $\beta^2 = -3$, i posem $\rho := \dfrac{-1+\beta}{2}$; finalment, sigui $\gamma \in \overline{k}$ tal que $\gamma^3 = \dfrac{-27q + 3\alpha\beta}{54}$. Amb aquestes notacions, les solucions $x_1, x_2, x_3 \in \overline{k}$ de l'equació $aX^3+bX^2+cX+d = 0$ s'expressen per les fórmules següents. Si $p \neq 0$,

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

Si $p = 0$, sigui $\theta \in \overline{k}$ tal que $\theta^3 = -q$; llavors, les solucions són

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

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 $B := \dfrac{b}{a}$, $C := \dfrac{c}{a}$, i $D := \dfrac{d}{a}$; i si fem $x := X + \dfrac{B}{3}$, obtenim que, per a $X \in \overline{k}$, $X^3 + BX^2 + CX + D = 0$ si, i només si, $x^3 + px + q = 0$, on $p := C - \dfrac{B^2}{3}$ i $q := D + \dfrac{2B^3}{27} - \dfrac{BC}{3}$. Això explica el canvi dels coeficients a, b, c, d als p, q en l'enunciat.

D'aquesta manera, només cal 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 $x_1 + \dfrac{b}{3a}$, $x_2 + \dfrac{b}{3a}$, $x_3 + \dfrac{b}{3a}$, 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, $\rho^2 = \dfrac{-1-\beta}{2}$, $\rho^3 = 1$, i $1+\rho+\rho^2 = 0$. 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 $p = 0$.

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

$$\begin{aligned} &y_1 + y_2 + y_3 = 0, \\ &y_1y_2 + y_1y_3 + y_2y_3 = -p(\rho+\rho^2) = p, \\ &y_1y_2y_3 = \gamma^3 - \frac{p^3}{27\gamma^3}. \end{aligned}$$

Ara bé, per al darrer terme, és

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

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 $y_1 := \theta$, $y_2 := \rho\theta$, $y_3 := \rho^2\theta$, és $y_1 + y_2 + y_3 = \theta(1+\rho+\rho^2) = 0$, $y_1y_2 + y_1y_3 + y_2y_3 = \theta^2(\rho+\rho^2+\rho^3) = 0$, i $y_1y_2y_3 = \theta^3 = -q$; per tant, $(x-\theta)(x-\rho\theta)(x-\rho^2\theta) = x^3 + q$. La prova s'acaba desfent el canvi de variables $x = X + \dfrac{b}{3a}$. $\square$

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 0.3.3; i en el cas $3 = 0$, la resolució comporta considerar també equacions cúbiques similars a la de l'exemple 0.3.3; 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 entretindrem en els detalls de la resolució de les equacions cúbiques en els casos $2 = 0$ o $3 = 0$.

Capítol 1

Equacions algebraiques

Els conceptes intuïtius de funció polinòmica i d'equació polinòmica s'adquireixen a l'ensenyament secundari; però en aquesta etapa no se sol fer cap construcció formal dels polinomis ni de la indeterminada. Comencem el capítol, doncs, amb aquesta construcció formal. A la secció segona, repassem la divisió entera de polinomis i, com a conseqüència, obtenim 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. La secció tercera està dedicada a l'estudi de la multiplicitat de les arrels dels polinomis i a la prova del fet que la suma de les multiplicitats de les arrels en un cos d'un polinomi no nul de coeficients en aquest cos no pot superar el grau del polinomi. Les seccions quarta i cinquena es dediquen 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.

1.1 Polinomis i equacions algebraiques

Definició 1.1.1. Sigui A un anell (cf. A.2.1). Podem considerar el conjunt B 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

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

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

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

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 internes en el conjunt B.

1.1.2. El conjunt B, amb la suma i el producte que acabem de definir, és un anell, que és commutatiu si A és commutatiu; els elements neutres de la suma i del producte són, respectivament, els polinomis

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

Cal notar la diferència entre aquest anell i l'anell producte d'una quantitat numerable de còpies de l'anell A (cf. A.2.28).

1.1.3. L'aplicació $A \longrightarrow B$ definida per $a \mapsto (a, 0, \dots, 0, \dots)$ és un morfisme d'anells (cf. A.2.4) injectiu, de manera que permet identificar A com un subanell (cf. A.2.9) de B. Els elements de A, pensats com a polinomis, s'anomenen els polinomis constants.

Definició 1.1.4. Llevat del polinomi 0, tot altre polinomi té algun coeficient diferent de zero; i com que tots els coeficients són zero d'un lloc endavant, podem considerar el màxim dels índexs n tal que $a_n \neq 0$; aquest nombre natural n s'anomena el grau del polinomi i el coeficient n-èsim s'anomena el coeficient dominant o principal del polinomi. Convé definir el grau del polinomi 0 com $-\infty$. I, com és habitual, es defineix, per a tot nombre natural n, $-\infty < n$, $-\infty + n = n + (-\infty) = -\infty$, 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; i, 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.2.15).

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 B i es diu que $A[X]$ és l'anell de polinomis en la indeterminada X i de coeficients en A.

1.1.7. Sigui A un domini d'integritat (cf. A.2.20). 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, llavors $\mathrm{gr}(f(X) \cdot g(X)) = \mathrm{gr}(f(X)) + \mathrm{gr}(g(X))$.

1.1.8. En $A[X]$ se satisfà la igualtat

$$(a_0, a_1, \dots, a_n, 0, \dots) = a_0 + a_1 X + \cdots + a_n X^n;$$

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

$$a_0 + a_1 X + \cdots + a_n X^n,$$

on $a_0, \dots, a_n \in A$.

1.1.9. Notem que X pertany al centre (cf. A.2.13) de l'anell de polinomis $A[X]$; més generalment, si tots els coeficients $a_i \in A$ d'un polinomi $f(X) = a_0 + a_1 X + \cdots + a_n X^n \in A[X]$ pertanyen al centre de l'anell A, llavors $f(X)$ pertany al centre de $A[X]$.

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

Definició 1.1.11. Donat un anell 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 $X_1, \ldots, X_n$ s'escriu de manera única en la forma

$$\sum_{i_1,\ldots,i_n} a_{i_1,\ldots,i_n} X_1^{i_1} X_2^{i_2} \cdots X_n^{i_n}, \qquad a_{i_1,\ldots,i_n} \in A,$$

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

Definició 1.1.13. Donats un anell A i un polinomi

$$f(X_1, \ldots, X_n) := \sum_{i_1,\ldots,i_n} a_{i_1,\ldots,i_n} X_1^{i_1} X_2^{i_2} \cdots X_n^{i_n}, \qquad a_{i_1,\ldots,i_n} \in A,$$

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

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

s'anomena l'aplicació polinòmica definida per $f(X_1, \ldots, X_n)$. Els elements $(x_1, \ldots, x_n) \in A^n$ tals que $f(x_1, \ldots, x_n) = 0$ s'anomenen les arrels o els zeros en A del polinomi $f(X_1, \ldots, X_n)$ o les solucions en A de l'equació algebraica $f(X_1, \ldots, X_n) = 0$.

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. Per exemple, 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 exericicis 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. Veurem 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.

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 de 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

Proposició 1.2.1. (Divisió de polinomis) *Sigui k un cos. Donats polinomis $f(X), g(X) \in k[X]$, $g(X) \neq 0$, existeixen polinomis $q(X), r(X) \in k[X]$ únics tals que $f(X) = g(X)q(X) + r(X)$ i $\mathrm{gr}(r(X)) < \mathrm{gr}(g(X))$.*

Demostració: Comencem per provar l'existència. Si $\mathrm{gr}(f(X)) < \mathrm{gr}(g(X))$ i posem $q(X) := 0$, $r(X) := f(X)$, és clar que se satisfan les propietats enunciades, $f(X) = g(X)q(X) + r(X)$ i $\mathrm{gr}(r(X)) < \mathrm{gr}(g(X))$. Suposem, doncs, que $\mathrm{gr}(f(X)) \geq \mathrm{gr}(g(X))$, i siguin $f(X) =: a_0 + a_1X + \cdots + a_nX^n$, $g(X) =: b_0 + b_1X + \cdots + b_mX^m$, on $a_0, a_1, \ldots, a_n, b_0, b_1, \ldots, b_m \in k$, $a_n \neq 0$, $b_m \neq 0$, i $n \geq m$. El polinomi

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

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

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

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

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

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

$$\begin{aligned} f(X) &= g(X)q_1(X)+r_1(X), \qquad \operatorname{gr}(r_1(X))<\operatorname{gr}(g(X)),\\ &= g(X)q_2(X)+r_2(X), \qquad \operatorname{gr}(r_2(X))<\operatorname{gr}(g(X)), \end{aligned}$$

on $q_1(X)$, $q_2(X)$, $r_1(X)$, $r_2(X)\in k[X]$. Se satisfà la igualtat $r_2(X)-r_1(X)=g(X)(q_1(X)-q_2(X))$, de manera 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 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. □

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 A 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 $\operatorname{gr}(r(X))<\operatorname{gr}(g(X))$.* □

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 $\operatorname{gr}(r(X))<\operatorname{gr}(g(X))$, s'anomena la divisió entera 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.

1.2.5. Si l'anell A no és commutatiu, caldria donar sentit a les fraccions com $\dfrac{a_n}{b_m}$ que apareixen a la demostració anterior; si $\dfrac{a_n}{b_m}=b_m^{-1}a_n$, i anàlogament les altres, obtindríem una divisió entera com la que hem escrit: $f(X)=g(X)q(X)+r(X)$; i si $\dfrac{a_n}{b_m}=a_nb_m^{-1}$, obtindríem una divisió entera de la forma $f(X)=q(X)g(X)+r(X)$, amb l'ordre de divisor i quocient permutat. No tractarem el cas no commutatiu, de manera que no ens caldrà 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.3.17).

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 $\mathrm{gr}(g(X))$; 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 $\mathfrak{a} = g(X)k[X]$. □

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

Definició 1.3.1. Sigui A un anell commutatiu. Donats elements f, $g \in A$, es diu que g divideix f, o que f és divisible per g, si existeix un element $q \in A$, $q \neq 0$, tal que $f = gq$.

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 1.3.2. *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. L'element 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) $X - a$:

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

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 1.3.3. La igualtat

$$f(X) = (X - a)q(X) + f(a)$$

es coneix sovint com la regla de Ruffini.

1.3.4. Suposem que $a \in A$ és una arrel del polinomi $f(X)$. 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, $f(X) = (X - a)^2 q_2(X)$. 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 1.3.5. 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 1.3.6. Siguin A un anell i $f(X) := a_0 + a_1X + \cdots + a_nX^n \in A[X]$, $a_0, a_1, \ldots, a_n \in A$, un polinomi. El polinomi

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

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

1.3.7. 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.3.23).

Proposició 1.3.8. *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: Escriguem $f(X) = a_0 + a_1X + \cdots + a_nX^n$, $a_0, a_1, \ldots, a_n \in A$, 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, $2a_2$, $\ldots$, 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 dóna exactament per a $k = 0$ i, si $\mathrm{car}(A) = p > 0$, 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. □

Observació 1.3.9. 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 1.3.10. *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 de $D(f, X)$.*

DEMOSTRACIÓ: Escrivim $f(X) = (X-a)^m q(X)$, 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 $D(f, a) = q(a) \neq 0$. □

Teorema 1.3.11. *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 $\mathrm{gr}(g(X)) = \mathrm{gr}(f(X)) - m < \mathrm{gr}(f(X))$. Les arrels de $f(X)$ diferents de a són exactament les arrels de $g(X)$, i les 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. □

Observació 1.3.12. Notem que no estem suposant que el domini d'integritat A sigui un domini de factorització única (cf. 1.4.12); 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. □

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 qualsevol. Un element $p \in A$ s'anomena primer si una 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.

Definició 1.4.2. Sigui A un anell commutatiu qualsevol. Un element $a \in A$ s'anomena irreductible si $a \neq 0$, 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, 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. D'altra banda, 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 element primer divideix un producte, llavors divideix algun dels factors. Tot i que, per exemple, en $\mathbb{Z}$ i en $k[X]$, k cos, els elements primers 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) però no són irreductibles, ja que $2 = 2^3$, $3 = 3^2$, i $4 = 2^2$.

Proposició 1.4.6. (cf. A.3.21) *Sigui A un anell commutatiu qualsevol. Tot ideal maximal és un ideal primer.* □

Proposició 1.4.7. *Sigui A un domini d'integritat qualsevol. Tot element primer $p \in A$ 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 p divideix el producte bc, o bé p divideix b, o bé p

divideix c. Podem suposar que p divideix b, 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. □

Proposició 1.4.8. *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 $pA \subseteq \mathfrak{a}$. □

Definició 1.4.9. Sigui A un anell commutatiu. Dos elements a, $b \in A$ s'anomenen associats si existeix un element invertible $u \in A$ tal que $b = au$.

1.4.10. 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.

1.4.11. 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 $a \in A$ divideix un element $b \in A$ si, i només si, cada element de la classe d'elements associats de a divideix cada element de la classe d'elements associats de b. Podem dir, doncs, que la relació de divisibilitat es dóna 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 1.4.12. Un domini d'integritat A s'anomena un domini de factorització única si tot element no nul i no invertible $a \in A$ admet una descomposició de la forma $a = up_1p_2 \cdots p_r$, $r \geq 1$, on $p_1, p_2, \ldots, p_r \in A$ 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.

1.4.13. No és veritat que tot domini d'integritat sigui un domini de factorització única. Per exemple, en $\mathbb{Z}[\sqrt{-5}] := \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$, se satisfà la igualtat $(2 + \sqrt{-5})(2 - \sqrt{-5}) = 9 = 3 \cdot 3$; d'altra banda, 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 $\mathbb{Z}[\sqrt{-5}]$. 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 1.4.14. *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 $a_0 = a_1b_1$. 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 que divideix a_1, de manera que podrem 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+1} divideix a_n, 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 contradiu 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, $\ldots$, p_r, q_1, q_2, $\ldots$, $q_s \in A$, $r, s \geq 1$, i elements invertibles u, $v \in A^*$ tals que

$$a = u p_1 p_2 \cdots p_r = v q_1 q_2 \cdots q_s.$$

Com que A és principal i $p_1 \in A$ és irreductible, l'ideal $p_1 A$ és primer i, com que el producte $v q_1 q_2 \cdots q_s$ 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 p_1 divideix q_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 1.4.15. 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 1.4.16. *Sigui k un cos qualsevol. L'anell de polinomis $k[X]$ és un domini de factorització única.* □

Corol·lari 1.4.17. *L'anell $\mathbb{Z}$ dels nombres enters és un domini de factorització única.* □

1.5 Factorització única a $A[X]$

Usualment treballem amb polinomis de coeficients enters; per tant, serà 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, de quina manera estan relacionades la irreductibilitat en $\mathbb{Z}[X]$ i en $\mathbb{Q}[X]$ d'un polinomi de coeficients enters.

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 $d = \mathrm{mcd}(a, b)$, si se satisfan les dues condicions següents.

(a) d és un divisor de a i de b;

(b) per a tot divisor $\delta \in A$ de a i de b, l'element δ és un divisor de d.

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 una igualtat $d = \mathrm{mcd}(a, b)$, igualtat que es dóna entre les classes d'elements associats, però no necessàriament entre els elements de A. Així, per exemple, de les dues igualtats $1 = \mathrm{mcd}(2, 3)$ i $-1 = \mathrm{mcd}(2, 3)$, vàlides en $\mathbb{Z}$, es dedueix la igualtat $1 = -1$, com a classes d'elements associats, però no, òbviament, com a 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. És a dir, en tot domini de factorització única se satisfà l'existència de màxim comú divisor. És a dir,

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

1.5.6. (L'algoritme d'Euclides) 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 $\mathrm{mcd}(f(X), g(X)) = \mathrm{mcd}(f(X) - g(X)q(X), g(X))$, i que $\mathrm{mcd}(f(X), 0) = f(X)$. Si $g(X) = 0$, tenim que $\mathrm{mcd}(f(X), 0) = f(X)$. 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 $\mathrm{gr}(r(X)) < \mathrm{gr}(g(X)$. Llavors, tenim que $\mathrm{mcd}(f(X), g(X)) = \mathrm{mcd}(g(X), r(X))$. 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 enrera, obtenim una prova del resultat següent. Els detalls de la demostració es proposen com a exercici.

Corol·lari 1.5.7. *Siguin k un cos, $f(X)$, $g(X) \in k[X]$ polinomis no nuls, i $d(X) \in k[X]$ un màxim comú divisor de $f(X)$ i $g(X)$. Existeixen polinomis*

$a(X)$, $b(X) \in k[X]$, amb $\mathrm{gr}(a(X)) < \mathrm{gr}(g(X))$ i $\mathrm{gr}(b(X)) < \mathrm{gr}(f(X))$, únics tals que $d(X) = f(X)a(X) + g(X)b(X)$. □

Definició 1.5.8. Una igualtat $d(X) = f(X)a(X) + g(X)b(X)$, on $d(X) = \mathrm{mcd}(f(X), g(X))$ i $a(X)$, $b(X) \in k[X]$, 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 $f(X)$. Escriurem $\mathrm{cont}(f(X))$ per a indicar el contingut del polinomi $f(X)$; és una classe d'elements associats de A.

Teorema 1.5.10. (Lema de Gauss) *Siguin A un domini de factorització única i $f(X), g(X) \in A[X]$ polinomis no nuls. Llavors,*

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

Demostració: Siguin $d_f, d_g \in A$ els continguts de $f(X), g(X)$, respectivament; podem escriure, doncs, $f(X) = d_f f'(X)$, $g(X) = d_g g'(X)$, amb $f'(X) = a'_0 + a'_1X + \cdots + a'_nX^n$, $g'(X) = b'_0 + b'_1X + \cdots + b'_mX^m \in A[X]$, $a'_i, b'_j \in A$, i $\mathrm{mcd}(a'_0, a'_1, \ldots, a'_n) = \mathrm{mcd}(b'_0, b'_1, \ldots, b'_m) = 1$. El polinomi producte, $f(X)g(X)$, es pot escriure en la forma $f(X)g(X) = d_f d_g(a'_0 + a'_1X + \cdots + a'_nX^n)(b'_0 + b'_1X + \cdots + b'_mX^m) = d_f d_g(c_0 + c_1X + \cdots + c_{n+m}X^{n+m})$, on $c_k = \sum_{i+j=k} a'_i b'_j$, per a $0 \leq k \leq n+m$. Cal, doncs, i és suficient, provar que $\mathrm{mcd}(c_0, c_1, \ldots, c_{n+m}) = 1$.

Ho farem per reducció a l'absurd. Si fos $\mathrm{mcd}(c_0, c_1, \ldots, c_{n+m}) \neq 1$, existiria un element irreductible $p \in A$ que dividiria tots els coeficients c_k, $0 \leq k \leq n+m$. Ara bé, p no divideix tots els coeficients $a'_0, a'_1, \ldots, a'_n$ ni tampoc tots els coeficients $b'_0, b'_1, \ldots, b'_m$, perquè $\mathrm{cont}(f'(X)) = \mathrm{cont}(g'(X)) = 1$. Podem considerar, doncs, els menors índexs r, s, $0 \leq r \leq n$, $0 \leq s \leq m$, tals que p no divideix a'_r, ni b'_s; així, p divideix a'_i, per a $0 \leq i < r$, i p divideix b'_j, per a $0 \leq j < s$. Ara, tenim que p divideix $c_{r+s} = \sum_{i+j=r+s} a'_i b'_j$ per hipòtesi; d'altra banda, p també divideix $\sum_{i+j=r+s,\,(i,j)\neq(r,s)} a'_i b'_j$, ja que un dels dos factors de cada sumand és divisible per p (en efecte, o bé $i < r$ o bé $j < s$); en conseqüència, la diferència, $a'_r b'_s$, entre les dues expressions és divisible per p. Però això és contradictori amb l'elecció de r i s, ja que A és

un domini de factorització única i p no pot dividir el producte $a'_r b'_s$ perquè no divideix cap dels dos factors. □

Corol·lari 1.5.11. *Siguin 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 $K[X]$ dóna lloc a una descomposició de $f(X)$ en $A[X]$.*

Demostració: Comencem per la definició dels 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 sigui $c_g := \dfrac{\delta_g}{d_g} \in K$. Definim d_h, δ_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 (lema de Gauss), 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 $c_g c_h = \dfrac{a}{b}$, amb $a, b \in A$, primers entre si, tenim que $bf(X) = ag'(X)h'(X)$, de manera que $a = \mathrm{cont}(ag'(X)h'(X)) = \mathrm{cont}(bf(X)) = b \cdot \mathrm{cont}(f(X))$, d'on és clar que b divideix a. Però com que A és un domini de factorització única i $\mathrm{mcd}(a, b) = 1$, b ha d'ésser invertible en A, de manera que $c_g c_h = \dfrac{a}{b} \in A$. □

Corol·lari 1.5.12. *Siguin 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.* □

Aquest resultat ens permetrà provar un resultat molt important que, en particular, ens dirà que, per a qualsevol cos k, els anells de polinomis $\mathbb{Z}[X_1, \ldots, X_n]$ i $k[X_1, \ldots, X_n]$ són de factorització única.

Teorema 1.5.13. *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, el corol·lari anterior ens ensenya a trobar, a partir d'una descomposició de $f(X)$ com a producte de factors irreductibles en $K[X]$, 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 dóna 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 $f(X) = cg_1(X) \cdots g_n(X) = dh_1(X) \cdots h_m(X)$, 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, $g_i(X)$ 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. □

Corol·lari 1.5.14. *Els anells de polinomis $\mathbb{Z}[X_1, X_2, \ldots, X_n]$ són dominis de factorització única.* □

Corol·lari 1.5.15. *Per a tot cos k, els anells de polinomis $k[X_1, X_2, \ldots, X_n]$ són dominis de factorització única.* □

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, donarem 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 $f(X) = a_0 + a_1X + \cdots + a_nX^n \in A[X]$, $a_0, a_1, \ldots, a_n \in A$, $a_n \neq 0$, un polinomi. Suposem que existeix un element irreductible $p \in A$ tal que p no divideix a_n, p divideix cada un dels $a_0, a_1, \ldots, a_{n-1}$, i p^2 no divideix a_0. Llavors, $f(X)$ és irreductible en $K[X]$. I si, a més a més, $f(X)$ és de contingut 1, $f(X)$ és irreductible en $A[X]$.*

Demostració: Com que p no divideix a_n, p no divideix el contingut de $f(X)$. Si canviem $f(X)$ dividint-lo pel seu contingut, ni les hipòtesis ni la tesi no canvien, de manera que podem suposar que el polinomi $f(X)$ és de contingut 1. En aquest cas, si existís una descomposició no trivial de $f(X)$ en $K[X]$, i en virtut del lema de Gauss, existiria una descomposició en $A[X]$ de la forma $f(X) = g(X)h(X)$, amb $g(X), h(X)$ polinomis no constants. Siguin $g(X) = b_0 + b_1X + \cdots + b_rX^r$, $h(X) = c_0 + c_1X + \cdots + c_sX^s$, amb $b_0, b_1, \ldots, b_r, c_0, c_1, \ldots, c_s \in A$, $b_r, c_s \neq 0$, i $1 \leq r, s \leq n-1$.

Com que $b_0c_0 = a_0$ és divisible per p, però no per p^2, exactament un dels dos elements b_0, c_0 no és divisible per p. Suposem que p no divideix b_0; llavors, p divideix c_0. D'altra banda, c_s no és divisible per p, ja que $b_rc_s = a_n$ no ho és; per tant, existeix t, $1 \leq t \leq s$, tal que per a $0 \leq j \leq t-1$ és $p \mid c_j$ però $p \nmid c_t$. Per hipòtesi, $a_t = \sum_{i+j=t} b_ic_j$ és divisible per p, ja que $t \leq s < n$; a més a més, $\sum_{i+j=t, j<t} b_ic_j$ és divisible per p, ja que ho és c_j; en conseqüència, b_0c_t és divisible per p. Però ni b_0 ni c_t són divisibles per p; aquesta contradicció ens permet assegurar que $f(X)$ és irreductible en $K[X]$. I una nova aplicació del lema de Gauss acaba la prova. □

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.

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

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

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

Proposició 1.6.6. *Sigui p un nombre natural primer. El polinomi $\Phi_p(X) := 1 + X + X^2 + \cdots + X^{p-1} \in \mathbb{Z}[X]$ és irreductible.*

Demostració: Sigui $g(X) := \Phi_p(X + 1)$. Llavors, $g(X) = \dfrac{(X+1)^p - 1}{(X+1) - 1} = \dfrac{(X+1)^p - 1}{X} = \displaystyle\sum_{i=1}^{p} \binom{p}{i} X^{i-1}$ és un polinomi d'Eiseistein per al primer p; per tant, $g(X)$ és irreductible; en conseqüència, $\Phi_p(X)$ és irreductible. □

Teorema 1.6.7. (Criteri de reducció) *Siguin A, B dominis d'integritat, L, el cos de fraccions de B, i $\varphi : A \longrightarrow B$ un morfisme d'anells qualsevol. Anomenem també $\varphi : A[X] \longrightarrow B[X]$ el morfisme d'anells que s'obté en aplicar φ als coeficients dels polinomis de $A[X]$. Sigui $f(X) \in A[X]$ un polinomi tal que $\varphi(f(X)) \neq 0$ i $\operatorname{gr}(\varphi(f(X))) = \operatorname{gr}(f(X))$. Llavors, si $\varphi(f(X))$ és irreductible en $L[X]$, $f(X)$ no admet cap factorització en $A[X]$ de la forma $f(X) = g(X)h(X)$, amb $g(X), h(X) \in A[X]$, $\operatorname{gr}(g(X)) \geq 1$ i $\operatorname{gr}(h(X)) \geq 1$.*

Demostració: Si $f(X)$ tingués una factorització com la de l'enunciat, en aplicar φ obtindríem una factorització de $\varphi(f(X))$ en $L[X]$, $\varphi(f(X)) = \varphi(g(X))\varphi(h(X))$; com que $\operatorname{gr}(\varphi(g(X))) \leq \operatorname{gr}(g(X))$ i també $\operatorname{gr}(\varphi(h(X))) \leq \operatorname{gr}(h(X))$, mentre que $\operatorname{gr}(\varphi(g(X))\varphi(h(X))) = \operatorname{gr}(g(X)h(X))$, hauria de ser $\operatorname{gr}(\varphi(g(X))) = \operatorname{gr}(g(X)) \geq 1$ i $\operatorname{gr}(\varphi(h(X))) = \operatorname{gr}(h(X)) \geq 1$, de manera que obtindríem una descomposició no trivial de $\varphi(f(X))$ en $L[X]$, contra la hipòtesi que $\varphi(f(X))$ és irreductible. □

Corol·lari 1.6.8. *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 de contingut 1, $f(X)$ és irreductible en $\mathbb{Z}[X]$.* □

Exemple 1.6.9. 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 (exercici).

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

En general no hi ha bons algoritmes per a determinar si un polinomi és o no irreductible. Per a polinomis de coeficients enters, però, es pot donar un algoritme 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 de nombres enters.

Sigui $f(X) := a_0 + a_1X + \cdots + a_nX^n \in \mathbb{Z}[X]$, $a_0, a_1, \ldots, a_n \in \mathbb{Z}$, $a_n \neq 0$, $n \geq 0$, un polinomi 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 $\mathbb{Z}[X]$. Si $d(X) := \operatorname{mcd}(f(X), D(f, X)) \in \mathbb{Z}[X]$, el polinomi $g(X) := \dfrac{f(X)}{d(X)} \in \mathbb{Z}[X]$ té els mateixos factors irreductibles que $f(X)$, però tots són de multiplicitat 1. Al final, per divisió, podrem 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 $\dfrac{f(X)}{h(X)}$, 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 $\dfrac{a}{b} \in \mathbb{Q}$ és una arrel de $f(X)$ en $\mathbb{Q}$, amb a, $b \in \mathbb{Z}$, $b > 0$, i $\mathrm{mcd}(a, b) = 1$, 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 $\dfrac{a}{b}$ 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 $f(X)$. 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 $z = 0$), $a + b + c \mid a_0 + a_1 + \cdots + a_n$ (que correspon a fer $z = 1$), $a - b + c \mid a_0 - a_1 + \cdots + (-1)^n a_n$ (que correspon a fer $z = -1$), $4a + 2b + c \mid a_0 + 2a_1 + \cdots + 2^n a_n$ (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), 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 ob-

tindrem un sistema d'equacions lineals de matriu

$$\left[\begin{array}{ccc|c} z_1^2 & z_1 & 1 & d(z_1) \\ z_2^2 & z_2 & 1 & d(z_2) \\ z_3^2 & z_3 & 1 & d(z_3) \end{array}\right],$$

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, obtindrem els possibles polinomis de grau 2 de $\mathbb{Z}[X]$ que divideixen $f(X)$; i, per divisió, obtindrem 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 permetrà 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 caldrà usar un mínim de

quatre nombres enters diferents z_1, z_2, z_3, z_4 per a obtenir un sistema lineal de matriu

$$\left[\begin{array}{cccc|c} z_1^3 & z_1^2 & z_1 & 1 & d(z_1) \\ z_2^3 & z_2^2 & z_2 & 1 & d(z_2) \\ z_3^3 & z_3^2 & z_3 & 1 & d(z_3) \\ z_4^3 & z_4^2 & z_4 & 1 & d(z_4) \end{array}\right],$$

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 $g(X) = X^2 + bX + c$. Prenent per a z els valors 0, 1, obtenim que $c = g(0) \mid f(0) = 1$ i que $1 + b + c = g(1) \mid f(1) = 1$. Per tant, tenim quatre sistemes de dues equacions lineals:

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

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

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

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

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

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

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

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'algoritme per a un polinomi de grau 4 de coeficients indeterminats per a deduir que $f(X)$ és irreductible.

Capítol 2

El teorema fonamental de l'àlgebra

Capítol 3

Arrels de la unitat

Després, potser, de les equacions quadràtiques, 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, la de grup cíclic. Dediquem la primera secció a establir aquesta estructura, i la segona a la definició i l'estudi dels polinomis ciclotòmics $\Phi_d(X)$; 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. Fem la prova de la irreductibilitat dels polinomis ciclotòmics a la secció tercera, on 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 caracerística diferent de 2, classificació que servirà de motivació i, alhora, d'exemple, de la teoria de Kummer de la classificació de les extensions cícliques que farem 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, responem a la qüestió "què succeeix si en comptes d'una arrel d'un polinomi irreductible en considerem una altra" amb l'estudi de les immersions de cossos i 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 a 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'elevar 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, $\mathrm{car}(k) = 2$, ja que l'equació $X^2 = 1$ té una arrel doble en k si $\mathrm{car}(k) = 2$, i dues arrels simples si $\mathrm{car}(k) \neq 2$.

