Caracterització, existència i unicitat dels cossos finits

Maria Bras-Amorós

29 de novembre de 2023

Algunes generalitats de cossos

Característica i cardinal d'un cos finit

Ordre multiplicatiu i teorema de l'element primitiu

Polinomi mínim i caracterització dels cossos finits

Existència d'un cos finit de p^m elements

Unicitat del cos finit de p^m elements

Solucions

Definició de grup

Recordem les definicions.

Una operació binària $*$ en un conjunt A pot tenir les següents propietats:

- **Propietat associativa** si $a * (b * c) = (a * b) * c$ per tot $a, b, c \in A$.
- **Existència d'element neutre** si existeix un element de A, que anomenem e_n, tal que $a * e_n = e_n * a = a$ per tot $a \in A$.
- **Existència d'element invers** si per tot element $a \in A$ existeix un element de A, que anomenem e_a, tal que $a * e_a = e_a * e = e_n$.
- **Propietat commutativa** si $a * b = b * a$ per tot $a, b \in A$.

Definició

Un **grup** és un conjunt A amb una operació associativa amb element neutre i invers. El grup és un **grup commutatiu** si l'operació és commutativa.

Definició de grup

Exemple

Considerem el conjunt $\{a, e, i\}$ *amb l'operació* $*$ *donada per la taula*

$*$	a	e	i
a	e	i	a
e	i	a	e
i	a	e	i

Observem que l'operació és commutativa per ser la taula simètrica i que té com a element neutre l'element i*. L'invers de* a *per* $*$ *és* e *i l'invers de* e *per* $*$ *és* a*. L'invers de* i *és ell mateix. També es pot comprovar que l'operació és associativa. Per tant, el conjunt* $\{a, e, i\}$ *amb l'operació* $*$ *és un grup commutatiu.*

Definició de grup

Exemple

Considerem el conjunt $\{a, e, i, o\}$ amb l'operació $+$ donada per la taula

$+$	a	e	i	o
a	o	i	e	a
e	i	o	a	e
i	e	a	o	i
o	a	e	i	o

Observem que l'operació és commutativa per ser la taula simètrica i que té com a element neutre l'element o. Tots els elements es tenen a ells mateixos com al seu propi invers. També es pot comprovar que l'operació és associativa. Per tant, el conjunt $\{a, e, i, o\}$ amb l'operació $+$ és un grup commutatiu.

Definició d'anell

Una segona operació $**$ en el conjunt A pot tenir la següent propietat respecte de la primera operació $*$.

- **Propietat distributiva** si $a * *(b * c) = (a * *b) * (a * *c)$ per tot $a, b, c \in A$.

Definició

Un **anell** és un conjunt A amb dues operacions $\oplus$ i $\otimes$ tal que $\oplus$ li confereix estructura de grup commutatiu i tal que $\otimes$ és associativa i satisfà la proietat distributiva respecte de $\oplus$.

Exercici 1

Demostreu que en un anell amb les operacions $\oplus$ i $\otimes$ l'element neutre de $\oplus$ multiplicat per qualsevol element de l'anell dona altra vegada el neutre respecte de $\oplus$.

Solució (p.76)

Definició de cos

Diem que un anell és **unitari** i **commutatiu** si $\otimes$ té element neutre i satisfà la propietat commutativa, respectivament.

Definició

Un **cos** és un anell unitari i commutatiu on $\otimes$ satisfà que tot element diferent del neutre de $\oplus$ té invers. En aquest cas l'invers d'un element respecte de $\oplus$ s'anomena el seu **element oposat**, i es deixa el nom d'**element invers** per a l'invers respecte de $\otimes$.

Definició de cos

Exemple

El conjunt $\{a, e, i, o\}$ dels exemples anteriors és un cos respecte de l'operació $\oplus = +$ amb neutre o, i respecte l'operació $\otimes = *$ ampliant-la amb el neutre de $+$, que multiplicat per qualsevol element dona o. És a dir

$*$	a	e	i	o
a	e	i	a	o
e	i	a	e	o
i	a	e	i	o
o	o	o	o	o

Només queda comprovar que l'operació $*$ és distributiva respecte $+$, que ho deixem com a exercici.

