# Polinomis i cossos finits

## 5.2 Anells. L'anell dels nombres enters

Recordem les definicions axiomàtiques d'anell commutatiu i de cos.

Un *anell commutatiu* és una terna $(A, +, \cdot)$ formada per un conjunt $A$ i dues operacions definides a $A$ que tenen les propietats següents:

1) $(a+b)+c = a+(b+c)$ per a tot $a, b, c \in A$;

2) $a+b = b+a$ per a tot $a, b \in A$;

3) hi ha un element, dit *neutre de la suma* i denotat usualment per 0, tal que $a+0 = a$ per a tot $a \in A$;

4) per cada $a \in A$ existeix un element, dit l'*oposat* de $a$ i denotat per $-a$, tal que $a+(-a) = 0$;

5) $(ab)c = a(bc)$ per a tot $a, b, c \in A$;

6) $ab = ba$ per a tot $a, b \in A$;

7) hi ha un element, dit *neutre del producte* i denotat usualment per 1, tal que $a \cdot 1 = a$ per a tot $a \in A$;

8) $a(b+c) = ab+ac$ per a tot $a, b, c \in A$.

Per abús de llenguatge es parla de l'*anell* $A$, i les operacions es sobreentenen pel context. Si $A$ és un conjunt amb un únic element 0 i definim la suma i el producte per $0+0 = 0 = 0 \cdot 0$, obtenim un anell dit *trivial*.

La propietat 1 s'anomena *associativa*. La conseqüència immediata de l'associativa es que es poden escriure sumes reiterades sense parèntesi. Per exemple, $a+b+c+d$ té un significat inequívoc perquè agrupem com agrupem els sumands, el resultat és el mateix:

$$\begin{aligned}(a+(b+c))+d &= ((a+b)+c)+d \\ &= (a+b)+(c+d) \\ &= a+(b+(c+d)) \\ &= a+((b+c)+d).\end{aligned}$$

El mateix podem dir per a la propietat 5, l'associativa del producte.

La propietat 2 és la *commutativa* de la suma. Juntament amb l'associativa permet, no només eliminar parèntesis, sinó permutar els elements a operar. Per exemple, $a+b+c=c+b+a$. Un comentari similar és vàlid per a la propietat 6, la commutativa del producte.

La propietat 8 s'anomena *distributiva* del producte respecte a la suma, i és la propietat que relaciona ambdues operacions. Llegida de dreta a esquerra és el que en llenguatge col·loquial es diu *treure factor comú*.

Notem que les propietats 1–3 de la suma guarden un evident paral·lelisme amb les propietats 5–7 del producte. En canvi, no s'exigeix una propietat similar a la 4 per al producte. Un element $u \in A$ és *invertible* si existeix un $v \in A$ tal que $uv = 1$; en aquest cas l'element $v \in A$ és unic, es diu l'*invers* de $u$ i es denota per $u^{-1}$. El conjunt dels elements invertibles es denota per $A^*$. Un anell $A$ no trivial és un *cos* si $A^* = A \setminus \{0\}$, és a dir, si tot element diferent de 0 (el neutre per la suma) té invers.

Als apartats següents veurem uns quants exemples d'anells commutatius i de cossos. El que ens interessa en aquest punt és l'*anell dels nombres enters*

$$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$$

amb la suma i el producte habituals. Resumirem en aquest apartat (sense demostracions) les propietats rellevants per a la discussió subsegüent.

1) L'anell $\mathbb{Z}$ té només dos invertibles, 1 i $-1$, cadascun dels quals és el seu propi invers.

2) $ab = 0$ implica $a = 0$ o $b = 0$, per a tot $a, b \in \mathbb{Z}$. Aquesta propietat, que sembla molt natural, no es compleix en alguns anells importants com els que es construeixen a l'apartat 5.3.

3) Com a conseqüència de la remarca anterior, es pot demostrar la propietat de *simplificació*: per a tot $a, b, x \in \mathbb{Z}$, $ax = bx$ i $x \neq 0$ implica $a = b$.

4) En el conjunt dels enters hi ha definida la relació d'ordre $\leq$ usual, les propietats de la qual donarem per conegudes, en particular el seu comportament respecte a les operacions suma i producte.

5) També donarem per conegut el concepte i propietats del *valor absolut* d'un nombre enter.

El teorema de la divisió és crucial:

**5.2.1 Teorema (de la divisió)** *Si $a$ i $b$ són dos enters i $b \neq 0$, aleshores existeixen dos enters $q$ i $r$ únics tals que*

$$a = bq + r, \quad 0 \leq r < |b|.$$

L'enter $q$ del teorema anterior és el *quocient* de la divisió de $a$ per $b$, i $r$ el *residu*. Si el residu és zero, és a dir, si $a = bq$, es diu que $a$ és *múltiple* de $b$ i que $b$ és *divisor* o un *factor* de $a$ i s'indica $b|a$. Per exemple, 0 es múltiple de tot enter $b \neq 0$. Noteu que, per a tot enter $a$, els enters $a, -a, 1, -1$ són divisors de $a$. Aquests quatre divisors s'anomenen *impropis* i tots els altres, si n'hi ha, *propis*. Un nombre *primer* és un enter $\geq 2$ sense divisors propis. El teorema següent dóna una propietat essencial i ben coneguda dels nombres primers.

**5.2.2 Proposició** *Per a tot enter $a \neq 0$ existeixen un invertible $\epsilon \in \{1, -1\}$, primers $p_1 < p_2 < \cdots < p_k$ i enters positius $e_1, \ldots, e_k$ únics tals que*

$$a = \epsilon p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}.$$

La igualtat anterior s'anomena la *descomposició* de $a$ en factors primers o la *factorització* de $a$.

El *màxim comú divisor* de dos enters $a, b$, és el major enter divisor de $a$ i de $b$ alhora; es denota per $\mathrm{mcd}(a, b)$ o, si el context ho permet $(a, b)$. Un mètode popular per obtenir $\mathrm{mcd}(a, b)$ és factoritzar $a$ i $b$; si no tenen cap factor primer en comú, resulta $\mathrm{mcd}(a, b) = 1$; altrament, el $\mathrm{mcd}(a, b)$ s'obté multiplicant els factors primers comuns a les dues factoritzacions, cadascun elevat al menor dels dos exponents en què apareix a les dues factoritzacions. Tanmateix, trobar efectivament la factorització d'enters grans és un problema molt difícil, fins al punt que hi ha mètodes de trametre missatges encriptats basats en aquesta dificultat. Un mètode més eficient per al càlcul del màxim comú divisor és l'*algorisme d'Euclides*, que es basa en el lema següent:

**5.2.3 Lema** *Siguin $a, b, q$ i $r$ enters tals que $a = bq + r$. Aleshores,*

$$\mathrm{mcd}(a, b) = \mathrm{mcd}(b, r).$$

**Demostració:** Si $d$ és divisor de $a$ i de $b$, tenim $a = da'$ i $b = db'$ per a certs enters $a'$ i $b'$. Aleshores $r = a - bq = da' - db'q = d(a' - b'q)$ i $d$ és divisor de $r$. Per tant, tot divisor de $a$ i $b$ és divisor de $b$ i $r$.

Si $d$ és divisor de $b$ i $r$, aleshores $b = db'$ i $r = dr'$ per a certs enters $b'$ i $r'$ i obtenim $a = bq + r = db'q + dr' = d(b'q + r')$, és a dir, $d$ és divisor de $a$. Per tant, tot divisor de $b$ i $r$ és divisor de $a$ i $b$.

Veiem, doncs, que els divisors comuns de $a$ i $b$ coincideixen amb els divisors comuns de $b$ i $r$. Per tant, el màxim dels dos conjunts és el mateix. □

El lema anterior s'aplica, en particular, quan $q$ i $r$ són el quocient i el residu de la divisió de $a$ per $b$. Com que $a$ i $-a$ tenen els mateixos divisors, ens podem restringir al càlcul del mcd per nombres positius.

**5.2.4 Teorema (Algorisme d'Euclides)** *Siguin $a \geq b > 0$ enters, $r_0 = a$, $r_1 = b$ i, per a cada $j \geq 2$, definim recurrentment $r_j$ com el residu de dividir $r_{j-2}$ per $r_{j-1}$. Aleshores existeix un $n$ tal que $r_{n+1} = 0$ i $r_n = \mathrm{mcd}(a, b)$.*

**Demostració:** D'acord amb el teorema de la divisió, tenim que, si $r_{j-1} \neq 0$, aleshores $r_j < r_{j-1}$. Com que els nombres $r_j$ són enters no negatius, la successió dels $r_j$ no pot ser estrictament decreixent. Per tant, existeix un $n$ tal que $r_{n+1} = 0$. Ara, d'acord amb el lema ,

$$\begin{aligned} \mathrm{mcd}(a, b) = \mathrm{mcd}(r_0, r_1) &= \mathrm{mcd}(r_1, r_2) \\ &= \mathrm{mcd}(r_2, r_3) \\ &= \cdots \\ &= \mathrm{mcd}(r_{n-1}, r_n) \\ &= \mathrm{mcd}(r_n, 0) \\ &= r_n. \qquad \square \end{aligned}$$

El quocient $q_{j-1}$ de dividir $r_{j-2}$ per $r_{j-1}$ es pot expressar com la part entera $q_{j-1} = \lfloor r_{j-2}/r_{j-1} \rfloor$, i el residu $r_j$ com la diferència $r_j = r_{j-2} - r_{j-1}q_{j-1}$. Emprem aquesta notació en el teorema següent.

**5.2.5 Teorema (Algorisme de la identitat de Bezout)** *Siguin $a \geq b > 0$ enters. Definim $(r_0, s_0, t_0) = (a, 1, 0)$, $(r_1, s_1, t_1) = (b, 0, 1)$ i, per a cada $j \geq 2$, definim recurrentment*

$$q_{j-1} = \lfloor r_{j-2}/r_{j-1} \rfloor, \qquad (r_j, s_j, t_j) = (r_{j-2} - r_{j-1}q_{j-1},\ s_{j-2} - s_{j-1}q_{j-1},\ t_{j-2} - t_{j-1}q_{j-1}).$$

*Aleshores,*

(i) *existeix un $n$ tal que $r_{n+1} = 0$;*

(ii) $r_n = \mathrm{mcd}(a, b)$*;*

(iii) *per a tota $j \geq 0$, es compleix $r_j = s_j a + t_j b$;*

(iv) $\mathrm{mcd}(a, b) = s_n a + t_n b$.