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; 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 $p_1, p_2, \ldots, p_r$ denoten nombres naturals primers diferents dos a dos, $a_0 \in \{0, 1\}$, i $a_1, \ldots, a_r \in \mathbb{Z}$ 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 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; és a dir, tot element de G és arrel del polinomi $X^n - 1$. Llavors, per al subgrup generat per ζ 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 ζ. □

Corol·lari 3.1.8. *El grup de les arrels n-èsimes de la unitat de $\mathbb{C}$, $\mu_n(\mathbb{C})$, 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 $\mathrm{mcd}(X^n - 1, nX^{n-1}) = 1$; per tant, té exactament n arrels diferents en $\mathbb{C}$. □

Corol·lari 3.1.9. (Petit teorema de Fermat) *Siguin $\mathbb{F}$ 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. □

Corol·lari 3.1.10. *Sigui p un nombre natural primer. Per a tot polinomi no nul $f(X) \in (\mathbb{Z}/p\mathbb{Z})[X]$ 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 $f(X)^p = \sum_{i=0}^{n} a_i^p X^{ip} = \sum_{i=0}^{n} a_i X^{pi} = f(X^p)$, ja que $a_i^p = a_i$, per a tot $a_i \in \mathbb{Z}/p\mathbb{Z}$. □

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 n-èsima primitiva 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 n-èsima primitiva de la unitat, les arrels n-èsimes de la unitat diferents són els nombres ζ^m, per a $1 \leq m \leq n$; i les arrels n-èsimes primitives de la unitat, els ζ^m, per a $1 \leq m \leq n$ tals que $\mathrm{mcd}(n, m) = 1$. És a dir, les arrels n-èsimes primitives 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 Moivre).

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 estès a totes les arrels n-èsimes de la unitat. El polinomi

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

on ara ζ 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 p-èsimes primitives de la unitat; per tant, $\Phi_p(X) = \displaystyle\prod_{\zeta^p=1,\,\zeta\neq 1}(X-\zeta) = \frac{X^p-1}{X-1} = 1+X+X^2+\cdots+X^{p-1}$.

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

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 $\varphi(n)$.* □

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

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 d-èsima primitiva 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 $\displaystyle\prod_{d|n}\Phi_d(X)$ tenen exactament les mateixes arrels. Com que totes són simples en tots dos polinomis i tots dos polinomins són mònics, obtenim la igualtat següent.

Proposició 3.2.11.

$$X^n-1 = \prod_{d|n}\Phi_d(X).\ \square$$

El càlcul del grau del polinomi X^n-1 a partir d'aquesta relació proporciona el resultat següent.

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

Observació 3.2.13. La igualtat $X^n-1=\prod_{d|n}\Phi_d(X)$ ens diu que el polinomi X^n-1 és divisible pel polinomi mònic $\prod_{d|n,\,d<n}\Phi_d(X)$; per tant, la divisió té sentit en l'anell de polinomis i obtenim l'expressió equivalent

$$\Phi_n(X)=\frac{X^n-1}{\prod_{d|n,\,d<n}\Phi_d(X)},$$

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 $p\geq 2$, $\Phi_p(X)=1+X+X^2+\cdots+X^{p-1}$. A continuació fem el càlcul recursiu d'alguns altres:

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

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

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

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

s'anomena la funció μ de Möbius.

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

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

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, $p_1, p_2, \ldots, p_r$. 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, la suma que volem calcular val $\displaystyle\sum_{k=0}^{r} \binom{r}{k} (-1)^k = (1-1)^r = 0$, ja que $r \geq 1$. □

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

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

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

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

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

Exemple 3.2.18. Recuperem, 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* $\dfrac{\varphi(n)}{n} = \displaystyle\sum_{d|n} \frac{\mu(d)}{d}$.

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

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

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

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

$$\Phi_n(X) = \frac{X^n - 1}{\displaystyle\prod_{d|n,\, d<n} \Phi_d(X)}.$$

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 $\mathbb{Q}[X]$.*

Deixem la demostració per a la secció següent.

3.3 Elements algebraics i 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 adonarem 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, θ 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 en θ tots els polinomis de $k[X]$; és a dir, podem considerar l'aplicació $\psi_\theta : k[X] \longrightarrow K$ definida per $\psi_\theta(f(X)) := f(\theta)$, per a tot polinomi $f(X) \in k[X]$. Aquesta aplicació és un morfisme d'anells i, de fet, l'únic tal que $\psi_\theta(X) = \theta$ i $\psi_\theta(a) = a$, per a tot $a \in k$.

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

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 θ com a arrel és un ideal de l'anell de polinomis $k[X]$. En particular, el morfisme ψ_θ és injectiu si, i només si, θ no és arrel de cap polinomi no nul de $k[X]$; és a dir, si θ és transcendent sobre k. En aquest cas, tenim un isomorfisme $k[\theta] \simeq k[X]$; i, en conseqüència, $k(\theta)$ és isomorf al cos de fraccions de l'anell de polinomnis en una indeterminada sobre k.

3.3.5. En cas contrari, és a dir, si θ és algebraic sobre k, $\ker(\psi_\theta)$ és un ideal no nul de $k[X]$; com que $k[X]$ és un domini d'ideals principals, si $f(X)$ és un generador qualsevol de $\ker(\psi_\theta)$, obtenim que $k[X]/(f(X)) \simeq k[\theta] \subseteq K$. 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 θ sobre k el polinomi mònic que genera l'ideal $\ker(\psi_\theta)$; és un polinomi irreductible de $k[X]$ que denotarem per $\mathrm{Irr}(\theta, k)(X)$.

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

Demostració: La hipòtesi $g(\theta) = 0$ ens diu que $g(X) \in \ker(\psi_\theta) = (f(X))$; és a dir, que $f(X) \mid g(X)$. □

Procedim, ara, a la demostració de la irreductibilitat dels polinomis ciclotòmics que havíem 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 mònics 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 ζ és una arrel n-èsima primitiva de la unitat i $\mathrm{mcd}(p, n) = 1$, la potència p-èsima ζ^p també és una arrel n-èsima primitiva de la unitat, de manera que ζ^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 $f(\zeta^p) \neq 0$; tindríem que $g(\zeta^p) = 0$; o sigui, que ζ seria una arrel del polinomi mònic de coeficients enters $g(X^p)$. Com que $f(X)$ és irreductible, se satisfà que $f(X) = \mathrm{Irr}(\zeta, \mathbb{Q})(X)$ i, per tant,

tindríem que $f(X) \mid g(X^p)$. Doncs, existiria 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 ζ 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 ζ és una arrel de $f(X)$, també és $f(\zeta^r) = 0$, per a tot nombre natural r tal que $\mathrm{mcd}(r, n) = 1$. Ara bé, si ζ és una arrel n-èsima primitiva de la unitat, tota altra arrel n-èsima primitiva de la unitat és de la forma ζ^r, amb $\mathrm{mcd}(r, n) = 1$; per tant, totes les arrels n-èsimes primitives de la unitat són arrels de $f(X)$. □

3.3.8. Siguin 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, $k[\theta] \simeq k[X]/(\mathrm{Irr}(\theta, k)(X))$ és un k-espai vectorial de dimensió finita, igual al grau, n, de $\mathrm{Irr}(\theta, k)(X)$, i $\{1, \theta, \theta^2, \ldots, \theta^{n-1}\}$ és una k-base de $k[\theta]$. En particular, per a tot element $\beta \in k[\theta]$, $\beta \neq 0$, existeix un polinomi $g(X) \in k[X]$, $\mathrm{gr}(g(X)) < n$, tal que $\beta = g(\theta)$.

Exercici 3.3.9. Siguin $\theta \in K$ 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 θ de coeficients en k a partir d'una expressió de β 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 $d \mid n$, irreductibles en $\mathbb{Q}[X]$. Aquestes

equacions satisfan una propietat especial: donada una arrel qualsevol, ζ, del polinomi ciclotòmic $\Phi_d(X)$, les altres arrels del polinomi són potències de ζ; en conseqüència, les altres arrels pertanyen al menor subcòs de $\mathbb{C}$ que conté $\mathbb{Q}$ i ζ.

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 direm que K és un cos extensió de k i escriurem $K \mid k$. Direm que una extensió $K \mid k$ de cossos és algebraica si tot element de K és algebraic sobre k; en cas contrari, direm que $K \mid k$ és una extensió transcendent.

Exemples 3.4.3. Les extensions $\mathbb{C} \mid \mathbb{Q}$ i $\mathbb{R} \mid \mathbb{Q}$ 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 $\mathbb{C} \mid \mathbb{R}$ és algebraica, perquè donat $\theta \in \mathbb{C}$, podem escriure $\theta = a + bi$, amb $a, b \in \mathbb{R}$ únics, de manera que θ és arrel del polinomi $X^2 - 2aX + (a^2 + b^2) \in \mathbb{R}[X]$.

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

Observació 3.4.5. En aquesta definició de grau com a nombre cardinal fem servir els resultats, que es discuteixen en un apèndix, que tot espai vectorial té una base i que dues bases d'un mateix espai vectorial tenen el mateix cardinal. 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 $\overline{k}$ un cos algebraicament tancat, $k \subseteq \overline{k}$ un subcòs, i $f(X) \in k[X]$ un polinomi irreductible qualsevol. Si considerem $\theta \in \overline{k}$ una arrel de $f(X)$ i

$K := k[\theta] = k(\theta)$, resulta que $K \simeq k[X]/(f(X))$, de manera que $[K : k] = \mathrm{gr}(f(X))$. Per exemple, si $n \geq 1$ i ζ és una arrel n-èsima primitiva 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 $K \mid k$ una extensió finita de cossos. Llavors, $K \mid k$ és algebraica.*

DEMOSTRACIÓ: Sigui $\theta \in K$ un element qualsevol; volem veure que θ 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 θ, $\{1, \theta, \theta^2, \ldots, \theta^n\}$, és k-linealment dependent i, en conseqüència, existeixen elements $a_0, a_1, \ldots, a_n \in k$, no tots nuls, tals que $\sum_{i=0}^{n} a_i\theta^i = 0$; és a dir, existeix un polinomi no nul $f(X) := \sum_{i=0}^{n} a_iX^i \in k[X]$ tal que $f(\theta) = 0$. Per tant, θ és algebraic sobre k. $\square$

Proposició 3.4.8. (Comportament del grau en torres d'extensions) *Siguin $k \subseteq K \subseteq L$ cossos qualssevol; 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. □

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

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 $\overline{k}$ un cos algebraicament tancat, $k \subseteq \overline{k}$ un subcòs, i $f(X) \in k[X]$ un polinomi no nul de coeficients en k. Siguin $\theta_1, \ldots, \theta_n$ les arrels de $f(X)$ en $\overline{k}$ i considerem la successió de subcossos de $\overline{k}$

$$k \subseteq k(\theta_1) \subseteq k(\theta_1, \theta_2) \subseteq \cdots \subseteq k(\theta_1, \ldots, \theta_n);$$

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

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

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

3.4.13. Si $L \mid k$ 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 $K \mid k$ és una subextensió finita de $L \mid k$. En efecte; com que tot element $\theta \in L$ és algebraic sobre k, la subextensió $k(\theta) \mid k$ de $L \mid k$ 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 $\{\theta_1, \ldots, \theta_n\}$, $k(F)$ denota el cos $k(\theta_1, \ldots, \theta_n)$.

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

Demostració: Sigui $f(X) := \mathrm{Irr}(\theta, k)(X) \in k[X]$ el polinomi minimal de θ sobre k. Com que $k \subseteq K$, també és $f(X) \in K[X]$ i $f(\theta) = 0$, de manera que el polinomi $\mathrm{Irr}(\theta, K)(X)$ divideix $f(X)$; en conseqüència, $[K(\theta) : K] = \mathrm{gr}(\mathrm{Irr}(\theta, K)(X)) \leq \mathrm{gr}(f(X)) = [k(\theta) : k]$. □

Definició 3.4.16. Siguin $\overline{k}$ un cos algebraicament tancat, i $k \subseteq K \subseteq \overline{k}$ i $k \subseteq L \subseteq \overline{k}$ subcossos. Anomenarem compost de K i L el subcòs $KL \subseteq \overline{k}$ generat per K i L; o sigui, el menor subcòs de $\overline{k}$ que conté K i 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 $L \mid k$ és finita, l'extensió $KL \mid K$ és finita i $[KL : K] \leq [L : k]$.*

b) Comportament del grau per composició. *Si les extensions $K \mid k$ i $L \mid k$ són finites, l'extensió $KL \mid k$ és finita i $[KL : k] \leq [L : k][K : k]$.*

Demostració: Si $L \mid k$ és una extensió finita, existeixen elements de L, posem $\theta_1, \ldots, \theta_n$, tals que $L = k(\theta_1, \ldots, \theta_n)$; llavors, $KL = K(\theta_1, \ldots, \theta_n)$. Com que cada element θ_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 $[K(\theta_1, \ldots, \theta_{i+1}) : K(\theta_1, \ldots, \theta_i)]$ i $[k(\theta_1, \ldots, \theta_{i+1}) : k(\theta_1, \ldots, \theta_i)]$. 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 primers entre si. Se satisfà la igualtat $\varphi(mn) = \varphi(m)\varphi(n)$.*

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

Per a tot nombre natural m, denotarem per ζ_m una arrel m-èsima primitiva de la unitat qualsevol de $\mathbb{C}$.

Proposició 3.5.2. *Siguin m, $n\geq 1$ nombres naturals primers entre si. Llavors, el producte $\zeta_m\zeta_n$ és una arrel mn-èsima primitiva 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

$$\begin{array}{ccccc} & & \mathbb{Q}(\zeta_m,\zeta_n) & & \\ & / & & \backslash & \\ \mathbb{Q}(\zeta_m) & & & & \mathbb{Q}(\zeta_n) \\ & \backslash & & / & \\ & & \mathbb{Q}(\zeta_m)\cap\mathbb{Q}(\zeta_n) & & \\ & & | & & \\ & & \mathbb{Q}. & & \end{array}$$

Sigui $\zeta:=\zeta_m\zeta_n$. Vegem que $\mathbb{Q}(\zeta_m,\zeta_n)=\mathbb{Q}(\zeta)=\mathbb{Q}(\zeta_{mn})$. Com que $\mathrm{mcd}(m,n)=1$, ζ és una arrel mn-èsima primitiva de la unitat; en particular, $\mathbb{Q}(\zeta)=\mathbb{Q}(\zeta_{mn})$. 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 ζ^m és una arrel n-èsima primitiva de la unitat, ζ_n és una potència de ζ^m i, per tant, una potència de ζ, 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, en particular, les igualtats següents entre els graus de les extensions: $[\mathbb{Q}(\zeta_m,\zeta_n):\mathbb{Q}(\zeta_n)]\varphi(n)=$

$[\mathbb{Q}(\zeta_m,\zeta_n) : \mathbb{Q}(\zeta_n)][\mathbb{Q}(\zeta_n) : \mathbb{Q}] = [\mathbb{Q}(\zeta_m,\zeta_n) : \mathbb{Q}] = \varphi(mn) = \varphi(m)\varphi(n)$; 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; i com que $\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) \subseteq \mathbb{Q}(\zeta_m)$, això implica la igualtat dels dos cossos. □

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

Proposició 3.5.3. *Siguin $\overline{k}$ un cos qualsevol, i k, K_1, K_2, subcossos de $\overline{k}$ tals que $k \subseteq K_1 \cap K_2$. Suposem que l'extensió $K_1K_2 \mid k$ és finita i que $[K_1K_2 : k] = [K_1 : k][K_2 : k]$. Llavors, $K_1 \cap K_2 = k$.* □

3.5.4. 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 $[K_1K_2 : k] = [K_1 : k][K_2 : k]$. 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) $[K_1K_2 : \mathbb{Q}] = 6$.

En primer lloc, el polinomi $X^3 - 2$ és irreductible en $\mathbb{Q}[X]$, de manera que $[K_1 : \mathbb{Q}] = [K_2 : \mathbb{Q}] = \mathrm{gr}(X^3 - 2) = 3$.

En segon lloc, com que el grau de l'extensió $K_1 \mid \mathbb{Q}$ 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) haurem vist c). I per a veure b), observem que per al nombre $\rho := \dfrac{\theta_2}{\theta_1}$ tenim que $\rho^2 + \rho + 1 = 0$, perquè $\rho^3 = 1$, però $\rho \neq 1$. Ara, si fos $K_1 = K_2$, tindríem que $\rho \in K_1$, de manera que $\mathbb{Q}(\rho) \subseteq K_1$; però ρ satisfà un polinomi irreductible de grau 2 sobre $\mathbb{Q}$, de manera que K_1 contindria una extensió de grau 2, però aquest fet és impossible perquè el grau $[K_1 : \mathbb{Q}]$ no és parell.

Finalment, $K_1K_2 = K_1(\rho)$, ja que, si un cos conté θ_1, condició necessària i suficient perquè contingui θ_2 és que contingui ρ. Així, $K_1K_2 \mid \mathbb{Q}$ és

la composició d'una extensió de grau 3, $K_1 \mid \mathbb{Q}$, i una extensió de grau 2, $\mathbb{Q}(\rho) \mid \mathbb{Q}$, de manera que $[K_1K_2 : \mathbb{Q}] \leq [K_1 : \mathbb{Q}][\mathbb{Q}(\rho) : \mathbb{Q}] = 6$. Ara, $K_1K_2 \mid \mathbb{Q}$ és una extensió de grau menor o igual que sis, divisible per 3 (ja que conté $K_1 \mid \mathbb{Q}$), i estrictament més gran que 3 (ja que K_1K_2 conté estrictament K_1, perquè $K_1 \neq K_2$); per tant, $[K_1K_2 : \mathbb{Q}] = 6$. □

Observació 3.5.5. 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 3.5.6. *Siguin $\overline{k}$ un cos qualsevol, i k, K_1, K_2, subcossos de $\overline{k}$ tals que $k \subseteq K_1 \cap K_2$. Suposem que les extensions $K_1 \mid k$ i $K_2 \mid k$ són finites i que $[K_1 : k]$ i $[K_2 : k]$ són primers entre si. Llavors, $K_1K_2 \mid k$ és finita i $[K_1K_2 : k] = [K_1 : k][K_2 : k]$.*

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 $\overline{k}$ un cos algebraicament tancat de característica diferent de 2 i $k \subseteq K \subseteq \overline{k}$ 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 η^2 és combinació lineal, de coeficients en k, de 1 i η. Siguin $b, c \in k$ 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 θ i $-\theta$, pertanyen a K, i no pertanyen a k. □

3.6.2. Si $\mathrm{car}(\overline{k}) \neq 2$ i si $\theta, \eta \in \overline{k}$ 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 θ^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 $K \subseteq \overline{k}$ 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 $K \subseteq \overline{k}$ 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, hem provat el resultat següent.

Proposició 3.6.4. *Siguin $\overline{k}$ un cos algebraicament tancat de característica diferent de 2 i $k \subseteq \overline{k}$ un subcòs. Existeix una correspondència bijectiva entre el conjunt de les subextensions $K \mid k$ de $\overline{k} \mid k$ 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^*.* □

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 $q = \dfrac{r}{s}$, $r, s \in \mathbb{Z}$, $s \neq 0$, 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 $q = \dfrac{a}{b}$, amb $a, b \in \mathbb{Z}$, $\mathrm{mcd}(a, b) = 1$; 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 $\mathbb{Q}^*/\mathbb{Q}^{*2} - \{1\}$. □

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 $k \mid k$. Discutirem aquest cas en el capítol següent.

3.7 Grup de Galois dels cossos ciclotòmics

Sigui $\zeta_n \in \mathbb{C}$ una arrel n-èsima primitiva de la unitat qualsevol, $n \geq 2$, i considerem el cos ciclotòmic $\mathbb{Q}(\zeta_n)$. Ja hem vist que, si r és un nombre natural primer amb n, ζ_n^r també és una arrel n-èsima primitiva de la unitat. Una pregunta que ens podem fer de manera natural és: quin efecte té el canvi de ζ_n per ζ_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 $\mathrm{mcd}(n, r) = 1$, llavors ζ_n també és una potència de ζ_n^r, ja que ζ_n^r és una arrel n-èsima primitiva de la unitat; per tant, $\mathbb{Q}(\zeta_n^r) = \mathbb{Q}(\zeta_n)$.

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

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

Demostració: Ja hem provat l'existència; vegem-ne la unicitat. Com que ζ_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 ζ_n. Però si σ és un morfisme de $\mathbb{Q}$ en un anell qualsevol (per exemple, la restricció a $\mathbb{Q}$ de σ_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 ζ_n determina, com a màxim, un automorfisme de $\mathbb{Q}(\zeta_n)$. □

Així, doncs, el canvi de ζ_n per ζ_n^r ens 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 $\mathbb{Q}(\zeta_n) \mid \mathbb{Q}$ el grup dels automorfismes de $\mathbb{Q}(\zeta_n)$, i es denota per $\mathrm{Gal}(\mathbb{Q}(\zeta_n) \mid \mathbb{Q})$.

3.7.5. Sigui $\sigma : \mathbb{Q}(\zeta_n) \longrightarrow \mathbb{Q}(\zeta_n)$ un automorfisme qualsevol; la restricció de σ 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 n-èsima primitiva 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 $\chi : \mathrm{Gal}(\mathbb{Q}(\zeta_n) \mid \mathbb{Q}) \longrightarrow (\mathbb{Z}/n\mathbb{Z})^*$.

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

Demostració: Siguin $\sigma, \tau \in \mathrm{Gal}(\mathbb{Q}(\zeta_n) \mid \mathbb{Q})$; llavors, $\zeta_n^{\chi(\sigma\circ\tau)} = (\sigma \circ \tau)(\zeta_n) = \sigma(\tau(\zeta_n)) = \sigma(\zeta_n^{\chi(\tau)}) = \sigma(\zeta_n)^{\chi(\tau)} = (\zeta_n^{\chi(\sigma)})^{\chi(\tau)} = \zeta_n^{\chi(\sigma)\chi(\tau)}$, de manera que $\chi(\sigma \circ \tau) = \chi(\sigma)\chi(\tau)$, en $(\mathbb{Z}/n\mathbb{Z})^*$; per tant, χ 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 σ i τ coincideixen sobre un generador de $\mathbb{Q}(\zeta_n)$ com a cos. Això ens diu que χ és un morfisme injectiu.

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

Resta veure que l'isomorfisme χ no depèn de l'arrel n-èsima de la unitat ζ_n que considerem per a definir-lo; però això és senzill. En efecte, si ζ_n' és una altra arrel n-èsima primitiva de la unitat, existeix $r \in \mathbb{Z}$ tal que $\zeta_n' = \zeta_n^r$; llavors, $\sigma(\zeta_n') = \sigma(\zeta_n^r) = \sigma(\zeta_n)^r = \zeta_n^{\chi(\sigma)r} = \zeta_n'^{\chi(\sigma)}$, com volíem demostrar. □

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

Corol·lari 3.7.8. *Per a tot $n \geq 1$, és $\mathrm{Gal}(\mathbb{Q}(\zeta_n) \mid \mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^*$.* □

Per a acabar aquesta secció, observarem un cas particular d'un resultat que, més endavant, serà 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 $\zeta := \zeta_n$, $G := \mathrm{Gal}(\mathbb{Q}(\zeta) \mid \mathbb{Q})$, 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 $\mathrm{Irr}(\zeta, K)(X)$. Sigui $f(X) := \mathrm{Irr}(\zeta, K)(X) \in K[X]$; donat $\sigma \in G$, és $f(\sigma(\zeta)) = \sigma(f(\zeta)) = \sigma(0) = 0$, ja que σ deixa fixos tots els coeficients de $f(X)$, perquè $f(X) \in K[X]$; per tant, totes les arrels n-èsimes primitives de la unitat són arrels de $f(X)$, de manera 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 $\mathrm{gr}(f(X)) = \varphi(n)$, com volíem demostrar. □

3.8 Grup de Galois d'una extensió algebraica

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

Definició 3.8.1. Siguin $K \mid k$, $L \mid k$ dues extensions d'un mateix cos k. Anomenarem morfisme d'extensions de $K \mid k$ en $L \mid k$, o bé k-immersió del cos K en el cos L, tot morfisme de cossos $\sigma : K \longrightarrow L$ tal que $\sigma(a) = a$, per a tot $a \in k$. Si σ és un isomorfisme, direm que és un k-isomorfisme o un isomorfisme d'extensions.

Definició 3.8.2. Si $\sigma : K \longrightarrow L$ és qualsevol morfisme de cossos, denotarem per $f^\sigma(X)$ el polinomi de $L[X]$ que s'obté en aplicar σ 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 $f^\sigma(X)$. En particular, si σ és una k-immersió i $f(X) \in k[X]$, llavors $f^\sigma(X) = f(X)$, 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 $\sigma : k(\theta) \longrightarrow k(\theta')$ tal que $\sigma(\theta) = \theta'$.*

Demostració: L'isomorfisme $k(\theta) \simeq k[X]/(f(X))$ de (3.3.5) que identifica θ amb la classe de X és un k-isomorfisme; per tant, la composició d'aquest amb l'invers de l'anàleg per a θ' és un k-isomorfisme de $k[\theta]$ en $k[\theta']$ que transforma θ en θ'. A més a més, com que θ genera $k(\theta)$ com a cos extensió de k, la imatge de θ 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. □

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 les dues arrels. Per tant, no importa quina arrel considerem, si l'afegim a k obtindrem extensions isomorfes de k.

3.8.6. Donats un polinomi irreductible $f(X) \in k[X]$, una arrel θ de $f(X)$ en un cos K extensió de k, i una k-immersió $\sigma : K \longrightarrow L$, on $L \mid k$ és una extensió qualsevol de k, $\sigma(\theta)$ també és una arrel de $f(X)$ i $k(\theta) \mid k$ i $k(\sigma(\theta)) \mid k$ 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 n-èsima primitiva 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 $K \mid k$ una extensió algebraica qualsevol de cossos. Tota k-immersió $\sigma : K \longrightarrow K$ és un k-automorfisme de K.*

Demostració: Com que σ és un morfisme d'anells d'un cos en un altre anell, σ és injectiu; vegem-ne l'exhaustivitat. El cas de les extensions finites $K \mid k$ és immediat, perquè σ 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 el seu polinomi minimal $f(X) := \mathrm{Irr}(\theta', k)(X) \in k[X]$, 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 θ' és imatge per σ 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 $K' \mid k$ és finita. D'altra banda, la restricció de σ a K' és una k-immersió de K' en K; però σ envia qualsevol arrel de $f(X)$ que pertanyi a K a una altra arrel de $f(X)$ que pertany a K, de manera que σ aplica K' en K'; això és dir que la restricció de σ a K' és una k-immersió de K' en K'. Com que $K' \mid k$ és finita, $\sigma : K' \longrightarrow K'$ és un automorfisme, de manera que existeix $\theta \in K' \subseteq K$ tal que $\sigma(\theta) = \theta'$, com volíem demostrar. □

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

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

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

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

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

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

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

3.8.14. En general, no podem esperar que χ sigui exhaustiu. Per exemple, si $k := \mathbb{Q}(\zeta_n)$, és clar que el grup $\mathrm{Gal}(k \mid k) = \{1\}$ 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 $\#\mathrm{Gal}(\mathbb{Q}(\zeta) \mid \mathbb{Q}) = [\mathbb{Q}(\zeta) : \mathbb{Q}]$, mostrarem 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 $\mathrm{Gal}(\mathbb{Q}(\theta) \mid \mathbb{Q}) = \{1\}$. En efecte, siguin θ, θ', $\theta'' \in \mathbb{C}$ 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 cúbica primitiva de la unitat de $\mathbb{C}$. Llavors, $K = \mathbb{Q}(\theta, \rho)$, de manera que $[K : \mathbb{Q}] = 6$ (cf. l'exemple 3.5.4) 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 θ que, alhora, ha d'ésser una arrel de $f(X)$, un tal automorfisme ha d'ésser la identitat. D'on $\mathrm{Gal}(\mathbb{Q}(\theta) \mid \mathbb{Q}) = \{1\}$.

Exemple 3.8.16. Considerem $A := (\mathbb{Z}/2\mathbb{Z})[t]$ l'anell de polinomis en una indeterminada t i coeficients en $\mathbb{Z}/2\mathbb{Z}$ i $k := (\mathbb{Z}/2\mathbb{Z})(t)$ el seu cos de fraccions. Siguin $f(X) := X^2 - t \in k[X]$, θ 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 θ 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 θ a θ. En conseqüència, $\mathrm{Gal}(K \mid k) = \{1\}$, 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 θ és un element algebraic sobre

un cos k, llavors $\#\mathrm{Gal}(k(\theta) \mid k) \leq [k(\theta) : k]_s \leq [k(\theta) : k]$, on $[k(\theta) : k]_s$ denota, momentàniament, el nombre de k-immersions diferents de $k(\theta)$ en un cos algebraicament tancat que conté k i θ. D'altra banda, en el cas en què $\theta = \zeta_n$ és una arrel n-èsima primitiva de la unitat, hem vist que

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

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

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

i en el darrer cas, hem vist que

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

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 θ de $g(X)$, podem observar que $g(X)$ té tres arrels diferents dobles, però K només en conté una; per tant, tenim que

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

3.9 Extensions normals

Convé que examinem més acuradament els exemples anteriors. Els casos en què $\#\mathrm{Gal}(k(\theta) \mid K) = [k(\theta) : k]_s$ són els casos en què el cos $k(\theta)$ és el cos de descomposició del polinomi irreductible $\mathrm{Irr}(\theta, k)(X) \in k[X]$; 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 $\#\mathrm{Gal}(k(\theta) \mid K) < [k(\theta) : k]_s$ són els casos en què $k(\theta)$ no és el cos de descomposició de $\mathrm{Irr}(\theta, k)(X) \in k[X]$.

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

a) Existeix una família de polinomis $\{f_i(X)\}_{i\in I}$, $f_i(X) \in k[X]$, *tal que* K *és el cos* $K = k(\{\theta \in \overline{k} : \text{existeix } i \in I \text{ i } f_i(\theta) = 0\})$; *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* $\theta \in K$ *és una arrel de* $f(X)$, *llavors* K *conté totes les arrels de* $f(X)$.

d) Tota k*-immersió de* K *en* $\overline{k}$ *és un* k*-automorfisme de* K; *és a dir, tota* k*-immersió de* K *en* $\overline{k}$ *té imatge dins* K *i és automorfisme de* K.