Isomorfismes de cossos

Definició

Un **morfisme** entre dos cossos E i F és una aplicació

$$f : E \to F$$

tal que per tot $a, b \in E$ es compleix $f(a+b) = f(a) + f(b)$ i $f(ab) = f(a)f(b)$.

Exercici 2

Demostreu que si f és un morfisme entre els cossos E i F, si 0_E i 0_F són els neutres per la suma de E i F, respectivament, i 1_E i 1_F són els neutres pel producte de E i F, respectivament, aleshores

- $f(0_E) = 0_F$, $f(1_E) = 1_F$,
- $f(-a) = -f(a)$ i $f(a^{-1}) = (f(a))^{-1}$ per tot $a \in E \setminus \{0_E\}$.

Solució (p.77)

Isomorfismes de cossos

Definició

Un **isomorfisme** entre dos cossos E i F és un morfisme injectiu i exhaustiu. Diem que dos cossos són **isomorfs** si existeix un isomorfisme entre ells. En aquest cas escrivim $E \cong F$.

Exemple

Considerem $E = \mathbb{Z}_2[x]/(x^3 + x^2 + 1)$ *i anomenem* α *a la classe de* x *en* E.
Considerem $F = \mathbb{Z}_2[x]/(x^3 + x + 1)$ *i anomenem* β *a la classe de* x *en* F.
Les taules d'equivalències a E *i a* F *són*

0	0
α^0	1
α^1	α
α^2	α^2
α^3	$\alpha^2 + 1$
α^4	$\alpha^2 + \alpha + 1$
α^5	$\alpha + 1$
α^6	$\alpha^2 + \alpha$

0	0
β^0	1
β^1	β
β^2	β^2
β^3	$\beta + 1$
β^4	$\beta^2 + \beta$
β^5	$\beta^2 + \beta + 1$
β^6	$\beta^2 + 1$

Isomorfismes de cossos

Considerem l'aplicació

$$\begin{array}{rcl} f : E & \to & F \\ 0 & \mapsto & 0 \\ \alpha^i & \mapsto & (\beta+1)^i \end{array}$$

És a dir,

$$\begin{array}{rcl} 0 & \mapsto & 0 \\ 1 & \mapsto & 1 \\ \alpha & \mapsto & \beta+1=\beta^3 \\ \alpha^2 & \mapsto & (\beta+1)^2=(\beta^3)^2=\beta^6 \\ \alpha^3 & \mapsto & (\beta+1)^3=(\beta^3)^3=\beta^2 \\ \alpha^4 & \mapsto & (\beta+1)^4=(\beta^3)^4=\beta^5 \\ \alpha^5 & \mapsto & (\beta+1)^5=(\beta^3)^5=\beta \\ \alpha^6 & \mapsto & (\beta+1)^6=(\beta^3)^6=\beta^4 \end{array}$$

Isomorfismes de cossos

Per veure si és morfisme ompliu i observeu les taules de $f(a+b)$ i de $f(a)+f(b)$:

$f(a+b)$	$a=0$	$a=1$	$a=\alpha$	$a=\alpha^2$	$a=\alpha^3$	$a=\alpha^4$	$a=\alpha^5$	$a=\alpha^6$
$b=0$	$f(0)=0$	$f(1)=1$	$f(\alpha)=\beta^3$	$f(\alpha^2)=\beta^6$	$f(\alpha^3)=\beta^2$	$f(\alpha^4)=\beta^5$	$f(\alpha^5)=\beta$	$f(\alpha^6)=\beta^4$
$b=1$	$f(1)=1$	$f(0)=0$	$f(\alpha+1)=\beta$	$f(\alpha^2+1)=\beta^2$	$f(\alpha^3+1)=\beta^6$	$f(\alpha^4+1)=\beta^4$	$f(\alpha^5+1)=\beta^3$	$f(\alpha^6+1)=\beta^5$
$b=\alpha$								
$b=\alpha^2$								
$b=\alpha^3$								
$b=\alpha^4$								
$b=\alpha^5$								
$b=\alpha^6$								