**Demostració:** (i) i (ii) estan provats al teorema 5.2.4.

(iii) Per inducció sobre $j$. Per $j = 0, 1$, les igualtats són immediates. Si la igualtat val per a $j = 0, 1, \ldots, k-1$, $k \geq 2$, aleshores

$$\begin{aligned} r_k &= r_{k-2} - r_{k-1}q_{k-1} \\ &= (s_{k-2}a + t_{k-2}b) - (s_{k-1}a + t_{k-1}b)q_{k-1} \\ &= (s_{k-2} - s_{k-1}q_{k-1})a + (t_{k-2} - t_{k-1}q_{k-1})b \\ &= s_k a + t_k b. \end{aligned}$$

(iv) Només cal aplicar l'anterior per a $j = n$. □

El teorema anterior indica que, donats enters positius $a, b$, existeixen enters $x, y$ tals que $xa + yb = \mathrm{mcd}(a, b)$. Només cal prendre $x = s_n$ i $y = t_n$ al teorema anterior. La igualtat

$$xa + yb = \mathrm{mcd}(a, b)$$

s'anomena *identitat de Bezout*, i els enters $x$ i $y$ *coeficients de Bezout.*

Els coeficients de Bezout no són pas únics. Per exemple, per a $\mathrm{mcd}(6, 15) = 3$, tenim (entre moltes altres) les dues identitats de Bezout següents:

$$3 \cdot 6 + (-1) \cdot 15 = 3 = (-2) \cdot 6 + 1 \cdot 15.$$

**5.2.6 Exemple** Prenem $a = 252$ i $b = 198$. El teorema 5.2.5 dóna els valors següents:

| $j$ | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| $s_j$ | 1 | 0 | 1 | $-3$ | **4** |
| $t_j$ | 0 | 1 | $-1$ | 4 | $\mathbf{-5}$ |
| $q_j$ | | 1 | 3 | 1 | 2 |
| $r_j$ | 252 | 198 | 54 | 36 | **18** |
| $r_{j+2}$ | 54 | 36 | 18 | 0 | |

Per tant, aquí tenim $r_5 = 0$, $\mathrm{mcd}(252, 198) = r_4 = 18$ i els coeficients de Bezout són 4 i $-5$:

$$4 \cdot 252 - 5 \cdot 198 = 18.$$

## 5.3 Els anells de classes de residus

Per a cada enter positiu $m$, volem donar estructura d'anell a un conjunt de $m$ elements, diguem $\{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{m-1}\}$. El mètode consisteix, bàsicament, a fer les operacions ordinàries, però si el resultat depassa $m$, quedar-se amb el residu de dividir-lo per $m$. Per exemple, per a $m = 7$, $\overline{3} \cdot \overline{5} = \overline{1}$ perquè el residu de dividir 15 per 7 és 1. Justificarem formalment que aquest mètode elemental funciona bé i que s'obté una estructura d'anell.

El lema següent és útil.

**5.3.1 Lema** *Sigui $m$ un enter positiu. Per a cada dos enters $x, y$, són equivalents:*

(a) *$x - y$ és un múltiple de $m$;*

(b) *$x$ i $y$ tenen el mateix residu en dividir-los per $m$.*

**Demostració:** Siguin

$$x = mq_1 + r_1, \quad y = mq_2 + r_2, \quad 0 \leq r_1, r_2 < m$$

les divisions de $x$ i $y$ per $m$. Tenim,

$$x - y = m(q_1 - q_2) + (r_1 - r_2).$$

Suposem que $x - y$ és múltiple de $m$. Si $r_1 \geq r_2$, resulta que $0 \leq r_1 - r_2 \leq r_1 < m$, és a dir, $r_1 - r_2$ és el residu de dividir $x - y$ per $m$, el qual és 0. Per tant, $r_1 = r_2$. Si $r_2 \geq r_1$, l'argument es repeteix amb $y - x$, que també és múltiple de $m$.

Recíprocament, si $r_1 = r_2$, tenim $x - y = m(q_1 - q_2)$, que és múltiple de $m$. □

Considerem l'anell $\mathbb{Z}$ dels nombres enters i fixem un enter positiu $m$. Dos enters $x$ i $y$ són *congrus mòdul $m$* si tenen el mateix residu en dividir-los per $m$ (o, equivalentment d'acord amb el lema 5.3.1, si $x - y$ és múltiple de $m$). S'indica

$$x \equiv y \pmod{m}.$$

La relació $\equiv$ és d'equivalència. La classe d'equivalència d'un enter $x$ és el conjunt

$$\overline{x} = \{y \in \mathbb{Z} \ : \ y \equiv x \pmod{m}\},$$

i el conjunt de totes les classes d'equivalència és una partició de $\mathbb{Z}$ que es representa per $\mathbb{Z}_m$. Notem que $\mathbb{Z}_m$ té $m$ elements, tants com possibles residus en dividir enters per $m$:

$$\mathbb{Z}_m = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}.$$

Les definicions suggerides a l'inici de l'apartat són:

$$\overline{x} + \overline{y} = \overline{x+y}, \quad \overline{x}\,\overline{y} = \overline{xy}.$$

Per exemple, per a $m = 5$, tenim $\overline{3} + \overline{4} = \overline{7} = \overline{2}$. Notem que $3 \equiv 8 \pmod{5}$ i $4 \equiv 14 \pmod{5}$, de forma que $\overline{3} = \overline{8}$ i $\overline{4} = \overline{14}$. Per tal que en la suma de classes no hi hagi ambigüitat, cal que $\overline{8} + \overline{14}$ sigui també $\overline{2}$. Aquest és el cas, en efecte: $\overline{8} + \overline{14} = \overline{22} = \overline{2}$. Això ha d'ocórrer en general i per a les dues operacions. El lema següent ho demostra.

**5.3.2 Lema** *Sigui $m$ un enter positiu i $x, x', y, y'$ enters. Si $x \equiv x' \pmod m$ i $y \equiv y' \pmod m$, aleshores $x + y \equiv x' + y' \pmod m$ i $xy \equiv x'y' \pmod m$.*

**Demostració:** $x \equiv x' \pmod m$ implica $x - x' = mt_1$ per a cert enter $t_1$. Anàlogament, $y - y' = mt_2$ per a cert enter $t_2$. Aleshores,

$$(x + x') - (y + y') = (x - x') + (y - y') = mt_1 + mt_2 = m(t_1 + t_2),$$

el que implica $x + x' \equiv y + y' \pmod m$. Pel producte tenim,

$$\begin{aligned} xy - x'y' &= xy - x'y + x'y - x'y' \\ &= (x - x')y + x'(y - y') \\ &= mt_1 y + x' mt_2 \\ &= m(t_1 y + x' t_2), \end{aligned}$$

la qual cosa implica $xy \equiv x'y' \pmod m$. □

Així, les operacions a $\mathbb{Z}_m$

$$\overline{x} + \overline{y} = \overline{x + y}, \quad \overline{x}\,\overline{y} = \overline{xy}$$

estan ben definides. És una qüestió de rutina comprovar que tenen les propietats requerides per obtenir un anell que, com és usual, es denota també per $\mathbb{Z}_m$, sobreentenent que les operacions són les anteriors. Notem que el neutre de la suma és $\overline{0}$ i el del producte $\overline{1}$. L'oposat de $\overline{x}$ és $-\overline{x} = \overline{-x} = \overline{m - x}$.

Si pel context queda clar quin és el mòdul $m$, sovint s'escriu $x \equiv y$ en lloc de $x \equiv y \pmod m$. També, si el context indica que els elements i les operacions són els de $\mathbb{Z}_m$, s'empra $x$ en lloc de $\overline{x}$. Aquest és un (altre) abús de llenguatge que permet simplificar la notació, i que emprarem amb freqüència d'ara endavant, com als exemples que segueixen.

**5.3.3 Exemple** Les taules de la suma i del producte de $\mathbb{Z}_3$ són les següents:

| $+$ | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | 1 | 2 |
| 1 | 1 | 2 | 0 |
| 2 | 2 | 0 | 1 |

| $\cdot$ | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 |
| 2 | 0 | 2 | 1 |

**5.3.4 Exemple** El mateix per a $\mathbb{Z}_6$:

| $+$ | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 | 5 |
| 1 | 1 | 2 | 3 | 4 | 5 | 0 |
| 2 | 2 | 3 | 4 | 5 | 0 | 1 |
| 3 | 3 | 4 | 5 | 0 | 1 | 2 |
| 4 | 4 | 5 | 0 | 1 | 2 | 3 |
| 5 | 5 | 0 | 1 | 2 | 3 | 4 |

| $\cdot$ | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 | 5 |
| 2 | 0 | 2 | 4 | 0 | 2 | 4 |
| 3 | 0 | 3 | 0 | 3 | 0 | 3 |
| 4 | 0 | 4 | 2 | 0 | 4 | 2 |
| 5 | 0 | 5 | 4 | 3 | 2 | 1 |

Noteu que la propietat commutativa de la suma i del producte es detecta per la simetria de les taules respecte a la diagonal. L'existència d'invers es detecta per l'aparició de 1 a cada fila (i columna) diferent de la de 0. Veiem, doncs, que $\mathbb{Z}_3$ és un cos: 1 és el seu propi invers i 2 i 3 són inversos l'un de l'altre. En canvi, $\mathbb{Z}_6$ no és cos: 2, 3 i 4 no són invertibles de $\mathbb{Z}_6$. La proposició següent permet decidir quins elements de $\mathbb{Z}_m$ són invertibles i, si n'hi ha, quin és l'invers.

**5.3.5 Proposició** *Sigui $m$ un enter positiu. Aleshores $\overline{a}$ és invertible de $\mathbb{Z}_m$ si, i només si,* $\mathrm{mcd}(a, m) = 1$. *En aquest cas, si $x$ és el coeficient de $a$ a la identitat de Bezout, aleshores $\overline{x}$ és l'invers de $\overline{a}$ a $\mathbb{Z}_m$.*

**Demostració:** Suposem que $\overline{a}$ és invertible. Per a cert $\overline{x} \in \mathbb{Z}_m$ tenim $\overline{x}\,\overline{a} = \overline{xa} = \overline{1}$. Això implica $xa - 1 = mt$ per a cert enter $t$, o sigui, $xa - mt = 1$. Si $d$ és un divisor positiu de $a$ i de $m$, aleshores $d$ divideix $xa - mt = 1$, cosa que implica $d = 1$. Per tant, $\mathrm{mcd}(a, m) = 1$.

Recíprocament, si $\mathrm{mcd}(a, m) = 1$, per la identitat de Bezout existeixen $x$ i $y$ tals que $xa + ym = 1$. Això implica

$$\overline{1} = \overline{xa + ym} = \overline{x}\,\overline{a} + \overline{y}\,\overline{m} = \overline{x}\,\overline{a} + \overline{y}\overline{0} = \overline{x}\,\overline{a},$$

la qual cosa prova que $\overline{a}$ és invertible amb invers $\overline{x}$. □

La proposició següent caracteritza els $m$ tals que $\mathbb{Z}_m$ és un cos.

**5.3.6 Proposició** *Sigui $m$ un enter positiu. Aleshores $\mathbb{Z}_m$ és un cos si, i només si, $m$ és primer.*

**Demostració:** Sigui $m$ primer. El màxim comú divisor de $m$ i qualsevol enter és $m$ o 1. Si $\overline{a} \in \mathbb{Z}_m$, $\overline{a} \neq \overline{0}$, aleshores $a$ no és múltiple de $m$. Per tant, $\mathrm{mcd}(a, m) = 1$ i, per la proposició anterior, $\overline{a}$ és invertible.

Recíprocament, suposem que $\mathbb{Z}_m$ és un cos. Si $m$ no és primer, existeixen divisors propis $a, b$ de $m$ tals que $m = ab$. Com que $a$ no és múltiple de $m$, tenim $\overline{a} \neq \overline{0}$. Ara, $\mathrm{mcd}(a, b) = a > 1$ i, per tant, $\overline{a}$ no és unitari, el que és contradictori. □

Si $p$ és un nombre primer, és usual posar $\mathbb{F}_p = \mathbb{Z}_p$ per emfasitzar el fet que es tracta d'un cos (*field*, en anglès).

Molts tipus de problemes que és habitual tractar i resoldre en cossos com $\mathbb{Q}, \mathbb{R}$ o $\mathbb{C}$ es poden fer en un cos $\mathbb{F}_p$ sense canvis substancials. Per exemple, el mètode de Gauss per resoldre sistemes d'equacions lineals és vàlid sense canvis quan els coeficients i les solucions pertanyen a $\mathbb{Z}_p$. Això és així perquè les operacions involucrades en l'algorisme de Gauss només depenen de les propietats de la suma i del producte d'un cos. Alguna diferència, però, hi ha. Per exemple, en els sistemes indeterminats no hi haurà infinites solucions, perquè cadascuna de les incògnites involucrades només té $p$ possibles valors. Així, si hi ha $k$ incògnites indeterminades, el nombre de solucions és $p^k$, un nombre finit. També cal interpretar correctament les notacions usuals. Així, si $a, b \in \mathbb{F}_p$, $b \neq 0$, una fracció $a/b$ cal interpretar-la com el producte de $a$ per l'invers de $b$. Per exemple, a $\mathbb{Z}_{11}$, $5/4$ significa $5 \cdot 4^{-1} = 5 \cdot 3 = 15 = 4$ perquè l'invers de 4 a $\mathbb{Z}_{11}$ és 3.