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

e) El nombre de k*-immersions de* K *en* $\overline{k}$ *coincideix amb* $\#\mathrm{Gal}(K \mid k)$.

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 $c) \implies b)$, només cal notar que K és el cos de descomposició de la família formada per tots els polinomis irreductibles $\mathrm{Irr}(\theta, k)(X) \in k[X]$ tals que $\theta \in K$.

Vegem que $b) \implies d)$. Sigui $\sigma : K \longrightarrow \overline{k}$ 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 hipòtesi sobre K; per tant, $\sigma(K) \subseteq K$; i, com que $K \mid k$ és algebraica, $\sigma : K \longrightarrow K$ és un k-automorfisme de K.

Vegem que $d) \implies c)$. Siguin $f(X) \in k[X]$ 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 $f(X)$, $\theta' \in \overline{k}$, sigui $\sigma : k(\theta) \longrightarrow k(\theta') \subseteq \overline{k}$ l'únic k-isomorfisme tal que $\sigma(\theta) = \theta'$. Ara, utilitzarem el resultat següent, que provarem més avall, per a veure que $\theta' \in K$.

Proposició 3.9.2. (Extensió algebraica de morfismes) *Siguin* $\overline{k}$ *un cos algebraicament tancat,* $k \subseteq \overline{k}$ *un subcòs qualsevol,* $k \subseteq K \subseteq L$ *subcossos tals que*

$L \mid k$ és una extensió algebraica, i $\sigma : K \longrightarrow \overline{k}$ una k-immersió qualsevol. Llavors, existeix una k-immersió $\sigma' : L \longrightarrow \overline{k}$ tal que la restricció a K de σ' és σ; és a dir, $\sigma'_{|K} = \sigma$.

Usem aquesta proposició de la manera següent: Sigui $\sigma : K \longrightarrow \overline{k}$ una extensió a K de $\sigma : k(\theta) \longrightarrow k(\theta') \subseteq \overline{k}$; per hipòtesi, σ 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 $K \mid k$ 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). □

Observació 3.9.3. Si $K \mid k$ és finita, la quantitat de k-immersions de K en $\overline{k}$ és finita. En efecte, existeix una quantitat finita d'elements $\theta_1, \ldots, \theta_n \in K$ tals que $K = k(\theta_1, \ldots, \theta_n)$; llavors, tota k-immersió de K és determinada per la imatge de cada un dels θ_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 $\overline{K}$, $\overline{L}$, són cossos algebraicament tancats, $K \subseteq \overline{K}$, un subcòs qualsevol, $\theta \in \overline{K}$ un element algebraic sobre K, i $\sigma : K \longrightarrow \overline{L}$ un morfisme de cossos qualsevol, existeix una extensió de σ a un morfisme $K(\theta) \xrightarrow{\sigma'} \overline{L}$.*

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

Un cop vista l'extensió d'un morfisme de cossos $\sigma : K \longrightarrow \overline{L}$ 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 usarem el lema de Zorn, que es discuteix en un apèndix.

Proposició 3.9.5. *Siguin $\overline{L}$ un cos algebraicament tancat, $K \mid k$ una extensió algebraica de cossos, i $\sigma : k \longrightarrow \overline{L}$ un morfisme de cossos qualsevol. Llavors, existeix una extensió de σ a un morfisme $\sigma' : K \longrightarrow \overline{L}$.*

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

Donades dues parelles $(K', \sigma'), (K'', \sigma'') \in C$, posarem $(K', \sigma') \leq (K'', \sigma'')$ si, i només si, $K' \subseteq K''$ i la restricció de σ'' a K' és σ'. 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', σ'); com que el conjunt D és totalment ordenat, F és un subcòs de K' que conté k. D'altra banda, podem definir una aplicació $\sigma_F : F \longrightarrow \overline{L}$ 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, σ_F està ben definida.

Vegem, ara, que σ_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, σ_F és un morfisme de cossos que, clarament, és una extensió de σ', 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, σ_F) tal que $k \subseteq F \subseteq K$ i $\sigma_F : F \longrightarrow \overline{L}$ és una extensió de σ, i tal que si $(F, \sigma_F) \leq (F', \sigma_{F'})$, per a alguna

parella $(F', \sigma_{F'}) \in C$, llavors $F = F'$ i $\sigma_F = \sigma_{F'}$. Si veiem que $F = K$, ja haurem acabat.

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 σ_F a un morfisme $\overline{\sigma}_F : F(\theta) \longrightarrow \overline{L}$ que estén σ_F, ja que θ és algebraic sobre k i, per tant, algebraic sobre F; de manera que la parella (F, σ_F) no seria un element maximal de C. Això acaba la demostració. □

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

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

Demostració: Si $K \mid k$ és finita, existeixen elements $\theta_1, \ldots, \theta_n \in K$ tals que $K = k(\theta_1, \ldots, \theta_n)$. Sigui $f(X)$ el producte dels polinomis $\mathrm{Irr}(\theta_i, k)(X) \in k[X]$; 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. □

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

En canvi, si $\theta \in \mathbb{C}$ és una arrel del polinomi $f(X) := X^3 - 2$, l'extensió $\mathbb{Q}(\theta) \mid \mathbb{Q}$ 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

La propietat equivalent *c*) de la definició d'extensió normal de cossos es pot llegir en el sentit que si $K \mid k$ 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 $\overline{k}$ un cos algebraicament tancat, $k \subseteq K \subseteq \overline{k}$ subcossos tals que l'extensió $K \mid k$ és normal, $f(X) \in k[X]$ un polinomi irreductible, i $g(X)$, $h(X)$ polinomis mònics irreductibles de $K[X]$ que divideixen $f(X)$. Llavors, existeix un k-automorfisme $\sigma \in \mathrm{Gal}(K \mid k)$ tal que $h(X) = g^\sigma(X)$.*

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

La restricció a K de σ és una k-immersió $\sigma : K \longrightarrow \overline{k}$, de manera que, per hipòtesi, σ és un k-automorfisme de K; és a dir, $\sigma \in \mathrm{Gal}(K \mid k)$.

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

Corol·lari 3.9.10. *Siguin $K \mid k$ 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.* □

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

Acabem la secció amb les propietats de la normalitat respecte del canvi de base i de la composició.

Proposició 3.9.12. *Siguin $\overline{k}$ un cos algebraicament tancat, i $k \subseteq K \subseteq \overline{k}$ i $k \subseteq L \subseteq \overline{k}$ subcossos. Si l'extensió $K \mid k$ és normal, llavors l'extensió $KL \mid L$ és normal.*

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

Proposició 3.9.13. *Siguin $\overline{k}$ un cos algebraicament tancat, i $k \subseteq K \subseteq \overline{k}$ i $k \subseteq L \subseteq \overline{k}$ subcossos. Si les extensions $K \mid k$ i $L \mid k$ són normals, llavors l'extensió $KL \mid k$ és normal.*

DEMOSTRACIÓ: Si K és el cos de descomposició d'una família $\{f_i(X)\}_{i \in I}$ de polinomis de $k[X]$, i L és el cos de descomposició d'una família $\{g_j(X)\}_{j \in J}$

de polinomis de $k[X]$, el cos compost KL és el cos de descomposició de la família reunió $\{f_i(X)\}_{i\in I} \cup \{g_j(X)\}_{j\in J}$. $\square$

Observació 3.9.14. 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 $\mathbb{Q}(\alpha) \mid \mathbb{Q}$ no és normal (per exemple, perquè $i \notin \mathbb{Q}(\alpha)$), mentre que les dues extensions $\mathbb{Q}(\alpha) \mid \mathbb{Q}(\alpha^2)$ i $\mathbb{Q}(\alpha^2) \mid \mathbb{Q}$ són normals (per exemple, perquè són quadràtiques).

3.10 Cossos finits

En aquesta secció, ens aturarem una mica i farem l'estudi d'una família molt important de cossos: els cossos finits. Com que, en particular, els cossos finits proporcionen sempre extensions normals, obtindrem exemples molt importants de la teoria de les extensions normals. D'altra banda, els cossos finits també proporcionen un exemple molt important (i motivador) 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 $p = \mathrm{car}(\mathbb{F})$ 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. *Suposem que $\overline{\mathbb{F}}$ és un cos algebraicament tancat de característica $p > 0$. Llavors:*

(a) *Per a tot nombre natural $f \geq 1$, existeix un únic subcòs $\mathbb{F}_{p^f} \subseteq \overline{\mathbb{F}}$ 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) *Encara més,* $\mathbb{F}_{p^f}$ *és el conjunt de les arrels del polinomi* $X^{p^f} - X \in (\mathbb{Z}/p\mathbb{Z})[X]$ *en* $\overline{\mathbb{F}}$. *En particular,* $\mathbb{F}_{p^f}^* = \mu_{p^f-1}(\overline{\mathbb{F}})$ *són les arrels* (p^f-1)*-èsimes de la unitat de* $\overline{\mathbb{F}}$.

(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* $\mathbb{F}_{p^n} \mid \mathbb{F}_{p^f}$ *és normal.*

Demostració: Siguin p un nombre natural primer, $f \geq 1$ un nombre natural, 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 θ, θ' dues arrels de $f(X)$ en $\overline{\mathbb{F}}$; llavors, és $\theta^q = \theta$, $\theta'^q = \theta'$, 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.

Vegem (d). Per a això, 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 $\mathbb{C}$, de manera que les seves arrels ho són del polinomi $h(X) := X^n - 1 \in \mathbb{Z}[X]$; per tant, 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 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 $\mathbb{F}_p \simeq \mathbb{Z}/p\mathbb{Z}$ i, per tant, l'extensió $\mathbb{F}_{p^n} \mid \mathbb{F}_p$ 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. □

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 θ 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 ζ una arrel d-èsima primitiva 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 $p^g - 1$, ζ també és una arrel $(p^g - 1)$-èsima de la unitat, de manera que ζ 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 $d \mid p^f - 1$. □

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

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

3.10.6. Sigui $\varphi_q : \mathbb{F}_{q^n} \longrightarrow \mathbb{F}_{q^n}$ 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 $1^q = 1$, φ_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 $\varphi_q \in \mathrm{Gal}(\mathbb{F}_{q^n} \mid \mathbb{F}_q)$.

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

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

Demostració: Com que $[\mathbb{F}_{q^n} : \mathbb{F}_q] = n$, i com que el cos $\mathbb{F}_{q^n}$ és engendrat sobre $\mathbb{F}_q$ per ζ, l'ordre $\#\mathrm{Gal}(\mathbb{F}_{q^n} \mid \mathbb{F}_q)$ és menor o igual que el nombre d'arrels del polinomi $\mathrm{Irr}(\zeta, \mathbb{F}_q)(X) \in \mathbb{F}_q[X]$, és a dir, que $[\mathbb{F}_{q^n} : \mathbb{F}_q]$; per tant, si demostrem que φ_q és un element d'ordre n de $\mathrm{Gal}(\mathbb{F}_{q^n} \mid \mathbb{F}_q)$, ja haurem acabat. 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 φ_q^k és la identitat, ha de ser $\zeta^{q^k} = \zeta$, de manera que k ha de ser un múltiple de n perquè ζ és una arrel $(q^n - 1)$-èsima primitiva de la unitat. Per tant, $\varphi_q \in \mathrm{Gal}(\mathbb{F}_{q^n} \mid \mathbb{F}_q)$ és d'ordre n, com volíem demostrar. □

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 φ_q en $\mathrm{Gal}(\mathbb{F}_{q^n} \mid \mathbb{F}_q)$ 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, hem demostrat que la imatge del caràcter ciclotòmic $\chi : \mathrm{Gal}(\mathbb{F}_{q^n} \mid \mathbb{F}_q) \to (\mathbb{Z}/(q^n - 1)\mathbb{Z})^*$ 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 $\mathbb{F}_{q^d} \mid \mathbb{F}_q$ de $\mathbb{F}_{q^n} \mid \mathbb{F}_q$; d'altra banda, observem que, per a cada divisor d de n, existeix un únic subgrup de $\mathrm{Gal}(\mathbb{F}_{q^n} \mid \mathbb{F}_q)$ d'ordre d, ja que $\mathrm{Gal}(\mathbb{F}_{q^n} \mid \mathbb{F}_q)$ és cíclic d'ordre n. La pregunta és, doncs, òbvia: hi ha alguna relació entre els subgrups de $\mathrm{Gal}(\mathbb{F}_{q^n} \mid \mathbb{F}_q)$ i les subextensions $\mathbb{F}_{q^d} \mid \mathbb{F}_q$ de $\mathbb{F}_{q^n} \mid \mathbb{F}_q$? La resposta és que sí. Vegem quina.

3.10.11. Teoria de Galois per als cossos finits. Siguin $\mathcal{S}(q^n, q)$ el conjunt dels subgrups de $\mathrm{Gal}(\mathbb{F}_{q^n} \mid \mathbb{F}_q)$ i $\mathcal{C}(q^n, q)$ el conjunt de les subextensions de $\mathbb{F}_{q^n} \mid \mathbb{F}_q$.

Observem, en primer lloc, que si $d \mid n$, el grup de Galois $\mathrm{Gal}(\mathbb{F}_{q^n} \mid \mathbb{F}_{q^d})$ és un subgrup del grup de Galois $\mathrm{Gal}(\mathbb{F}_{q^n} \mid \mathbb{F}_q)$, 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 $C(q^n, q) \xrightarrow{f} S(q^n, q)$ per l'assignació $f(\mathbb{F}_{q^d} \mid \mathbb{F}_q) := \mathrm{Gal}(\mathbb{F}_{q^n} \mid \mathbb{F}_{q^d})$.

D'altra banda, podem definir una aplicació $S(q^n, q) \xrightarrow{g} C(q^n, q)$ assignant a cada subgrup H de $\mathrm{Gal}(\mathbb{F}_{q^n} \mid \mathbb{F}_q)$ la subextensió $\mathbb{F}_{q^n}^H \mid \mathbb{F}_q$, 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 $\mathrm{Gal}(\mathbb{F}_{q^n} \mid \mathbb{F}_q) = \langle \varphi_q \rangle$, 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 $\mathbb{F}_{q^n} \mid \mathbb{F}_{q^d}$ és exactament $\langle \varphi_q^d \rangle$. Per tant, les dues aplicacions f i g són inverses l'una de l'altra. Així, hem demostrat el 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 $\mathbb{F}_{q^n} \mid \mathbb{F}_q$ i el conjunt dels subgrups de* $\mathrm{Gal}(\mathbb{F}_{q^n} \mid \mathbb{F}_q)$. □

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 $K \mid \mathbb{Q}$ 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 $K \mid \mathbb{Q}$ i $\mathbb{Q} \mid \mathbb{Q}$.

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

Més endavant, caracteritzarem les extensions per a les quals se satisfà el teorema anterior.

Capítol 4

Radicals

Després de l'equació $X^n = 1$, la més senzilla és l'equació $X^n = a$, per a $a \neq 0, 1$. Dediquem 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. Dediquem la secció segona a la irreductibilitat dels polinomis $X^{p^r} - a$, $a \in k$, p primer, i $r \geq 1$. A continuació, estudiem el concepte d'element separable i de grau de separabilitat d'una extensió algebraica de cossos, concepte que ja ha aparegut de passada en el capítol anterior, 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 pel 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. L'objecte de la secció sisena és l'estudi de les traces i les normes de les extensions finites 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. Dediquem la secció vuitena a la prova del teorema 90 de Hilbert, en les seves formes additiva i multiplicativa, que farem 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. Dediquem la secció desena a establir 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 acabarem de desenvolupar al 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 $\overline{k}$ un cos algebraicament tancat que conté k. Per a $a = 0$, l'equació $X^n = a$ només té la solució $\alpha = 0$ en $\overline{k}$, de manera que, a partir d'ara, suposarem que $a \neq 0$.

4.1.1. Mirem-nos les solucions de l'equació. Suposem que α, $\alpha' \in \overline{k}$ són solucions de l'equació $X^n = a$; com que $a \neq 0$, ha de ser α, $\alpha' \neq 0$, de manera que té sentit considerar el quocient $\dfrac{\alpha'}{\alpha} \in \overline{k}$; i aquest quocient és una solució de l'equació $X^n = 1$; això és, existeix una arrel n-èsima de la unitat, $\zeta \in \overline{k}$, tal que $\alpha' = \zeta\alpha$. I, recíprocament, si α és una solució de $X^n = a$ i ζ 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 $X^n = 1$.

Corol·lari 4.1.2. *Siguin $\overline{k}$ un cos algebraicament tancat, $k \subseteq \overline{k}$ un subcòs qualsevol, $a \in k$, un element no nul, $n \geq 2$ un nombre enter, i $\mu_n(\overline{k})$ el grup de les arrels n-èsimes de la unitat de $\overline{k}$. El cos de descomposició sobre k del polinomi $X^n - a \in k[X]$ és el cos $k(\zeta, \alpha)$, on $\alpha \in \overline{k}$ és una arrel qualsevol del polinomi $X^n - a$, i ζ un generador qualsevol del grup $\mu_n(\overline{k})$.* □

4.1.3. Si $\mathrm{car}(k)$ no divideix n, en $\overline{k}$ hi ha exactament n arrels n-èsimes de la unitat diferents (cf. 3.2.1), de manera que l'equació $X^n = a$ també té n solucions diferents. En canvi, si $\mathrm{car}(k) = p > 0$ 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.

Corol·lari 4.1.4. *Suposem que $\mathrm{car}(k) = p > 0$, 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 $\alpha \in \overline{k}$ l'únic element tal que $\alpha^{p^r} = a$. Llavors, el polinomi $X^n - a$ admet una descomposició en $\overline{k}[X]$ del tipus $X^n - a = (X^{n'} - \alpha)^{p^r}$, i el polinomi $X^{n'} - \alpha$ té n' arrels diferents en $\overline{k}$.

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 $\mathrm{car}(k) = p$, es té que $(X^{n'} - \alpha)^{p^r} = (X^{n'})^{p^r} - \alpha^{p^r} = X^n - a$. □

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 α és una arrel qualsevol de $X^{mn} - a$, llavors α^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 $[k(\alpha^m, \alpha^n) : k] = mn$. D'altra banda, 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, $k(\alpha^m, \alpha^n) = k(\alpha)$. El fet que sigui $[k(\alpha) : k] = mn$ ens diu que $X^{mn} - a = \mathrm{Irr}(\alpha, k)(X) \in k[X]$; en particular, doncs, que $X^{mn} - a$ és irreductible. □

4.1.6. Notem que si sabem calcular les solucions de les equacions $X^m = a$ i $X^n = a$, on $\mathrm{mcd}(m, n) = 1$, també sabem calcular les de l'equació $X^{mn} = a$. En efecte, si α, $\beta \in \overline{k}$ són solucions particulars de les equacions $X^m = a$ i $X^n = a$, respectivament, i si per a x, $y \in \mathbb{Z}$ tals que $mx + ny = 1$, posem $\gamma := \alpha^y\beta^x$, tenim que $\gamma^{mn} = \alpha^{ymn}\beta^{xmn} = a^{yn}a^{xm} = a^{mx+ny} = a$, de manera que $\gamma \in \overline{k}$ 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, sabrem 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 α recorre el conjunt de les arrels del polinomi $X^m - a$, i és $m < n$. En particular, l'objecte pincipal d'estudi d'aquest capítol seran 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 de caracteritzar la irreductibilitat dels polinomis $X^{p^r} - a \in k[X]$, p primer, i de donar una descripció del grup de Galois del cos de descomposició del polinomi $X^n - a \in k[X]$, $n \geq 1$ 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 $\mathrm{car}(k) = 2$; i* (c) *$p = 2$, $\mathrm{car}(k) \neq 2$, i $r = 1$; el polinomi $X^{p^r} - a$ és irreductible en $k[X]$. En el cas* (d) *$p = 2$, $\mathrm{car}(k) \neq 2$, i $r \geq 2$, el polinomi $X^{2^r} - a$ és irreductible en $k[X]$ si, i només si, el polinomi $X^4 + 4a \in k[X]$ no té arrels en k.*

Observació 4.2.2. Doncs, en el cas $p = 2$ i $\mathrm{car}(k) \neq 2$, 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: Suposem 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 $\alpha \in \overline{k}$ una arrel de $X^p - a$ en un cos algebraicament tancat $\overline{k}$ que conté k. Les arrels d'aquest polinomi en $\overline{k}$ són de la forma $\alpha\zeta$, on $\zeta \in \overline{k}$ 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 α és fix i ζ, 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 $\mathrm{mcd}(d, p) = 1$, existeixen nombres enters x, y tals que $dx + py = 1$, i podem definir $\beta := \alpha\zeta^x$; així, tenim que $\beta = \alpha^{py}\alpha^{dx}\zeta^x = a^y b^x \in k$ i que $\beta^p = a$, de manera que el polinomi $X^p - a$ té l'arrel β en k. □

Per a establir l'argument inductiu de la demostració de la proposició 4.2.1, farem 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 $\alpha \in \overline{k}$ una arrel de $X^p - a$ en un cos algebraicament tancat $\overline{k}$ que conté k. En els casos* (a) *i* (b)*, en què o bé $p \neq 2$ o bé $p = 2$ i $\mathrm{car}(k) = 2$, el polinomi $X^p - \alpha$ no té arrels en $k(\alpha)$; en canvi, si $p = 2$ i $\mathrm{car}(k) \neq 2$, 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 $\mathrm{Irr}(\alpha, k)(X) = X^p - a$. També ara distingirem casos, però no els mateixos que abans. El cas més simple és el cas en què $\mathrm{car}(k) = p$. 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 $\mathrm{car}(k) = p$, llavors tenim que $\beta^p = g(\alpha)^p = h(\alpha^p) = h(a) \in k$. Així, si β 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 $\mathrm{car}(k) = p$, el polinomi $X^p - \alpha$ no té arrels en $k(\alpha)$, com es tractava de demostrar.

Estudiem ara el cas en què $\mathrm{car}(k) \neq p$. Siguin ζ una arrel p-èsima primitiva de la unitat, $K := k(\zeta)$, i $L := K(\alpha) = k(\zeta, \alpha)$, el cos de descomposició del polinomi $X^p - a \in k[X]$. 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 $\mathrm{Irr}(\alpha, K)(X)$ i és, per tant, irreductible en $K[X]$. I, com que l'extensió $L \mid k$ és normal, per a tot $i \in \{0, 1, \ldots, p-1\}$ podem considerar un k-automorfisme

$\sigma_i \in \mathrm{Gal}(L \mid k)$, extensió a L de l'única k-immersió $\sigma_i : k(\alpha) \longrightarrow L$ tal que $\sigma_i(\alpha) = \zeta^i \alpha$.

Com més amunt, suposem que existeix alguna arrel $\beta \in k(\alpha)$ del polinomi $X^p - \alpha$. Com que $k(\beta) \subseteq k(\alpha)$, el grau $[k(\alpha) : k] = p$ és primer, i $\beta \notin k$, perquè $\beta^p = \alpha \notin k$, tenim que $k(\alpha) = k(\beta)$ i, en conseqüència, $\mathrm{Irr}(\beta, k)(X)$ 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 $\beta_i^p = \sigma_i(\beta)^p = \sigma_i(\beta^p) = \sigma_i(\alpha) = \zeta^i \alpha$ són tots diferents, tenim que els elements β_i, $0 \leq i \leq p-1$, també són tots diferents; i com que $\sigma_i(\beta)$ és arrel del polinomi $\mathrm{Irr}(\beta, k)(X)$, ha d'ésser $\mathrm{Irr}(\beta, k)(X) = \prod_{i=0}^{p-1}(X - \beta_i)$. En particular, el coeficient del monomi de grau zero d'aquest polinomi pertany a k i, per tant, $\gamma := \prod_{i=0}^{p-1} \beta_i \in k$. A més a més, la potència p-èsima de γ és $\gamma^p = \prod_{i=0}^{p-1}(\zeta^i \alpha) = \alpha^p \zeta^S = a\zeta^S$, on $S = \sum_{i=0}^{p-1} i = \dfrac{p(p-1)}{2}$.

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 (recordem, $p = 2$ i $\mathrm{car}(k) \neq 2$), 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. Podem escriure $\beta =: x + y\alpha$, on x, $y \in k$, i aleshores, de l'equació $\beta^2 = \alpha$, és $x^2 + ay^2 = 0$ i $2xy = 1$. La primera equació, multiplicada per $4x^2$, ens proporciona, tenint en compte la segona, la nova igualtat $4x^4 + a = 4x^4 + 4x^2y^2a = 0$, que ens dóna la nova $-4a = 16x^4 = (2x)^4$, que 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 $\beta := \dfrac{\theta}{2} + \alpha\theta^{-1} \in k(\alpha)$ i $\beta^2 = \dfrac{\theta^2}{4} + a\theta^{-2} + \alpha = \dfrac{\theta^4 + 4a}{4\theta^2} + \alpha = \alpha$, de manera que el polinomi $X^2 - \alpha$ té una arrel β 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: Per inducció sobre r, 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 $\theta \in \overline{k}$ 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 $p = 2 = \mathrm{car}(k)$, 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 ireductible sobre $k(\alpha)$, però això ens diu 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 θ 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 que $p = 2$, que $\mathrm{car}(k) \neq 2$, i que el polinomi $X^4 + 4a$ té alguna arrel $\beta \in k$; si posem $\alpha := \dfrac{\beta}{2} \in k$, 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 $k[X]$.

Recíprocament, suposem que $p = 2$, que $\mathrm{car}(K) \neq 2$, 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 θ 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 $r = 2$, obtindrem això si veiem que $X^2 - \alpha$ no té arrels en $k(\alpha)$; en el cas $r > 2$, ho obtindrem en aplicar la hipòtesi d'inducció al cos base $k(\alpha)$, si veiem que els polinomis $X^4 + 4\alpha$ i $X^2 - \alpha$ no tenen arrels en $k(\alpha)$.

En aquest darrer cas, observem que si el polinomi $X^4 + 4\alpha$ té una arrel $\beta \in k(\alpha)$, llavors és $\dfrac{\beta^2}{2} \in k(\alpha)$ i $\left(\dfrac{\beta^2}{2}\right)^2 = -\alpha$, 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 α, $-\alpha$ són les arrels del polinomi irreductible $X^2 - a \in k[X]$, existeix un únic k-automorfisme $\tau : k(\alpha) \longrightarrow k(\alpha)$ 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 ja ho hem vist a la demostració del lema 4.2.4, quan hem provat 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 $X^4 + 4a$. □

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 $\overline{k}$ un cos algebraicament tancat, $k \subseteq \overline{k}$ un subcòs, $n \geq 2$ un nombre natural no divisible per* $\mathrm{car}(k)$*, $a \in k$, $a \neq 0, 1$, i L el cos de descomposició sobre k del polinomi $X^n - a$. El grup de Galois de l'extensió $L \mid k$ 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 $\mathrm{car}(k)$ no divideix n, existeixen arrels n-èsimes primitives de la unitat en $\overline{k}$. Siguin, doncs, $\zeta \in \overline{k}$ una arrel n-èsima primitiva de la unitat, $K := k(\zeta)$, $\alpha \in \overline{k}$ una arrel qualsevol de $X^n - a$, i $L = k(\alpha, \zeta) = K(\alpha)$, el cos de descomposició sobre k del polinomi $X^n - a$. En particular, tot automorfisme $\sigma \in \mathrm{Gal}(L \mid k)$ és determinat pels valors $\sigma(\alpha)$ i $\sigma(\zeta)$. Ara bé, si $\chi : \mathrm{Gal}(K \mid k) \longrightarrow (\mathbb{Z}/n\mathbb{Z})^*$ és el n-èsim caràcter ciclotòmic sobre k (cf. el corol·lari 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 n-èsima primitiva de la unitat ζ que haguem triat. D'altra banda, com que α 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 $\dfrac{\sigma(\alpha)}{\alpha}$ és una arrel n-èsima de la unitat; és a dir, existeix $\tau(\sigma) \in \mathbb{Z}/n\mathbb{Z}$, determinat unívocament per σ i α (de fet, depèn de l'elecció de l'arrel α 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 $\rho : \mathrm{Gal}(L \mid k) \longrightarrow \mathbf{GL}(2, \mathbb{Z}/n\mathbb{Z})$ definida d'aquesta manera és un morfisme de grups injectiu, amb imatge continguda, per definició, en el subgrup de les matrius de la forma $\begin{bmatrix} * & * \\ 0 & 1 \end{bmatrix}$. □

4.2.6. Suposem que $\mathrm{car}(k) = p > 0$ i que $n = p^r n'$, amb $r \geq 1$ i n' no divisible per p. Llavors, si $\beta \in \overline{k}$ 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 β 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 $\mathrm{Gal}(L \mid k)$ coincideix amb $\mathrm{Gal}(L \mid k(\beta))$; 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 $\mathrm{car}(k)$ divideix n.

Proposició 4.2.7. *Siguin $\overline{k}$ un cos algebraicament tancat de característica positiva, $p := \mathrm{car}(k) > 0$, $k \subseteq \overline{k}$ 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 $L \mid k$ és isomorf a un subgrup del grup de les matrius de la forma $\begin{bmatrix} * & * \\ 0 & 1 \end{bmatrix}$ de $\mathbf{GL}(2, \mathbb{Z}/n'\mathbb{Z})$.*
□

Corol·lari 4.2.8. *Suposem que k conté una arrel n-èsima primitiva de la unitat, ζ, i que el polinomi $X^n - a \in k[X]$ és irreductible. Sigui $\alpha \in \overline{k}$ una arrel de $X^n - a$. Llavors, el grup de Galois de l'extensió $k(\alpha) \mid k$ és cíclic d'ordre n.*

Demostració: En aquest cas, l'acció del caràcter ciclotòmic sobre les arrels n-èsimes de la unitat és trivial, ja que pertanyen al cos base; és a dir, $\chi(\sigma) = 1$, per a tot $\sigma \in \mathrm{Gal}(L \mid k)$; 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 α 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 $\mathrm{Gal}(k(\alpha) \mid k)$; per tant, l'aplicació $\rho : \mathrm{Gal}(k(\alpha) \mid k) \longrightarrow \begin{bmatrix} 1 & * \\ 0 & 1 \end{bmatrix}$ és un isomorfisme de grups. □

Observació 4.2.9. En general, el grup de Galois de l'extensió $k(\alpha, \zeta) \mid k$, quan $\alpha^n \in k$, ζ 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, $\mathrm{Gal}(\mathbb{Q}(\alpha, \zeta) \mid \mathbb{Q}) \simeq S_3$, 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 $K \mid k$ una extensió de cossos i $\theta \in K$ un element algebraic sobre k. Es diu que θ és separable sobre k si θ és arrel d'un polinomi de $k[X]$ que no té arrels múltiples; equivalentment, si el polinomi $\mathrm{Irr}(\theta, k)(X) \in k[X]$ 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 $\mathrm{mcd}(f(X), D(f, X))$ 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 $p := \mathrm{car}(k) > 0$. L'exhaustivitat de l'automorfisme de Frobenius $\varphi_p : k \longrightarrow k$ ens proporciona l'existència d'un polinomi $g(X) \in k[X]$ tal que $h(X)$ s'obté de $g(X)$ en elevar els seus coeficients 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 mònics 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, ens ha aparegut algunes vegades el nombre de k-immersions d'un cos de la forma $k(\theta)$, θ algebraic sobre k, en algun cos algebraicament tancat $\overline{k}$ que conté k, nombre que 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 $\overline{k}$ del polinomi mònic irreductible de $k[X]$ que té θ per arrel. Anem a estudiar aquest nombre més d'aprop; en primer lloc, veurem que no depèn del cos algebraicament tancat $\overline{k}$ que considerem.