$f(a)+f(b)$	$a=0$	$a=1$	$a=\alpha$	$a=\alpha^2$	$a=\alpha^3$	$a=\alpha^4$	$a=\alpha^5$	$a=\alpha^6$
$b=0$	$0+0=0$	$1+0=1$	$\beta^3+0=\beta^3$	$\beta^6+0=\beta^6$	$\beta^2+0=\beta^2$	$\beta^5+0=\beta^5$	$\beta+0=\beta$	$\beta^4+0=\beta^4$
$b=1$	$0+1=1$	$1+1=0$	$\beta^3+1=\beta$	$\beta^6+1=\beta^2$	$\beta^2+1=\beta^6$	$\beta^5+1=\beta^4$	$\beta+1=\beta^3$	$\beta^4+1=\beta^5$
$b=\alpha$								
$b=\alpha^2$								
$b=\alpha^3$								
$b=\alpha^4$								
$b=\alpha^5$								
$b=\alpha^6$								

Isomorfismes de cossos

Ompliu i observeu les taules de $f(ab)$ i de $f(a)f(b)$:

$f(ab)$	$a=0$	$a=1$	$a=\alpha$	$a=\alpha^2$	$a=\alpha^3$	$a=\alpha^4$	$a=\alpha^5$	$a=\alpha^6$
$b=0$	$f(0)=0$	$f(0)=0$	$f(0)=0$	$f(0)=0$	$f(0)=0$	$f(0)=0$	$f(0)=0$	$f(0)=0$
$b=1$	$f(0)=0$	$f(1)=1$	$f(\alpha)=\beta^3$	$f(\alpha^2)=\beta^6$	$f(\alpha^3)=\beta^2$	$f(\alpha^4)=\beta^5$	$f(\alpha^5)=\beta$	$f(\alpha^6)=\beta^4$
$b=\alpha$	$f(0)=0$	$f(\alpha)=\beta^3$	$f(\alpha^2)=\beta^6$	$f(\alpha^3)=\beta^2$	$f(\alpha^4)=\beta^5$	$f(\alpha^5)=\beta$	$f(\alpha^6)=\beta^4$	$f(1)=1$
$b=\alpha^2$								
$b=\alpha^3$								
$b=\alpha^4$								
$b=\alpha^5$								
$b=\alpha^6$								

$f(a)f(b)$	$a=0$	$a=1$	$a=\alpha$	$a=\alpha^2$	$a=\alpha^3$	$a=\alpha^4$	$a=\alpha^5$	$a=\alpha^6$
$b=0$	$0\cdot 0=0$	$1\cdot 0=0$	$\beta^3\cdot 0=0$	$\beta^6\cdot 0=0$	$\beta^2\cdot 0=0$	$\beta^5\cdot 0=0$	$\beta\cdot 0=0$	$\beta^4\cdot 0=0$
$b=1$	$0\cdot 1=0$	$1\cdot 1=1$	$\beta^3\cdot 1=\beta^3$	$\beta^6\cdot 1=\beta^6$	$\beta^2\cdot 1=\beta^2$	$\beta^5\cdot 1=\beta^5$	$\beta\cdot 1=\beta$	$\beta^4\cdot 1=\beta^4$
$b=\alpha$	$0\cdot\beta^3=0$	$1\cdot\beta^3=\beta^3$	$\beta^3\cdot\beta^3=\beta^6$	$\beta^6\cdot\beta^3=\beta^2$	$\beta^2\cdot\beta^3=\beta^5$	$\beta^5\cdot\beta^3=\beta$	$\beta\cdot\beta^3=\beta^4$	$\beta^4\cdot\beta^3=1$
$b=\alpha^2$								
$b=\alpha^3$								
$b=\alpha^4$								
$b=\alpha^5$								
$b=\alpha^6$								

Isomorfismes de cossos

Es tracta d'un morfisme? I d'un isomorfisme?

Extensions de cossos

Definició

Si E és un cos, diem que $F \subseteq E$ és un **subcòs** de E si F també té estructura de cos amb les mateixes operacions que E. Diem que E és una **extensió** de F.

Per demostrar que un subconjunt F d'un cos E és un subcòs s'ha de comprovar que

1. Si $a, b \in F$, aleshores $a + b, a - b \in F$ i $ab \in F$,
2. Si $a \in F$, aleshores a té invers a F.

Extensions de cossos

Exercici 3

Demostreu que si E és una extensió de F, aleshores E és un espai vectorial sobre F.

Definició

Anomenem **grau** de l'extensió de E sobre F a la dimensió de E com a F-espai vectorial, si aquesta és finita. La denotem $[\boldsymbol{E : F}]$.