## 5.4 Polinomis

De la mateixa manera que es defineixen els polinomis amb coeficients racionals o reals es defineixen polinomis amb coeficients en un anell commutatiu $A$. El conjunt dels polinomis en la *indeterminada* $x$ i coeficients a l'anell $A$ es denota per $A[x]$. Les operacions suma i producte també es defineixen anàlogament: Siguin

$$a(x) = a_0 + a_1 x + \cdots + a_n x^n, \qquad b(x) = b_0 + b_1 x + \cdots + b_m x^m$$

dos polinomis de $A[x]$. Suposem que $n \geq m$. Podem escriure $b(x)$ en la forma

$$b(x) = b_0 + b_1 x + \cdots + b_m x^m + b_{m+1} x^{m+1} + \cdots + b_n x^n$$

prenent $b_{m+1} = \cdots = b_n = 0$.

La *suma* $a(x) + b(x)$ i el *producte* $a(x)b(x)$ es defineixen com segueix:

$$\begin{aligned} a(x) + b(x) &= (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_n + b_n)x^n, \\ a(x)b(x) &= a_0 b_0 + (a_0 b_1 + a_1 b_0)x \\ &\quad + (a_0 b_2 + a_1 b_1 + a_2 b_0)x^2 + \cdots + a_n b_m x^{n+m}. \end{aligned}$$

És pesat, però rutinari, comprovar que $A[x]$, amb aquestes dues operacions, és un anell commutatiu. El neutre de la suma és el polinomi 0 i el neutre del producte és el polinomi 1.

Les propietats d'anell commutatiu són les que permeten operar amb polinomis tal com es fa normalment i justifiquen els convenis usuals: si un coeficient $a_i$ és zero, no s'escriu el corresponent sumand $a_i x^i$ i els coeficients 1 tampoc no s'escriuen (llevat que sigui el terme independent) Per exemple, prenem $A = \mathbb{F}_3$ i

$$a(x) = 1 + 2x + 2x^2, \quad b(x) = 2 + x.$$

Tenim

$$\begin{aligned} a(x) + b(x) &= (1 + 2) + (2 + 1)x + (2 + 0)x^2 = 2x^2, \\ a(x)b(x) &= (1 \cdot 2) + (1 \cdot 1 + 2 \cdot 2)x + (2 \cdot 1 + 2 \cdot 2)x^2 + (2 \cdot 1)x^3 \\ &= 2 + 2x + 2x^3. \end{aligned}$$

Els polinomis $a(x)$ amb $a_n = 0$ per a tot $n \geq 1$ s'anomenen polinomis *constants*. Noteu que les operacions amb polinomis constants coincideixen amb les corresponents operacions a $A$, així que podem identificar cada element de $A$ amb el corresponent polinomi constant de $A[x]$.

Sigui $a(x)$ un polinomi diferent de 0. El *grau* de $a(x)$, denotat per $\deg a(x)$, és el màxim $n$ tal que $a_n \neq 0$. Per exemple, els polinomis constants no nuls són els polinomis de grau 0. Convenim que el grau del polinomi 0 és $-\infty$.

Si un polinomi $a(x)$ té grau $n \geq 0$, aleshores es pot escriure

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

amb $a_n \neq 0$. En aquest cas el coeficient $a_n$ s'anomena el coeficient *principal*. Un polinomi és *mònic* si el seu coeficient principal és 1. Per exemple a $\mathbb{Z}_4[x]$, el polinomi $1 + 2x + x^2$ és mònic, però $2 + x + 2x^2$ no ho és.

L'estudi dels polinomis és especialment ric quan l'anell $A$ dels coeficients és un cos. Aquesta és la situació que assumirem en la resta del capítol. Potser els exemples més usuals són els cossos numèrics dels racionals $\mathbb{Q}$, dels reals $\mathbb{R}$ o dels complexos $\mathbb{C}$, però en el nostre context els més rellevants són els cossos $\mathbb{F}_p$ amb $p$ primer i, més generalment, els cossos finits que considerarem més endavant.

El comportament del grau dels polinomis respecte a les operacions és senzill:

**5.4.1 Proposició** *Sigui $K$ un cos i $a(x), b(x) \in K[x]$. Aleshores,*

(i) $\deg(a(x)+b(x)) \leq \max\{\deg a(x), \deg b(x)\}$;

(ii) $\deg(a(x)b(x)) = \deg a(x) + \deg b(x)$.

**Demostració:** Siguin $a_n$ i $b_m$ els coeficients principals de $a(x)$ i $b(x)$, respectivament. Sense pèrdua de generalitat podem suposar $n \geq m$.

(i) Si $n > m$, el coeficient principal de $a(x)+b(x)$ és $a_n$ i val la igualtat. Si $n = m$ i $a_n+b_m \neq 0$, el coeficient principal de $a(x)+b(x)$ és $a_n+b_m$, i també val la igualtat. Si $n = m$ i $a_n+b_m = 0$, aleshores $a(x)+b(x)$ té grau menor que $m = n$ (eventualment $-\infty$ si $a(x)+b(x) = 0$).

(ii) Si $a(x) = 0$ o $b(x) = 0$, aleshores $a(x)b(x) = 0$ i els dos termes de la igualtat són $-\infty$. Si $a(x)$ i $b(x)$ són tots dos diferents de zero amb coeficients principals $a_n$ i $b_m$ respectivament, aleshores $a_n b_m \neq 0$ i $a(x)b(x) \neq 0$ té grau $n+m$. □

Notem que la segona propietat pot no complir-se si els coeficients no pertanyen a un cos. Per exemple, si $A = \mathbb{Z}_6$, $a(x) = 2+2x+3x^2$ i $b(x) = 5+4x+x^2+2x^3$, aleshores

$$\begin{aligned} a(x)b(x) &= 10+(8+10)x+(2+8+15)x^2+(4+2+12)x^3+(4+3)x^4+6x^5 \\ &= 4+x^2+x^4, \end{aligned}$$

així que

$$\deg a(x)b(x) = 4 \neq 5 = \deg a(x) + \deg b(x).$$

El fet que $2 \times 3 = 0$ a $\mathbb{Z}_6$ fa que el grau del producte sigui menor que la suma dels graus.

Com a conseqüència de la proposició anterior, podem caracteritzar els invertibles de $K[x]$ per a qualsevol cos $K$.

**5.4.2 Proposició** *Si $K$ és un cos, els elements invertibles de $K[x]$ són els polinomis constants no nuls, és a dir, $K[x]^* = K^*$.*

**Demostració:** Certament, un polinomi constant no nul $\lambda \in K^*$ té invers $\lambda^{-1}$. Per tant, $K^* \subseteq K[x]^*$.

Recíprocament, si $a(x) \in K[x]^*$, aleshores té invers, diguem $b(x)$. Prenent graus a la igualtat $a(x)b(x) = 1$ resulta $\deg a(x) + \deg b(x) = 0$. Com que $a(x) \neq 0 \neq b(x)$, resulta $\deg a(x) = \deg b(x) = 0$ i ambdós polinomis són constants no nuls. □

La proposició següent formalitza la divisió de polinomis.

**5.4.3 Teorema (de la divisió)** *Sigui $K$ un cos i siguin $a(x), b(x)$ polinomis de $K[x]$ amb $b(x) \neq 0$. Aleshores existeixen polinomis $q(x)$ i $r(x)$ únics tals que*

$$a(x) = b(x)q(x) + r(x), \quad \deg r(x) < \deg b(x).$$

**Demostració:** Provem primer l'existència per inducció sobre el grau de $a(x)$. Si $\deg a(x) < \deg b(x)$, només cal prendre $q(x) = 0$ i $r(x) = a(x)$. Si $b(x) = b$ és constant, només cal prendre $q(x) = b^{-1}a(x)$ i $r(x) = 0$. Suposem, doncs, que $\deg a(x) \geq \deg b(x) \geq 1$ i suposem que el resultat és cert per a polinomis de grau estrictament menor que $\deg a(x)$. Posem

$$a(x) = a_{m+k}x^{m+k} + \cdots + a_0, \quad b(x) = b_m x^m + \cdots + b_0,$$

amb $a_{m+k} \neq 0$, $b_m \neq 0$, $m \geq 1$ i $k \geq 0$. Sigui

$$\tilde{a}(x) = a(x) - a_{m+k} b_m^{-1} x^k b(x).$$

El coeficient de grau $m+k$ de $\tilde{a}(x)$ és

$$a_{m+k} - (a_{m+k} b_m^{-1}) b_m = 0,$$

així que $\deg \tilde{a}(x) < \deg a(x)$. Per la hipòtesi d'inducció, existeixen $\tilde{q}(x)$ i $r(x)$ tals que

$$\tilde{a}(x) = b(x)\tilde{q}(x) + r(x),$$

amb $\deg r(x) < \deg b(x)$. Si posem

$$q(x) = \tilde{q}(x) + a_{m+k} b_m^{-1} x^k,$$

resulta que

$$a(x) = b(x)q(x) + r(x)$$

i està provada l'existència.

Per a la unicitat, suposem que

$$a(x) = b(x)q_1(x) + r_1(x) = b(x)q_2(x) + r_2(x),$$

amb $\deg r_1(x) < \deg b(x)$ i $\deg r_2(x) < \deg b(x)$. Aleshores,

$$b(x)(q_1(x) - q_2(x)) = r_2(x) - r_1(x).$$

Si $q_1(x) \neq q_2(x)$, el costat esquerre és un polinomi de grau $\geq \deg b(x)$, mentre que el costat dret és un polinomi de grau $< \deg b(x)$. Per tant, ha de ser $q_1(x) = q_2(x)$, la qual cosa implica també $r_1(x) = r_2(x)$. □

Remarquem que la construcció de $\tilde{a}(x)$ a la prova anterior és precisament el mètode que se segueix a la pràctica en la divisió de polinomis. Per exemple, si $K = \mathbb{F}_5$ i

$$a(x) = x^4 + 4x^3 + x^2 + 3x + 4 \quad \text{i} \quad b(x) = x^2 + 3x + 2,$$

a la primera etapa s'obté

$$\tilde{a}(x) = a(x) - x^2 b(x) = x^3 - x^2 + (3x + 4),$$

encara que a la pràctica no baixem els termes $3x$ i 4 fins que siguin necessaris.

Els polinomis $q(x)$ i $r(x)$ del teorema 5.4.3 s'anomenen el *quocient* i el *residu* de la divisió de $a(x)$ per $b(x)$. Si $r(x) = 0$, es diu que $a(x)$ és un *múltiple* de $b(x)$ i que $b(x)$ és un *divisor* de $a(x)$ o que *divideix* $a(x)$, i s'indica $b(x)|a(x)$. Per exemple, el polinomi 0 és múltiple de tot polinomi. Un polinomi constant $\lambda \in K^*$ és divisor de tot polinomi $a(x)$ perquè $a(x) = \lambda\lambda^{-1}a(x)$. Si $a(x) \in K[x]$ i $\lambda \in K^*$, aleshores el polinomi $\lambda a(x)$ és divisor de $a(x)$. Donat $a(x)$, els polinomis constants no nuls i els polinomis $\lambda a(x)$ amb $\lambda \in K^*$ s'anomenen *divisors impropis* de $a(x)$. Els altres divisors es diuen *divisors propis*. Notem que els divisors propis de $a(x)$ són els divisors de $a(x)$ de grau positiu i estrictament menor que $\deg a(x)$.