Proposició 4.3.5. *Sigui $K \mid k$ una extensió algebraica qualsevol de cossos. El cardinal del conjunt de k-immersions de K en un cos algebraicament tancat $\overline{k}$ que conté k no depèn de $\overline{k}$.*

Demostració: Siguin $\overline{k}$ i k^a cossos algebraicament tancats que contenen k, suposem que $K \subseteq \overline{k}$, i sigui $N \mid k$ la clausura normal en $\overline{k}$ de l'extensió $K \mid k$. 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 $\sigma_0 : N \longrightarrow k^a$. Llavors, per a $N' := \sigma_0(N)$, l'extensió $N' \mid k$ és la clausura normal en k^a de l'extensió $\sigma_0(K) \mid k$, i $\sigma_0 : N \longrightarrow N'$ és un k-isomorfisme. Notem que si l'extensió algebraica $K \mid k$ és generada per una certa família d'elements algebraics sobre k, llavors N és el cos de descomposició en $\overline{k}$ dels polinomis minimals 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 $\overline{k}$ té imatge inclosa en N i tota k-immersió de K en k^a té imatge inclosa en N'.

Ara, la composició amb σ_0 transforma una k-immersió de K en $\overline{k}$ en una k-immersió de K en k^a i, recíprocament, la composició amb σ_0^{-1} transforma una k-immersió de K en k^a en una k-immersió de K en $\overline{k}$. S'obté, d'aquesta manera, una aplicació bijectiva entre els conjunts de les k-immersions de K en $\overline{k}$ i en k^a. □

Aquest resultat ens permet definir en general el grau de separabilitat d'una extensió algebraica de cossos, no necessàriament de la forma $k(\theta) \mid k$, o sigui, no necessàriament generada per un sol element algebraic.

Definició 4.3.6. Sigui $K \mid k$ una extensió algebraica qualsevol de cossos. S'anomena grau de separabilitat de l'extensió $K \mid k$ el cardinal del conjunt de k-immersions de K en qualsevol cos algebraicament tancat $\overline{k}$ 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 $K \mid k$ normals pel fet que l'ordre del grup de Galois $\mathrm{Gal}(K \mid k)$ 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 $\overline{k}$ que contingui k, l'ordre del grup de Galois $\mathrm{Gal}(K \mid k)$ és el nombre de k-automorfismes de K, i l'extensió $K \mid k$ és normal si, i només si, tota k-immersió de K en $\overline{k}$ 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 $K \mid k$ i $L \mid K$ extensions algebraiques qualssevol. Llavors, $[L : k]_s = [L : K]_s[K : k]_s$.*

Demostració: Sigui $\overline{k}$ 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 $\overline{k}$, de totes les k-immersions de L en $\overline{k}$, i de totes les K-immersions de L en $\overline{k}$. 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 $S(k, L) \longrightarrow S(k, K)$ tal que l'antiimatge de tot element de $S(k, K)$ sigui un conjunt del mateix cardinal que $S(K, L)$.

Sigui $N \mid k$ la clausura normal en $\overline{k}$ de l'extensió $L \mid k$. Podem definir una aplicació $f : S(k, L) \longrightarrow S(k, K)$ per $f(\sigma) := \sigma_{|K}$, on $\sigma_{|K}$ indica la restricció a K de σ. Com que l'extensió $L \mid K$ és algebraica, tota k-immersió de K en $\overline{k}$ s'estén a una k-immersió de L en $\overline{k}$ (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 $S(K, L)$.

Per a això, per a tota k-immersió σ de L en $\overline{k}$, fixem una extensió σ' de σ a una k-immersió de N en $\overline{k}$; com que $N \mid k$ és normal, tenim que σ' 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 τ' a N, i la restricció a L de la composició $\sigma_1' \circ \tau'$ és una k-immersió de L en $\overline{k}$ tal que la seva restricció a K és σ_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 σ_1'; per tant, aquests dos conjunts tenen el mateix cardinal, com volíem demostrar. □

Corol·lari 4.3.9. *Sigui $K \mid k$ una extensió finita. Llavors, $[K : k]_s \leq [K : k]$.*

Demostració: Com que per a tota extensió finita $K \mid k$ existeixen elements $\theta_1, \theta_2, \ldots, \theta_n \in K$ tals que $K = k(\theta_1, \ldots, \theta_n)$, tenim que

$$[K : k] = \prod_{i=0}^{n-1} [k(\theta_1, \ldots, \theta_{i+1}) : k(\theta_1, \ldots, \theta_i)].$$

D'altra banda, la proposició anterior ens diu que

$$[K : k]_s = \prod_{i=0}^{n-1} [k(\theta_1, \ldots, \theta_{i+1}) : k(\theta_1, \ldots, \theta_i)]_s.$$

Però en el cas de les extensions de la forma $k(\theta) \mid k$, 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

$$[k(\theta_1, \ldots, \theta_{i+1}) : k(\theta_1, \ldots, \theta_i)]_s \leq [k(\theta_1, \ldots, \theta_{i+1}) : k(\theta_1, \ldots, \theta_i)],$$

i obtenim la propietat desitjada per multiplicació. □

Corol·lari 4.3.10. *Siguin $k \subseteq K \subseteq L$ cossos tals que l'extensio $L \mid k$ és finita. Llavors, la igualtat $[L : k]_s = [L : k]$ se satisfà si, i només si, se satisfan les igualtats $[L : K]_s = [L : K]$ i $[K : k]_s = [K : k]$.* □

Proposició 4.3.11. *Sigui $K \mid k$ una extensió finita qualsevol de cossos. Llavors, $[K : k]_s$ divideix $[K : k]$.*

DEMOSTRACIÓ: Com que podem escriure K en la forma $K = k(\theta_1, \ldots, \theta_n)$, per a certs elements $\theta_1, \ldots, \theta_n \in K$, és suficient provar el resultat per a les extensions de la forma $k(\theta) \mid k$, amb θ algebraic sobre k, per a qualsevol cos k i tenir en compte la multiplicativitat dels graus

$$[k(\theta_1, \ldots, \theta_{i+1}) : k(\theta_1, \ldots, \theta_i)] \quad \text{i} \quad [k(\theta_1, \ldots, \theta_{i+1}) : k(\theta_1, \ldots, \theta_i)]_s.$$

Siguin, doncs, k un cos qualsevol, θ un element algebraic sobre k, $K := k(\theta)$, i $f(X) := \mathrm{Irr}(\theta, k)(X) \in k[X]$ el polinomi minimal de θ sobre k; llavors, $[k(\theta) : k]_s$ és exactament el nombre d'arrels diferents de $f(X)$. Si θ 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 θ 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, $p = \mathrm{car}(k) > 0$, i $r \geq 1$ és un nombre natural, que podem considerar que és el màxim per al qual se satisfà aquesta propietat. Aquest darrer fet implica que θ^{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, θ 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. □

4.4 Extensions separables

Acabem de veure que, per a tota extensió finita de cossos $K \mid k$, $[K : k]_s$ divideix $[K : k]$. Es tracta de veure en quines condicions se satisfà la igualtat.

Proposició 4.4.1. *Sigui $K \mid k$ 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 $K \mid k$ és finita, podem pensar $K = k(\theta_1, \ldots, \theta_n)$, per a certs elements $\theta_i \in K$. Per hipòtesi, cadascun dels elements θ_i és separable sobre k, de manera que θ_{i+1} és separable sobre $k(\theta_1, \ldots, \theta_i)$. Així, obtenim que

$$[k(\theta_1, \ldots, \theta_{i+1}) : k(\theta_1, \ldots, \theta_i)]_s = [k(\theta_1, \ldots, \theta_{i+1}) : k(\theta_1, \ldots, \theta_i)],$$

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 θ és separable sobre k. □

Definició 4.4.2. Sigui $K \mid k$ una extensió algebraica de cossos. Es diu que l'extensió $K \mid k$ 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 $K \mid k$ és normal i separable si, i només si, se satisfà la igualtat $\#\mathrm{Gal}(K \mid k) = [K : k]$.* □

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 $K \mid k$ és separable. El resultat no es restringeix a famílies finites d'elements.

Proposició 4.4.4. *Sigui $K \mid k$ una extensió algebraica qualsevol de cossos. Suposem que K és generat sobre k per una família 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 $K \mid k$ 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, θ és separable sobre k. □

Definició 4.4.5. Un cos k s'anomena perfecte si tota extensió algebraica $K \mid k$ és separable; equivalentment, si tota extensió finita $K \mid k$ és separable.

Per la seva importància, destaquem el resultat següent.

Corol·lari 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.* □

Definició 4.4.7. Si $K \mid k$ és una extensió finita de cossos, hem vist més amunt que $[K : k]_s$ divideix $[K : k]$. S'anomena grau d'inseparabilitat de l'extensió $K \mid k$ el quocient $[K : k]_i := \dfrac{[K : k]}{[K : k]_s}$.

Observació 4.4.8. El grau d'inseparabilitat d'una extensió finita de cossos $K \mid k$, o bé és 1 (i això pot succeir en característica qualsevol) o bé k és un cos de característica positiva $p := \mathrm{car}(k) > 0$ 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 θ^{p^r} és separable sobre k, o sigui, que $k(\theta^{p^r}) \mid k$ 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 $k(\theta) \mid k$, que coincideix amb aquest grau, és una potència de p. Això demostra l'enunciat per a les extensions de la forma $k(\theta) \mid k$; el cas general s'obté, de nou, per la multiplicativitat dels graus i dels graus de separabilitat.

Acabarem la secció amb un estudi del comportament de la separabilitat en situacions diverses: per a torres d'extensions, per al canvi de base, per a la composició d'extensions, i per pas a la clausura normal.

Proposició 4.4.9. *Siguin $L \mid K$ i $K \mid k$ extensions algebraiques separables de cossos. Llavors, l'extensió $L \mid k$ també és separable.*

Demostració: Sigui $\theta \in L$ un element qualevol. Cal veure que θ és separable sobre k. Considerem el polinomi $\mathrm{Irr}(\theta, K)(X) \in K[X]$, i siguin $\alpha_0, \ldots, \alpha_n$ els seus coeficients; com que $K \mid k$ és separable, els elements α_i, $0 \leq i \leq n$, són separables sobre k, de manera que l'extensió finita $k(\alpha_0, \ldots, \alpha_n) \mid k$

és separable. D'altra banda, el polinomi $\mathrm{Irr}(\theta, K)(X) \in K[X]$ no té arrels múltiples, té θ per arrel, i pertany a $k(\alpha_0, \ldots, \alpha_n)[X]$; per tant, θ és separable sobre $k(\alpha_0, \ldots, \alpha_n)$. En conseqüència, $[k(\alpha_0, \ldots, \alpha_n, \theta) : k]_s = [k(\alpha_0, \ldots, \alpha_n, \theta) : k(\alpha_0, \ldots, \alpha_n)]_s[k(\alpha_0, \ldots, \alpha_n) : k]_s = [k(\alpha_0, \ldots, \alpha_n, \theta) : k(\alpha_0, \ldots, \alpha_n)][k(\alpha_0, \ldots, \alpha_n) : k] = [k(\alpha_0, \ldots, \alpha_n, \theta) : k]$, de manera que θ és separable sobre k, com volíem veure. □

Proposició 4.4.10. *Siguin $K \mid k$ i $L \mid k$ extensions algebraiques de cossos tals que existeix un cos $\overline{k}$ que conté K i L. Si l'extensió $K \mid k$ és separable, llavors $KL \mid L$ també és separable.*

Demostració: Podem elegir una família $\{\theta_i\}_{i\in I}$ d'elements $\theta_i \in K$ tals que $K = k(\{\theta_i\}_{i\in I})$. Per hipòtesi, els elements θ_i són separables sobre k; per tant, també són separables sobre L, de manera que $L(\{\theta_i\}_{i\in I}) \mid L$ també és separable; però $L(\{\theta_i\}_{i\in I}) = KL$. □

Proposició 4.4.11. *Siguin $K_1 \mid k$ i $K_2 \mid k$ extensions algebraiques de cossos tals que existeix un cos $\overline{k}$ que conté K_1 i K_2. Si les extensions $K_1 \mid k$ i $K_2 \mid k$ són separables, la composició $K_1K_2 \mid k$ també és separable.*

Demostració: En efecte; les extensions $K_1 \mid k$ i $K_1K_2 \mid K_1$ són separables, la primera per hipòtesi i la segona en virtut de la proposició anterior. Com que la separabilitat es manté per a torres d'extensions, l'extensió $K_1K_2 \mid k$ també és separable. □

Corol·lari 4.4.12. *Sigui $K \mid k$ 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 $K_s \mid k$ és la màxima subextensió de $K \mid k$ que és separable.* □

Definició 4.4.13. La màxima subextensió separable $K_s \mid k$ de $K \mid k$ s'anomena la clausura separable de k en K.

Proposició 4.4.14. *Sigui $K \mid k$ una extensió algebraica separable de cossos, i suposem que K està inclòs en un cos algebraicament tancat $\overline{k}$. Llavors, la clausura normal $N \mid k$ de $K \mid k$ també és separable.*

Demostració: Sigui $\{\theta_i\}_{i\in I}$ una família qualsevol d'elements $\theta_i \in K$ tals que $K = k(\{\theta_i\}_{i\in I})$; llavors, per a tot $i \in I$, θ_i és un element algebraic i separable sobre k; per tant, totes les arrels dels polinomis $\mathrm{Irr}(\theta_i, k)(X) \in k[X]$, $i \in I$, són elements algebraics i separables sobre k; ara bé, la clausura

normal $N \mid k$ de l'extensió $K \mid k$ és tal que N és el cos de descomposició de la família de polinomis $\{\mathrm{Irr}(\theta_i)(X)\}_{i\in I}$; per tant, l'extensió $N \mid k$ és 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 n-èsima primitiva 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 n-èsima primitiva de la unitat i una arrel m-èsima primitiva de la unitat coincideix amb el cos generat sobre k per una arrel mn-èsima primitiva de la unitat; i també hem vist 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 $X^{nm} - a$. 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 $K \mid k$ és tal que existeix un element $\theta \in K$ per al qual és $K = k(\theta)$, llavors l'extensió $K \mid k$ és, per força, finita. Però la pregunta encara té sentit per a les extensions finites $K \mid k$. És veritat que, donada una extensió finita $K \mid k$, existeix un element $\theta \in K$ tal que $K = k(\theta)$?

Definició 4.5.1. Sigui $K \mid k$ una extensió algebraica finita. Si existeix un element $\theta \in K$ tal que $K = k(\theta)$, es diu que θ és un element primitiu per a l'extensió $K \mid k$.

El propòsit d'aquesta secció és, d'una banda, caracteritzar les extensions finites $K \mid k$ 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, provarem un resultat que és important per si mateix.

Proposició 4.5.2. *Siguin $L \mid k$ una extensió finita que admet un element primitiu, θ, i $K \subseteq L$ un subcòs de L que conté k. Llavors, el cos K és generat sobre k pel conjunt dels coeficients del polinomi* $\mathrm{Irr}(\theta, K)(X) \in K[X]$. *És a*

dir, si $\mathrm{Irr}(\theta, K)(X) = \alpha_0 + \alpha_1 X + \cdots + \alpha_{n-1}X^{n-1} + X^n \in K[X]$*, llavors* $K = k(\alpha_0, \ldots, \alpha_{n-1})$.

Demostració: En primer lloc, observem que θ és un element primitiu de l'extensió $L \mid K$ i que, en conseqüència, el grau $[L : K]$ és el grau del polinomi $\mathrm{Irr}(\theta, K)(X) \in K[X]$. Sigui $K_0 := k(\alpha_0, \ldots, \alpha_{n-1}) \subseteq K$ el subcòs de K generat sobre k pels coeficients de $\mathrm{Irr}(\theta, K)(X)$; en particular, $\mathrm{Irr}(\theta, K)(X) \in K_0[X]$, de manera que és irreductible en $K_0[X]$ (un factor d'un polinomi en $K_0[X]$ seria un factor en $K[X]$). 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 volíem demostrar. □

Proposició 4.5.3. (Criteri de separabilitat) *Sigui $L \mid k$ una extensió finita. L'extensió $L \mid k$ admet un element primitiu si, i només si, el conjunt format per totes les subextensions $K \mid k$ de $L \mid k$ és finit.*

Demostració: En primer lloc, suposem que L és un cos finit; és clar que el conjunt de les subextensions de $L \mid k$ 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 $L \mid k$. Per tant, no hi ha res a provar. Així, podem suposar que el cos L, i, en conseqüència, el cos k, és infinit.

Suposem que $\theta \in L$ és un element primitiu de l'extensió $L \mid k$ i sigui $f(X) := \mathrm{Irr}(\theta, k)(X) \in k[X]$ el seu polinomi minimal sobre k. Per a cada subextensió $K \mid k$ de $L \mid k$ el polinomi $\mathrm{Irr}(\theta, K)(X) \in K[X]$ 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. Per tant, a cada subextensió $K \mid k$ de $L \mid k$ 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 $K \mid k$ de $L \mid k$ en el conjunt dels divisors mònics de $f(X)$ en $L[X]$. Ara bé, el conjunt dels divisors mònics d'un polinomi qualsevol és finit, de manera que el conjunt de subextensions $K \mid k$ de $L \mid k$ és finit.

Recíprocament, suposem que el conjunt de les subextensions $K \mid k$ de $L \mid k$ és finit, i siguin $\theta_1, \theta_2 \in K$ elements qualssevol. Com que el conjunt de les subextensions de $K \mid k$ de la forma $k(\theta_1 + c\theta_2) \mid k$, quan c recorre k, és finit, i com que k és infinit, existeixen dos 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 $c_2-c_1\neq 0$, conté l'element θ_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 θ_1, $\theta_2\in L$, llavors, existeix un element $c_1\in k$ tal que $K=k(\theta_1+c_1\theta_2)$.

Podem aplicar aquest fet inducctivament a tota subextensió $K\mid k$ de $L\mid k$, perquè, com que $K\mid k$ és una extensió finita, és finitament generada sobre k per elements de L. En particular, també s'aplica a l'extensió $L\mid k$, i obtenim que, si $L=k(\theta_1,\ldots,\theta_n)$, llavors existeixen elements $c_2,\ldots,c_n\in k$ tals que, per a $\theta:=\theta_1+c_2\theta_2+\cdots+c_n\theta_n\in L$, és $L=k(\theta)$. □

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 de separabilitat 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.

Sigui, doncs, $K\mid k$ una extensió finita i separable de cossos infinits, i siguin $\theta_1,\ldots,\theta_m\in K$ elements tals que $K=k(\theta_1,\ldots,\theta_m)$. Per inducció sobre m, i anàlogament a la demostració del criteri, és suficient provar que per a tota parella d'elements θ_1, $\theta_2\in K$, l'extensió $k(\theta_1,\theta_2)\mid k$ admet un element primitiu. Com que θ_1, $\theta_2\in K$ i l'extensió $K\mid k$ és separable, per hipòtesi, el grau de separabilitat de l'extensió $k(\theta_1,\theta_2)\mid k$ coincideix amb el seu grau, posem n. Siguin, doncs, $\sigma_1,\ldots,\sigma_n$ les n k-immersions diferents de $k(\theta_1,\theta_2)$ en un cos algebraicament tancat $\overline{k}$ 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 del polinomi, $\sigma_i(\theta_1)+\sigma_i(\theta_2)X-\sigma_j(\theta_1)-\sigma_j(\theta_2)X$, 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 σ_i i σ_j coincidirien sobre θ_1, i sobre θ_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 $\mathrm{Irr}(\theta_1 + c\theta_2, k)(X) \in k[X]$ és, com a mínim, n; 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 volíem demostrar. □

Observació 4.5.5. Notem que si $\mathrm{car}(k) = 0$, 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 $K \mid k$ 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 θ, $m_\theta : K \longrightarrow K$; és a dir, l'aplicació donada per $m_\theta(x) := \theta x$, per a tot $x \in K$. Llavors, l'aplicació $m : K \longrightarrow \mathrm{End}_k(K)$ donada per $m(\theta) := m_\theta$ és un morfisme d'anells; 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_θ és un automorfisme k-lineal de K, m també es pot veure com un morfisme de grups $m : K^* \longrightarrow \mathbf{GL}(K)$, 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_θ, $\det(m_\theta - X\mathrm{id}) \in k[X]$; és un polinomi de $k[X]$ que té θ per arrel i que, si posem $n := [K : k]$ i escrivim

$$\det(m_\theta - X\mathrm{id}) = a_0(\theta) - a_1(\theta)X + \cdots + (-1)^{n-1}a_{n-1}(\theta)X^{n-1} + (-1)^n X^n,$$

dóna lloc a n aplicacions $a_i : K \longrightarrow k$, $0 \leq i \leq n-1$. Per causa de les seves propietats, les aplicacions a_0 i a_{n-1} són especialment interessants. D'una banda, l'aplicació a_0 és 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 $K \xrightarrow{m} \mathrm{End}_k(K) \xrightarrow{\mathrm{tr}} k$, i és k-lineal. Aquestes dues aplicacions es coneixen amb els noms de norma i traça de l'extensió $K \mid k$, d'acord amb la definició següent.

Definició 4.6.2. Sigui $K \mid k$ una extensió finita de cossos. S'anomena norma de K sobre k l'aplicació $N_{K|k} : K \longrightarrow k$ donada, sobre $\theta \in K$, pel determinant de la multiplicació per θ. S'anomena traça de K sobre k l'aplicació k-ineal $\mathrm{Tr}_{K|k} : K \longrightarrow k$ donada, sobre $\theta \in K$, per la traça de la multiplicació per θ.

En particular, doncs, i si posem $n := [K : k]$, se satisfan les propietats:

(a) $\mathrm{N}_{K|k}(\theta_1\theta_2) = \mathrm{N}_{K|k}(\theta_1)\mathrm{N}_{K|k}(\theta_2)$, per a θ_1, $\theta_2 \in K$;

(b) $\mathrm{Tr}_{K|k}(c_1\theta_1 + c_2\theta_2) = c_1\mathrm{Tr}_{K|k}(\theta_1) + c_2\mathrm{Tr}_{K|k}(\theta_2)$, per a θ_1, $\theta_2 \in K$; c_1, $c_2 \in k$;

(c) $\mathrm{N}_{K|k}(\theta) = \theta^n$, per a $\theta \in k$; i

(d) $\mathrm{Tr}_{K|k}(\theta) = n\theta$, per a $\theta \in k$.

Proposició 4.6.3. (Càlcul de normes i traces) *Siguin $K \mid k$ una extensió finita de cossos i $\theta \in K$ un element qualsevol. Llavors,*

$$\mathrm{N}_{K|k}(\theta) = \mathrm{N}_{k(\theta)|k}(\theta)^{[K:k(\theta)]}, \qquad \mathrm{Tr}_{K|k}(\theta) = [K : k(\theta)]\,\mathrm{Tr}_{k(\theta)|k}(\theta).$$

A més a més, si posem

$$\mathrm{Irr}(\theta, k)(X) = X^n - a_{n-1}X^{n-1} + \cdots + (-1)^{n-1}a_1X + (-1)^n a_0,\ a_0, \ldots, a_{n-1} \in k,$$

tenim que

$$\mathrm{N}_{k(\theta)|k}(\theta) = a_0, \qquad \mathrm{Tr}_{k(\theta)|k}(\theta) = a_{n-1}.$$

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 θ 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 θ, de manera que, afectat del signe $(-1)^n$, coincideix amb el polinomi $\mathrm{Irr}(\theta, k)(X)$. Per tant,

$$\mathrm{N}_{k(\theta)|k}(\theta) = a_0, \qquad \mathrm{Tr}_{k(\theta)|k}(\theta) = a_{n-1}.$$

Els valors de la norma i de la traça de θ relatives a l'extensió $K \mid k$ s'obtenen fàcilment a partir dels valors de la norma i de la traça de θ relatives a l'extensió $k(\theta) \mid k$. 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 θ en K relativa a aquesta base és de la forma $\begin{bmatrix} M & 0 & \ldots & 0 \\ 0 & M & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & M \end{bmatrix}$. Per tant, el polinomi característic de la multiplicació per θ en K és la potència $[K : k(\theta)]$-èsima del polinomi característic de M. En particular, per a la norma i la traça de θ, obtenim les fórmules enunciades. □

Proposició 4.6.4. *Siguin $K \mid k$ una extensió finita de cossos, $\theta \in K$ un element qualsevol, i τ_u, $1 \leq u \leq [K:k]_s$, les k-immersions diferents de K en un cos algebraicament tancat $\overline{k}$ que conté k. Llavors,*

$$\mathrm{N}_{K|k}(\theta) = \left(\prod_{u=1}^{[K:k]_s} \tau_u(\theta) \right)^{[K:k]_i}, \qquad \mathrm{Tr}_{K|k}(\theta) = [K:k]_i \sum_{u=1}^{[K:k]_s} \tau_u(\theta).$$

Demostració: Posem $d := [k(\theta) : k]$ i siguin $\theta_1 := \theta, \theta_2, \ldots, \theta_d$ les d arrels del polinomi $\mathrm{Irr}(\theta, k)(X)$ (aquí, cadascuna de les arrels diferents està repetida tantes vegades com indica la seva multiplicitat). Tenim que

$$\mathrm{Tr}_{k(\theta)|k}(\theta) = \theta_1 + \cdots + \theta_d, \qquad \mathrm{N}_{k(\theta)|k}(\theta) = \theta_1 \cdots \theta_d,$$

perquè

$$\mathrm{Irr}(\theta, k)(X) = (-1)^d \det(m_\theta - X\mathrm{Id}) = (X - \theta_1) \cdots (X - \theta_d).$$

Com que totes les arrels del polinomi $\mathrm{Irr}(\theta, k)(X)$ són de la mateixa multiplicitat, si $d_s := [k(\theta) : k]_s$ designa el grau de separabilitat de l'extensió $k(\theta) \mid k$ i $\sigma_1, \ldots, \sigma_{d_s}$ són les d_s k-immersions diferents de $k(\theta)$ en qualsevol cos algebraicament tancat $\overline{k}$ que conté k, obtenim que

$$\mathrm{N}_{k(\theta)|k}(\theta) = \left(\prod_{t=1}^{d_s} \sigma_t(\theta) \right)^{p^i}, \qquad \mathrm{Tr}_{k(\theta)|k}(\theta) = p^i \sum_{t=1}^{d_s} \sigma_t(\theta),$$

on p^i designa el grau d'inseparabilitat de l'extensió $k(\theta) \mid k$.

Notem que cada k-immersió de $k(\theta)$ en $\overline{k}$ s'estén a una k-immersió de K en $\overline{k}$ exactament de $[K : k(\theta)]_s$-maneres diferents. Per tant,

$$\prod_{u=1}^{[K:k]_s} \tau_u(\theta) = \left(\prod_{t=1}^{d_s} \sigma_t(\theta) \right)^{[K:k(\theta)]_s}, \qquad \sum_{u=1}^{[K:k]_s} \tau_u(\theta) = [K : k(\theta)]_s \sum_{t=1}^{d_s} \sigma_t(\theta).$$

Com a conseqüència,

$$\begin{aligned} \left(\prod_{u=1}^{[K:k]_s} \tau_u(\theta) \right)^{[K:k]_i} &= \left(\prod_{t=1}^{d_s} \sigma_t(\theta) \right)^{[K:k(\theta)]_s [K:k]_i} = \left(\prod_{t=1}^{d_s} \sigma_t(\theta) \right)^{[k(\theta):k]_i [K:k(\theta)]} \\ &= (\mathrm{N}_{k(\theta)|k}(\theta))^{[K:k(\theta)]} = \mathrm{N}_{K|k}(\theta); \end{aligned}$$

i, anàlogament,

$$[K:k]_i \sum_{u=1}^{[K:k]_s} \tau_u(\theta) = [K:k]_i[K:k(\theta)]_s \sum_{t=1}^{d_s} \sigma_t(\theta)$$

$$= [K:k(\theta)][k(\theta):k]_i \sum_{t=1}^{d_s} \sigma_t(\theta) = [K:k(\theta)]\mathrm{Tr}_{k(\theta)|k}(\theta) = \mathrm{Tr}_{K|k}(\theta). \square$$

Corol·lari 4.6.5. *Si $K \mid k$ és una extensió finita i no separable de cossos, llavors* $\mathrm{Tr}_{K|k} = 0$. $\square$

Teorema 4.6.6. (Transitivitat de la traça i de la norma) *Siguin $L \mid K$ i $K \mid k$ extensions finites. Llavors,*

$$\mathrm{N}_{L|k} = \mathrm{N}_{K|k} \circ \mathrm{N}_{L|K}, \qquad \mathrm{Tr}_{L|k} = \mathrm{Tr}_{K|k} \circ \mathrm{Tr}_{L|K}.$$

Demostració: Siguin $n := [K:k]$, $m := [L:K]$, els graus, $n_s := [K:k]_s$, $m_s := [L:K]_s$, els graus de separabilitat, i $p^i := [K:k]_i$, $p^j := [L:K]_i$, els graus d'inseparabilitat de les dues extensions $K \mid k$ i $L \mid K$, respectivament; 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 $[L:k]_i = p^{i+j}$. Sigui $N \mid k$ una clausura normal de l'extensió $L \mid k$ i siguin $\sigma_1, \ldots, \sigma_{n_s} \in \mathrm{Gal}(N \mid k)$ extensions a N de les n_s k-immersions diferents de K en $\overline{k}$, i $\tau_1, \ldots, \tau_{m_s} \in \mathrm{Gal}(N \mid K) \subseteq \mathrm{Gal}(N \mid k)$ extensions a N de les m_s K-immersions diferents de L en $\overline{k}$. Llavors, les composicions $\sigma_t \circ \tau_u \in \mathrm{Gal}(N \mid k)$ 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 $\overline{k}$. Amb aquestes notacions, el càlcul de la traça i la norma de cadascuna d'aquestes extensions és senzill. Si $\theta \in L$ és un element qualsevol, llavors

$$\mathrm{N}_{L|k}(\theta) = \Big(\prod_{t,u}(\sigma_t \circ \tau_u)(\theta)\Big)^{p^{i+j}} = \Big(\prod_{t,u}\sigma_t(\tau_u(\theta))^{p^j}\Big)^{p^i}$$

$$= \Big(\prod_t \sigma_t\Big(\prod_u \tau_u(\theta)\Big)^{p^j}\Big)^{p^i} = \prod_t \sigma_t(\mathrm{N}_{L|K}(\theta))^{p^i} = \mathrm{N}_{K|k}(\mathrm{N}_{L|K}(\theta)),$$

i, anàlogament,

$$\mathrm{Tr}_{L|k}(\theta) = p^{i+j}\sum_{t,u}(\sigma_t \circ \tau_u)(\theta) = p^i \sum_{t,u}\sigma_t(p^j\tau_u(\theta)) = p^i \sum_t \sigma_t\Big(p^j \sum_u \tau_u(\theta)\Big)$$

$$= p^i \sum_t \sigma_t(\mathrm{Tr}_{L|K}(\theta)) = \mathrm{Tr}_{K|k}(\mathrm{Tr}_{L|K}(\theta)). \square$$

4.7 Separabilitat i traça

4.7.1. Sigui $K \mid k$ una extensió finita de cossos i considerem la forma k-lineal traça, $\mathrm{Tr}_{K|k} : K \longrightarrow k$. 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 $\mathrm{Tr}_{K|k} : K \times K \longrightarrow k$, definida per l'assignació $\mathrm{Tr}_{K|k}(x, y) := \mathrm{Tr}_{K|k}(xy)$.