Extensions de cossos

Exemple

$\mathbb{R}$ és una extensió de $\mathbb{Q}$ de dimensió infinita mentres que $\mathbb{C}$ és una extensió de $\mathbb{R}$ de dimensió 2. Una base de $\mathbb{C}$ respecte $\mathbb{R}$ és $\{1, i\}$.

Exemple

$\mathbb{Z}_2[x]/(x^3 + x + 1)$ és una extensió de $\mathbb{Z}_2$ de dimensió 3, que té per base respecte $\mathbb{Z}_2$ els elements $\{1, \alpha, \alpha^2\}$, on α és la classe de x.

Polinomis sobre un cos

Donat un cos F direm $F[X]$ al conjunt de polinomis amb coeficients a F en la indeterminada X.

Per exemple, si $F = \mathbb{Z}_3[x]/(x^2 + 2x + 2)$ i diem α a la classe de x en $\mathbb{Z}_3[x]/(x^2 + 2x + 2)$, aleshores $F = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^7\}$.

L'element $\alpha^2 X^7 + \alpha^6 X^4 + 2X^3 + 1$ serà un polinomi de $F[X]$. Podem avaluar-lo, per exemple, en α i ens donarà $\alpha^9 + \alpha^{10} + 2\alpha^3 + 1 = \alpha + \alpha^2 + \alpha^7 + 1 = \ldots$.

L'element $X^8 + X^5 + 2X + 1$ serà un polinomi que el podem veure tant com un polinomi de $\mathbb{Z}_3[X]$ com un polinomi de $F[X]$ perquè els seus coeficients són de $\mathbb{Z}_3 \subset F$.

Quan la distinció entre x i X quedi clara pel context, emprarem x en ambdós casos. Així, si estem treballant a F, podrem dir que el polinomi $\alpha^2 x^7 + \alpha^6 x^4 + 2x^3 + 1$ és un polinomi de $F[x]$.

Algunes generalitats de cossos

Característica i cardinal d'un cos finit

Ordre multiplicatiu i teorema de l'element primitiu

Polinomi mínim i caracterització dels cossos finits

Existència d'un cos finit de p^m elements

Unicitat del cos finit de p^m elements

Solucions

Característica d'un cos finit

Definició

Diem que un cos té **característica** a si a és el menor enter positiu tal que

$$\underbrace{1 + 1 + \cdots + 1}_{a} = 0,$$

si aquest enter existeix. Diem que la característica del cos és 0 en cas contrari.

Exemple

El cos $\{a, e, i, o\}$ *definit en exemples anteriors té característica* 2*, el cos* $\mathbb{Z}_3[x]/(x^2 + 2x + 2)$ *té característica* 3*.*

Característica d'un cos finit

Lema 1

Si un cos té característica positiva, aleshores la seva característica és necessàriament un nombre primer.

Demostració

Diem F al cos. Si la característica a de F pogués descomposar de manera no trivial en dos enters positius, $a = bc$, aleshores,

$$0 = \underbrace{\underbrace{1 + 1 + \cdots + 1}_{b} + \underbrace{1 + 1 + \cdots + 1}_{b} + \cdots + \underbrace{1 + 1 + \cdots + 1}_{b}}_{c}.$$

Com que $b < a$, l'element $\underbrace{1 + 1 + \cdots + 1}_{b}$ és no nul i, per tant, té un invers dins de F. Anomenem $\tilde{b}$ aquest invers. Multiplicant la igualtat anterior per $\tilde{b}$ obtenim que $\underbrace{1 + 1 + \cdots + 1}_{c} = 0$, en contradicció amb l'elecció de c.

□

Característica d'un cos finit

Lema 2

En un cos F de característica $p > 0$, per tota col·lecció finita d'elements $a_1, \ldots a_i \in F$ es té

$$(a_1 + a_2 + \cdots + a_i)^p = a_1^p + a_2^p + \cdots + a_i^p.$$

Demostració

Per $i = 2$, $(a_1 + a_2)^p = \sum_{j=0}^{p} \binom{p}{j} a_1^j a_2^{p-j}$. Però tots els coeficients $\binom{p}{j}$ són múltiples de p llevat de $\binom{p}{0}$ i $\binom{p}{p}$, d'on es dedueix que $(a_1 + a_2)^p = \binom{p}{0} a_2^p + \binom{p}{p} a_1^p = a_1^p + a_2^p$.