Un element $\alpha \in K$ és una *arrel* del polinomi $a(x) \in K[x]$ si en substituir $x$ per $\alpha$ a $a(x)$ i fer les operacions indicades a $K$, resulta l'element 0 de $K$. Breument, si $a(\alpha) = 0$. Per exemple, $\alpha = 2$ és una arrel de $a(x) = 3x + x^2 \in \mathbb{Z}_5[x]$ perquè $a(2) = 3 \cdot 2 + 2^2 = 6 + 4 = 10 = 0$ a $\mathbb{Z}_5$. Com a conseqüència del teorema de la divisió, tenim l'anomenat teorema del residu:

**5.4.4 Teorema (del residu)** *Sigui $K$ un cos, $\alpha \in K$ i $a(x) \in K[x]$. Aleshores, $a(\alpha) = 0$ si, i només si, $(x-\alpha)|a(x)$.*

**Demostració:** Siguin $q(x)$ i $r(x)$ el quocient i el residu de dividir $a(x)$ per $x-\alpha$. Com que $x-\alpha$ és de grau 1, el residu és una constant $r = r(x)$. Tenim, doncs,

$$a(x) = (x-\alpha)q(x) + r$$

i, substituint $x$ per $\alpha$, s'obté $a(\alpha) = r$. Per tant, $a(\alpha) = 0$ si, i només si, $r = 0$, és a dir, si, i només si, $x-\alpha$ divideix $a(x)$. □

**5.4.5 Corol·lari** *Si $K$ és un cos i $a(x) \in K[x] \setminus \{0\}$, aleshores el nombre d'arrels de $a(x)$ en el cos $K$ és menor o igual que* $\deg a(x)$.

**Demostració:** Per inducció sobre el grau $n$ de $a(x)$. Si $n = 0$, aleshores $a(x)$ és constant no nul i, per tant, no té arrels. Suposem que $n \geq 1$ i que el resultat és vàlid per a polinomis de grau estrictament menor que $n$. Si $a(x)$ no té arrels, el resultat és trivialment cert. Si en té alguna, diguem $\alpha$, aleshores $a(x) = (x-\alpha)q(x)$ per cert polinomi $q(x)$ de grau $n-1$. Ara, tota arrel de $a(x)$ és o una arrel de $x-\alpha$, o sigui $\alpha$, o una arrel de $q(x)$. Per hipòtesi d'inducció $q(x)$ té, com a molt, $n-1$ arrels. Comptant $\alpha$, obtenim que $a(x)$ té, com a molt, $n$ arrels. □

Notem que la hipòtesi que els polinomis ho siguin sobre un cos és essencial. Per exemple, el polinomi $2x + 2x^2 \in \mathbb{Z}_4$ és de grau 2, però té quatre arrels, els quatre elements de $\mathbb{Z}_4$. El problema és que el teorema de la divisió no es compleix per polinomis amb coeficients a $\mathbb{Z}_4$, que no és cos. Aleshores, no es poden deduir ni el teorema del residu ni el corol·lari 5.4.5.

Sigui $K$ un cos. Un polinomi $a(x) \in K[x]$ de grau $\geq 1$ és *irreductible* si no té divisors propis.

Per polinomis de grau petit la irreductibilitat està lligada a l'existència d'arrels, com mostra la proposició següent.

**5.4.6 Proposició** *Sigui $K$ un cos i $a(x) \in K[x]$.*

(i) *Si $\deg a(x) = 1$, aleshores $a(x)$ és irreductible i té exactament una arrel.*

(ii) *Si $\deg a(x) \geq 2$, i $a(x)$ té una arrel, aleshores $a(x)$ no és irreductible.*

(iii) *Si $\deg a(x) \in \{2, 3\}$, aleshores $a(x)$ és irreductible si, i només si, no té arrels.*

**Demostració:**

(i) Un polinomi de grau 1 no té divisors propis, i per tant és irreductible. Si $a(x) = a_0 + a_1 x$ amb $a_1 \neq 0$, aleshores $a(x)$ té l'única arrel $-a_0/a_1$.

(ii) Suposem que $a(x)$ té una arrel $\alpha \in K$. D'acord amb el teorema 5.4.4, tenim $a(x) = (x-\alpha)q(x)$ per a cert $q(x) \in K[x]$. Com que $\deg a(x) \geq 2$, el polinomi $x-\alpha$ és un divisor propi de $a(x)$, el qual, per tant, no és irreductible.

(iii) D'acord amb (ii), si $a(x)$ té una arrel, aleshores no és irreductible. Recíprocament, si $a(x)$ no és irreductible, aleshores $a(x) = p(x)q(x)$ per a certs polinomis $p(x)$ i $q(x)$, ambdós de grau $\geq 1$. Com que $\deg p(x) + \deg q(x) = \deg a(x) \in \{2, 3\}$, almenys un dels dos polinomis $p(x)$ o

$q(x)$, diguem $p(x)$, té grau 1. D'acord amb (i), $p(x)$ té una arrel $\alpha$, i resulta $a(\alpha) = p(\alpha)q(\alpha) = 0$. Per tant, $a(x)$ té una arrel. □

La propietat esmentada a (iii) deixa de complir-se per a polinomis de grau $\geq 4$. Per exemple, el polinomi $1 + x + x^2 \in \mathbb{Z}_2[x]$ no té arrels, la qual cosa comporta que $a(x) = (1 + x + x^2)^2$ tampoc no en té. Tanmateix, $a(x)$ no és irreductible perquè és producte de dos polinomis de grau 2.

No donem la demostració del teorema anàleg a 5.2.2 per a polinomis.

**5.4.7 Proposició** *Sigui $K$ un cos i $a(x) \in K[x] \setminus K$. Aleshores existeixen un $\lambda \in K^*$, enters positius $n_1, \ldots, n_k$ i polinomis mònics irreductibles $f_1(x), \ldots, f_k(x)$ únics llevat l'ordre, tals que*

$$a(x) = \lambda f_1(x)^{n_1} \cdots f_k(x)^{n_k}.$$

La igualtat anterior s'anomena la *factorització* de $a(x)$ en producte de factors irreductibles.

Notem que els factors irreductibles d'un producte $a(x)b(x)$ són els de $a(x)$ i els de $b(x)$. Això implica que si un polinomi irreductible $f(x)$ divideix un producte $a(x)b(x)$, aleshores divideix almenys un dels dos factors. Sovint aquesta observació elemental és clau en l'estudi de divisibilitat de polinomis.

Cal remarcar que el caràcter d'irreductible d'un polinomi depèn essencialment del cos en què es consideri. Per exemple, el polinomi $x^2-2 \in \mathbb{R}[x]$ no és irreductible perquè admet la factorització $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$. En canvi, considerat amb els coeficients racionals, $x^2 - 2 \in \mathbb{Q}[x]$ és irreductible perquè els dos factors anteriors no pertanyen a $\mathbb{Q}[x]$. Anàlogament, el polinomi $x^2 + x + 1 \in \mathbb{Z}_2[x]$ és irreductible perquè és de grau dos i no té arrels, però considerat a $\mathbb{Z}_3[x]$ admet la factorització $x^2 + x + 1 = (x + 2)(x + 2)$ i, per tant, no és irreductible.

És sabut que sobre el cos $\mathbb{C}$ dels nombres complexos els únics polinomis irreductibles són els de grau 1. Sobre el cos $\mathbb{R}$ dels nombres reals, els irreductibles són els polinomis de grau 1 i els polinomis $ax^2 + bx + c$ de grau 2 amb discriminant $b^2 - 4ac$ negatiu. En el cos $\mathbb{Q}$ dels racionals, en canvi, hi ha polinomis irreductibles de tots els graus. Per al cas que aquí més ens interessa, que és el dels cossos finits, demostrarem més endavant que hi ha polinomis irreductibles de tots els graus.

Continuem considerant només polinomis amb coeficients en un cos $K$. Siguin $a(x), b(x)$ dos polinomis de $K[x]$ almenys un dels quals és diferent de zero. Un *màxim comú divisor* de $a(x)$ i $b(x)$ és un polinomi $d(x)$ que és divisor de $a(x)$ i de $b(x)$ i tal que tot divisor de $a(x)$ i de $b(x)$ és també divisor de $d(x)$; es denota per $\mathrm{mcd}(a(x), b(x))$.

Com que 1 divideix a tot polinomi, la definició comporta l'existència d'un màxim comú divisor. En canvi, no comporta la unicitat. Per exemple, si $d(x)$ és un màxim comú divisor de $a(x)$ i $b(x)$, aleshores és clar que $\lambda d(x)$ és també un màxim comú divisor de $a(x)$ i $b(x)$ per a tot $\lambda \in K^*$. D'altra banda, si $d_1(x)$ i $d_2(x)$ són màxims comuns divisors de $a(x)$ i $b(x)$, aleshores cadascun és divisor de l'altre i tenim $d_1(x) = d_2(x)f(x)$, $d_2(x) = d_1(x)g(x)$ per a certs polinomis $f(x)$, $g(x)$. Llavors,

$$d_1(x) = d_2(x)f(x) = d_1(x)g(x)f(x).$$

Igualant graus, veiem que $g(x)f(x)$ ha de ser un polinomi constant i, per tant, $g(x)$ i $f(x)$ són constants. Per tant, dos màxims comuns divisors difereixen només en un factor constant no nul. Així doncs, donats $a(x)$ i $b(x)$ existeix exactament un màxim comú divisor mònic, el qual,

si es vol, es pot especificar com *el* màxim comú divisor de $a(x)$ i $b(x)$. Però sovint no cal fer aquesta restricció.

Si es disposa de les factoritzacions de $a(x)$ i $b(x)$, aleshores és immediat trobar el màxim comú divisor: si no tenen cap factor irreductible en comú, resulta $\mathrm{mcd}(a(x), b(x)) = 1$; altrament, el $\mathrm{mcd}(a(x), b(x))$ s'obté multiplicant els factors irreductibles comuns a les dues factoritzacions, cadascun elevat al menor dels dos exponents en què apareix a les dues factoritzacions. Però trobar efectivament la factorització d'un polinomi és un problema en general difícil, de forma que aquest mètode de càlcul de $\mathrm{mcd}(a(x), b(x))$ sovint no és viable. Un mètode més eficient és l'anàleg al que hem emprat per als enters, l'*algorisme d'Euclides*, que es basa en el teorema de la divisió i en el lema següent.

**5.4.8 Lema** *Siguin $K$ un cos i $a(x), b(x), q(x), r(x) \in K[x]$, tals que $a(x) = b(x)q(x) + r(x)$. Aleshores,*

$$\mathrm{mcd}(a(x), b(x)) = \mathrm{mcd}(b(x), r(x)).$$

**Demostració:** Si $d(x)$ és divisor de $a(x)$ i de $b(x)$, tenim $a(x) = d(x)a'(x)$ i $b(x) = d(x)b'(x)$ per a certs polinomis $a'(x), b'(x) \in K[x]$. Aleshores,

$$\begin{aligned} r(x) &= a(x) - b(x)q(x) \\ &= d(x)a'(x) - d(x)b'(x)q(x) = d(x)(a'(x) - b'(x)q(x)) \end{aligned}$$

i veiem que $d(x)$ és divisor de $r(x)$. Per tant, tot divisor de $a(x)$ i $b(x)$ és divisor de $b(x)$ i $r(x)$.

Si $d(x)$ és divisor de $b(x)$ i $r(x)$, aleshores $b(x) = d(x)b'(x)$ i $r(x) = d(x)r'(x)$ per a certs polinomis $b'(x), r'(x) \in K[x]$. Així tenim,

$$\begin{aligned} a(x) &= b(x)q(x) + r(x) \\ &= d(x)b'(x)q(x) + d(x)r'(x) = d(x)(b'(x)q(x) + r'(x)), \end{aligned}$$

és a dir, $d(x)$ és divisor de $a(x)$. Per tant, tot divisor de $b(x)$ i $r(x)$ és divisor de $a(x)$ i de $b(x)$.