Si l'extensió $K \mid k$ no és separable, la forma k-bilineal traça és nul·la (cf. el corol·lari 4.6.5); en canvi, si $K \mid k$ 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 $\chi_1, \ldots, \chi_n : G \longrightarrow K^*$ morfismes de grups, diferents dos a dos. Llavors, $\chi_1, \ldots, \chi_n$ són aplicacions K-linealment independents de G en K.*

Demostració: Suposem que $\chi_1, \ldots, \chi_n$ siguin K-linealment dependents, i triem una combinació lineal $\alpha_1\chi_1 + \cdots + \alpha_m\chi_m = 0$ 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 $\beta_1\chi_1 + \cdots + \beta_d\chi_d = 0$, on $\beta_i \in K$ i $d < m$, és $\beta_i = 0$ per a tot índex i. Com que un sol morfisme de grups $\chi : G \longrightarrow K^*$ 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 $\alpha_1\chi_1 + \cdots + \alpha_m\chi_m = 0$ ens diu que, per a tot $h \in G$, és

$$\alpha_1\chi_1(h) + \cdots + \alpha_m\chi_m(h) = 0;$$

en particular, com que $gh \in G$, és

$$\alpha_1\chi_1(gh) + \cdots + \alpha_m\chi_m(gh) = 0,$$

per a tot $h \in G$; equivalentment, i com que els χ_j són morfismes de grups,

$$\alpha_1\chi_1(g)\chi_1(h) + \cdots + \alpha_m\chi_m(g)\chi_m(h) = 0.$$

D'altra banda, si multipliquem la relació $\alpha_1\chi_1(h) + \cdots + \alpha_m\chi_m(h) = 0$ per $\chi_m(g)$ i restem, obtenim que, per a tot $h \in G$, és

$$\alpha_1(\chi_1(g) - \chi_m(g))\chi_1(h) + \cdots + \alpha_{m-1}(\chi_{m-1}(g) - \chi_m(g))\chi_{m-1}(h) = 0.$$

Però $\chi_{m-1}(g) - \chi_m(g) \neq 0$, de manera que obtenim una combinació lineal de la forma $\beta_i\chi_1 + \cdots + \beta_{m-1}\chi_{m-1} = 0$ amb $\beta_{m-1} \neq 0$, fet que contradiu l'elecció de m. Això acaba la demostració. □

Proposició 4.7.3. *Sigui $K \mid k$ una extensió finita i separable de cossos. Llavors, la forma k-bilineal simètrica traça, $\mathrm{Tr}_{K|k} : K \times K \longrightarrow k$, donada per $\mathrm{Tr}_{K|k}(x, y) := \mathrm{Tr}_{K|k}(xy)$, és no degenerada.*

Demostració: És suficient provar que l'aplicació k-lineal $\mathrm{Tr}_{K|k}$ és no nul·la, ja que si $x_0 \in K$ és un element tal que $\mathrm{Tr}_{K|k}(x_0) \neq 0$, llavors, per a tot $x \neq 0$, existeix $y := x_0x^{-1} \in K$ tal que $\mathrm{Tr}_{K|k}(xy) = \mathrm{Tr}_{K|k}(x(x_0x^{-1})) \neq 0$.

Com que $K \mid k$ 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 $\theta_1 := \theta, \theta_2, \ldots, \theta_n \neq 0$ les arrels del polinomi $\mathrm{Irr}(\theta, k)(X) \in k[X]$, on $n := [K : k]$ és el grau de l'extensió. Com que θ és separable, tots els θ_i, $1 \leq i \leq n$ són diferents, i, per a tot $r \in \mathbb{Z}$, és $\mathrm{Tr}_{K|k}(\theta^r) = \sum_{i=1}^{n} \theta_i^r$.

Si fos $\mathrm{Tr}_{K|k} = 0$, tindríem que, per a tot $r \in \mathbb{Z}$, seria $\mathrm{Tr}_{K|k}(\theta^r) = 0$, de manera que $\sum_{i=1}^{n} \theta_i^r = 0$, per a tot $r \in \mathbb{Z}$. Així, si posem $L := k(\theta_1, \ldots, \theta_n)$, els morfismes de grups $f_i : \mathbb{Z} \longrightarrow L^*$, 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 obtenim una contradicció amb el teorema anterior. □

4.8 El teorema 90 de Hilbert

L'estudi que hem fet de les traces i les normes de les extensions finites de cossos ens permet establir les formes multiplicativa i additiva del teorema 90 de Hilbert, que és un resultat bàsic per a la classificació de les extensions cícliques de cossos en el cas que el cos base contingui les arrels de la unitat necessàries.

Definició 4.8.1. Una extensió algebraica de cossos $K \mid k$ 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 $\mathrm{Gal}(K \mid k)$ coincideix amb el grau de l'extensió, $[K : k]$.

Definició 4.8.2. Una extensió de Galois $K \mid k$ s'anomena cíclica si el grup de Galois $\mathrm{Gal}(K \mid k)$ és cíclic; s'anomena abeliana si $\mathrm{Gal}(K \mid k)$ és commutatiu.

Teorema 4.8.3. (Teorema 90 de Hilbert) *Siguin $K \mid k$ una extensió finita i cíclica de cossos, $G := \mathrm{Gal}(K \mid k)$ el seu grup de Galois, $n := [K : k] \geq 2$ el seu grau, i $\sigma \in G$ un generador del grup de Galois.*

(a) Forma multiplicativa. *Un element $\theta \in K$ és tal que $\mathrm{N}_{K|k}(\theta) = 1$ si, i només si, existeix un element $\alpha \in K$, $\alpha \neq 0$, tal que $\theta = \dfrac{\alpha}{\sigma(\alpha)}$.*

(b) Forma additiva. *Un element $\theta \in K$ és tal que $\mathrm{Tr}_{K|k}(\theta) = 0$ si, i només si, existeix un element $\alpha \in K$ tal que $\theta = \alpha - \sigma(\alpha)$.*

Demostració: Com que $G = \{\sigma, \sigma^2, \ldots, \sigma^n = \mathrm{Id}\}$, donat un element qualsevol $\alpha \in K$ és $\mathrm{N}_{K|k}(\alpha) = \displaystyle\prod_{i=1}^{n} \sigma^i(\alpha)$ i $\mathrm{Tr}_{K|k}(\alpha) = \displaystyle\sum_{i=1}^{n} \sigma^i(\alpha)$; en particular, per a tot nombre enter r, se satisfan les igualtats $\mathrm{Tr}_{K|k}(\alpha) = \mathrm{Tr}_{K|k}(\sigma^r(\alpha))$ i $\mathrm{N}_{K|k}(\alpha) = \mathrm{N}_{K|k}(\sigma^r(\alpha))$. Així, si existeix $\alpha \in K$, $\alpha \neq 0$, tal que $\theta = \dfrac{\alpha}{\sigma(\alpha)}$, és $\mathrm{N}_{K|k}(\theta) = \mathrm{N}_{K|k}\left(\dfrac{\alpha}{\sigma(\alpha)}\right) = \dfrac{N_{K|k}(\alpha)}{\mathrm{N}_{K|k}(\sigma(\alpha))} = 1$; i, si existeix $\alpha \in K$ tal que $\theta = \alpha - \sigma(\alpha)$, és $\mathrm{Tr}_{K|k}(\theta) = \mathrm{Tr}_{K|k}(\alpha - \sigma(\alpha)) = \mathrm{Tr}_{K|k}(\alpha) - \mathrm{Tr}_{K|k}(\sigma(\alpha)) = 0$.

Recíprocament, suposem, en primer lloc, que existeix $\theta \in K$ tal que $\mathrm{N}_{K|k}(\theta) = 1$; 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, l'aplicació

$$\varphi := \mathrm{Id} + \theta\sigma + \theta\sigma(\theta)\sigma^2 + \cdots + \theta\sigma(\theta)\cdots\sigma^{n-2}(\theta)\sigma^{n-1}$$

és no nul·la; per tant, existeix un element $\beta \in K$ tal que $\alpha := \varphi(\beta) \neq 0$. Per a aquest element α 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, si tenim en compte que

$$\theta\sigma(\theta)\sigma^2(\theta)\cdots\sigma^{n-1}(\theta) = \mathrm{N}_{K|k}(\theta) = 1$$

i que $\sigma^n = \mathrm{Id}$, és

$$\theta\sigma(\alpha) = \beta + \theta\sigma(\beta) + \theta\sigma(\theta)\sigma^2(\beta) + \cdots + \theta\sigma(\theta)\cdots\sigma^{n-2}(\theta)\sigma^{n-1}(\beta) = \alpha,$$

de manera que $\theta = \dfrac{\alpha}{\sigma(\alpha)}$, com volíem veure.

Demostrarem anàlogament la forma additiva del teorema. sigui $\theta \in K$ un element tal que $\mathrm{Tr}_{K|k}(\theta) = 0$. Com que l'extensió $K \mid k$ és separable, és $\mathrm{Tr}_{K|k} \neq 0$, de manera que existeix $\beta \in K$ tal que $\mathrm{Tr}_{K|k}(\beta) \neq 0$; és a dir,

$$\sigma(\beta) + \sigma^2(\beta) + \cdots + \sigma^n(\beta) \neq 0.$$

Posem

$$\alpha := \frac{1}{\mathrm{Tr}_{K|k}(\beta)}(\theta\sigma(\beta)+(\theta+\sigma(\theta))\sigma^2(\beta)+\cdots+(\theta+\sigma(\theta)+\cdots+\sigma^{n-2}(\theta))\sigma^{n-1}(\beta)).$$

Llavors, se satisfà que $\sigma(\alpha) = \dfrac{1}{\mathrm{Tr}_{K|k}(\beta)}(\sigma(\theta)\sigma^2(\beta) + (\sigma(\theta) + \sigma^2(\theta))\sigma^3(\beta) +$
$\cdots+(\sigma(\theta)+\sigma^2(\theta)+\cdots+\sigma^{n-1}(\theta))\sigma^n(\beta)) = \dfrac{1}{\mathrm{Tr}_{K|k}(\beta)}(\theta\sigma(\beta)+(\theta+\sigma(\theta))\sigma^2(\beta)+$
$\cdots+(\theta+\sigma(\theta)+\cdots+\sigma^{n-1}(\theta))\sigma^n(\beta))-\dfrac{1}{\mathrm{Tr}_{K|k}(\beta)}(\theta\sigma(\beta)+\theta\sigma^2(\beta)+\cdots+\theta\sigma^n(\beta))$;
i, ara, com que $\theta + \sigma(\theta) + \cdots + \sigma^{n-1}(\theta) = \mathrm{Tr}_{K|k}(\theta) = 0$ tenim que $\sigma(\alpha) =$
$\dfrac{1}{\mathrm{Tr}_{K|k}(\beta)}(\theta\sigma(\beta)+(\theta+\sigma(\theta))\sigma^2(\beta)+\cdots+(\theta+\sigma(\theta)+\cdots+\sigma^{n-2}(\theta))\sigma^{n-1}(\beta))-$
$\dfrac{1}{\mathrm{Tr}_{K|k}(\beta)}\theta(\sigma(\beta) + \sigma^2(\beta) + \cdots + \sigma^n(\beta)) = \alpha - \theta$, d'on $\theta = \alpha - \sigma(\alpha)$, com volíem veure. □

Observació 4.8.4. El teorema 90 de Hilbert és la formulació multiplicativa del teorema 4.8.3; s'anomena d'aquesta manera perquè ocupa el lloc 90 entre els resultats retolats com a "teorema" en el llibre [**?**], 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 4.8.3.

4.9 Extensions cícliques

4.9.1. Siguin un cos algebraicament tancat, $k \subseteq \overline{k}$ un subcòs, $a \in k$ un element, i $\alpha \in \overline{k}$ 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 n-èsima primitiva de la unitat, ζ. Recordem que, en aquestes condicions, hem vist que l'extensió $k(\alpha) \mid k$ és cíclica de grau n i que el grup de Galois $\mathrm{Gal}(k(\alpha) \mid k)$ és generat per l'únic k-automorfisme σ de $k(\alpha)$ tal que $\sigma(\alpha) = \zeta\alpha$. Podem utilitzar el teorema 90 de Hilbert per a perfilar més aquest resultat. En efecte, ara podem establir el següent.

Teorema 4.9.2. *Siguin $\overline{k}$ un cos algebraicament tancat, $n \geq 1$ un nombre natural no divisible per la característica de $\overline{k}$, $\zeta \in \overline{k}$ una arrel n-èsima primitiva de la unitat, i $k \subseteq \overline{k}$ un subcòs tal que $\zeta \in k$.*

a) *Siguin $a \in k^*$, $\alpha \in \overline{k}$, elements tals que $\alpha^n = a$. L'extensió $k(\alpha) \mid k$ és cíclica, de grau d divisor de n, $\alpha^d \in k$, i $X^d - \alpha^d \in k[X]$ és irreductible.*

b) *Si $K \mid k$ és una extensió de Galois cíclica de grau n, existeix un element primitiu $\alpha \in K$ tal que $\mathrm{Irr}(\alpha, k)(X)$ és de la forma $X^n - a \in k[X]$.*

Demostració: Demostrem, en primer lloc, 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 $\mathrm{car}(k)$; per tant, l'extensió $k(\alpha) \mid k$ és de Galois. A més a més, l'aplicació $\tau : \mathrm{Gal}(k(\alpha) \mid k) \longrightarrow \mathbb{Z}/n\mathbb{Z}$ 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 $\mathrm{Gal}(k(\alpha) \mid k)$ amb un subgrup $G \subseteq \mathbb{Z}/n\mathbb{Z}$ (cf. el corol·lari 4.2.8). Com que $\mathbb{Z}/n\mathbb{Z}$ és un grup cíclic d'ordre n, el grup de Galois $\mathrm{Gal}(k(\alpha) \mid k)$ és cíclic d'ordre d divisor de n.

El polinomi minimal de α sobre k és $\mathrm{Irr}(\alpha, k)(X) = \prod_{m \in G} (X - \zeta^m \alpha)$, el terme independent del qual és $(-1)^d \mathrm{N}_{k(\alpha)|k}(\alpha) = (-1)^d \alpha^d \prod_{m \in G} \zeta^m \in k$. Com que G és l'únic subgrup de $\mathbb{Z}/n\mathbb{Z}$ d'ordre d, és generat per $\dfrac{n}{d}$ 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 també és senar i $\dfrac{d-1}{2} \in \mathbb{Z}$, de manera que S és múltiple de n i $\zeta^S = 1 = (-1)^{d-1}$; 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 $\mathrm{Irr}(\alpha,k)(X)$ és $(-1)^d\alpha^d\zeta^S=(-1)^{d+(d-1)}\alpha^d=-\alpha^d$. 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 α per arrel, és $X^d-\alpha^d=\mathrm{Irr}(\alpha,k)(X)$ i, per tant, irreductible.

Demostrem, ara, b). Sigui $\sigma\in\mathrm{Gal}(K\mid k)$ un generador del grup de Galois. Com que $\zeta^{-1}\in k$ i $[K:k]=n$, és $\mathrm{N}_{K|k}(\zeta^{-1})=\zeta^{-n}=1$ i, en virtut de la formulació multiplicativa del teorema 90 de Hilbert, 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 de K, $\zeta^i\alpha$, $0\leq i\leq n-1$, són arrels de $\mathrm{Irr}(\alpha,k)(X)\in k[X]$ 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), el polinomi irreductible de α sobre k és $\mathrm{Irr}(\alpha,k)(X)=\prod_{i=0}^{n-1}(X-\zeta^i\alpha)=X^n-\alpha^n$, de manera que $\alpha^n\in k$, com volíem veure. □

A continuació, estudiarem 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 $\overline{k}$ 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 $\alpha\in\overline{k}$ és una arrel de $f(X)$, l'extensió $k(\alpha)\mid k$ és cíclica de grau p.*

b) *Si $K\mid k$ és una extensió cíclica de grau p, existeix un element primitiu α de l'extensió $K\mid k$ tal que $\alpha^p-\alpha\in k^*$.*

Demostració: *a)* Sigui $\alpha\in\overline{k}$ 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 en el cos generat per α sobre k. Això ens diu dues coses; d'una banda, que l'extensió $k(\alpha)\mid k$ 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 mònics 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).

b). Sigui $\sigma \in \mathrm{Gal}(K \mid k)$ un generador del grup de Galois. Com que $-1 \in k$ i $[K : k] = p = \mathrm{car}(k)$, és $\mathrm{Tr}_{K|k}(-1) = 0$, i la forma additiva del teorema 90 de Hilbert 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 α 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 $\mathrm{Irr}(\alpha, k)(X) \in k[X]$ té per arrels els elements $\sigma^i(\alpha) = \alpha + i$, per a $i \in \mathbb{F}_p$; és a dir, $\mathrm{Irr}(\alpha, k)(X) = \prod_{i\in\mathbb{F}_p}(X-(\alpha+i))$. 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,

$$\mathrm{Irr}(\alpha, k)(X) = X^p - X - (\alpha^p - \alpha) \in k[X],$$

de manera que $\alpha^p - \alpha \in k$; i, a més a més, $\alpha^p - \alpha \neq 0$ perquè el polinomi és irreductible. □

4.10 Teoria 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. *Siguin $\overline{k}$ un cos algebraicament tancat, $n \geq 1$ un nombre natural no divisible per la característica de $\overline{k}$, $\zeta \in \overline{k}$ una arrel n-èsima primitiva de la unitat, i $k \subseteq \overline{k}$ un subcòs tal que $\zeta \in k$.*

a) *Sigui $\alpha \in \overline{k}$ un element tal que $\alpha^n \in k$. Llavors, per a tot element β de la forma $\beta = x\alpha^s$, amb $x \in k^*$, $0 \leq s \leq n-1$, i $\mathrm{mcd}(s,n) = 1$, és $k(\beta) = k(\alpha)$.*

b) *Sigui $K \mid k$ una extensió cíclica de grau n i $\alpha, \beta \in K^*$ elements primitius de l'extensió $K \mid k$ tals que $\alpha^n, \beta^n \in k$. Llavors, existeixen un element $x \in k^*$ i un nombre enter s tals que $0 \leq s \leq n-1$, $\mathrm{mcd}(s,n) = 1$, i $\beta = x\alpha^s$.*

Demostració: 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 $\mathrm{mcd}(s,n) = 1$, 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, $k(\alpha) \subseteq k(\alpha^s)$.

b) Com que $1, \alpha, \ldots, \alpha^{n-1}$ és una k-base de $k(\alpha)$, podem escriure $\beta \in k(\alpha)$ en la forma $\beta = \sum_{i=0}^{n-1} x'_i\alpha^i$, on $x'_i \in k$, $0 \leq i \leq n-1$, i algun dels coeficients x'_i és diferent de zero, perquè α, $\beta \neq 0$. 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 $\mathrm{mcd}(s,n) = 1$; però si demostrem que $\beta\alpha^{-s} \in k$, també serà $\mathrm{mcd}(s,n) = 1$. En efecte, si posem $\delta := \mathrm{mcd}(s,n)$ i tenim en compte que $(\alpha^{-s})^{\frac{n}{\delta}} = (\alpha^n)^{-\frac{s}{\delta}} \in k$, obtenim que $[k(\alpha^{-s}) : k] \leq \dfrac{n}{\delta}$. Ara, si $\beta\alpha^{-s} \in k^*$, és $k(\alpha) = k(\beta) = k(\alpha^s)$, de manera que $n = [k(\alpha^s) : k] \leq \dfrac{n}{\delta}$, fet que només pot succeir si $\delta = 1$.

Vegem, doncs, que $\beta\alpha^{-s} \in k$. Sigui $f(X) := \mathrm{Irr}(\beta\alpha^{-s}, k)(X) \in k[X]$; en virtut del teorema 4.9.2, i com que $(\beta\alpha^{-s})^n \in k$, l'extensió $k(\beta\alpha^{-s}) \mid k$ 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 $\sigma \in \mathrm{Gal}(k(\alpha) \mid k)$ 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 $\sigma^j(\beta\alpha^{-s})$, $0 \leq j \leq n-1$; és a dir, existeix un cert subconjunt no buit $C \subseteq \{0, 1, \ldots, n-1\}$, 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

$$\begin{aligned}\sum_{j\in C}\sigma^j(\beta\alpha^{-s}) = \sum_{j\in C}\sigma^j\Big(\sum_{i=0}^{n-1}x_i\alpha^i\Big) &= \sum_{i=0}^{n-1}\sum_{j\in C}x_i\sigma^j(\alpha^i) &= \sum_{i=0}^{n-1}\sum_{j\in C}x_i\alpha^i\zeta^{ij}\\ = \sum_{i=0}^{n-1}\Big(\sum_{j\in C}x_i\zeta^{ij}\Big)\alpha^i &= \sum_{j\in C}x_0 &= x_0 d \neq 0,\end{aligned}$$

ja que, d'una banda, és un element que pertany a k i està expressat en la k-base $\{1, \alpha, \ldots, \alpha^{n-1}\}$ 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 $\mathrm{car}(k)$ no divideix n i, per tant, no divideix d. □

La classificació de les extensions cícliques de k de grau n 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 $\overline{k}$ un cos algebraicament tancat, $n \geq 1$ un nombre natural no divisible per la característica de $\overline{k}$, $\zeta \in \overline{k}$ una arrel n-èsima primitiva de la unitat, i $k \subseteq \overline{k}$ un subcòs tal que $\zeta \in k$. Siguin $\mathcal{C}_n(k)$ el conjunt format per tots els subgrups cíclics d'ordre n del grup quocient k^*/k^{*n} i $\mathfrak{C}_n(k)$ el conjunt de totes les extensions cícliques de k de grau n. Llavors, existeix una aplicació bijectiva $f : \mathfrak{C}_n(k) \longrightarrow \mathcal{C}_n(k)$.*

Demostració: Donada una extensió cíclica de grau n de k, $K \mid k$, 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 $K \mid k$ 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 $K \mid k$ tal que $b := \beta^n \in k^*$, la proposició 4.10.1 ens proporciona l'existència d'un nombre

enter s, $0 \leq s \leq n-1$ i tal que $\mathrm{mcd}(s,n) = 1$, i d'un element $x \in k^*$, tals que $\beta = \alpha^s x$; llavors, b genera el mateix subgrup cíclic d'ordre n de k^*/k^{*n} que a, ja que $b = \beta^n = \alpha^{sn}x^n = a^s x^n$, de manera que 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 $\mathrm{mcd}(s,n) = 1$.

Això permet definir una aplicació f com la desitjada: a cada extensió cíclica $K \mid k$ de grau n li fem correspondre el subgrup cíclic d'ordre n del grup quocient k^*/k^{*n} generat per α^n, on $\alpha \in K$ és qualsevol element primitiu tal que $\alpha^n \in k^*$.

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 α del polinomi $X^n - a \in k[X]$ genera una extensió cíclica $k(\alpha) \mid k$ 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 $k(\alpha) \mid k$ és cíclica d'ordre n. Això demostra que l'aplicació f admet una inversa i, en conseqüència, que és bijectiva. □

Podem fer una descripció semblant de les extensions cícliques de grau $p = \mathrm{car}(k)$; això inclou el cas de les extensions quadràtiques per a $p = 2$.

Teorema 4.10.3. *Siguin $p > 0$ un nombre primer, k un cos de característica p, i $\overline{k}$ un cos algebraicament tancat que conté k.*

a) L'aplicació $\wp : k \longrightarrow k$ 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 $\wp(k)$ de k.

b) Sigui $\alpha \in \overline{k}$ un element tal que $\alpha^p - \alpha \in k$. Per a tot element $\beta \in \overline{k}$ 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 $k(\beta) = k(\alpha)$.

c) Per a un element $\alpha \in \overline{k}$ tal que $\alpha^p - \alpha \in k$, l'extensió $k(\alpha) \mid k$ 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.

d) Suposem que $K \mid k$ és una extensió cíclica de grau p, i α, $\beta \in K$ són elements primitius de l'extensió $K \mid k$ tals que $\alpha^p - \alpha$, $\beta^p - \beta \in k$. Existeixen un element $x \in k$ i un nombre enter s no divisible per p tals que $\beta = s\alpha + x$.

e) Existeix una aplicació bijectiva del conjunt $\mathfrak{C}_p(k)$ de les extensions cícliques de grau p de k en el conjunt $\mathcal{C}_p(k)$ dels subgrups cíclics d'ordre p de $k/\wp(k)$.

DEMOSTRACIÓ: Les comprovacions de a) i b) són immediates, i c) és conseqüència del teorema d'Artin–Schreier (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 d). Sigui $K \mid k$ una extensió cíclica de grau p i suposem que $K = k(\alpha) = k(\beta)$, on $a := \alpha^p - \alpha$, $b := \beta^p - \beta \in k$. Notem que $a,\ b \notin \wp(k)$, perquè $\alpha,\ \beta \notin k$. Com que $1, \alpha, \ldots, \alpha^{p-1}$ és una k-base de $k(\alpha)$, existeixen elements $a_0, a_1, \ldots, a_{p-1} \in k$ tals que $\beta = \sum_{i=0}^{p-1} a_i \alpha^i$. Es tracta de veure que $a_2, \ldots, a_{p-1} = 0$, i que $a_1 \in \mathbb{F}_p^*$.

Podem reescriure la igualtat $b = \beta^p - \beta$, en la forma següent:

$$\begin{aligned} b = \beta^p - \beta = \sum_{i=0}^{p-1} a_i^p \alpha^{pi} - \sum_{i=0}^{p-1} a_i \alpha^i \qquad &= \sum_{i=0}^{p-1} a_i^p (\alpha + a)^i - \sum_{i=0}^{p-1} a_i \alpha^i \\ = \sum_{i=0}^{p-1} a_i^p \sum_{j=0}^{i} \binom{i}{j} \alpha^j a^{i-j} - \sum_{j=0}^{p-1} a_j \alpha^j \quad &= \sum_{j=0}^{p-1} \sum_{i=j}^{p-1} \binom{i}{j} a_i^p a^{i-j} \alpha^j - \sum_{j=0}^{p-1} a_j \alpha^j \\ = \sum_{j=0}^{p-1} \left(\sum_{i=j}^{p-1} \binom{i}{j} a_i^p a^{i-j} - a_j \right) \alpha^j. \end{aligned}$$

I, com que els coeficients $\sum_{i=j}^{p-1} \binom{i}{j} a_i^p a^{i-j} - a_j$ d'aquesta combinació lineal pertanyen a k, ha de ser $\sum_{i=j}^{p-1} \binom{i}{j} a_i^p a^{i-j} - a_j = 0$ per a $1 \leq j \leq p-1$, i $\sum_{i=0}^{p-1} a_i^p a^i - a_0 = b$.

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 $\beta = a_0 \in k$).

Si $p > 2$, 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, $a_{p-2} \in \mathbb{F}_p$.

Repetint aquest argument inductivament, 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, obtenim que $a_{p-1} = a_{p-2} = \cdots = a_2 = 0$, i $a_1 \in \mathbb{F}_p$; per tant, $\beta = a_1\alpha + a_0$, amb $a_1 \in \mathbb{F}_p$, i $x := a_0 \in k$. I ha d'ésser $s := a_1 \neq 0$, ja que $k(\alpha) = k(\beta) \neq k$.

Resta provar e). Donada una extensió cíclica $K \mid k$ de grau p, 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, $\beta^p - \beta = s^p\alpha^p + x^p - s\alpha - x = s(\alpha^p - \alpha) + (x^p - x)$; 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 $k/\wp(k)$, que és cíclic d'ordre p. Així, podem definir una aplicació $f : \mathfrak{C}_p(k) \longrightarrow \mathcal{C}_p(k)$ per $f(K \mid k) := \langle \alpha^p - \alpha \rangle \subseteq k/\wp(k)$, 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 α és una arrel del polinomi $X^p - X - a$, l'extensió $k(\alpha) \mid k$ és cíclica de grau p i $f(k(\alpha) \mid k) = \langle a \rangle$. Això ens diu que f és exhaustiva. Finalment, vegem que f és injectiva. Suposem que $k(\alpha) \mid k$, $k(\beta) \mid k$ són dues extensions cícliques de grau p tals que $f(k(\alpha) \mid k) = f(k(\beta) \mid k)$, 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 $y \in \wp(k)$; 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 $k(\beta) \mid k$ 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. □

4.11 Radicals en característica zero

Siguin k un cos de característica diferent de 2, $\overline{k}$ 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 $\dfrac{-b \pm \alpha}{2a} \in \overline{k}$, 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 $\mathrm{car}(k) \neq 2, 3$, 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 $p := \dfrac{c}{a} - \dfrac{b^2}{3a^2}$, $q := \dfrac{d}{a} + \dfrac{2b^3}{27a^3} - \dfrac{bc}{3a^2}$, 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 $\gamma \in \overline{k}$ és tal que $\gamma^3 = \dfrac{-27q + 3\alpha\beta}{54}$, i α, $\beta \in \overline{k}$ 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 $\theta \in \overline{k}$ és tal que $\theta^3 = -q$ i $\rho := \dfrac{-1 + \beta}{2}$ (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, $z \in \overline{k}$ 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 Arithmeticæ*, demostra que les equacions ciclotòmiques $\Phi_p(X) = 0$, p primer, són "reductibles a pures" (cf. [**?**], 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 curs 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 $f(X)$.