Per $i > 2$, utilitzant el cas anterior i la hipòtesi d'inducció,

$(a_1 + a_2 + \cdots + a_i)^p = ((a_1 + a_2 + \cdots + a_{i-1}) + a_i)^p =$
$(a_1 + a_2 + \cdots + a_{i-1})^p + a_i^p = a_1^p + a_2^p + \cdots + a_i^p.$ □

Característica d'un cos finit

Exercici 4

Què passa en el lema anterior si canviem algun $+$ per $-$? Indicació: Podeu separar els casos de característica parell i de característica senar.

Cos primer d'un cos finit

Suposem que F és un cos de característica positiva i diem p a la característica de F. El conjunt

$$K = \{1, 1+1, \ldots, \underbrace{1+1+\cdots+1}_{p-1}, \underbrace{1+1+\cdots+1}_{p} = 0\}$$

és un subcòs de F. De fet, K és isomorf a $\mathbb{Z}_p$.

Definició

El **cos primer** de F és el seu subcòs $K = \{1, 1+1, \ldots, \underbrace{1+1+\cdots+1}_{p-1}, \underbrace{1+1+\cdots+1}_{p} = 0\}$ o, simplement, $\mathbb{Z}_p$.

Cos primer d'un cos finit

Lema 3

El cos primer K d'un cos F de característica positiva p compleix que K és el conjunt d'arrels de $x^p - x \in F[x]$.

Demostració

L'element 0 *és òbviament una arrel de* $x^p - x$ *i, pel teorema petit de Fermat, també tots els elements de* $\mathbb{Z}_p$ *no nuls són arrels de* $x^p - x$*. Com que* F *és un cos, el polinomi* $x^p - x$ *té com a molt* p *arrels i com que hem vist que els* p *elements de* $\mathbb{Z}_p$ *són arrels, aquestes seran exactament totes les arrels.* □

Com a conseqüència, un element $a \in F$ pertany a K si i només si $a^p = a$.

Cos primer d'un cos finit

Lema 4

Sigui F un cos de característica $p > 0$. Un polinomi $f(x) \in F(x)$ pertany a $\mathbb{Z}_p[x]$ si i només si $(f(x))^p = f(x^p)$.

Demostració

Suposem que $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_r x^r$ *per algun enter* r *i per* $a_0, \ldots, a_r \in F$.
Aleshores $(f(x))^p = (a_0 + a_1 x + a_2 x^2 + \cdots + a_r x^r)^p = a_0^p + a_1^p x^p + a_2^p (x^p)^2 + \cdots + a_r^p (x^p)^r$ *mentres que* $f(x^p) = a_0 + a_1 x^p + a_2 (x^p)^2 + \cdots + a_r (x^p)^r$.
Per tant, $(f(x))^p = f(x^p)$ *si i només si* $a_i^p = a_i$ *per tot* i *entre* 0 *i* r, *és a dir, si i només si* $f(x) \in \mathbb{Z}_p[x]$. □

Cardinal d'un cos finit

Teorema 1

Si un cos F és finit, aleshores el seu cardinal és p^m per algun primer p i un enter positiu m.

Demostració

Sigui p la caraterística i sigui K el cos primer de F. Per l'Exercici 3, sabem que F és un K-espai vectorial. Si la dimensió de F sobre K és m, aleshores existeix una base $x_1, \ldots, x_m$ de F sobre K. Aleshores els elements de F són totes les combinacions lineals $\lambda_1 x_1 + \cdots + \lambda_m x_m$ amb tots els $\lambda_i \in K$. Com que K té p elements, necessàriament, $|F| = p^m$. □

Ordre multiplicatiu

Lema 5

En un cos finit F de q elements, qualsevol element $\alpha \in F \setminus \{0\}$ satisfà que $a^{q-1} = 1$.