Veiem, doncs, que els divisors comuns de $a(x)$ i de $b(x)$ coincideixen amb els divisors comuns de $b(x)$ i de $r(x)$. Per tant, els màxims comuns divisors són els mateixos. □

El lema anterior s'aplica, en particular, quan $q(x)$ i $r(x)$ són el quocient i el residu de la divisió de $a(x)$ per $b(x)$.

**5.4.9 Teorema (Algorisme d'Euclides)** *Siguin $K$ un cos i $a(x), b(x) \in K[x]$, $b(x) \neq 0$. Definim $r_0(x) = a(x)$, $r_1(x) = b(x)$ i, per a cada $j \geq 2$, definim recurrentment $r_j(x)$ com el residu de dividir $r_{j-2}(x)$ per $r_{j-1}(x)$. Aleshores, existeix un $n$ tal que $r_{n+1}(x) = 0$ i $r_n(x) = \mathrm{mcd}(a(x), b(x))$.*

**Demostració:** D'acord amb el teorema de la divisió, tenim que, si $r_j(x) \neq 0$, aleshores $\deg r_{j+1}(x) < \deg r_j(x)$. Com que els graus dels polinomis $r_j(x)$ són enters no negatius, existeix un $n$ tal que $r_{n+1}(x) = 0$. Ara, d'acord amb el lema 5.4.8,

$$\begin{aligned} \mathrm{mcd}(a(x), b(x)) = \mathrm{mcd}(r_0(x), r_1(x)) &= \mathrm{mcd}(r_1(x), r_2(x)) \\ &= \mathrm{mcd}(r_2(x), r_3(x)) \\ &= \cdots \\ &= \mathrm{mcd}(r_n(x), r_{n+1}(x)) \\ &= \mathrm{mcd}(r_n(x), 0) \\ &= r_n(x). \qquad \square \end{aligned}$$

Notem que, si el grau de $r_0(x) = a(x)$ és menor que el de $r_1(x) = b(x)$, la primera divisió dóna 0 de quocient i $r_2(x) = a(x)$ de residu. Per tant, la resta de l'algorisme segueix com si l'haguéssim inicialitzat amb $r_0(x) = b(x)$ i $r_1(x) = a(x)$. Així, és millor prendre d'entrada $r_0(x)$ i $r_1(x)$ de manera que $\deg r_0(x) \leq \deg r_1(x)$.

Com en el cas dels enters, l'algorisme d'Euclides té la versió estesa següent, que hem anomenat *algorisme de la identitat de Bezout.*

**5.4.10 Teorema (Algorisme de la identitat de Bezout)** *Sigui $K$ un cos i $a(x), b(x) \in K[x]$ polinomis amb $b(x) \neq 0$. Definim*

$$(r_0(x),\, s_0(x),\, t_0(x)) = (a(x),\, 1,\, 0), \qquad (r_1(x),\, s_1(x),\, t_1(x)) = (b(x),\, 0,\, 1),$$

*i, per cada $j \geq 2$, definim recurrentment $q_{j-1}(x)$ com al quocient de la divisió de $r_{j-2}(x)$ per $r_{j-1}(x)$ i*

$$\begin{aligned} r_j(x) &= r_{j-2}(x) - r_{j-1}(x)q_{j-1}(x), \\ s_j(x) &= s_{j-2}(x) - s_{j-1}(x)q_{j-1}(x), \\ t_j(x) &= t_{j-2}(x) - t_{j-1}(x)q_{j-1}(x). \end{aligned}$$

*Aleshores,*

(i) *existeix un enter $n$ tal que $r_{n+1}(x) = 0$;*

(ii) $r_n(x) = \operatorname{mcd}(a(x), b(x))$*;*

(iii) $r_j(x) = s_j(x)a(x) + t_j(x)b(x)$ *per a tot $j \geq 0$;*

(iv) $\operatorname{mcd}(a(x), b(x)) = s_n(x)a(x) + t_n(x)b(x)$*;*

**Demostració:** Notem que $r_j(x)$ és, precisament, el residu de dividir $r_{j-2}(x)$ per $r_{j-1}(x)$. Per tant, (i) i (ii) estan demostrats al teorema 5.4.9.

(iii) Per inducció sobre $j$. Per $j = 0, 1$, les igualtats són immediates. Si la igualtat val per $j = 0, 1, \ldots, k-1$, $k \geq 2$, aleshores

$$\begin{aligned} r_k(x) &= r_{k-2}(x) - r_{k-1}(x)q_{k-1}(x) \\ &= (s_{k-2}(x)a(x) + t_{k-2}(x)b(x)) - (s_{k-1}(x)a(x) + t_{k-1}(x)b(x))q_{k-1}(x) \\ &= (s_{k-2}(x) - s_{k-1}(x)q_{k-1}(x))a(x) + (t_{k-2}(x) - t_{k-1}(x)q_{k-1}(x))b(x) \\ &= s_k(x)a(x) + t_k(x)b(x). \end{aligned}$$

(iv) Només cal prendre $j = n$ a l'apartat anterior.

Si, amb la notació de la proposició anterior, prenem $s(x) = s_n(x)$ i $t(x) = t_n(x)$, obtenim $s(x)a(x)+t(x)b(x) = \operatorname{mcd}(a(x), b(x))$, igualtat que s'anomena *identitat de Bezout.* Els polinomis $s(x)$ i $t(x)$ s'anomenen els *coeficients de Bezout* de la identitat.

**5.4.11 Exemple** Considerem el cos $K = \mathbb{Z}_7$ i els polinomis $x^2 + x + 5$ i $x^3 + 2x^2 + x + 1$. Per calcular el màxim comú divisor i els coeficients de Bezout s'aplica el teorema 5.4.10 prenent

com a $a(x)$ el polinomi de major grau, en aquest cas $a(x) = x^3 + 2x^2 + x + 1$, i com a $b(x)$ l'altre, $b(x) = x^2 + x + 5$. A l'esquema següent es detallen els càlculs. Hem inclòs la primera fila amb els valors de $j$ i la primera columna amb les etiquetes $s_j(x)$, $t_j(x)$, $q_j(x)$ i $r_j(x)$ per facilitar la correspondència amb el teorema 5.4.10, però a la pràctica són innecessàries. Notem que, d'acord amb l'algorisme d'Euclides, els residus inicials són $r_0(x) = a(x)$ i $r_1(x) = b(x)$.

| $j$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| $s_j(x)$ | 1 | 0 | 1 | $\mathbf{-4x+2}$ |
| $t_j(x)$ | 0 | 1 | $-x-1$ | $\mathbf{4x^2+2x-1}$ |
| $q_j(x)$ | | $x+1$ | $4x-2$ | $4x+6$ |
| $r_j(x)$ | $x^3+2x^2+x+1$ | $x^2+x+5$ | $-5x-4$ | $\mathbf{4}$ |
| | $-x^3-x^2-5x$ | $-x^2-5x$ | $-2x$ | |
| | $x^2-4x+1$ | $-4x+5$ | $3$ | |
| | $-x^2-x-5$ | $4x+6$ | $-3$ | |
| | $-5x-4$ | $4$ | $0$ | |

Per tant, el màxim comú divisor és 4 i la identitat de Bezout és

$$(-4x+2)(x^3+2x^2+x+1)+(4x^2+2x-1)(x^2+x+5)=4.$$

Si es vol prendre 1 com a màxim comú divisor, els coeficients de Bezout s'obtenen multiplicant l'anterior igualtat per l'invers de 4 a $\mathbb{Z}_7$, que és 2:

$$(6x+4)(x^3+2x^2+x+1)+(x^2+4x-2)(x^2+x+5)=1.$$

## 5.5 Anells quocients de polinomis

En tot aquest apartat $K$ segueix representant un cos. Comencem amb un lema similar al 5.3.1.

**5.5.1 Lema** *Sigui $K$ un cos i $f(x) \in K[x] \setminus \{0\}$. Per a cada dos polinomis $a(x)$ i $b(x)$ són equivalents:*

(a) *$a(x) - b(x)$ és múltiple de $f(x)$;*

(b) *$a(x)$ i $b(x)$ tenen el mateix residu en dividir-los per $f(x)$.*

**Demostració:** Siguin

$$a(x) = f(x)q_1(x) + r_1(x), \quad b(x) = f(x)q_2(x) + r_2(x),$$

les divisions de $a(x)$ i $b(x)$ per $f(x)$. Tenim,

$$a(x) - b(x) = f(x)(q_1(x) - q_2(x)) + (r_1(x) - r_2(x)).$$

Tant $r_1(x)$ com $r_2(x)$ tenen grau menor que el de $f(x)$, així que el grau de $r_1(x) - r_2(x)$ és menor que el de $f(x)$. Per tant, $r_1(x) - r_2(x)$ és el residu de la divisió de $a(x) - b(x)$ per $f(x)$. En conseqüència, $a(x) - b(x)$ és múltiple de $f(x)$ si, i només si, $r_1(x) = r_2(x)$ . □

Fixem un polinomi $f(x) \in K[x] \setminus \{0\}$. Dos polinomis $a(x)$ i $b(x)$ són *congrus mòdul* $f(x)$ si tenen el mateix residu en dividir-los per $f(x)$ o, equivalentment, si $a(x) - b(x)$ és múltiple de $f(x)$. S'indica

$$a(x) \equiv b(x) \pmod{f(x)}.$$

La relació $\equiv$ és una relació d'equivalència definida al conjunt $K[x]$. La classe d'equivalència de $a(x)$ és el conjunt $\overline{a(x)} = \{f(x) \in K[x] : f(x) \equiv a(x)\}$ i el conjunt de classes d'equivalència és una partició de $K[x]$ que es representa per $K[x]/(f(x))$. Notem que hi ha una bijecció entre el conjunt $K[x]/(f(x))$ i els possibles residus en dividir per $f(x)$, és a dir, els polinomis de grau estrictament menor que $\deg f(x)$.

Ara veurem que la relació $\equiv$ es comporta bé respecte a les operacions:

**5.5.2 Lema** *Sigui $K$ un cos, $f(x) \in K[x] \setminus \{0\}$ i $a_1(x), b_1(x), a_2(x), b_2(x) \in K[x]$ tals que*

$$a_1(x) \equiv a_2(x), \quad b_1(x) \equiv b_2(x) \pmod{f(x)}.$$

*Aleshores,*

$$a_1(x) + b_1(x) \equiv a_2(x) + b_2(x), \quad a_1(x)b_1(x) \equiv a_2(x)b_2(x) \pmod{f(x)}.$$

**Demostració:** $a_1(x) \equiv a_2(x) \pmod{f(x)}$ implica $a_1(x) - a_2(x) = f(x)t_1(x)$ per a cert polinomi $t_1(x)$. Anàlogament, $b_1(x) - b_2(x) = f(x)t_2(x)$ per a cert $t_2(x)$. Aleshores,

$$\begin{aligned}(a_1(x) + b_1(x)) - (a_2(x) + b_2(x)) &= (a_1(x) - a_2(x)) + (b_1(x) - b_2(x)) \\ &= f(x)t_1(x) + f(x)t_2(x) \\ &= f(x)(t_1(x) + t_2(x)),\end{aligned}$$

cosa que implica $a_1(x) + b_1(x) \equiv a_2(x) + b_2(x) \pmod{f(x)}$.