Definició 4.11.1. 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. Direm que l'equació $f(X) = 0$ és resoluble per radicals sobre k si existeix una successió finita de cossos de la forma

$$k \subseteq k(\theta_1) \subseteq k(\theta_1, \theta_2) \subseteq \cdots \subseteq k(\theta_1, \ldots, \theta_m) =: K \subseteq \overline{k},$$

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 $a_i := \theta_i^{n_i} \in k(\theta_1, \ldots, \theta_{i-1})$. També anomenarem resolució de $K \mid k$ d'exponents n_i una successió d'elements θ_1, θ_2, …, $\theta_m \in K$ com aquesta, extensió radical de k qualsevol extensió com $K \mid k$, 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 $K \mid k$ 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 hem donat d'extensió radical admet que alguns (o bé tots) dels elements θ_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 $k(\theta_1, \ldots, \theta_{i-1})[X]$, 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 $k(\zeta) \mid k$, on ζ és una arrel de la unitat, existeix una extensió radical $K \mid k$ en què cada un dels polinomis $X^{n_i} - \theta_i^{n_i}$ és irreductible en $k(\theta_1, \ldots, \theta_{i-1})[X]$.

Proposició 4.11.3. *Siguin k un cos de característica zero, i $\overline{k}$ un cos algebraicament tancat que conté k.*

a) Si $k \subseteq K \subseteq L \subseteq \overline{k}$ són cossos tals que les extensions $K \mid k$ i $L \mid K$ són radicals (respectivament, resolubles per radicals), llavors, l'extensió $L \mid k$ és radical (respectivament, resoluble per radicals).

b) (Canvi de base) *Si $k \subseteq K, L \subseteq \overline{k}$ són cossos tals que l'extensió $K \mid k$ és radical (respectivament, resoluble per radicals), l'extensió $KL \mid L$ també és radical (respectivament, resoluble per radicals).*

c) (Composició) *Si $k \subseteq K_1, K_2 \subseteq \overline{k}$ són cossos tals que $K_1 \mid k$, $K_2 \mid k$ són extensions radicals (respectivament, resolubles per radicals), l'extensió $K_1K_2 \mid k$ també és radical (respectivament, resoluble per radicals).* □

Corol·lari 4.11.4. *Siguin k un cos de característica zero, $f(X) \in k[X]$ un polinomi no nul, i $P_1(X), \ldots, P_m(X) \in k[X]$ 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 $P_1(X) = 0, \ldots, P_m(X) = 0$.* □

4.12 Extensions radicals

En aquesta secció farem un estudi més detallat de les extensions resolubles per radicals. En primer lloc, estudiarem la relació entre una extensió radical $K \mid k$ i la seva clausura normal $N \mid k$.

Proposició 4.12.1. *Siguin k un cos de característica zero, $\overline{k}$ un cos algebraicament tancat que conté k, $K \mid k$ una subextensió radical de $\overline{k} \mid k$, i $N \mid k$ la clausura normal de $K \mid k$. Llavors, l'extensió $N \mid k$ també és radical.*

Demostració: Siguin $\theta_1, \ldots, \theta_m \in \overline{k}$ una resolució de K d'exponents n_i, $\sigma : K \longrightarrow \overline{k}$ una k-immersió qualsevol, i considerem una extensió a N de σ. Llavors $\sigma : N \longrightarrow N$ és un k-automorfisme i $\sigma(K) = k(\sigma(\theta_1), \ldots, \sigma(\theta_m))$ i $\sigma(\theta_i)^{n_i} \in k(\sigma(\theta_1), \ldots, \sigma(\theta_{i-1}))$; per tant, l'extensió $\sigma(K) \mid k$ també és radical. Com que el cos N és la composició dels cossos $\sigma(K)$, per a totes les k-immersions σ de K en $\overline{k}$, l'extensió $N \mid k$ és la composició d'una quantitat finita d'extensions radicals; per tant, és una extensió radical. □

Corol·lari 4.12.2. *Siguin k un cos de característica zero, $K \mid k$ una extensió resoluble per radicals, i $N \mid k$ una clausura normal de $K \mid k$. Llavors, l'extensió $N \mid k$ també és resoluble per radicals.* □

L'ús de les extensions de la forma $k(\zeta) \mid k$, on ζ 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, $\overline{k}$ un cos algebraicament tancat que conté k, $K \mid k$ una extensió radical, i $\theta_1, \ldots, \theta_m \in K$ una resolució de K d'exponents n_i. Suposem, a més a més, que l'extensió $K \mid k$ és normal.

Siguin n el mínim comú múltiple dels nombres $n_1, \ldots, n_m$, i $\zeta \in \overline{k}$ una arrel n-èsima primitiva de la unitat. Si fem el canvi de base a $k(\zeta)$, les extensions $k(\zeta)(\theta_1, \ldots, \theta_i) \mid k(\zeta)(\theta_1, \ldots, \theta_{i-1})$, $1 \leq i \leq m$, són cícliques, cada una de grau divisor del nombre n_i corresponent. D'altra banda, l'extensió $K(\zeta) \mid k(\zeta)$ és normal i per al seu grup de Galois podem considerar la cadena de subgrups

$$\begin{aligned} \mathrm{Gal}(K(\zeta) \mid k(\zeta)) &\supseteq \mathrm{Gal}(K(\zeta) \mid k(\zeta)(\theta_1)) \\ &\supseteq \mathrm{Gal}(K(\zeta) \mid k(\zeta)(\theta_1, \theta_2)) \\ &\supseteq \cdots \\ &\supseteq \mathrm{Gal}(K(\zeta) \mid k(\zeta)(\theta_1, \ldots, \theta_{m-1})) \\ &\supseteq \mathrm{Gal}(K(\zeta) \mid K(\zeta)) = \{1\}. \end{aligned}$$

Lema 4.12.4. *Per a* $1 \leq i \leq n$, $\mathrm{Gal}(K(\zeta) \mid k(\zeta)(\theta_1, \ldots, \theta_i))$ *és un subgrup normal de* $\mathrm{Gal}(K(\zeta) \mid k(\zeta)(\theta_1, \ldots, \theta_{i-1}))$ *i el quocient és cíclic, isomorf al grup de Galois* $\mathrm{Gal}(k(\zeta)(\theta_1, \ldots, \theta_i) \mid k(\zeta)(\theta_1, \ldots, \theta_{i-1}))$.

Aquest resultat és un cas particular del següent, molt més general.

Proposició 4.12.5. *Siguin $L \mid K$ i $K \mid k$ dues extensions normals de cossos, no necessàriament finites ni de característica zero, i tals que l'extensió $L \mid k$ sigui normal. Llavors,* $\mathrm{Gal}(L \mid K)$ *és un subgrup normal de* $\mathrm{Gal}(L \mid k)$ *i el grup quocient* $\mathrm{Gal}(L \mid k)/\mathrm{Gal}(L \mid K)$ *és isomorf al grup de Galois* $\mathrm{Gal}(K \mid k)$.

Demostració: Podem definir una aplicació $\mathrm{Gal}(L \mid k) \xrightarrow{\mathrm{res}} \mathrm{Gal}(K \mid k)$ per l'assignació $\sigma \mapsto \sigma_{|K}$, perquè l'extensió $K \mid k$ és normal. L'aplicació res és, clarament, un morfisme de grups, i és exhaustiu perquè l'extensió $L \mid k$ és normal i, per tant, tot k-automorfisme de K s'estén a un k-automorfisme de L. A més a més, el nucli del morfisme res és exactament $\mathrm{Gal}(L \mid K)$. En conseqüència, $\mathrm{Gal}(L \mid K)$ és un subgrup normal de $\mathrm{Gal}(L \mid k)$ i el quocient és isomorf a $\mathrm{Gal}(K \mid k)$. □

4.12.6. Siguin $\overline{k}$ un cos algebraicament tancat, $k \subseteq \overline{k}$ un subcòs qualsevol, i $f(X) \in k[X]$ un polinomi no nul. Suposem que $\mathrm{car}(k) = 0$ i que l'equació $f(X) = 0$ és resoluble per radicals sobre k, i sigui $\theta_1, \ldots, \theta_m \in \overline{k}$ una resolució d'exponents n_i d'un cos K que contingui totes les arrels de $f(X)$ i tal que

l'extensió $K \mid k$ sigui normal. Posem $n := \mathrm{mcm}(n_1, \ldots, n_m)$, $\zeta \in \overline{k}$ una arrel n-èsima primitiva de la unitat, i $K_i := k(\zeta, \theta_1, \ldots, \theta_i)$, per a $0 \leq i \leq m$. Com que l'extensió $K_m \mid k$ és la composició de les dues extensions normals $K \mid k$ i $K_0 \mid k$, l'extensió $K_m \mid k$ és normal. Considerem la successió de cossos

$$k \subseteq K_0 \subseteq K_1 \subseteq \cdots \subseteq K_m,$$

i la dels grups de Galois

$$\begin{aligned} \mathrm{Gal}(K_m \mid k) \supseteq \mathrm{Gal}(K_m \mid K_0) \supseteq \mathrm{Gal}(K_m \mid K_1) \supseteq \cdots \\ \ldots \supseteq \mathrm{Gal}(K_m \mid K_{m-1}) \supseteq \mathrm{Gal}(K_m \mid K_m) = \{1\}. \end{aligned}$$

Si posem $K_{-1} := k$, obtenim que, per a $0 \leq i \leq m$, el grup de Galois $\mathrm{Gal}(K_m \mid K_i)$ és un subgrup normal de $\mathrm{Gal}(K_m \mid K_{i-1})$ i també que el quocient $\mathrm{Gal}(K_m \mid K_{i-1})/\mathrm{Gal}(K_m \mid K_i)$, que és isomorf a $\mathrm{Gal}(K_i \mid K_{i-1})$, 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 $\mathrm{Gal}(K_m \mid K_{i-1})/\mathrm{Gal}(K_m \mid K_i)$ és cíclic), i, per a $i = 0$, podem aplicar la proposició anterior, de manera que $\mathrm{Gal}(K_m \mid K_{-1})/\mathrm{Gal}(K_m \mid K_0) \simeq \mathrm{Gal}(k(\zeta) \mid k)$ és isomorf a un subgrup de $(\mathbb{Z}/n\mathbb{Z})^*$, i, per tant, abelià. Així, hem demostrat el 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 $K \mid k$ que satisfà les condicions següents:*

a) El cos K conté el cos de descomposició de $f(X)$ sobre k.

b) Si $G := \mathrm{Gal}(K \mid k)$, el grup G admet una successió decreixent de subgrups $G_0 := G \supseteq G_1 \supseteq \cdots \supseteq G_m = \{1\}$ 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. □

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.

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, 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 de Galois i, de l'altra, el conjunt dels subgrups del grup de Galois d'aquesta extensió, i estudiem el comportament 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. Dediquem 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 i 4, no pel possible interès de les fórmules que expressen les seves arrels per radicals, sinó per a il·lustrar de quina manera es pot usar la teoria per a resoldre algunes equacions. Les dues darreres seccions es destinen a l'exposició d'una variació de la teoria, la caracterització de les seccions del cercle constructibles amb regle i compàs; a la secció desena, mitjançant la introducció formal de les construccions amb regle 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 i darrera, amb la caracterització dels nombres naturals $n \geq 1$ tals que el polígon regular de n costats es pot construir amb regle i compàs, fet que aprofitem per a la introducció del concepte de p-grup.

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 punt 3.10.12); és a dir,

$$L^H := \{x \in L : \sigma(x) = x, \text{ per a tot } \sigma \in H\}.$$

A la proposició 3.7.9 hem vist que, si ζ és una arrel de la unitat, el subcòs de $\mathbb{Q}(\zeta)$ fix per $\mathrm{Gal}(\mathbb{Q}(\zeta) \mid \mathbb{Q})$ coincideix amb el cos base $\mathbb{Q}$; és a dir, que $\mathbb{Q}(\zeta)^{\mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q})} = \mathbb{Q}$. Aquest mateix fet succeeix també en el cas dels cossos finits: el subcòs de $\mathbb{F}_{q^n}$ fix per l'automorfisme de Frobenius $\varphi_q \in \mathrm{Gal}(\mathbb{F}_{q^n} \mid \mathbb{F}_q)$ és el cos base $\mathbb{F}_q$; i com que l'automorfisme de Frobenius és un generador del grup $\mathrm{Gal}(\mathbb{F}_{q^n} \mid \mathbb{F}_q)$, obtenim que $\mathbb{F}_{q^n}^{\mathrm{Gal}(\mathbb{F}_{q^n}|\mathbb{F}_q)} = \mathbb{F}_q$ (cf. el punt 3.10.6). Aquest fet no és aïllat. Comencem per destacar un parell de propietats generals, que se satisfàn per definició de cos fix per un subgrup d'automorfismes.

Proposició 5.1.1. *Sigui $L \mid k$ una extensió algebraica de cossos.*

(a) *Per a tot subgrup $H \subseteq \mathrm{Gal}(L \mid k)$, és $H \subseteq \mathrm{Gal}(L \mid L^H)$.*

(b) $\mathrm{Gal}(L \mid L^{\mathrm{Gal}(L|k)}) = \mathrm{Gal}(L \mid k)$. □

5.1.2. La correspondència fonamental de la teoria de Galois. Considerem una extensió algebraica qualsevol de cossos, $L \mid k$, el seu grup de

Galois, $G := \mathrm{Gal}(L \mid k)$, i siguin $\mathcal{S}(L \mid k)$ el conjunt de tots els subgrups de G, i $\mathcal{E}(L \mid k)$ el conjunt de totes les subextensions $K \mid k$ de $L \mid k$.

Per a cada subgrup $H \subseteq G$, podem considerar el cos L^H, i es tenen les inclusions $k \subseteq L^H \subseteq L$, de manera que $L^H \mid k$ pertany a $\mathcal{E}(L \mid k)$. Així, l'assignació $H \mapsto L^H \mid k$ defineix una aplicació $\mathcal{S}(L \mid k) \longrightarrow \mathcal{E}(L \mid k)$. Aquesta aplicació inverteix l'ordre donat per la inclusió; és a dir, si $H_1 \subseteq H_2$, llavors $L^{H_2} \mid k$ és una subextensió de $L^{H_1} \mid k$. A més a més, l'extensió assignada al subgrup trivial $\{\mathrm{Id}\}$ és l'extensió $L \mid k$; és a dir, $L^{\{\mathrm{Id}\}} = L$.

Recíprocament, a tota subextensió $K \mid k$ de $L \mid k$, podem assignar-li el grup de Galois $\mathrm{Gal}(L \mid K)$, que és un subgrup de $\mathrm{Gal}(L \mid k)$; això defineix una aplicació $\mathcal{E}(L \mid k) \longrightarrow \mathcal{S}(L \mid k)$. Aquesta aplicació també inverteix l'ordre donat per inclusió; és a dir, si $K_1 \mid k$ és una subextensió de $K_2 \mid k$, llavors $\mathrm{Gal}(L \mid K_1) \supseteq \mathrm{Gal}(L \mid K_2)$. I, a més a més, a l'extensió total $L \mid k$ li correspon el subgrup trivial $\mathrm{Gal}(L \mid L) = \{\mathrm{Id}\}$.

En el cas d'extensions de cossos finits, hem vist que aquestes aplicacions són inverses l'una de l'altra (cf. el teorema 3.10.12). Aquesta propietat no es limita als cossos finits, sinó que se satisfà per a totes les extensions de Galois finites. La propietat essencial que resta veure és la següent.

Proposició 5.1.3. *Sigui $L \mid k$ una extensió de Galois finita. Per a tota subextensió $K \mid k$ se satisfà que $K = L^{\mathrm{Gal}(L|K)}$.*

Demostració: Posem $H := \mathrm{Gal}(L \mid K)$ 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 $L \mid K$ i $L \mid L^H$ 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 $\mathrm{Gal}(L \mid L^H) \subseteq H$ s'obté immediatament del fet que $K \subseteq L^H$. I l'altra inclusió, $H \subseteq \mathrm{Gal}(L \mid L^H)$, és el contingut de la proposició 5.1.1, (a). □

Proposició 5.1.4. *Una extensió finita $L \mid k$ és de Galois si, i només si, $L^{\mathrm{Gal}(L|k)} = k$.*

Demostració: La proposició 5.1.1, (b) dóna la igualtat $\mathrm{Gal}(L \mid L^{\mathrm{Gal}(L|k)}) = \mathrm{Gal}(L \mid k)$. Si suposem que l'extensió $L \mid k$ és de Galois, se satisfà que l'extensió $L \mid L^{\mathrm{Gal}(L|k)}$ també és de Galois; i com que les dues són finites, tenim

les igualtats $\#\mathrm{Gal}(L \mid k) = [L : k]$ i, $\#\mathrm{Gal}(L \mid L^{\mathrm{Gal}(L|k)}) = [L : L^{\mathrm{Gal}(L|k)}]$. Però, llavors, en la successió de cossos $k \subseteq L^{\mathrm{Gal}(L|k)} \subseteq L$, les extensions són finites i tals que $[L : L^{\mathrm{Gal}(L|k)}] = [L : k]$; per tant, $L^{\mathrm{Gal}(L|k)} = k$. La propietat recíproca és el cas particular $G = \mathrm{Gal}(L \mid k)$ del teorema següent. □

Teorema 5.1.5. (Artin) *Siguin L un cos qualsevol i G un grup finit d'automorfismes de L. L'extensió $L \mid L^G$ és finita i de Galois i* $\mathrm{Gal}(L \mid L^G) = G$.

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 σ a C_θ defineix una aplicació injectiva i, per tant, bijectiva, $\sigma_{|C_\theta} : C_\theta \longrightarrow C_\theta$. 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 θ és una arrel d'aquest polinomi, totes les arrels del qual són simples.

L'extensió $L \mid L^G$ 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 $L \mid L^G$ 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 $L \mid L^G$ és finita i $[L : L^G] \leq \#G$.

Ja només resta veure que $\mathrm{Gal}(L \mid L^G) = G$. Però, per construcció, és clar que $G \subseteq \mathrm{Gal}(L \mid L^G)$; i, d'altra banda, $\#\mathrm{Gal}(L \mid L^G) \leq [L : L^G] \leq \#G$; per tant, tenim la igualtat $G = \mathrm{Gal}(L \mid L^G)$ que volíem. □

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 $L \mid k$ una extensió de Galois finita de cossos. Com en* 5.1.2*, posem $\mathcal{E}(L \mid k)$ el conjunt de les subextensions $K \mid k$ de $L \mid k$ i $\mathcal{S}(L \mid k)$ el conjunt dels subgrups de $\mathrm{Gal}(L \mid k)$. Les dues aplicacions $\mathcal{E}(L \mid k) \longrightarrow \mathcal{S}(L \mid k)$ i $\mathcal{S}(L \mid k) \longrightarrow \mathcal{E}(L \mid k)$ definides per les assignacions $K \mid k \mapsto \mathrm{Gal}(L \mid K)$ i $H \mapsto L^H \mid k$ són bijectives, inverses l'una de l'altra, i inverteixen l'ordre donat per la inclusió. A més a més, l'extensió $L^H \mid k$ és normal si, i només si, $H \subseteq \mathrm{Gal}(L \mid k)$ és un subgrup normal.*

Demostració: Pràcticament ho hem vist tot, però, per comoditat, repetirem alguns arguments. Com que l'extensió $L \mid k$ és de Galois i finita, totes les subextensions $K \mid k$ de $L \mid k$ són separables i finites, i totes les extensions $L \mid K$, per a $k \subseteq K \subseteq L$, són de Galois i finites.

Donat un subgrup qualsevol $H \subseteq \mathrm{Gal}(L \mid k)$, el teorema d'Artin ens diu que se satisfà la igualtat $\mathrm{Gal}(L \mid L^H) = H$; i recíprocament, donada una subextensió qualsevol $K \mid k$ de $L \mid k$, se satisfà que $L^{\mathrm{Gal}(L|K)} = K$, perquè $L \mid K$ 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 $\mathrm{Gal}(L \mid K) \subseteq \mathrm{Gal}(L \mid k)$ és un subgrup normal si, i només si, l'extensió $K \mid k$ és normal. Si l'extensió $K \mid k$ és normal, la reducció $\mathrm{Gal}(L \mid k) \longrightarrow \mathrm{Gal}(K \mid k)$ és un morfisme exhaustiu de grups de nucli $\mathrm{Gal}(L \mid K)$ (cf. la proposició 4.12.5); per tant, $\mathrm{Gal}(L \mid K)$ és un subgrup normal de $\mathrm{Gal}(L \mid k)$. Recíprocament, suposem que $\mathrm{Gal}(L \mid K)$ és un subgrup normal de $\mathrm{Gal}(L \mid k)$. Per a veure que l'extensió $K \mid k$ és normal, veurem que per a tota k-immersió σ de K en un cos algebraicament tancat que contingui L, és $\sigma(K) = K$, de manera que σ és un automorfisme de K. Però, com que l'extensió $L \mid k$ és normal, una tal σ s'estén a un k-automorfisme de L i $\sigma(K) \subseteq L$, i podem considerar les dues extensions $L \mid K$ i $L \mid \sigma(K)$. És clar que $\mathrm{Gal}(L \mid \sigma(K)) = \sigma\mathrm{Gal}(L \mid K)\sigma^{-1}$; i com que $\mathrm{Gal}(L \mid K)$ és un subgrup normal de $\mathrm{Gal}(L \mid k)$ i $\sigma \in \mathrm{Gal}(L \mid k)$, és $\sigma\mathrm{Gal}(L \mid K)\sigma^{-1} = \mathrm{Gal}(L \mid K)$, de manera que $\mathrm{Gal}(L \mid \sigma(K)) = \mathrm{Gal}(L \mid K)$. Com a conseqüència, és $\sigma(K) = K$, ja que $\sigma(K)$ és el cos que correspon al grup $\mathrm{Gal}(L \mid \sigma(K))$ i K el que correspon al grup $\mathrm{Gal}(L \mid K)$. □

Per a acabar aquesta secció, establirem algunes propietats complementàries que es dedueixen fàcilment del teorema fonamental.

Proposició 5.2.2. *Siguin $L \mid k$ una extensió de Galois finita i $K_1 \mid k$, $K_2 \mid k$, subextensions qualssevol. Llavors,*

(a) $\mathrm{Gal}(L \mid K_1K_2) = \mathrm{Gal}(L \mid K_1) \cap \mathrm{Gal}(L \mid K_2)$*; i*

(b) $\mathrm{Gal}(L \mid K_1 \cap K_2) = \langle \mathrm{Gal}(L \mid K_1), \mathrm{Gal}(L \mid K_2) \rangle$*, el subgrup de* $\mathrm{Gal}(L \mid k)$ *generat per* $\mathrm{Gal}(L \mid K_1) \cup \mathrm{Gal}(L \mid K_2)$.

Demostració: La propietat (a) és gairebé immediata a partir de les definicions; provem (b). Posem $H = \langle \mathrm{Gal}(L \mid K_1), \mathrm{Gal}(L \mid K_2) \rangle$; 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 $\mathrm{Gal}(L \mid K_i) \subseteq \mathrm{Gal}(L \mid K_1 \cap K_2)$; per tant, $H \subseteq \mathrm{Gal}(L \mid K_1 \cap K_2)$; 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 $\sigma \in \mathrm{Gal}(L \mid K_i)$, $i = 1, 2$, és $\sigma(x) = x$; és a dir, $x \in L^{\mathrm{Gal}(L|K_i)} = K_i$; això és, $x \in K_1 \cap K_2$, de manera que tenim l'altra inclusió, $L^H \subseteq K_1 \cap K_2$. □

Proposició 5.2.3. *Siguin k un cos, $K_1 \mid k$, una extensió de Galois, $K_2 \mid k$ una extensió qualsevol, i suposem que $K_1, K_2 \subseteq \overline{k}$, on $\overline{k}$ és un cos algebraicament tancat que conté k. Llavors:*

(a) *L'extensió $K_1K_2 \mid K_2$ és de Galois.*

(b) *L'aplicació de restricció $\mathrm{Gal}(K_1K_2 \mid K_2) \longrightarrow \mathrm{Gal}(K_1 \mid k)$, donada per $\sigma \mapsto \sigma_{|K_1}$, és un morfisme injectiu de grups.*

(c) *La imatge del morfisme de restricció és $\mathrm{Gal}(K_1 \mid K_1 \cap K_2)$.*

(d) *Si $K_1 \mid k$ és finita, llavors $K_1K_2 \mid K_2$ és finita i $[K_1K_2 : K_2]$ divideix $[K_1 : k]$.*

Demostració: La propietat (a) és conseqüència immediata dels fets que la separabilitat i la normalitat es conserven per canvi de base (cf. les proposicions 3.9.12 i 4.4.10). Per a veure (b), adonem-nos que si $\sigma \in \mathrm{Gal}(K_1K_2 \mid K_2)$, llavors la restricció $\sigma_{|K_1}$ és un k-automorfisme de K_1, perquè l'extensió $K_1 \mid k$ és normal; per tant, l'aplicació de restricció $\mathrm{Gal}(K_1K_2 \mid K_2) \longrightarrow \mathrm{Gal}(K_1 \mid k)$ està ben definida i és, evidentment, un morfisme de grups. A més a més, aquest morfisme és injectiu, perquè si $\sigma_{|K_1} = 1$, com que $\sigma_{|K_2} = 1$ (perquè $\sigma \in \mathrm{Gal}(K_1K_2 \mid K_2)$), ha de ser $\sigma = 1$ en K_1K_2. Vegem, ara, (c); això és, calculem la imatge del morfisme de restricció. Clarament, com que per a $\sigma \in \mathrm{Gal}(K_1K_2 \mid K_2)$ és $\sigma_{|K_2} = 1$, obtenim que $\sigma_{|K_1}$ és la identitat en $K_1 \cap K_2$; per tant, $\sigma_{|K_1} \in \mathrm{Gal}(K_1 \mid K_1 \cap K_2)$; i recíprocament, si $\tau \in \mathrm{Gal}(K_1 \mid K_1 \cap K_2)$, podem estendre τ a una K_2-immersió de K_1K_2 en $\overline{k}$;

i com que $K_1K_2 \mid K_2$ és normal, l'extensió de τ esdevé un K_2-automorfisme de K_1K_2; és a dir, un element de $\mathrm{Gal}(K_1K_2 \mid K_2)$. I, òbviament, la restricció de τ a K_1 coincideix amb τ; per tant, el morfisme de restricció és exhaustiu sobre $\mathrm{Gal}(K_1 \mid K_1 \cap K_2)$, com volíem veure. Finalment, per a veure (d), només cal observar que si $K_1 \mid k$ és finita, llavors $K_1K_2 \mid K_2$ també és finita i $\mathrm{Gal}(K_1K_2 \mid K_2) \simeq \mathrm{Gal}(K_1 \mid K_1 \cap K_2) \subseteq \mathrm{Gal}(K_1 \mid k)$; per tant,

$$[K_1K_2 : K_2] = \#\mathrm{Gal}(K_1K_2 \mid K_2) \text{ divideix } \#\mathrm{Gal}(K_1 \mid k) = [K_1 : k],$$

com volíem veure. □

Proposició 5.2.4. *Siguin $\overline{k}$ un cos algebraicament tancat, $k \subseteq \overline{k}$ un subcòs, i $K_1 \mid k$ i $K_2 \mid k$ dues extensions de Galois finites, i suposem que $K_1, K_2 \subseteq \overline{k}$. Llavors:*

(a) *L'extensió $K_1K_2 \mid k$ és de Galois.*

(b) *L'aplicació $\mathrm{Gal}(K_1K_2 \mid k) \xrightarrow{\varphi} \mathrm{Gal}(K_1 \mid k) \times \mathrm{Gal}(K_2 \mid k)$, donada per $\sigma \mapsto (\sigma_{|K_1}, \sigma_{|K_2})$, és un morfisme de grups injectiu.*

(c) *Si $K_1 \cap K_2 = k$, llavors φ és un isomorfisme.*

(d) *En general, l'aplicació*

$$\mathrm{Gal}(K_1K_2 \mid K_1 \cap K_2) \longrightarrow \mathrm{Gal}(K_1 \mid K_1 \cap K_2) \times \mathrm{Gal}(K_2 \mid K_1 \cap K_2)$$

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 3.9.13), i la composició de dues extensions separables és una extensió separable (cf. la proposició 4.4.11); 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 $K_1 \mid k$ i $K_2 \mid k$ són normals, la restricció a K_i d'un k-automorfisme de K_1K_2 és un k-automorfisme de K_i; per tant, φ 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 σ és la identitat en K_1K_2; per tant, φ és injectiu. Vegem (c). Siguin $\sigma_1 \in \mathrm{Gal}(K_1 \mid k)$, $\sigma_2 \in \mathrm{Gal}(K_2 \mid k)$, dos elements qualssevol; en virtut de la proposició anterior, tenim isomorfismes de grups $\mathrm{Gal}(K_1K_2 \mid K_2) \longrightarrow \mathrm{Gal}(K_1 \mid k)$ i $\mathrm{Gal}(K_1K_2 \mid K_1) \longrightarrow \mathrm{Gal}(K_2 \mid k)$, donats per restricció, ja que suposem que $K_1 \cap K_2 = k$; per tant, existeixen extensions

$\sigma_1 \in \mathrm{Gal}(K_1K_2 \mid K_2)$, de σ_1, i $\sigma_2 \in \mathrm{Gal}(K_1K_2 \mid K_1)$, de σ_2; llavors, σ_1, σ_2 són k-automorfismes de K_1K_2, i té sentit considerar $\sigma := \sigma_2 \circ \sigma_1 \in \mathrm{Gal}(K_1K_2 \mid k)$. Ara bé, com que $\sigma_1 \in \mathrm{Gal}(K_1K_2 \mid K_2)$, és $\sigma_{|K_2} = \sigma_{2|K_2} \circ \sigma_{1|K_2} = \sigma_2$, i $\sigma_{|K_1} = \sigma_{2|K_1} \circ \sigma_{1|K_1} = \sigma_1$, de manera que σ és una antiimatge de la parella (σ_1, σ_2); això demostra que φ és exhaustiu i, en conseqüència, un isomorfisme. La propietat (d) només és una reformulació de les dues anteriors, ja que si $K_1 \mid k$ i $K_2 \mid k$ són extensions de Galois, també ho són les dues extensions $K_1 \mid K_1 \cap K_2$ i $K_2 \mid K_1 \cap K_2$, de manera que podem aplicar els dos resultats (b) i (c), ja demostrats. $\square$

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 $L \mid k$ que conté el cos de descomposició sobre k del polinomi $f(X)$, i que és tal que el grup de Galois $G := \mathrm{Gal}(L \mid k)$ admet una successió de subgrups de la forma $G_0 := G \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_n = \{\mathrm{Id}\}$, 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, $G := G_0 \supseteq G_1 \supseteq \cdots \supseteq G_n = \{1\}$, 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 ζ és una arrel n-èsima primitiva de la unitat, i L és el cos de descomposició sobre k del polinomi

$X^n - a$, la cadena de grups $\mathrm{Gal}(L \mid k) \supseteq \mathrm{Gal}(L \mid K) \supseteq \{1\}$ és una resolució de $\mathrm{Gal}(L \mid k)$, ja que l'extensió $L \mid K$ és cíclica i, en conseqüència, abeliana, i l'extensió $K \mid k$ és normal i $\mathrm{Gal}(L \mid k)/\mathrm{Gal}(L \mid K) \simeq \mathrm{Gal}(K \mid k)$ és isomorf a un subgrup de $(\mathbb{Z}/n\mathbb{Z})^*$.