Demostració

Per tot $\beta, \beta' \in F \setminus \{0\}$, *es té que* $\alpha\beta = \alpha\beta'$ *si i només si* $\beta = \beta'$ *i, a més a més,* $\alpha\beta \neq 0$. *Per tant,* $\{\alpha\beta : \beta \in F \setminus \{0\}\} = \{\beta : \beta \in F \setminus \{0\}\}$ *i*

$$\prod_{\beta \in F \setminus \{0\}} \alpha\beta = \prod_{\beta \in F \setminus \{0\}} \beta.$$

En conseqüència, $\alpha^{q-1} \prod_{\beta \in F \setminus \{0\}} \beta = \prod_{\beta \in F \setminus \{0\}} \beta$, *d'on deduïm que* $\alpha^{q-1} = 1$, *ja que el producte* $\prod_{\beta \in F \setminus \{0\}} \beta$ *és invertible.* □

Ordre multiplicatiu

Definició

En un cos finit F, l'**ordre multiplicatiu** d'un element $\alpha \in F \setminus \{0\}$ és el mínim exponent $i > 0$ tal que $\alpha^i = 1$. L'anomenem $ord_F(\alpha)$.

Lema 6

En un cos finit F, si $\alpha \in F \setminus \{0\}$ satisfà $\alpha^c = 1$ amb $c > 0$, aleshores $\text{ord}_F(\alpha) \mid c$.

Demostració

Suposem que $a = \text{ord}_F(\alpha)$. *Sigui* r *el residu de la divisió euclidiana de* c *entre* a. *Tindrem* $\alpha^r = \alpha^c = 1$ *amb* $0 \leq r < a$. *Això només és possible si* $r = 0$ *i, per tant, si* a *divideix* c. □

Ordre multiplicatiu

Corol·lari 1

Si F és un cos finit de q elements i $\alpha \in F \setminus \{0\}$, aleshores $\text{ord}_F(\alpha) \mid q-1$.

Ordre multiplicatiu

Lema 7

En un cos finit F, si existeixen $\alpha, \beta \in F \setminus \{0\}$ amb $a = ord_F(\alpha)$ i $b = ord_F(\beta)$, aleshores existeix $\gamma \in F \setminus \{0\}$ tal que $ord_F(\gamma) = \text{mcm}(a, b)$.

Demostració

Si $\text{mcd}(a, b) = 1$*, aleshores* $\alpha\beta$ *té ordre ab. En efecte, d'una banda* $(\alpha\beta)^{ab} = 1^b 1^a = 1$*. D'altra banda, si per algun* $c < ab$ *es compleix* $(\alpha\beta)^c = 1$*, aleshores* $1 = (\alpha\beta)^{bc} = \alpha^{bc}$*. Deduïm que* $a \mid bc$ *i, com que* $\text{mcd}(a, b) = 1$*, aleshores* $a \mid c$*. De manera anàloga podem veure que* $b \mid c$*. Per tant,* $ab \mid c$*, en contradicció amb l'elecció de c.* □

Ordre multiplicatiu

Lema 7

En un cos finit F, si existeixen $\alpha, \beta \in F \setminus \{0\}$ amb $a = ord_F(\alpha)$ i $b = ord_F(\beta)$, aleshores existeix $\gamma \in F \setminus \{0\}$ tal que $ord_F(\gamma) = \text{mcm}(a, b)$.

Demostració

Si $\text{mcd}(a, b) = d > 1$,

- *Podem descompondre* d *en producte de primers* $d = p_1^{e_1} \cdot \cdots \cdot p_s^{e_s}$ *de manera que* $p_1^{e_1+1} \nmid a, \ldots, p_k^{e_k+1} \nmid a$ *mentres que* $p_{k+1}^{e_{k+1}+1} \nmid b$, $\ldots, p_s^{e_s+1} \nmid b$. *Diem* $d_1 = p_1^{e_1} \cdot \cdots \cdot p_k^{e_k}$, $d_2 = p_{k+1}^{e_{k+1}} \cdot \cdots \cdot p_s^{e_s}$. *Tindrem* $\text{mcd}(\frac{a}{d_1}, \frac{b}{d_2}) = 1$ *mentres que* $\text{mcm}(a, b) = \frac{a}{d_1}\frac{b}{d_2}$.
- α^{d_1} *té ordre* $\frac{a}{d_1}$. *En efecte, d'una banda* $(\alpha^{d_1})^{\frac{a}{d_1}} = 1$. *D'altra banda, si per algun enter* $c < \frac{a}{d_1}$ *es compleix* $(\alpha^{d_1})^c = 1$, *aleshores* $\alpha^{d_1 c} = 1$ *i, per tant,* $a \mid d_1 c$. *Deduïm que* $\frac{a}{d_1} \mid c$. *Anàlogament,* β^{d_2} *té ordre* $\frac{b}{d_2}$.
- *Com que* $\text{mcd}(\frac{a}{d_1}, \frac{b}{d_2}) = 1$, *aleshores* $\alpha^{d_1}\beta^{d_2}$ *té ordre* $\frac{a}{d_1}\frac{b}{d_2} = \text{mcm}(a, b)$.