Pel producte tenim

$$\begin{aligned}a_1(x)b_1(x) - a_2(x)b_2(x) &= a_1(x)b_1(x) - a_2(x)b_1(x) + a_2(x)b_1(x) - a_2(x)b_2(x) \\ &= (a_1(x) - a_2(x))b_1(x) + a_2(x)(b_1(x) - b_2(x)) \\ &= f(x)t_1(x)b_1(x) + a_2(x)f(x)t_2(x) \\ &= f(x)(t_1(x)b_1(x) + a_2(x)t_2(x)),\end{aligned}$$

la qual cosa implica $a_1(x)b_1(x) \equiv a_2(x)b_2(x) \pmod{f(x)}$. □

Com en el cas dels enters, el lema anterior comporta que les operacions definides a $K[x]/(f(x))$ per

$$\overline{a(x)} + \overline{b(x)} = \overline{a(x) + b(x)}, \quad \overline{a(x)}\ \overline{b(x)} = \overline{a(x)b(x)},$$

estan ben definides. És rutinari comprovar que aquestes operacions tenen les propietats requerides per obtenir un anell commutatiu i unitari. El neutre de la suma és $0 = \overline{0} = \overline{f(x)}$ i el del producte $1 = \overline{1}$. L'anell $K[x]/(f(x))$ es diu *anell quocient* de $K[x]$ *mòdul* $f(x)$.

Si $f(x)$ és un polinomi constant no nul, el quocient $K[x]/(f(x))$ té una única classe i és un anell trivial. Considerarem, doncs, quocients mòdul polinomis $f(x)$ de grau $\geq 1$. En aquest cas, podem comprovar que l'aplicació $\pi\colon K \to K[x]/(f(x))$ definida fent correspondre a cada $a \in K$ la seva classe $\pi(a) = \overline{a}$ és injectiva. En efecte, si $\overline{a} = \overline{b}$, tenim que $a - b$ és múltiple de $f(x)$. Però l'únic múltiple constant de $f(x)$ és 0. Per tant $a - b = 0$ i $a = b$. Això indica que la classe de $a \in K$ conté un únic element constant, que és el mateix $a$. A més a més, les operacions amb elements de $K$ es corresponen amb les operacions amb les corresponents classes:

$$\begin{aligned}\pi(a + b) &= \overline{a + b} = \overline{a} + \overline{b} = \pi(a) + \pi(b), \\ \pi(ab) &= \overline{ab} = \overline{a}\,\overline{b} = \pi(a)\pi(b), \\ \pi(1) &= \overline{1}.\end{aligned}$$

En definitiva, podem identificar cada $a \in K$ amb $\overline{a}$, considerar $K$ com un subconjunt del quocient $K[x]/(f(x))$ i les operacions a $K$ com la restricció a aquest subconjunt de les operacions de $K[x]/(f(x))$. D'acord amb aquesta discussió, en endavant no posarem la ratlla per a la classe dels polinomis constants.

Sigui $a(x) = a_0 + a_1x + \cdots + a_nx^n \in K[x]$ i posem $\alpha = \overline{x}$. L'aplicació repetida de les operacions i la identificació anterior comporta que

$$\overline{a(x)} = a_0 + a_1\overline{x} + \cdots + a_n\overline{x}^n = a_0 + a_1\alpha + \cdots + a_n\alpha^n = a(\alpha).$$

En particular, $0 = \overline{f(x)} = f(\alpha)$. A efectes pràctics, les operacions al quocient $K[x]/(f(x))$ es fan igual que a $K[x]$ substituint $x$ per $\alpha$ i amb la peculiaritat que $f(\alpha) = 0$.

Seguirem el conveni, llevat que s'indiqui explícitament el contrari, de denotar la classe de $x$ en un quocient $K[x]/(f(x))$ per $\alpha$.

**5.5.3 Exemple** Sigui $f(x) = 1 + x + x^2 \in \mathbb{Z}_2[x]$. Hi ha quatre possibles residus en dividir per $f(x)$, que són els quatre polinomis de $\mathbb{Z}_2[x]$ de grau $\leq 1$. Per tant, hi ha quatre classes d'equivalència. Si, tal com hem convingut, $\alpha = \overline{x}$,

$$\mathbb{Z}_2[x]/(f(x)) = \{0, 1, \overline{x}, \overline{1+x}\} = \{0, 1, \alpha, 1+\alpha\}.$$

Com que $1 + \alpha + \alpha^2 = 0$, tenim $\alpha^2 = -1 - \alpha = 1 + \alpha$. Les taules de la suma i del producte de $\mathbb{Z}_2[x]/(f(x))$ són les següents:

| $+$ | $0$ | $1$ | $\alpha$ | $\alpha+1$ |
|---|---|---|---|---|
| $0$ | $0$ | $1$ | $\alpha$ | $1+\alpha$ |
| $1$ | $1$ | $0$ | $1+\alpha$ | $\alpha$ |
| $\alpha$ | $\alpha$ | $1+\alpha$ | $0$ | $1$ |
| $1+\alpha$ | $1+\alpha$ | $\alpha$ | $1$ | $0$ |

| $\cdot$ | $0$ | $1$ | $\alpha$ | $1+\alpha$ |
|---|---|---|---|---|
| $0$ | $0$ | $0$ | $0$ | $0$ |
| $1$ | $0$ | $1$ | $\alpha$ | $1+\alpha$ |
| $\alpha$ | $0$ | $\alpha$ | $1+\alpha$ | $1$ |
| $1+\alpha$ | $0$ | $\alpha+1$ | $1$ | $\alpha$ |

Investigarem ara quins elements de l'anell quocient són invertibles.

**5.5.4 Proposició** *Sigui $K$ un cos i $f(x) \in K[x] \setminus \{0\}$. Aleshores $a(\alpha) \in K[x]/(f(x))$ té invers si, i només si,* $\operatorname{mcd}(a(x), f(x)) = 1$. *En aquest cas, si $s(x)$ és el coeficient de $a(x)$ a la identitat de Bezout, aleshores $s(\alpha)$ és l'invers de $a(\alpha)$.*

**Demostració:** Suposem que $a(\alpha)$ és invertible. Per a cert $s(x) \in K[x]$, tenim $1 = s(\alpha)\,a(\alpha) = \overline{s(x)a(x)}$. Això implica $s(x)a(x) - 1 = t(x)f(x)$ per a cert polinomi $t(x) \in K[x]$, o sigui, $s(x)a(x) - t(x)f(x) = 1$. Si $d(x)$ és un divisor comú de $a(x)$ i de $f(x)$, aleshores $d(x)$ és un divisor de 1, i per tant és constant no nul. Això implica $\operatorname{mcd}(a(x), f(x)) = 1$.

Recíprocament, si $\operatorname{mcd}(a(x), f(x)) = 1$, per la identitat de Bezout, existeixen polinomis $s(x)$ i $t(x)$ tals que $s(x)a(x) + t(x)f(x) = 1$. Prenent classes mòdul $f(x)$, resulta $s(\alpha)\,a(\alpha) = 1$ i veiem que $s(\alpha)$ és l'invers de $a(\alpha)$ a l'anell $K[x]/(f(x))$. □

**5.5.5 Exemple** Considerem el cos $\mathbb{Z}_3$ i el polinomi $f(x) = x^2 + x + 2 \in \mathbb{Z}_3[x]$. Considerem l'element $2\alpha + 1 \in \mathbb{Z}_3[x]/(f(x))$. Primer calculem el màxim comú divisor de $a(x) = 2x + 1$ i

$f(x)$.

$$\begin{array}{rll} & 2x-2 & 2x+1 \\ x^2+x+2 & 2x+1 & 1 \\ \hline -x^2-2x & 0 & \\ -x+2 & & \\ x+2 & & \\ 1 & & \end{array}$$

Com que el màxim comú divisor és 1, concloem que $2\alpha+1$ té invers. Per calcular-lo, obtenim els coeficients de Bezout:

$$\begin{array}{lll} 1 & 0 & 1 \\ 0 & 1 & -2x+2 \\ & 2x-2 & 2x+1 \\ x^2+x+2 & 2x+1 & 1 \\ \hline -x^2-2x & 0 & \\ -x+2 & & \\ x+2 & & \\ 1 & & \end{array}$$

La identitat de Bezout és

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

Prenent classes mòdul $f(x)$, resulta que l'invers de $2\alpha+1$ és $-2\alpha+2 = \alpha+2$. En efecte:

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

Finalment, podem caracteritzar els polinomis $f(x)$ tals que el quocient $K[x]/(f(x))$ és un cos.

**5.5.6 Proposició** *Sigui $K$ un cos i $f(x) \in K[x] \setminus \{0\}$. Aleshores $K[x]/(f(x))$ és un cos si, i només si, $f(x)$ és irreductible.*

**Demostració:** Suposem que $f(x)$ és irreductible. Per a tot $a(\alpha) \neq 0$, el polinomi $a(x)$ no és múltiple de $f(x)$ i, per tant, $\mathrm{mcd}(a(x), f(x)) = 1$. D'acord amb la proposició anterior, $a(\alpha)$ és invertible. Així, tot element no nul de $K[x]/(f(x))$ té invers. Per tant, el quocient $K[x]/(f(x))$ és un cos.

Recíprocament, suposem que $K[x]/(f(x))$ és un cos i sigui $f(x) = a(x)b(x)$ amb $a(x), b(x) \in K[x]$. Prenent classes obtenim $0 = a(\alpha)\, b(\alpha)$. Si $a(x)$ no és múltiple de $f(x)$, $a(\alpha) \neq 0$ i $a(\alpha)$ té invers, diguem $s(\alpha)$. Llavors $0 = s(\alpha)a(\alpha)\, b(\alpha) = b(\alpha)$, la qual cosa implica que $b(x)$ és múltiple de $f(x)$ i, per tant, un divisor impropi de $f(x)$. Així, $f(x)$ no té divisors propis i és irreductible. □

Com es pot comprovar, les proposicions 5.5.4 i 5.5.6 tenen una evident similitud amb les proposicions 5.3.5 i 5.3.6 respectivament, no només en l'enunciat, sinó també en les demostracions.

## 5.6 Cossos finits

L'*ordre* d'un cos finit és el seu cardinal. Així, si $p$ és un nombre primer, $\mathbb{F}_p$ és un cos d'ordre $p$, i si $f(x) \in \mathbb{F}_p[x]$ és un polinomi irreductible de grau $r \geq 2$, aleshores $\mathbb{F}_p[x]/(f(x))$ és un cos d'ordre $p^r$. En aquest apartat representarem per $\mathbb{F}_q$ un cos finit d'ordre $q$.

Sigui $\beta \in \mathbb{F}_q^*$. Com que $\mathbb{F}_q^*$ té $q-1$ elements, les $q$ primeres potències de $\beta$,

$$\beta, \beta^2, \ldots, \beta^q,$$

no són totes diferents. Per tant, existeixen enters positius $s, t \in [q-1]$, tals que $\beta^s = \beta^{s+t} = \beta^s\beta^t$. Simplificant, $1 = \beta^t$. Concloem que, per a tot $\beta \in \mathbb{F}_q^*$ existeix un enter $t \in [q-1]$ tal que $\beta^t = 1$. El menor d'aquests enters s'anomena l'*ordre* de $\beta$ i es denota $\operatorname{ord}\beta$:

$$\operatorname{ord}\beta = \min\{t \geq 1 : \beta^t = 1\}.$$

Tal com hem vist, $1 \leq \operatorname{ord}\beta \leq q-1$. Cal remarcar que si $t = \operatorname{ord}\beta$, aleshores les potències

$$\beta, \beta^2, \ldots, \beta^t = 1$$

són totes diferents. En efecte, si $1 \leq i < i+j \leq t$ i $\beta^i = \beta^{i+j} = \beta^i\beta^j$, aleshores $1 = \beta^j$ amb $j < t$, en contra de la definició d'ordre. Sovint, les potències s'ordenen començant per l'exponent 0, és a dir: $1, \beta, \ldots, \beta^{t-1}$. Notem que 1 és l'únic element de $\mathbb{F}_q^*$ d'ordre 1.

La proposició següent recull les propietats de l'ordre.