(c) Siguin A un anell, H el subgrup de $\mathbf{GL}(2, A)$ format per les matrius de la forma $\begin{bmatrix} * & * \\ 0 & 1 \end{bmatrix}$, i G el subgrup de $\mathbf{GL}(2, A)$ format per les matrius de la forma $\begin{bmatrix} * & * \\ 0 & * \end{bmatrix}$. Llavors, G i H són grups resolubles.

Les matrius de $\mathbf{GL}(2, A)$ de la forma $\begin{bmatrix} 1 & * \\ 0 & 1 \end{bmatrix}$ formen un subgrup normal K de H; en efecte, aquest conjunt és el nucli de la restricció a H del morfisme determinant, $\det : H \longrightarrow \mathbf{GL}_1(A) = A^*$. Com que aquest morfisme és exhaustiu, el grup quocient H/K és isomorf a $\mathbf{GL}_1(A) = A^*$; en particular, commutatiu. D'altra banda, K és isomorf al grup additiu de A, perquè l'aplicació $f : A \longrightarrow K$ 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 $g : G \longrightarrow \mathbf{GL}_1(A)$ 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. □

Per al tractament dels grups resolubles molt sovint és útil comparar el grup amb els seus subgrups normals i els seus quocients respectius. Convé establir, prèviament, el teorema d'isomorfia següent.

Proposició 5.3.3. *Siguin 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 grup quocient H/N és un subgrup de G/N, que és normal si, i només si, H és un subgrup normal de G.*

(c) *Si H és un subgrup normal de G, llavors el grup quocient G/H és isomorf al grup* $\dfrac{G/N}{H/N}$.

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 $\psi : G \longrightarrow G/N$ 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 $\pi : G \longrightarrow G/H$, que és un morfisme exhaustiu de grups; el nucli de π és H i conté N, de manera que π factoritza per un morfisme exhaustiu de grups $\overline{\pi} : G/N \longrightarrow G/H$, el nucli del qual és H/N; per tant, el grup quocient $\dfrac{G/N}{H/N}$ és isomorf a G/H, com volíem veure. □

Proposició 5.3.4. *Siguin G un grup resoluble i H un subgrup qualsevol de G. Llavors, H és resoluble.*

DEMOSTRACIÓ: Sigui $G_0 := G \supseteq G_1 \supseteq \cdots \supseteq G_n = \{1\}$ una resolució de G; es tracta de veure que la cadena $H = H_0 \supseteq H_1 \supseteq \cdots \supseteq H_n = \{1\}$, 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 $H_{i-1} = H \cap G_{i-1} \longrightarrow G_{i-1} \longrightarrow G_{i-1}/G_i$ 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. □

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 $HK \subseteq KH$. Per tant, $KH = HK$. 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 per a $k_1, k_2 \in K$, 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 $1 = 1 \cdot 1 \in HK$, de manera que el 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. □

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 $G_0 := G \supseteq G_1 \supseteq \cdots \supseteq G_n = \{1\}$ una resolució de G; es tracta de veure que la cadena $G/N = \overline{G} = \overline{G}_0 \supseteq \overline{G}_1 \supseteq \cdots \supseteq \overline{G}_n = \{1\}$ 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, com que G_i és un subgrup normal de G_{i-1}, també G_iN és un subgrup normal de $G_{i-1}N$, de manera que $\overline{G}_i$ 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. □

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 són 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 canònica $\pi : G \longrightarrow G/N$, 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. □

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 $L \mid k$ 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 $G := \mathrm{Gal}(L \mid k)$ és resoluble. Llavors, l'equació $f(X) = 0$ és resoluble per radicals.*

Abans de procedir a la demostració, establirem un resultat previ que ens ajudarà 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. □

Proposició 5.4.4. *Tot grup finit, commutatiu, i no trivial admet una resolució cíclica d'índexs primers.*

Demostració: Siguin G un grup finit commutatiu, $m := \#G$, l'ordre de G, i posem $m = p_1 \cdots p_k$, on $p_1, \ldots, p_k$ 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. Siguin $g \in G$, $g \neq 1$, 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. □

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 $L \mid k$ és resoluble per radicals. Siguin $n := \#\mathrm{Gal}(L \mid k) = [L : k]$ i $\zeta \in \overline{k}$ una arrel n-èsima primitiva de la unitat, i considerem l'extensió $L(\zeta) \mid k$, que és de Galois, ja que és la composició de les dues extensions de Galois $L \mid k$ i $k(\zeta) \mid k$ (cf. la proposició 5.2.4). Si provem que l'extensió $L(\zeta) \mid k$ és radical, ja haurem acabat, perquè $L \mid k$ és una subextensió de $L(\zeta) \mid k$.

Sigui $G_0 := \mathrm{Gal}(L \mid k) \supseteq G_1 \supseteq \cdots \supseteq G_m = \{1\}$ una resolució cíclica d'índexs primers de $\mathrm{Gal}(L \mid k)$, que existeix perquè G és un grup resoluble finit. Siguin $k_i := L^{G_i}$, $0 \leq i \leq m$, els cossos fixos; 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 $k_i \mid k_{i-1}$ són cícliques de graus primers que divideixen n, amb grups de Galois $\mathrm{Gal}(k_i \mid k_{i-1}) \simeq G_{i-1}/G_i$, per a $1 \leq i \leq m$. Com a conseqüència, si afegim ζ 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 $K_i \mid K_{i-1}$, són trivials o bé cícliques de graus primers que divideixen n, perquè s'obtenen de les extensions $k_i \mid k_{i-1}$ pel canvi de base $K_{i-1} \mid k_{i-1}$ i, per tant, tenim morfismes injectius dels grups de Galois $\mathrm{Gal}(K_i \mid K_{i-1}) \longrightarrow \mathrm{Gal}(k_i \mid k_{i-1}) \simeq G_{i-1}/G_i$ (cf. la proposició 5.2.3); i, d'altra banda, l'extensió $K_0 \mid K_{-1}$ 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 $K_i \mid K_{i-1}$, que és cíclica de grau divisor de n, admet un element primitiu θ_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 $L(\zeta) \mid k$. □

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.

Corol·lari 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 $\mathrm{Gal}(L \mid k)$ és resoluble.* □

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. 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 $K \mid k$ per a la qual existeix una successió finita de subcossos de la forma

$$k \subseteq k(\theta_1) \subseteq k(\theta_1, \theta_2) \subseteq \cdots \subseteq k(\theta_1, \ldots, \theta_m) = K$$

tal que, per a $1 \leq i \leq m$, i si posem $n_i := [k(\theta_1, \ldots, \theta_i) : k(\theta_1, \ldots, \theta_{i-1})]$, se satisfà que

(a) $\theta_i^{n_i} \in k(\theta_1, \ldots, \theta_{i-1})$, si p no divideix n_i,

(b) i $n_i = p$ i $\theta_i^p - \theta_i \in k(\theta_1, \ldots, \theta_{i-1})$, si p divideix n_i.

Anomenarem extensió resoluble per radicals tota subextensió $K \mid k$ 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* $\mathrm{Gal}(L \mid k)$ *és resoluble.*

Demostració: Aquest teorema es pot demostrar de manera idèntica al cas de característica zero, llevat que en el cas de les extensions cícliques de grau p cal tenir en compte el teorema d'Artin–Schreier (cf. 4.9.3) i considerar elements primitius θ tals que $\theta^p - \theta$ sigui un element del cos base de l'extensió cíclica corresponent. □

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 $K \mid k$ 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 $L \mid k$ 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, ζ una arrel p-èsima primitiva de la unitat, i $K := k(\zeta)$.

L'extensió $K \mid k$ 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 $\mathrm{Gal}(K \mid k)$ és un grup cíclic d'ordre divisor de $p-1 < p$. Així, $K \mid k$ és una extensió cíclica de grau divisor de $p-1$; per tant, si ξ és una arrel $p-1$-èsima primitiva de la unitat, l'extensió $K(\xi) \mid k(\xi)$ admet un element primitiu θ 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 $k \subseteq k(\theta_1) \subseteq \cdots \subseteq k(\theta_1, \ldots, \theta_n)$ tal que $\zeta \in k(\theta_1, \ldots, \theta_n)$, i que $\theta_i^{n_i} \in k(\theta_1, \ldots, \theta_{i-1})$, amb $n_i < p$.

Si algun dels elements θ_i és alguna arrel de la unitat, podem substituir l'extensió $k(\theta_1, \ldots, \theta_i) \mid k(\theta_1, \ldots, \theta_{i-1})$ 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 $K \mid k$ és radical si, i només si, existeix una successió de cossos de la forma*

$$k \subseteq k(\theta_1) \subseteq k(\theta_1, \theta_2) \subseteq \cdots \subseteq k(\theta_1, \ldots, \theta_m) = K$$

tal que, per a cada índex i, $1 \leq i \leq n$, existeix un nombre natural $n_i \geq 1$ tal que $\theta_i^{n_i} \in k(\theta_1, \ldots, \theta_{i-1})$ i $X^{n_i} - \theta_i^{n_i} \in k(\theta_1, \ldots, \theta_{i-1})[X]$ és irreductible. □

Per als cossos de característica positiva se satisfà el resultat anàleg següent.

Corol·lari 5.5.2. *Una extensió $K \mid k$ de cossos de característica $p > 0$ és radical si, i només si, existeix una successió de cossos de la forma*

$$k \subseteq k(\theta_1) \subseteq k(\theta_1, \theta_2) \subseteq \cdots \subseteq k(\theta_1, \ldots, \theta_m) = K$$

tal que, per a cada índex i, $1 \leq i \leq n$, existeix un nombre natural $n_i \geq 1$ tal que
(a) *$\theta_i^{n_i} \in k(\theta_1, \ldots, \theta_{i-1})$ i $X^{n_i} - \theta_i^{n_i} \in k(\theta_1, \ldots, \theta_{i-1})[X]$ és irreductible, si p no divideix n_i, i*
(b) *$n_i = p$, $\theta_i^p - \theta_i \in k(\theta_1, \ldots, \theta_{i-1})$, i $X^p - X - (\theta_i^p - \theta_i) \in k(\theta_1, \ldots, \theta_{i-1})[X]$ és irreductible, si p divideix n_i.* □

5.6 Grups de Galois com a grups de permutacions

Siguin k un cos, $\overline{k}$ un cos algebraicament tancat que conté k, $f(X) \in k[X]$ un polinomi no nul, $Z_f := \{\theta_1, \ldots, \theta_n\} \subseteq \overline{k}$ el conjunt de les arrels de $f(X)$, i $L := k(\theta_1, \ldots, \theta_n)$ el cos de descomposició del polinomi $f(X)$. Llavors, l'extensió $L \mid k$ és normal, i podem considerar el grup de Galois $\mathrm{Gal}(L \mid k)$ i una aplicació $g : \mathrm{Gal}(L \mid k) \times Z_f \xrightarrow{g} Z_f$ definida per $(\sigma, \theta) \mapsto \sigma(\theta)$. Efectivament, donat un k-automorfisme σ de L (és a dir, un element de $\mathrm{Gal}(L \mid k)$), i una arrel θ 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 $\sigma, \tau \in \mathrm{Gal}(L \mid k)$ 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 $\mathrm{Gal}(L \mid k)$.

Aquestes propietats per a una aplicació de la forma $g : G \times C \longrightarrow C$, on G és un grup qualsevol i C és un conjunt qualsevol, ja han aparegut abans en el curs. En efecte, si A és un anell, $A[X_1, \ldots, X_n]$ és l'anell de polinomis en n indeterminades de coeficients en A, i S_n és el grup de les permutacions de $\{1, 2, \ldots, n\}$, ja hem vist una aplicació $S_n \times A[X_1, \ldots, X_n] \longrightarrow A[X_1, \ldots, X_n]$ donada per $(\sigma, P(X_1, \ldots, X_n)) \mapsto P(X_{\sigma(1)}, \ldots, X_{\sigma(n)})$. I que el conjunt dels polinomis $P(X_1, \ldots, X_n) \in A[X_1, \ldots, X_n]$ tals que $P(X_{\sigma(1)}, \ldots, X_{\sigma(n)}) = P(X_1, \ldots, X_n)$, per a tot $\sigma \in S_n$, és l'anell dels polinomis simètrics.

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 $g : G \times C \longrightarrow C$

tal que, si denotem per $\sigma \cdot x$ la imatge de la parella (σ, 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 $L \mid k$, 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 $f(X)$.* □

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 $G \times C \longrightarrow C$ tal que, si denotem per x^σ la imatge de la parella (σ, 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 $g : G \times C \longrightarrow C$ 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 dóna lloc a un morfisme de grups $\psi_g : G \longrightarrow S(C)$. En efecte, donat $\sigma \in G$, podem considerar l'aplicació $g_\sigma : C \longrightarrow C$ 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 $g_1 = \mathrm{Id}$, on Id és la identitat en el conjunt C; en particular, g_σ és bijectiva amb inversa $g_{\sigma^{-1}}$, de manera que l'aplicació $\psi_g : G \longrightarrow S(C)$ està ben definida, i, a més a més, és un morfisme de grups. I recíprocament, si $\psi : G \longrightarrow S(C)$ és un morfisme de grups, l'aplicació $g_\psi : G \times C \longrightarrow C$ definida per $g_\psi(\sigma, x) := \psi(\sigma)(x)$ és una acció per l'esquera 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 $G \times C \longrightarrow C$ és una acció per la dreta d'un grup G en un conjunt C, l'aplicació $\psi : G \longrightarrow S(C)$ definida per $\psi(\sigma)(x) := x^{\sigma^{-1}}$ és un morfisme de grups i recíprocament, a tot morfisme de grups $\psi : G \longrightarrow S(C)$ 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 $G \longrightarrow S_n$.

Definició 5.6.7. Sigui $G \times C \longrightarrow C$, o bé, equivalentment, $G \longrightarrow S(C)$, 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 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. Sigui $G \longrightarrow S(C)$ 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 G qualsevol, 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 $G \times G \longrightarrow G$ donada per $(x, y) \mapsto xy$. D'altra banda, l'acció per conjugació; és a dir, l'aplicació $G \times G \longrightarrow G$ 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 tanslació, 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 i per l'esquerra són les mateixes.

Proposició 5.6.11. *Siguin k un cos, $\overline{k}$ un cos algebraicament tancat que conté k, $f(X) \in k[X]$ un polinomi no nul, $Z_f := \{\theta_1, \ldots, \theta_n\} \subseteq \overline{k}$ el conjunt de les arrels de $f(X)$, i $L := k(\theta_1, \ldots, \theta_n)$ el cos de descomposició del polinomi $f(X)$. Llavors, l'acció del grup de Galois $\mathrm{Gal}(L \mid k)$ en el conjunt de les arrels de $f(X)$ identifica $\mathrm{Gal}(L \mid k)$ amb un subgrup del grup simètric S_n.*

Demostració: Només cal veure que el morfisme de grups donat per l'acció, $\mathrm{Gal}(L \mid k) \longrightarrow S(Z_f) \simeq S_n$, és injectiu. Però això és immediat, ja que si $\sigma \in \mathrm{Gal}(L \mid k)$ és tal que $\sigma(\theta) = \theta$, per a tota arrel de $f(X)$, com que σ és un k-automorfisme de L i L està generat sobre k per les arrels de $f(X)$, σ és la identitat de L. □

Aquest resultat justifica la definició següent.

Definició 5.6.12. Sigui S_n el grup simètric sobre $\{1, 2, \ldots, n\}$. Un subgrup $H \subseteq S_n$ s'anomena transitiu si l'acció de H sobre $\{1, 2, \ldots, n\}$ és transitiva; és a dir, si donats $i, j \in \{1, 2, \ldots, n\}$, existeix $\sigma \in H$ tal que $\sigma(i) = j$.

Corol·lari 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 $L \mid k$ s'identifica amb un subgrup transitiu del grup simètric S_n.*

Demostració: En efecte, donades dues arrels del polinomi $f(X)$, θ_1, θ_2, existeix una k-immersió $\sigma : k(\theta_1) \longrightarrow k(\theta_2)$ tal que $\sigma(\theta_1) = \theta_2$; una extensió de σ a un k-automorfisme de L dóna 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. □

Exercici 5.6.14. Sigui $K \mid k$ 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, $L \mid k$, de grau, posem, [L:k]=n, el grup de Galois Gal($L \mid k$) 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 Gal($L \mid k$) 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 $A := \mathbb{Z}[a_n, x_1, \ldots, x_n]$ i el seu cos de fraccions $K := \mathbb{Q}(a_n, x_1, \ldots, x_n)$, i, de l'altra, els anells de polinomis en una indeterminada i de coeficients en A, $A[X]$, i de coeficients en K, $K[X]$.

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 $x_1, \ldots, x_n$ per a_n; més concretament, si $s_1(x_1, \ldots, x_n) := x_1 + \cdots + x_n$, $\ldots$, $s_n(x_1, \ldots, x_n) := x_1 \cdots x_n$ són els polinomis simètrics elementals en $x_1, \ldots, x_n$, i, si posem

$$a_i := (-1)^{n-i} a_n s_{n-i}(x_1, \ldots, x_n),$$

per a $0 \leq i \leq n-1$, el polinomi $f(X)$ admet l'expressió

$$f(X) = \sum_{i=0}^{n} a_i X^i \in A[X].$$

Evidentment, el grup simètric S_n actua de manera natural en K per permutació de les indeterminades $x_1, \ldots, x_n$, de manera que aquestes permutacions produeixen automorfismes de K, per tant, en virtut del teorema d'Artin,

l'extensió $K \mid K^{S_n}$ és una extensió de Galois de grup de Galois isomorf a S_n. Ara bé, $K^{S_n} = \mathbb{Q}(a_0, a_1, \ldots, a_n)$; és a dir, K^{S_n} és el cos de les funcions racionals simètriques de coeficients en $\mathbb{Q}(a_n)$ i indeterminades $x_1, \ldots, x_n$; aquest cos és isomorf al cos de fraccions racionals en les $n+1$ indeterminades $a_0, a_1, \ldots, a_n$, $f(X) \in \mathbb{Q}(a_0, a_1, \ldots, a_n)[X]$ és irreductible, i el cos de descomposició de $f(X)$ és $\mathbb{Q}(a_n, x_1, \ldots, x_n) = K$. 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. Sigui G un grup. S'anomena derivat de G el subgrup DG de G generat per tots els elements de G de la forma $a^{-1}b^{-1}ab$, per a $a, b \in G$.

Exercici 5.7.4. 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 τ i τ^{-1} descomponen en el mateix nombre de permutacions, i σ i σ^{-1} també. Per tant, tots els commutadors pertanyen a A_n; és a dir, $DA_n \subseteq DS_n \subseteq A_n$. Recíprocament, per a $n \geq 3$, un 3-cicle (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 $DS_2 = A_2 = \{1\}$. 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; això acaba la prova. □

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. □

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.* □

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, $a_0, a_1, \ldots, a_n \in k$, $a_n \neq 0$, 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 $\overline{k}$ que conté k siguin totes simples, $\theta_1, \ldots, \theta_n \in \overline{k}$ les arrels de $f(X)$, i $L \subseteq \overline{k}$ el cos de descomposició del polinomi. Posem $\delta := a_n^{n-1} \prod_{i<j} (\theta_i - \theta_j)$, de manera que $\Delta := \delta^2 \in k$ és el discriminant del polinomi $f(X)$, i sigui $K := k(\delta)$. Si identifiquem $\mathrm{Gal}(L \mid k)$ amb un subgrup del grup simètric S_n, aleshores el grup de Galois de l'extensió $L \mid K$ és $\mathrm{Gal}(L \mid K) = \mathrm{Gal}(L \mid k) \cap A_n$.*

DEMOSTRACIÓ: En fer una transposició de dues arrels del polinomi $f(X)$, i deixar les altres invariants, δ canvia de signe; per tant, en aplicar permutacions parelles, δ no varia. Així, δ és invariant exactament per les permutacions parelles, de manera que el cos fix per $\mathrm{Gal}(L \mid k) \cap A_n$ és $k(\delta) = K$. □

Corol·lari 5.7.10. *Amb les mateixes notacions i hipòtesis, $\mathrm{Gal}(L \mid k)$ és subgrup de A_n si, i només si, el discriminant Δ és un quadrat de k; és a dir, si, i només si, $k = K$.* □

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,

$$f(X) = a(X - x_1)(X - x_2)(X - x_3) = aX^3 + bX^2 + cX + d \\ \in \mathbb{Z}[a, x_1, x_2, x_3][X] \subseteq \mathbb{Q}(a, x_1, x_2, x_3)[X],$$

on 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 $\mathbb{Q}(a, x_1, x_2, x_3) \mid \mathbb{Q}(a, b, c, d)$ 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 $S_3 \supsetneq A_3 \supsetneq \{1\}$. 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, ρ, ρ^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 $L \mid k$, 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 δ^2 és el discriminant del polinomi $f(X)$ (cf. la proposició 5.7.9).

5.8.3. L'extensió $L \mid K$ 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 η de $L \mid K$ tal que $\eta^3 \in K$; volem determinar un tal element primitiu. Per a això, sigui $\sigma \in \mathrm{Gal}(L \mid K)$ el generador del grup de Galois determinat per la permutació $\sigma(x_1) = x_2$, $\sigma(x_2) = x_3$, i $\sigma(x_3) = x_1$ 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 $x_0 = x_3$, $x_4 = x_1$, $\ldots$, $x_{n+3} = x_n$, 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 $L \mid K$ tal que $\eta^3 \in K$.

Per a això, observem que

$$\begin{aligned}\eta = &\quad x_0+ &\quad \rho x_1+ &\quad \rho^2 x_2,\\ \sigma(\eta) = &\quad \rho^2 x_0+ &\quad x_1+ &\quad \rho x_2 = \rho^2\eta,\\ \sigma^2(\eta) = &\quad \rho x_0+ &\quad \rho^2 x_1+ &\quad x_2 = \rho\eta,\end{aligned}$$

de manera que els tres conjugats de η per $\mathrm{Gal}(L \mid K)$ són diferents; és a dir, η és un element de L de grau 3 sobre K i, per tant, un element primitiu de l'extensió $L \mid K$.

D'altra banda, $\sigma(\eta^3) = \sigma(\eta)^3 = \rho^6\eta^3 = \eta^3$, de manera que η^3 és fix per σ i, en conseqüència, $\theta := \eta^3 \in L^{\langle\sigma\rangle} = K$. Notem que η, $\sigma(\eta)$, $\sigma^2(\eta)$ 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 $L \mid K$ tal que $\eta'^3 \in K$, ja que

$$\begin{aligned}\eta' = &\quad x_0+ &\quad \rho^2 x_1+ &\quad \rho x_2,\\ \sigma(\eta') = &\quad \rho x_0+ &\quad x_1+ &\quad \rho^2 x_2 = \rho\eta',\\ \sigma^2(\eta') = &\quad \rho^2 x_0+ &\quad \rho x_1+ &\quad x_2 = \rho^2\eta',\end{aligned}$$

i $\theta' := \eta'^3 \in L^{\langle\sigma\rangle} = K$. Igual que abans, η', $\sigma(\eta')$, $\sigma^2(\eta')$ són les tres arrels cúbiques de $\theta' \in K$.

5.8.5. Ara, notem que el sistema lineal

$$\begin{aligned}x_0+ &\quad x_1+ &\quad x_2 = -\frac{b}{a},\\ x_0+ &\quad \rho x_1+ &\quad \rho^2 x_2 = \eta,\\ x_0+ &\quad \rho^2 x_1+ &\quad \rho x_2 = \eta',\end{aligned}$$

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 η, η' i ρ; i, com que $\rho^2 + \rho + 1 = 0$, $\eta^3 = \theta$ i $\eta'^3 = \theta'$, a disposar-ne de θ i θ'.

5.8.6. Es tracta, doncs, d'expressar θ i θ' per radicals a partir de a, b, c i d. Notem que, si $\tau \in \mathrm{Gal}(L \mid k)$ 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 τ és d'ordre 2, obtenim que els dos elements $\theta + \theta'$, $\theta\theta'$ són fixos per τ, de manera que pertanyen a $L^{\langle\tau\rangle} \cap K = k$. Per tant, θ i θ' 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, θ, θ' 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 θ, θ'. 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 α, β, ρ, θ, η i η' elements, d'un cos algebraicament tancat que contingui $\mathbb{Q}(a, x_0, x_1, x_2)$, tals que

$$\alpha^2 = \Delta,\ \beta^2 = -3,\ \rho = \frac{-1 + \beta}{2},\ \theta = \frac{-27q + 3\alpha\beta}{2},\ \eta^3 = \theta,\ \eta' = -\frac{3p}{\eta}.$$

Llavors,

$$\frac{1}{3}\left(-\frac{b}{a} + \eta + \eta' \right),\ \frac{1}{3}\left(-\frac{b}{a} + \rho^2\eta + \rho\eta' \right),\ \frac{1}{3}\left(-\frac{b}{a} + \rho\eta + \rho^2\eta' \right)$$

són expressions per radicals de les arrels x_0, x_1, x_2 de $f(X)$. □

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; començarem per l'equació general.

5.9.1. Considerem l'equació general de grau 4,

$$\begin{aligned} f(X) &= a(X-x_0)(X-x_1)(X-x_2)(X-x_3) \\ &= aX^4+bX^3+cX^2+dX+e \\ &\in \mathbb{Z}[a,x_0,x_1,x_2,x_3][X] \subseteq \mathbb{Q}(a,x_0,x_1,x_2,x_3)[X], \end{aligned}$$

on 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 $\mathbb{Q}(a,x_0,x_1,x_2,x_3) \mid \mathbb{Q}(a,b,c,d,e)$ 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 $S_4 \supsetneq A_4 \supsetneq V_4 \supsetneq C \supsetneq \{1\}$ 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 $S_4/V_4 \simeq S_3$; i, amb aquesta identificació, és $A_4/V_4 \simeq A_3$.

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. □

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 $L \mid k$ i els subgrups de S_4 que correspon als subgrups de la resolució de S_4. I també serà útil considerar una resolvent cúbica de $f(X)$.

Definició 5.9.4. Amb les notacions anteriors, posem

$$y_1 := x_0x_1 + x_2x_3, \qquad y_2 := x_0x_2 + x_1x_3, \qquad y_3 := x_0x_3 + x_1x_2,$$

i sigui $g(X) := a^3(X - y_1)(X - y_2)(X - y_3) \in L[X]$. El polinomi $g(X)$ s'anomena una resolvent cúbica 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* Δ_f, Δ_g *denoten, respectivament, els discriminants dels polinomis* $f(X)$, $g(X)$.

Demostració: El polinomi $g(X)$, pensat com a polinomi en les indeterminades x_0, x_1, x_2, x_3 i de coeficients en l'anell $\mathbb{Q}(a)[X]$, 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. □

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* $K_i = K(x_0 + x_i) = K(x_0 x_i) = K(x_j + x_k) = K(x_j x_k)$.

(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) Si $\sigma \in V_4$, 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 els elements y_1, y_2, y_3 és exactament V_4; és a dir, $\mathrm{Gal}(L \mid k(y_1, y_2, y_3)) = V_4$, 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 $x_0 + x_i$, $x_0 x_i$, $x_j + x_k$, $x_j x_k$; com que $\mathrm{Gal}(L \mid K) = V_4$, obtenim que $L^{C_i} = K(x_0 + x_i) = K(x_0 x_i) = K(x_j + x_k) = K(x_j x_k)$.

(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 $L \mid K$; és a dir, $L = K(x_i)$, per a $0 \leq i \leq 3$.