□

Teorema de l'element primitiu

Lema 8

Suposem que en un cos finit F els ordres multiplicatius de tots els elements no nuls són $a_1, a_2, \ldots, a_k$. Aleshores existeix un element $\xi \in F \setminus \{0\}$ tal que $ord_F(\xi) = \text{mcm}(a_1, \ldots, a_k)$.

El lema es pot demostrar per inducció utilitzant el resultat demostrat per dos elements i la recurrència

$$\text{mcm}(a_1, \ldots, a_k) = \text{mcm}(\text{mcm}(a_1, \ldots, a_{k-1}), a_k).$$

Teorema de l'element primitiu

Lema 9

En un cos finit de q elements, el mínim comú múltiple dels ordres de tots els elements no nuls del cos és $q-1$.

Demostració

Diem M al mínim comú múltiple dels ordres de tots els elements no nuls del cos. D'una banda $M \leq q-1$, ja que tots els ordres de tots elements no nuls del cos són divisors de $q-1$ i, per tant, M serà un divisor de $q-1$. D'altra banda es pot veure que $M \geq q-1$. En efecte, per a tot $\alpha \in F \setminus \{0\}$ es té $\alpha^M = 1$, per tant tot $\alpha \in F \setminus \{0\}$ és arrel de $x^M - 1 \in F[x]$ i, com que F és un cos, $q-1 \leq M$. □

Teorema de l'element primitiu

Definició

Diem que un element no nul ξ d'un cos finit F de q elements és un **element primitiu** del cos si el seu ordre multiplicatiu és $q-1$.

De tots els lemes anteriors es dedueix el teorema següent:

Teorema 2: Teorema de l'element primitiu

Tot cos finit té un element primitiu.

Exercici 5

Demostreu que en un cos finit de q elements hi ha exactament $\phi(q-1)$ elements primitius.

Teorema de l'element primitiu

Lema 10

En un cos finit F de q elements, per a tot divisor de $q-1$ existeix un element del cos amb ordre multiplicatiu igual a aquest divisor.

Demostració

Sigui ξ un element primitiu de F i sigui d un divisor de $q-1$. L'element $\xi' = \xi^{(q-1)/d}$ tindrà ordre d. En efecte, d'una banda $\xi'^d = 1$. D'altra banda, si $\xi'^c = 1$, aleshores $\xi^{c(q-1)/d} = 1$ amb el que $c(q-1)/d \geq q-1$ i, per tant, $c \geq d$.

□

Polinomi mínim

Suposem que tenim un cos finit F de p^m elements.

Observem que si un element $\gamma \in F$ té $ord_F(\gamma) = r$, aleshores anul·la els polinomis $x^r - 1$ i $x^{p^m-1} - 1$.

Considerem el polinomi

$$m_\gamma(x) = (x-\gamma)(x-\gamma^p)(x-\gamma^{p^2}) \cdot \cdots \cdot (x-\gamma^{p^{s-1}}) \in \mathbb{Z}_p[x],$$

on s és el mínim enter positiu tal que $\gamma^{p^s} = \gamma$.

En particular, $s \leq m$ i, si γ és primitiu, aleshores $s = m$.

Veurem que $m_\gamma(x) \in \mathbb{Z}_p[x]$ i que té grau mínim d'entre tots els polinomis de $\mathbb{Z}_p[x]$ que s'anul·len quan els avaluem a γ.

Per això s'anomena el **polinomi mínim** de γ respecte $\mathbb{Z}_p$

Polinomi mínim

Lema 11

Sigui F un cos finit i sigui $\gamma \in F \setminus \{0\}$.