**5.6.1 Proposició** *Siguin $\mathbb{F}_q$ un cos finit d'ordre $q$ i $\beta \in \mathbb{F}_q^*$ un element d'ordre $t$. Aleshores:*

(i) $t|(q-1)$;

(ii) *si $s$ és un enter, aleshores $\beta^s = 1$ si, i només si, $t|s$;*

(iii) $\beta^{q-1} = 1$;

(iv) *per a tot $k \geq 1$, l'ordre de $\beta^k$ és $t/\operatorname{mcd}(k,t)$.*

**Demostració:** (i) Sigui $H = \{1, \beta, \ldots, \beta^{t-1}\}$, que és un conjunt de cardinal $t$. Si $\gamma \in \mathbb{F}_q^*$, el conjunt $\gamma H = \{\gamma, \gamma\beta, \ldots, \gamma\beta^{t-1}\}$ també té cardinal $t$. Observem que $\beta^s H = H$ per a tot enter $s$. Si $\gamma\beta^i = \gamma'\beta^j$ amb $i \leq j$, resulta $\gamma = \gamma'\beta^{j-i}$ i $\gamma H = \gamma'\beta^{j-i}H = \gamma' H$. Això comporta que dos conjunts $\gamma H$, $\gamma' H$ són iguals o disjunts. Per tant, existeixen elements $\gamma_1, \ldots, \gamma_h$ de $\mathbb{F}_q^*$ tals que $\gamma_1 H, \ldots, \gamma_h H$ és una partició de $\mathbb{F}_q^*$. Aleshores el cardinal de $\mathbb{F}_q^*$ és $q-1 = ht$ i $t|(q-1)$.

(ii) Si $s = tk$, tenim $\beta^s = \beta^{tk} = (\beta^t)^k = 1$. Recíprocament, si $\beta^s = 1$, dividim $s$ per $t$ i obtenim $s = tc + r$ amb $r < t$. Llavors $\beta^r = \beta^{s-tc} = \beta^s(\beta^t)^{-c} = 1$. Com que $t$ és l'ordre de $\beta$ i $r < t$, resulta $r = 0$ i $s$ és múltiple de $t$.

(iii) D'acord amb (i), $q-1$ és múltiple de $t$. Per (ii), $\beta^{q-1} = 1$.

(iv) Siguin $d = \operatorname{mcd}(k,t)$, $k = k'd$ i $t = t'd$. Sabem que $\operatorname{mcd}(k',t') = 1$. Primer notem que

$$(\beta^k)^{t/d} = (\beta^t)^{k/d} = 1,$$

la qual cosa implica que $\operatorname{ord}\beta^k$ és divisor de $t/d$. Ara, si $(\beta^k)^s = 1$, tenim, $\beta^{ks} = 1$ i $ks$ ha de ser múltiple de $t$. Aleshores $t = t'd$ és divisor de $ks = k'ds$, cosa que implica $t'|k's$. Atès que $\operatorname{mcd}(k',t') = 1$, tenim que $s$ és múltiple de $t' = t/d$. Per tant, l'ordre de $\beta^k$ és múltiple de $t/d$. En definitiva, $\operatorname{ord}\beta^k = t/d$. □

L'objectiu immediat és comptar quants elements de cada ordre hi ha en un cos finit. La discussió es basa parcialment en la *funció $\phi$ d'Euler* que hem estudiat en el context del principi d'inclusió-exclusió.

**5.6.2 Proposició** *Sigui $\mathbb{F}_q$ un cos finit d'ordre $q$. Per a cada enter positiu $d$, el nombre d'elements de $\mathbb{F}_q^*$ d'ordre $d$ és $\phi(d)$ si $d|(q-1)$, i 0 altrament.*

**Demostració:** D'acord amb la proposició 5.6.1(i), tot element de $\mathbb{F}_q^*$ té per ordre un divisor de $q-1$. Així, si $d$ no divideix $q-1$, el nombre d'elements d'ordre $d$ és 0.

Per a cada divisor $d$ de $q-1$, sigui $\psi(d)$ el nombre d'elements de $\mathbb{F}_q^*$ d'ordre $d$. Com que tot element de $\mathbb{F}_q^*$ té per ordre un divisor de $q-1$, tenim

$$\sum_{d|(q-1)} \psi(d) = q-1.$$

Suposem que hi ha un element $\beta$ d'ordre $d$. Llavors, $1, \beta, \beta^2, \ldots, \beta^{d-1}$ són tots diferents i arrels de $x^d - 1 \in \mathbb{F}_q[x]$, per tant són totes les arrels d'aquest polinomi. Així, tot element d'ordre $d$ és arrel del polinomi $x^d - 1$ i, per tant, potència de $\beta$. Però, per la proposició 5.6.1(iv), d'aquestes potències, només $\phi(d)$ tenen ordre $d$. Per tant, si hi ha un element d'ordre $d$, resulta $\psi(d) = \phi(d)$. Si no n'hi ha cap, aleshores $0 = \psi(d) < \phi(d)$. Així que

$$q-1 = \sum_{d|(q-1)} \psi(d) \leq \sum_{d|(q-1)} \phi(d) = q-1$$

i, per tant, $\psi(d) = \phi(d)$ per a cada divisor $d$ de $q-1$. □

Un element $\beta \in \mathbb{F}_q^*$ és *primitiu* si té ordre $q-1$. La proposició anterior implica el corol·lari següent, del qual es farà un ús intensiu.

**5.6.3 Corol·lari** *Tot cos finit té un element primitiu.*

**Demostració:** Un cos té almenys dos elements, 0 i 1. Per tant, si $\mathbb{F}_q$ és un cos finit, tenim $q \geq 2$. Aleshores $\phi(q-1) \geq 1$ i el teorema anterior garanteix l'existència d'elements d'ordre $q-1$, és a dir, d'elements primitius. □

Si $\beta \in \mathbb{F}_q^*$ és primitiu, tot element no nul del cos és potència de $\beta$ amb l'exponent unívocament determinat entre 0 i $q-2$:

$$\mathbb{F}_q^* = \{\beta, \beta^2, \ldots, \beta^{q-1} = 1, \} = \{1, \beta, \ldots, \beta^{q-2}\}.$$

L'aplicació $\mathbb{Z}_{q-1} \to \mathbb{F}_q^*$ definida per $i \mapsto \beta^i$ és bijectiva i a la suma de $\mathbb{Z}_{q-1}$ correspon el producte de $\mathbb{F}_q^*$:

$$i + j \mapsto \beta^{i+j} = \beta^i \beta^j.$$

Si es disposa explícitament de la correspondència $i \mapsto \beta^i$, aleshores els càlculs de productes es simplifiquen notòriament perquè es redueixen a una suma mòdul $q-1$. L'aplicació $i \mapsto \beta^i$ s'anomena la *taula de logaritmes* en base $\beta$ per al cos finit $\mathbb{F}_q$. Si $\gamma \in \mathbb{F}_q^*$, existeix un únic enter $i \in \{0, 1, \ldots, q-2\}$ tal que $\gamma = \beta^i$. Aquest $i$ s'anomena el *logaritme en base $\beta$ de $\gamma$* i es denota $\log_\beta \gamma$.

Sigui $\mathbb{F}_q$ un cos finit d'ordre $q$. Un polinomi $f(x) \in \mathbb{F}_q[x]$ és *primitiu* si és irreductible i $\alpha = \overline{x}$ és un element primitiu del cos $\mathbb{F}_q[x]/(f(x))$.

**5.6.4 Exemple** Considerem el polinomi $f(x) = x^2 + 2x + 2 \in \mathbb{F}_3[x]$. Tenim $f(0) = 2$, $f(1) = 2$, $f(2) = 1$. Així, $f(x)$ és de grau 2 i no té arrels, per tant és irreductible. Considerem el cos $\mathbb{F}_9 = \mathbb{F}_3[x]/(f(x))$ i sigui $\alpha = \overline{x}$. Com que $\overline{f(x)} = 0$, resulta $\alpha^2 + 2\alpha + 2 = 0$ i $\alpha^2 = -2\alpha - 2 = \alpha + 1$. L'ordre de tot element és divisor de 8, i per tant l'ordre de $\alpha$ és 2, 4 o 8. Tenim,

$$\alpha^2 = \alpha + 1 \neq 1, \quad \alpha^4 = (\alpha + 1)^2 = \alpha^2 + 2\alpha + 1 = \alpha + 1 + 2\alpha + 1 = 2 \neq 1.$$

L'ordre de $\alpha$ no és ni 2 ni 4, per tant és 8. Concloem que $\alpha$ és primitiu i que $f(x)$ és un polinomi primitiu.

Tal com hem indicat, als efectes de calcular a $\mathbb{F}_9$, convé disposar de tots els seus elements no nuls en forma de potències de $\alpha$, és a dir, de la taula de logaritmes en base $\alpha$. És la següent:

$$\begin{array}{lcl} 1 & = & 1 \\ \alpha & = & \alpha \\ \alpha^2 & = & \alpha + 1 \\ \alpha^3 & = & \alpha^2 + \alpha = \alpha + 1 + \alpha = 2\alpha + 1 \\ \alpha^4 & = & 2\alpha^2 + \alpha = 2(\alpha + 1) + \alpha = 2 \\ \alpha^5 & = & 2\alpha \\ \alpha^6 & = & 2\alpha^2 = 2(\alpha + 1) = 2\alpha + 2 \\ \alpha^7 & = & 2\alpha^2 + 2\alpha = 2(\alpha + 1) + 2\alpha = \alpha + 2 \end{array}$$

Com és natural, per a $\alpha^8$ tenim

$$\alpha^8 = \alpha^2 + 2\alpha = \alpha + 1 + 2\alpha = 1.$$

Per fer un producte com $(\alpha + 2)(2\alpha + 1)^{10}$ només cal notar que $\alpha + 2 = \alpha^7$ i $2\alpha + 1 = \alpha^3$; per tant, $(2\alpha + 1)^{10} = \alpha^{30} = \alpha^6$ i $(\alpha + 2)(2\alpha + 1)^{10} = \alpha^7\alpha^6 = \alpha^{13} = \alpha^5$.

Disposant de la taula de logaritmes, els inversos es calculen sense necessitat de l'algorisme d'Euclides. Per exemple, l'invers de $2\alpha = \alpha^5$ és $\alpha^{8-5} = \alpha^3 = 2\alpha + 1$.

**5.6.5 Exemple** Considerem el polinomi $f(x) = x^4 + x + 1 \in \mathbb{Z}_2[x]$ i comprovem que és irreductible. Com que $f(0) = f(1) = 1$, no té arrels i no té factors de grau 1. Si factoritza, ho fa com a producte de dos polinomis mònics de grau 2. A més, els termes independents dels dos factors han de ser iguals a 1:

$$f(x) = x^4 + x + 1 = (x^2 + ax + 1)(x^2 + bx + 1).$$

Igualant els coeficients de grau 3 i de grau 1 s'obtenen les condicions incompatibles $0 = b + a$ i $1 = a + b$. Per tant, $f(x)$ és irreductible.

Considerem el cos finit $\mathbb{F}_{16} = \mathbb{F}_2[x]/(f(x))$. Tenim $0 = f(\alpha) = \alpha^4 + \alpha + 1$, és a dir, $\alpha^4 = \alpha + 1$. La taula següent és la taula de logaritmes en base $\alpha$ per a aquest cos.

$$\begin{array}{lcl} 1 & = & 1 \\ \alpha & = & \alpha \\ \alpha^2 & = & \alpha^2 \\ \alpha^3 & = & \alpha^3 \\ \alpha^4 & = & \alpha + 1 \\ \alpha^5 & = & \alpha^2 + \alpha \\ \alpha^6 & = & \alpha^3 + \alpha^2 \\ \alpha^7 & = & \alpha^4 + \alpha^3 = \alpha^3 + \alpha + 1 \end{array} \qquad \begin{array}{lcll} \alpha^8 & = & (\alpha + 1) + \alpha^2 + \alpha & = \alpha^2 + 1 \\ \alpha^9 & & & = \alpha^3 + \alpha \\ \alpha^{10} & = & (\alpha + 1) + \alpha^2 & = \alpha^2 + \alpha + 1 \\ \alpha^{11} & & & = \alpha^3 + \alpha^2 + \alpha \\ \alpha^{12} & = & (\alpha + 1) + \alpha^3 + \alpha^2 & = \alpha^3 + \alpha^2 + \alpha + 1 \\ \alpha^{13} & = & (\alpha + 1) + \alpha^3 + \alpha^2 + \alpha & = \alpha^3 + \alpha^2 + 1 \\ \alpha^{14} & = & (\alpha + 1) + \alpha^3 + \alpha & = \alpha^3 + 1 \end{array}$$

Naturalment, $\alpha^{15} = \alpha^4 + \alpha = \alpha + 1 + \alpha = 1$. Veiem, doncs, que $\alpha$ és primitiu.