(d) Finalment, com que $[L : K] = \#\mathrm{Gal}(L \mid K) = \#V_4 = 4$, i com que x_0 és un element primitiu, $\mathrm{Irr}(x_0, K)(X) \in K[X]$ 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 $K[X]$. □

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 $y_1 = x_0 x_1 + x_2 x_3$, $y_2 = x_0 x_2 + x_1 x_3$, $y_3 = x_0 x_3 + x_1 x_2$, 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 $L \mid K_1$, 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,

$$\mathrm{Irr}(x_0, K_1)(X) = (X - x_0)(X - x_1) = X^2 - (x_0 + x_1)X + x_0x_1;$$

i, anàlogament,

$$\mathrm{Irr}(x_2, K_1)(X) = (X - x_2)(X - x_3) = X^2 - (x_2 + x_3)X + x_2x_3.$$

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 $K_1 \mid K$, de manera que satisfà una equació de grau 2 sobre K; més concretament, com que $\mathrm{Gal}(K_1 \mid K) = \mathrm{Gal}(L \mid K)/\mathrm{Gal}(L \mid K_1) \simeq \{1, (0,2)(1,3)\}$, obtenim que

$$\begin{aligned}
\mathrm{Irr}(x_0 + x_1, K)(X) &= (X - (x_0 + x_1))(X - (x_2 + x_3)) \\
&= X^2 - (x_0 + x_1 + x_2 + x_3)X + (x_0 + x_1)(x_2 + x_3) \\
&= X^2 + \frac{b}{a}X + \frac{c}{a} - y_1, \\
\mathrm{Irr}(x_0x_1, K)(X) &= (X - x_0x_1)(X - x_2x_3) = \\
&= X^2 - (x_0x_1 + x_2x_3)X + x_0x_1x_2x_3 = \\
&= X^2 - y_1X + \frac{e}{a}.
\end{aligned}$$

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 $K_1 \mid K$; 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 proporciona la igualtat

$$\begin{aligned}
\left(\frac{b^2}{a^2} - 4\frac{c}{a} + 4y_1\right)\left(y_1^2 - 4\frac{e}{a}\right) &= \frac{1}{a^3}\left(4g(y_1) + ab^2y_1^2 + 4ad^2 - 4abdy_1\right) \\
&= \left(\frac{by_1 - 2d}{a}\right)^2,
\end{aligned}$$

ja que y_1 és arrel de $g(X)$. Així, si α 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 β i γ 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, β^2 i γ^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 de la resolvent cúbica $g(X)$, que podem suposar expressada per radicals a partir de a, b, c, d, e, i α, β, γ 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

$$\frac{-b\alpha - by_1 + 2d + 2a\alpha\beta}{4a\alpha}, \quad \frac{-b\alpha - by_1 + 2d - 2a\alpha\beta}{4a\alpha},$$
$$\frac{-b\alpha + by_1 - 2d + 2a\alpha\gamma}{4a\alpha}, \quad \frac{-b\alpha + by_1 - 2d - 2a\alpha\gamma}{4a\alpha}.\square$$

Corol·lari 5.9.10. *Siguin k un cos qualsevol de característica diferent de 2 i de 3, $f(X) := aX^4 + bX^3 + cX^2 + dX + e \in k[X]$ un polinomi, 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 α, β, γ tals que

$$\alpha^2 = y_1^2 - 4\frac{e}{a} \neq 0, \quad \beta^2 = \left(\frac{-b\alpha - by_1 + 2d}{2a\alpha}\right)^2 - 4\frac{y_1 + \alpha}{2},$$
$$\gamma^2 = \left(\frac{-b\alpha + by_1 - 2d}{2a\alpha}\right)^2 - 4\frac{y_1 - \alpha}{2}.$$

Llavors, les arrels del polinomi $f(X)$ són

$$\frac{-b\alpha - by_1 + 2d + 2a\alpha\beta}{4a\alpha}, \qquad \frac{-b\alpha - by_1 + 2d - 2a\alpha\beta}{4a\alpha},$$
$$\frac{-b\alpha + by_1 - 2d + 2a\alpha\gamma}{4a\alpha}, \qquad \frac{-b\alpha + by_1 - 2d - 2a\alpha\gamma}{4a\alpha}.$$

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 $\mathbb{Z}[a, x_0, x_1, x_2, x_3] \longrightarrow k(\alpha_0, \alpha_1, \alpha_2, \alpha_3)$ que envia la indeterminada a a l'element $a \in k$, i les indeterminades x_i als elements α_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. □

5.10 Construccions amb regle i compàs

Sovint haurem sentit a parlar de tres problemes clàssics:

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 de les matemàtiques, 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 regle i compàs, encara cal precisar què vol dir "construir amb regle i compàs".

5.10.4. Considerarem el model de pla euclidià donat pel cos $\mathbb{C}$ dels nombres complexos; és a dir, 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 regle (sense distàncies marcades en ell) i un compàs?

Cal definir acuradament què entendrem per construir un punt amb regle i compàs a partir d'uns quants punts donats. Les operacions vàlides seran les següents:

(a) Donats dos punts diferents ja construïts, dibuixar qualsevol segment rectilini de longitud finita que contingui els dos punts (és a dir, usar el regle).
(b) Donats tres punts ja construïts, dos d'ells, com a mínim, diferents, dibuixar una circumferència, o un arc de circumferència, amb centre en un d'ells i radi la distància entre dos diferents dels tres punts (és a dir, usar el compàs).

Ara podem dir què entendrem per construir un nou punt.

Definició 5.10.5. Sigui C_i un conjunt no buit de punts del pla. El conjunt C_{i+1} dels punts que es construeixen amb regle i compàs en un pas a partir de C_i és format pels punts que són:

(a) Els punts de C_i.

(b) El punt intersecció de dos segments rectilinis no paral·lels dibuixats, cadascun d'ells, a partir de dos punts diferents de C_i.

(c) Els dos punts intersecció de dues circumferències no tangents dibuixades, cadascuna d'elles, a partir de dos o tres punts diferents de C_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_i, i de manera que el segment i l'arc no siguin tangents.

Direm que un punt P del pla és constructible a partir d'un conjunt C_0 si existeix $i \in \mathbb{N}$ tal que $P \in C_i$.

Exercici 5.10.6. A partir de punts i segments ja construïts, és possible:

(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;

(e) construir un segment paral·lel a un segment donat que contingui un punt donat exterior al segment.

Observació 5.10.7. 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 constructibles 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).

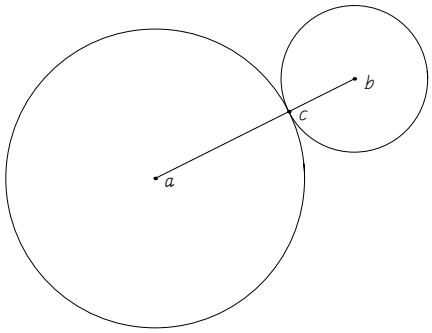

Figura 5.1: Punt de tangència de dues circumferències

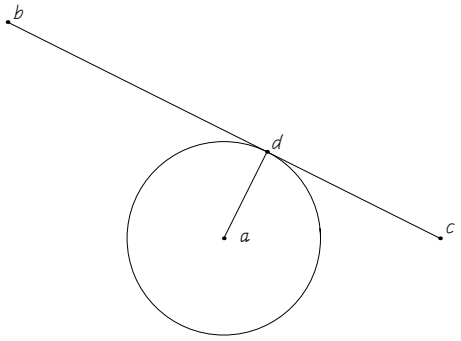

Figura 5.2: Punt de tangència d'una circumferència i un segment

5.10.8. 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 5.10.9. A partir d'angles ja construïts, és possible:

(a) transportar un angle donat i fer-lo adjacent a un segment donat;

(b) bisecar un angle donat;

(c) sumar i restar angles donats.

Proposició 5.10.10. *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 constructibles amb regle 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 del pla, és a dir, dos nombres complexos, la regla del paral·lelògram ens permet construir la seva suma; i, donat un punt del pla, podem construir el seu oposat respecte a l'origen; per tant, el conjunt dels punts del pla constructibles amb regle i compàs 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 regle 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). I, finalment, la possibilitat de sumar i restar angles amb regle 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 (només cal tenir present la forma polar dels nombres complexos). Per tant, el conjunt dels punts del pla constructibles amb regle i compàs és tancat per productes i quocients; és a dir, és un subcòs de $\mathbb{C}$. Aquest cos conté, òbviament, $\mathbb{Q}$ (ja que conté $0, 1$), i C_0 (per hipòtesi); per tant, conté el cos engendrat 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 regle i compàs, només cal veure que podem construir les arrels quadrades dels nombres reals positius; però això

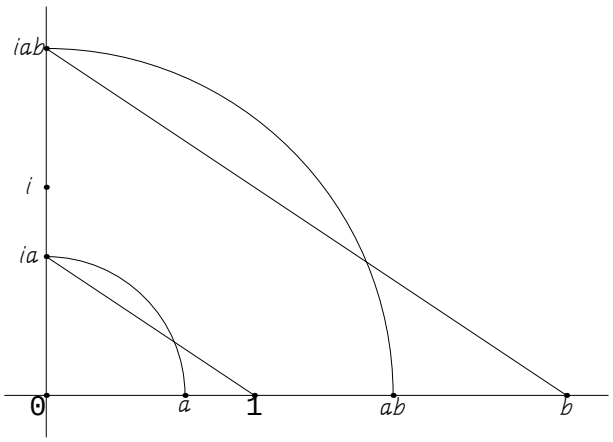

Figura 5.3: Producte de nombres reals positius

es pot fer a partir de la construcció d'una circumferència de diàmetre $d+1$, on d és el nombre del qual volem construir la seva arrel quadrada, i 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). □

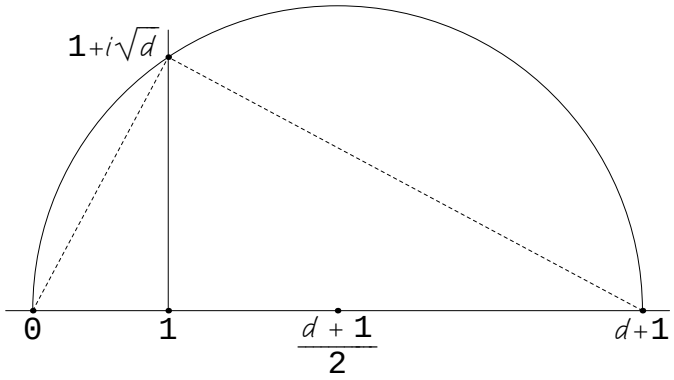

Figura 5.4: Arrel quadrada d'un nombre real positiu

Teorema 5.10.11. *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 constructibles amb regle i compàs a partir de C_0. Sigui $k \subseteq \mathbb{C}$ el cos generat sobre $\mathbb{Q}$ per C_0. Llavors, si α és un punt qualsevol de C, l'extensió $k(\alpha) \mid k$ és de grau una potència de 2; a més a més, l'extensió $k(\alpha) \mid k$ és radical i admet una cadena de subcossos de la forma

$$k \subseteq k(\theta_1) \subseteq k(\theta_1, \theta_2) \subseteq \cdots \subseteq k(\theta_1, \ldots, \theta_m) = k(\alpha)$$

tal que $\theta_i^2 \in k(\theta_1, \ldots, \theta_{i-1})$. I recíprocament, si $\alpha \in \mathbb{C}$ és un nombre complex tal que el cos $k(\alpha)$ admet una cadena com aquesta, llavors α és constructible amb regle 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 α es construeix a partir d'una quantitat finita de punts de C_0 amb un nombre finit d'operacions vàlides. Ara bé, cada operació vàlida 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 α a partir de C_0 dóna una successió d'elements de $\mathbb{C}$ tal com la $\theta_1, \ldots, \theta_m$, 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 regle i compàs, tots els elements de $k(\theta_1, \ldots, \theta_m)$ es poden construir amb regle i compàs a partir de k, és a dir, a partir de C_0. □

Ja només amb aquest resultat, podem demostrar la impossibilitat de la construcció amb regle i compàs de molts nombres complexos. Per exemple:

5.10.12. 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, α, és constructible amb regle

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 α, 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 α, és a dir, el cub de volum 2, no és constructible amb regle i compàs a partir del cub d'aresta unitat.

5.10.13. Impossibilitat de la trisecció de l'angle. En general, hi ha alguns angles que es poden trisecar; per exemple, podem construir amb regle i compàs l'angle d'un sisè de volta (o l'angle d'un terç de volta). Però aquests dos angles no poden ser trissecats amb regle i compàs. En efecte, donar l'angle d'un terç de volta equival a donar una arrel cúbica primitiva de la unitat, posem ρ. Per tant, el problema de la trisecció d'aquest angle equival al de la construcció amb regle i compàs d'una arrel novena primitiva de la unitat, posem ζ, a partir de $0,1,\rho$. Ara bé, $[\mathbb{Q}(\zeta):\mathbb{Q}(\rho)]=\dfrac{[\mathbb{Q}(\zeta):\mathbb{Q}]}{[\mathbb{Q}(\rho):\mathbb{Q}]}=\dfrac{\varphi(9)}{\varphi(3)}=\dfrac{6}{2}=3$, que no és una potència de 2.

Més generalment, si α és un angle qualsevol, construir α amb regle i compàs equival a construir $\cos(\alpha)$ amb regle i compàs. La relació algebraica entre el cossinus de l'angle α i el cossinus 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 α es podrà trisecar amb regle i compàs si, i només si, l'extensió $\mathbb{Q}(\cos(\alpha/3)) \mid \mathbb{Q}(\cos(\alpha))$ és trivial o bé quadràtica.

Observació 5.10.14. Genèricament, el polinomi $4X^3-3X-\cos(\alpha)$ és irreductible en $\mathbb{Q}(\cos(\alpha))[X]$, de manera que, genèricament, α no es podrà trisecar amb regle i compàs. Per exemple, si $\cos(\alpha)$ és un nombre transcendent, llavors 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 α, encara que $\cos(\alpha)$ sigui un nombre algebraic.

5.10.15. Impossibilitat de la quadratura del cercle. Aquest problema equival a construir amb regle i compàs, a partir del cercle de radi 1, això és, a partir de $0,1$, l'aresta d'un quadrat d'àrea π; és a dir, a construir amb regle i compàs, a partir de $0,1$, el nombre $\sqrt{\pi}$. Ara bé, aquest nombre no és ni tan sols algebraic sobre $\mathbb{Q}$. Per tant, no pot ser de grau potència de 2 sobre $\mathbb{Q}$.

5.11 Seccions del cercle constructibles

Una pregunta clàssica, a la qual respongué Gauss, és quines seccions circulars són constructibles amb regle i compàs; és a dir, quines arrels de la unitat són constructibles amb regle i compàs.

Per a respondre aquesta qüestió, és útil caracteritzar els nombres constructibles amb regle i compàs d'una altra manera. Recordem que hem vist que, donat un nombre $\alpha \in \mathbb{C}$, i si posem $k := \mathbb{Q}(C_0)$, α és constructible amb regle i compàs a partir de C_0 si, i només si, l'extensió $k(\alpha) \mid k$ és radical i admet una cadena de subcossos de la forma

$$k \subseteq k(\theta_1) \subseteq k(\theta_1, \theta_2) \subseteq \cdots \subseteq k(\theta_1, \ldots, \theta_m) = k(\alpha)$$

tal que $\theta_i^2 \in k(\theta_1, \ldots, \theta_{i-1})$. Podem caracteritzar aquest fet d'una altra manera més convenient per als nostres propòsits.

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 constructible amb regle i compàs a partir de C_0 si, i només si, la clausura normal de l'extensió $k(\alpha) \mid k$ és de grau una potència de 2.*

Demostració: Suposem que α és constructible amb regle i compàs a partir de C_0, i sigui $k \subseteq k(\theta_1) \subseteq k(\theta_1, \theta_2) \subseteq \cdots \subseteq k(\theta_1, \ldots, \theta_m) = k(\alpha)$ una cadena radical de manera que $\theta_i^2 \in k(\theta_i, \ldots, \theta_{i-1})$, per a $1 \leq i \leq m$. Si $L \mid k$ és la clausura normal de l'extensió $k(\alpha) \mid k$, llavors $L = \bigcup_\sigma \sigma(k(\alpha)) = \bigcup_\sigma k(\sigma(\alpha))$, quan σ recorre $\mathrm{Gal}(L \mid k)$. Ara bé, per a tot $\sigma \in \mathrm{Gal}(L \mid k)$, és $\sigma(\theta_i)^2 \in k(\sigma(\theta_1), \ldots, \sigma(\theta_{i-1}))$, de manera que podem construir una cadena radical per a l'extensió $L \mid k$ afegint, successivament, els elements $\sigma(\theta_i)$, per a $1 \leq i \leq m$ i per a $\sigma \in \mathrm{Gal}(L \mid k)$; així, obtenim una cadena radical d'extensions quadràtiques per a $L \mid k$, de manera que el grau $[L : k]$ és una potència de 2.

Suposem, ara, que la clausura normal $L \mid k$ de l'extensió $k(\alpha) \mid k$ és de grau potència de 2. Si provem que el grup de Galois $\mathrm{Gal}(L \mid k)$ és resoluble, llavors podrem trobar una resolució de $\mathrm{Gal}(L \mid k)$ per una cadena de subgrups tals que els quocients successius siguin d'ordre 2, de manera que l'extensió

$L \mid k$ admetrà una cadena radical formada per extensions quadràtiques, com cal provar. I el fet que $\mathrm{Gal}(L \mid k)$ és un grup resoluble és un cas particular del resultat següent de teoria de grups. □

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. □

Ara, la demostració del teorema és senzilla.

Demostració: Siguin $G_0 := G$, 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. □

Amb la caracterització que hem fet dels nombres constructibles amb regle i compàs, podem fer la caracterització dels n-àgons regulars constructibles amb regle i compàs; és a dir, de les arrels de la unitat constructibles amb

regle i compàs, o, si es vol, de les seccions circulars constructibles amb regle i compàs.

Corol·lari 5.11.5. *Sigui $n \geq 3$ un nombre natural. Un n-àgon regular és constructible amb regle i compàs si, i només si, $\varphi(n)$ és una potència de 2.*

DEMOSTRACIÓ: Un n-àgon regular és constructible amb regle 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. □

Corol·lari 5.11.6. *Els n-àgons regulars constructibles amb regle 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 $p_1, \ldots, p_m$ són nombres primers diferents 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 $p_1, \ldots, p_m$ 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. □

Observació 5.11.7. 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 α sigui constructible amb regle i compàs sobre $\mathbb{Q}$. Cal que la clausura normal de l'extensió sigui de grau potència de 2.

Per exemple, si α 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 $\mathrm{Gal}(L \mid \mathbb{Q}) \simeq S_4$.

En efecte, la resovent cúbica de $f(X)$ és el polinomi $g(X) = X^3 - 8X - 4$, el discriminant del qual és $-4 \cdot (-8)^3 - 27 \cdot (-4)^2 = 1616 = 2^4 \cdot 101$, 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 $\mathrm{Gal}(L \mid \mathbb{Q})$ 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 $L \mid \mathbb{Q}$ 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 5.11.8. L'únic subgrup transitiu de S_4 que admet per quocient un grup isomorf a S_3 és el propi S_4.

Acabarem aquesta secció amb un estudi que ens explicarà quins poden ser els grups de Galois dels cossos de descomposició de les equacions 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 5.11.9. *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, $\mathrm{Gal}(L \mid k)$ és isomorf a un dels tres grups V_4, de Klein, C_4, cíclic d'ordre 4, o bé $D_{2\cdot 4}$, diedral d'ordre 8.*

Observació 5.11.10. 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

$$D_{2\cdot 4} = V_4 \cup \{(1,2,3,4), (1,4,3,2), (1,3), (2,4)\}$$

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, $\mathrm{Gal}(L \mid k)$ 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 5.11.11. Els subgrups transitius de S_4 d'ordre potència de 2, són isomorfs als subgrups V_4, C_4, o bé $D_{2\cdot 4}$ explicitats en l'observació anterior.

Exercici 5.11.12. Sigui $L \mid k$ una extensió de Galois de cossos de característica diferent de 2 i de 3 i tal que el grup de Galois $\mathrm{Gal}(L \mid k)$ sigui isomorf a un dels grups V_4, de Klein, C_4, cíclic d'ordre 4, o bé $D_{2\cdot 4}$, 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 $c, e \in k$.

Apèndix A

Definicions i propietats bàsiques

A.1 Grups

A.1.1 Grups

Definició A.1.1. Un *grup* G és un conjunt amb una operació interna, que 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

(a) $\forall a, b, c \in G\ a(bc) = (ab)c$;

(b) $\exists 1 \in G\ \forall a \in G\ 1a = a1 = a$;

(c) $\forall a \in G\ \exists b \in G\ ab = ba = 1$.

I els grups abelians són els grups per als quals se satisfà, a més a més, la propietat

(d) $\forall a, b \in G\ ab = ba$.

A.1.3. 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.

A.1.2 Subgrups normals

Observació A.1.4. El nom de subgrup normal que es dóna als subgrups normals no és arbitrari; la seva definició prové de copiar les propietats dels subgrups que corresponen a les extensions normals de cossos.

Exercici A.1.5. Siguin G, H, grups qualssevol, $N \subseteq G$ un subgrup normal, $\pi : G \longrightarrow G/N$ la projecció canònica, i $f : G \longrightarrow H$ un morfisme qualsevol. Condició necessària i suficient perquè existeixi un morfisme de grups $\overline{f} : G/N \longrightarrow H$ tal que $f = \overline{f} \circ \pi$ és que $N \subseteq \mathrm{Ker}(f)$. A més a més, en aquest cas, f és exhaustiu si, i només si, ho és $\overline{f}$.

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*.

Així, 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 $1 = 0$.

A.2.2. 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.2.3. Com a exemples bàsics, 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.2.4. Donats anells A, B, un *morfisme d'anells* de A en B és una aplicació $f : A \longrightarrow B$ 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.2.5. Les condicions $f(0) = 0$ i $f(-a) = -f(a)$ es dedueixen de les dues primeres i dels axiomes d'anell, però no succeeix el mateix per a la condició $f(1) = 1$; cal imposar-la.

A.2.6. Per a tot anell A, la *identitat* $\mathrm{id}_A : A \longrightarrow A$, definida per $a \mapsto a$, és un morfisme d'anells.

Definició A.2.7. 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 $g \circ f = \mathrm{id}_A$ i $f \circ g = \mathrm{id}_B$.

A.2.8. Els isomorfismes d'anells són els morfismes d'anells bijectius.

A.2.3 Subanells

Definició A.2.9. Donat un anell A, un *subanell* de A és un subconjunt $B \subseteq A$ tal que $1 \in B$ i per a tot $a, b \in B$ és $a + b, ab \in B$.

A.2.10. Aquestes condicions impliquen que les operacions de A es poden restringir a B; llavors, els axiomes d'anell se satisfan immediatament, perquè imposem 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.2.11. En particular, A és un subanell de A; però si $A \neq \{0\}$, llavors $\{0\}$ no és un subanell de A.

A.2.12. Els subanells d'un anell A són exactament les imatges dels morfismes d'anells $B \longrightarrow A$, per a tots els anells B per als quals n'existeixi algun.

Definició A.2.13. 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.2.14. Si A és un anell i $\{B_i\}_{i\in I}$ s 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.

A.2.4 Elements invertibles. Cossos

Definició A.2.15. 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 $b \in k$ tal que $ab = ba = 1$.

Definició A.2.16. Un anell commutatiu k s'anomena un *cos* si $0 \neq 1$ i tot element no nul de k és invertible.

A.2.17. 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.2.18. Sigui A un anell commutatiu. Un element $a \in A$ s'anomena un *divisor de zero* si existeix un element $b \in A$, $b \neq 0$, tal que $ab = 0$.

A.2.19. Si l'anell A és diferent de l'anell $\{0\}$, l'element 0 és un divisor de zero.

Definició A.2.20. Un *domini d'integritat* és un anell commutatiu A tal que $1 \neq 0$ i que no té cap més divisor de zero que 0.

A.2.21. 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.2.22. D'altra banda, l'anell quocient $\mathbb{Z}/6\mathbb{Z}$ no és un domini d'integritat. En efecte, els divisors de zero de $\mathbb{Z}/6\mathbb{Z}$ són els elements 0, 2, 3 i 4.

A.2.23. Més generalment, per a un nombre enter $n \geq 2$, l'anell quocient $\mathbb{Z}/n\mathbb{Z}$ 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, $\mathrm{mcd}(n, a) \neq 1$.

A.2.24. 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 $z \in k$ i $za = 0$, tenim que $0 = 0 \cdot b = zab = z \cdot 1 = z$; per tant, l'únic divisor de zero de k és 0.

A.2.25. Com a conseqüència, tot subanell d'un cos o d'un domini d'integritat és un domini d'integritat.

A.2.26. 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.

Exercici A.2.27. Sigui A un domini d'integritat. En el conjunt $A \times (A - \{0\})$, 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 $\dfrac{a}{b}$ la classe d'equivalència de la parella (a, b) i per K el conjunt de totes les classes d'equivalència. En K, podem definim les operacions suma i producte per les fórmules

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + cb}{bd}, \qquad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd},$$

per a $a, b, c, d \in A$, $b, d \neq 0$.

(b) El conjunt K amb aquestes operacions és un cos. El cos K s'anomena el *cos de fraccions* de A.

(c) L'aplicació $A \longrightarrow K$ definida per l'assignació $a \mapsto \dfrac{a}{1}$ és un morfisme d'anells injectiu, de manera que podem identificar cada element $a \in A$ amb la classe $\dfrac{a}{1} \in K$ i l'anell A amb un subanell de K.

(d) Si $f : A \longrightarrow B$ és un morfisme d'anells tal que per a tot $a \in A - \{0\}$ l'element $f(a) \in B$ és invertible, aleshores f s'estén de manera única a un morfisme d'anells $K \longrightarrow B$, que és injectiu si $B \neq \{0\}$. Com a conseqüència, K és el més petit de tots els cossos que contenen A com a subanell.

A.2.6 L'anell producte

Definició A.2.28. 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, si $\alpha := \{a_i\}_{i\in I}$, $\beta := \{b_i\}_{i\in I} \in A$, 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 $I = \{1, 2, \ldots, n\}$, s'escriu $A = \prod_{i=1}^{n} A_i = A_1 \times A_2 \times \cdots \times A_n$.

A.2.29. 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.2.30. 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 ψ_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.2.31. 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 $\psi : A \longrightarrow A^I$ definida per $a \mapsto \{a_i\}_{i\in I}$, on $a_i := a$, per a tot $i \in I$. Llavors, ψ s 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 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 són els ideals A i $\{0\}$; són ideals bilaterals.

A.3.4. Si $f : A \longrightarrow B$ és un morfisme d'anells, el seu *nucli*, $\ker(f) := \{a \in A : f(a) = 0\}$, és un ideal bilateral de A.

A.3.5. Més generalment, si $f : A \longrightarrow B$ 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 $k \longrightarrow A$ és injectiu.

A.3.8. Si A és un anell i $\{\mathfrak{a}_i\}_{i\in I}$ s 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 quocient

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 de A és exactament la condició que es necessita a fi que el grup abelià quocient $(A/\mathfrak{a}, +)$ sigui un anell i el morfisme de projecció $A \longrightarrow A/\mathfrak{a}$, donat per $a \mapsto a + \mathfrak{a}$, sigui un morfisme d'anells. D'aquesta manera s'obté l'*anell quocient* de A per l'ideal $\mathfrak{a}$. Si l'anell A és commutatiu, llavors l'anell quocient $A/\mathfrak{a}$ també és commutatiu.

A.3.13. Anàlogament al cas dels grups commutatius, el morfisme de projecció $A \longrightarrow A/\mathfrak{a}$ permet definir una bijecció entre el conjunt dels ideals de l'anell quocient $A/\mathfrak{a}$ i el conjunt dels ideals de A que contenen $\mathfrak{a}$. I se satisfà el *teorema d'isomorfia*: si $f : A \longrightarrow B$ és un morfisme d'anells, l'anell quocient $A/\ker(f)$ és isomorf a l'anell imatge $f(A)$.

A.3.14. 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 $A \longrightarrow A/\mathfrak{a}$ 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.3.19) i (A.3.20) per a les definicions d'ideal primer i d'ideal maximal).

A.3.3 Dominis d'ideals principals

Definició A.3.15. 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.3.16. Com que $\{0\} = 0A$ i $A = 1A$, els ideals trivials són principals.

Definició A.3.17. Un *domini d'ideals principals*, o *domini principal*, és un domini d'integritat tal que tots els seus ideals són principals.

Observació A.3.18. No és cert que tot subanell d'un domini d'ideals principals sigui un domini d'ideals principals. Per exemple, $\mathbb{Q}[X]$ és un domini d'ideals principals, perquè $\mathbb{Q}$ és un cos, mentre que $\mathbb{Z}[X]$, 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.3.19. 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.3.20. 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.3.21. 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.3.22. Sigui A un anell; llavors, existeix un únic morfisme d'anells $\mathbb{Z} \longrightarrow A$.

En efecte, la imatge de $1 \in \mathbb{Z}$ ha d'ésser $1 \in A$ i, en conseqüència, la imatge de $n = \overbrace{1 + \cdots + 1}^{n} \in \mathbb{N}$ en A ha d'ésser $n := \overbrace{1 + \cdots + 1}^{n} \in A$ 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.3.23. Sigui A un anell qualsevol. El nucli de l'únic morfisme d'anells $\mathbb{Z} \longrightarrow A$ 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 únic nombre enter $c \geq 0$. Aquest nombre enter c s'anomena la *característica* de l'anell A.

A.3.24. 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.

Exercici A.3.25. Sigui A un anell de característica $c > 0$. Llavors, c és el menor nombre natural no nul tal que $c = \overbrace{1 + \cdots + 1}^{c} = 0$ en A. Si A és de característica 0, llavors per a tot nombre natural $c > 0$ és $c = \overbrace{1 + \cdots + 1}^{c} \neq 0$ en A.

A.3.26. 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.

Apèndix B

El lema de Zorn

Algunes vegades, els axiomes usuals de la teoria de conjunts no són suficients per a explicar propietats interessants de les diferents teories; cal usar un altre axioma: l'axioma de l'elecció.

Aquest axioma és tan evident que, molt sovint, passaria desapercebut. Una de les maneres equivalents de formular-lo és la següent:

Axioma de l'elecció. El producte cartesià d'una família no buida de conjunts no buits és un conjunt no buit.

Formulat d'aquesta manera, sembla que, efectivament, aquest axioma s'hauria d'acceptar sense discussió. (Esteu segurs que no l'heu usat implícitament alguna vegada?) En canvi, és equivalent, per exemple, a la propietat següent, no tan evident.

Teorema de Zermelo. Sigui C un conjunt no buit qualsevol. Existeix en C una relació de bon ordre.

Observació B.0.27. 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, per a tot subconjunt $D \subseteq C$, $D \neq \varnothing$, 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 sembla evident; però hom pot pensar en l'exemple següent: Donat un conjunt infinit

no numerable C, sigui $\leq$ un bon ordre en C. Siguin $a_1 \in C$ 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. Podríem 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.0.28. Les preguntes anteriors es poden contestar, d'una manera completament satisfactòria però que ens portaria massa lluny, 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.0.29. 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 $a \in D$.

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.

Teorema de Tychonov. 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.0.30. Tot espai vectorial té una base.

B.0.31. Tot anell commutatiu té un ideal maximal.

B.0.32. Tot anell té un ideal maximal per l'esquerra, un ideal maximal per la dreta, i un ideal maximal.

B.0.33. Tot cos és subcòs d'un cos algebraicament tancat.

B.0.34. 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. Ara, i a tall d'exemple, demostrarem que tot espai vectorial diferent de (0) té una base, resultat que hem usat en el curs per a definir el grau d'una exensió de cossos qualsevol.

Demostració: 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 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. Sigui, doncs, $\mathcal{D} \subseteq \mathcal{C}$ un subconjunt no buit de $\mathcal{C}$ i totalment ordenat. Posem F la reunió de tots els elements de $\mathcal{D}$ (que són subconjunts de E K-linealment independents). 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 finitut 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, contra la definició de $\mathcal{D}$ com a subconjunt de $\mathcal{C}$. Per tant, F és un conjunt K-linalment 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 C. Si veiem que B és un conjunt de generadors de E com a K-espai vectorial, obtindrem que B és una base de E, de manera que el resultat estarà provat. Ara bé, si B no engendrés 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; però 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. $\square$