Com ja s'ha vist, si es disposa de la taula de logaritmes d'un cos finit $\mathbb{F}_q$ en base un element primitiu $\beta$, el producte de dos elements $\beta^i\beta^j$ es fa simplement sumant els exponents mòdul $q-1$. Per calcular $\beta^i + \beta^j$, en canvi, cal passar per les expressions de $\beta^i$ i $\beta^j$ com a polinomis en $\beta$.

Apart de l'estructura de $\mathbb{F}_q^*$ que hem vist, des del punt de vista teòric els resultats més importants sobre els cossos finits són els tres següents:

**5.6.6 Teorema** (i) *Si $\mathbb{F}_q$ és un cos finit, aleshores existeix un primer $p$ tal que $\mathbb{F}_q$ és de la forma $\mathbb{F}_p$ o bé és de la forma $\mathbb{F}_p[x]/(f(x)$ per cert polinomi irreductible $f(x) \in \mathbb{F}_p[x]$; en aquest segon cas, $q = p^r$.*

(ii) *Per a cada enter $r$ i cada primer $p$ existeix un cos finit de $q = p^r$ elements.*

(iii) *Dos cossos finits del mateix ordre són isomorfs (és a dir, tenen exactament les mateixes propietats).*

Notem que el primer apartat de 5.6.6 implica que si $q$ és l'ordre d'un cos finit, aleshores $q = p^r$ per cert primer $p$ i cert enter $r$. El nombre $p$ s'anomena la *característica* de $\mathbb{F}_q$. Si $\mathbb{F}_q$ és de característica $p$, aleshores $\mathbb{F}_q$ conté $\mathbb{F}_p$.

La prova del segon apartat involucra un argument algebraic, en el que no entrarem, i un argument combinatori que comentem. L'argument algebraic és la prova de la proposició següent:

**5.6.7 Proposició** *Sigui $\mathbb{F}_q$ un cos finit i $m \geq 1$ un enter. El polinomi $x^{q^m} - x$ és el producte de tots els polinomis de $\mathbb{F}_q[x]$ mònics, irreductibles i de grau divisor de $m$, sense repeticions.*

Suposant que disposem d'un algorisme prou eficient per factoritzar polinomis a $\mathbb{F}_q$, la proposició 5.6.7 ens dóna una manera de trobar tots els polinomis irreductibles de $\mathbb{F}_q[x]$ d'un grau donat $d$.

Considerem ara l'argument combinatori. La *funció de Möbius* $\mu$ està definida sobre els enters positius com segueix:

$$\mu(m) = \begin{cases} 1 & \text{si} \quad m = 1, \\ (-1)^k & \text{si} \quad m \text{ és producte de } k \text{ primers diferents}, \\ 0 & \text{si} \quad m \text{ és divisible pel quadrat d'un primer.} \end{cases}$$

Per exemple, $\mu(15) = \mu(3 \cdot 5) = (-1)^2 = 1$; $\mu(30) = \mu(2 \cdot 3 \cdot 5) = (-1)^3 = -1$; i $\mu(18) = \mu(2 \cdot 3^2) = 0$ perquè el 3 té un exponent $\geq 2$.

La funció de Möbius té la propietat següent.

**5.6.8 Lema** *Per a tot enter $n \geq 2$ es compleix*

$$\sum_{d|n} \mu(d) = 0.$$

**Demostració:** Sigui $n = p_1^{e_1} \cdots p_r^{e_r}$ la descomposició de $n$ en factors primers. Cada divisor $d$ de $n$ és de la forma $d = p_1^{f_1} \cdots p_r^{f_r}$ amb $0 \leq f_i \leq e_i$ i $\mu(d)$ és zero excepte quan tots els $f_i$ són 0 o 1.

Així, cada divisor $d$ de $n$ amb $\mu(d) \neq 0$ es correspon amb el subconjunt de $\{p_1, \ldots, p_r\}$ que conté els $p_i$ tals que $f_i = 1$. El nombre d'aquests subconjunts de cardinal $k$ és $\binom{r}{k}$ i $\mu(d) = (-1)^k$. Aleshores,

$$\sum_{d|n} \mu(d) = 1 - \binom{r}{1} + \binom{r}{2} - \cdots + (-1)^r \binom{r}{r} = 0. \qquad \square$$

**5.6.9 Proposició (Fórmula d'inversió de Möbius)** *Sigui $g\colon \mathbb{N} \to \mathbb{N}$ una aplicació i definim l'aplicació $f\colon \mathbb{N} \to \mathbb{N}$ per*

$$f(n) = \sum_{d|n} g(d).$$

*Aleshores,*

$$g(n) = \sum_{d|n} \mu(d) f(\frac{n}{d}).$$

**Demostració:** Sigui $S$ el conjunt de parelles de naturals $(c, d)$ tals que $d|n$ i $c|(n/d)$. Comprovem que $(c, d) \in S$ si, i només si, $c|n$ i $d|(n/c)$. En efecte, si $(c, d) \in S$, existeixen $r$ i $s$ tals que $n = dr$ i $n/d = r = cs$. Així, $n = csd$ i tenim que $c|n$. A més $n/c = sd$ és enter i $d|(n/c)$. El recíproc és similar canviant els rols de $c$ i $d$.

Aleshores,

$$\begin{aligned} \sum_{d|n} \mu(d) f(\frac{n}{d}) &= \sum_{d|n} \mu(d) \sum_{c|(n/d)} g(c) \\ &= \sum_{(c,d)\in S} \mu(d) g(c) \\ &= \sum_{c|n} g(c) \sum_{d|(n/c)} \mu(d) \end{aligned}$$

Segons el lema 5.6.8, si $n/c \geq 2$, la suma $\sum_{d|(n/c)} \mu(d)$ és zero. Per tant, roman només el sumand corresponent a $c = n$ i l'expressió anterior queda

$$\sum_{d|n} \mu(d) f(\frac{n}{d}) = g(n) \sum_{d|1} \mu(d) = g(n)\mu(1) = g(n). \qquad \square$$

Fixem un cos finit $\mathbb{F}_q$ d'ordre $q$. Per a cada enter $r \geq 1$, denotarem per $N_q(r)$ el nombre de polinomis mònics, irreductibles i de grau $r$ amb coeficients a $\mathbb{F}_q$. Els polinomis irreductibles de grau $r$ s'obtenen multiplicant els irreductibles mònics per qualsevol escalar no nul. Per tant, el nombre d'irreductibles de grau $r$ (mònics o no) és $(q-1)N_q(r)$.

**5.6.10 Proposició** *Sigui $\mathbb{F}_q$ un cos finit d'ordre $q$ i $r \geq 1$ un enter. Aleshores, el nombre de polinomis mònics, irreductibles i de grau $r$ amb coeficients a $\mathbb{F}_q$ és*

$$N_q(r) = \frac{1}{r} \sum_{d|r} \mu(d) q^{r/d} \geq 1.$$

*En particular, per a cada enter $r \geq 1$, a $\mathbb{F}_q[x]$ existeixen polinomis irreductibles de grau $r$.*

**Demostració:** Per la proposició 5.6.7 el polinomi $x^{q^r} - x$ és el producte de tots els polinomis mònics, irreductibles i de grau divisor de $r$. Igualant els graus en aquesta factorització, tenim:

$$q^r = \sum_{d|r} dN_q(d).$$

Apliquem la fórmula d'inversió de Möbius a la funció $g(r) = rN_q(r)$. Si definim

$$f(r) = \sum_{d|r} g(d) = \sum_{d|r} dN_q(d) = q^r,$$

la fórmula d'inversió de Möbius dóna

$$rN_q(r) = g(r) = \sum_{d|r} \mu(d) f(r/d) = \sum_{d|r} \mu(d) q^{r/d}.$$

Dividint per $r$ obtenim la igualtat.

Per $d = 1$ el sumand corresponent és $q^r$. Tots els altres sumands diferents de zero són de la forma $\pm q^i$ amb $i < r$. Per tant,

$$N_q(r) \geq \frac{1}{r}(q^r - (q^{r-1} + q^{r-2} + \cdots + q + 1)) = \frac{1}{r}\left(q^r - \frac{q^r - 1}{q - 1}\right) > 0.$$

Com que $N_q(r)$ és enter, resulta que $N_q(r) \geq 1$. □

**5.6.11 Exemple** Calculem el nombre $N_5(4)$ de polinomis mònics irreductibles de grau 4 a $\mathbb{F}_5[x]$. Els divisors de 4 són $1, 2$ i 4. Per tant,

$$N_5(4) = \frac{1}{4}(\mu(1)5^4 + \mu(2)5^2 + \mu(4)5) = \frac{1}{4}(5^4 - 5^2) = 150.$$

Com a conseqüència obtenim el teorema d'existència de cossos finits: Donats un primer $p$ i un enter $r \geq 2$, el teroema garanteix l'existència d'un polinomi $f(x) \in \mathbb{F}_p[x]$ de grau $r$. Llavors $\mathbb{F}_p[x]/(f(x))$ és un cos d'ordre $q = p^r$.

El problema pràctic en aquest procediment és trobar efectivament el polinomi irreductible $f(x)$. En les aplicacions s'empren taules ja elaborades per valors de $p$ i $r$ recorrent tot el rang de valors probables d'aparèixer en casos pràctics, o bé mètodes computacionals per generar polinomis i testar la seva irreductibilitat. Des del punt de vista pràctic, és suficient saber construir cossos finits de l'ordre desitjat. Des del punt de vista teòric, la unicitat és un resultat significatiu. El tercer punt de 5.6.6 asegura la unicitat.

Si $f_1(x)$ i $f_2(x)$ són polinomis irreductibles de grau $r$ amb coeficients a $\mathbb{F}_p$, el teorema 5.6.6 assegura que els cossos $K_1 = \mathbb{F}_p[x]/(f_1(x))$ i $K_2 = \mathbb{F}_p[x]/(f_2(x))$ són isomorfs. Tanmateix, l'isomorfisme no és el que fa correspondre a un element $a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}$ de $K_1$ l'element que s'escriu igual $a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}$ a $K_2$. Per exemple, els polinomis $f_1(x) = 1 + x + x^3$ i $f_2(x) = 1 + x^2 + x^3$ de $\mathbb{F}_2[x]$ no tenen arrels i, per tant, són tots dos irreductibles. En el quocient $K_1 = \mathbb{F}_2[x]/(f_1(x))$ tenim

$$\alpha^2\alpha^2 = \alpha^3\alpha = (\alpha + 1)\alpha = \alpha^2 + \alpha,$$

mentre que, a $K_2 = \mathbb{F}_2[x]/(f_2(x))$,

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

Això indica que, si bé $K_1$ i $K_2$ són isomorfs i que qualsevol propietat d'un d'ells es pot traslladar a una propietat de l'altre, el polinomi $f_i(x)$ escollit determina la retolació dels elements. Per tant, en càlculs concrets, cal detallar el polinomi irreductible $f(x)$ escollit per construir el cos.

Josep M. Brunat
Departament de Matemàtica Aplicada II
Universitat Politècnica de Catalunya
Febrer 2006