1. $m_\gamma(x) \in \mathbb{Z}_p[x]$.
2. Tot polinomi de $\mathbb{Z}_p[x]$ que s'anul·li a γ serà un múltiple de $m_\gamma(x)$.
3. $m_\gamma(x)$ és irreductible a $\mathbb{Z}_p[x]$.

Demostració

1. *Observem que* $(m_\gamma(x))^p = (x^p - \gamma^p)(x^p - \gamma^{p^2}) \cdot \cdots \cdot (x^p - \gamma^{p^{s-1}})(x^p - \gamma) = m_\gamma(x^p)$. *Per tant,* $m_\gamma(x) \in \mathbb{Z}_p[x]$.
2. *Si un polinomi* $f(x) \in \mathbb{Z}_p[x]$ *satisfà* $f(\gamma) = 0$, *aleshores* $(f(\gamma))^{p^i} = 0$ *per qualsevol* i. *Però* $(f(\gamma))^{p^i} = f(\gamma^{p^i}) = 0$ i, *per això,* f *haurà de tenir les arrels* $\gamma, \gamma^p, \ldots, \gamma^{p^{s-1}}$. *En conseqüència, haurà de ser un múltiple de* $m_\gamma(x)$.
3. *Com que* $m_\gamma(\gamma) = 0$, *algun dels factors irreductibles de* $m_\gamma(x)$ *s'haurà d'anul·lar també a* γ. *Pel punt anterior, aquest factor irreductible haurà de ser un múltiple de* $m_\gamma(x)$ *amb el que no queda més remei que* $m_\gamma(x)$ *sigui el propi factor irreductible.*

□

Caracterització dels cossos finits

Teorema 3: Caracterització dels cossos finits

Tot cos finit és de la forma $\mathbb{Z}_p/(f(x))$ amb p primer i $f(x)$ un polinomi irreductible de $\mathbb{Z}_p[x]$.

Demostració

Sigui F un cos finit i sigui p la seva característica. Considerem un element primitiu $\xi \in F$ i el seu polinomi mínim $m_\xi(x) \in \mathbb{Z}_p[x]$. Aleshores F és el cos $\mathbb{Z}_p[x]/(m_\xi(x))$. □

Existència d'un cos amb les arrels de $x^{p^m} - x$

Donat un cos qualsevol F i un polinomi $f(x)$ de $F[x]$ podem definir les classes de congruència dels elements de $F[x]$ mòdul el polinomi $f(x)$ tal i com havíem fet per $\mathbb{Z}_p[x]$.

El conjunt de classes formarà un cos si i només si el polinomi $f(x)$ és irreductible a $F[x]$. El grau de l'extensió serà el grau del polinomi.

Exemple

El polinomi x^2+1 és irreductible a $\mathbb{R}[x]$. En el conjunt de classes de $C = \mathbb{R}[x]/(x^2+1)$ podem anomenar i a la classe de x. Qualsevol element de C el podrem escriure com $a+bi$ amb $a, b \in \mathbb{R}$. Les operacions suma i producte seran

$$(a+bi)+(a'+b'i) = (a+a')+(b+b')i,$$

$$(a+bi)(a'+b'i) = (aa')+(ab'+a'b)i+(bb')i^2 = (aa'-bb')+(ab'+a'b)i.$$

Observem que $C \cong \mathbb{C}$.

Existència d'un cos amb les arrels de $x^{p^m} - x$

Definició

Donat un cos F i un polinomi irreductible $f(x) \in F[x]$, del cos format pel conjunt de classes de congruència mòdul el polinomi $f(x)$ en diem l'**extensió de F pel polinomi $f(x)$** i el denotem $F[x]/(f(x))$.

És fàcil comprovar que $F[x]/(f(x))$ tindrà la mateixa característica i el mateix cos primer que F.

Observem com el polinomi $f(x)$, que no tenia arrels a F, ara té l'arrel corresponent a la classe de x dins de $F[x]/(f(x))$. En particular, el nombre d'arrels de $f(x)$ ha augmentat, de F a $F[x]/(f(x))$.

Existència d'un cos amb les arrels de $x^{p^m} - x$

Lema 12

Per tot enter positiu m existeix una extensió de $\mathbb{Z}_p$ que conté totes les arrels de $x^{p^m} - x$.

Existència d'un cos amb les arrels de $x^{p^m} - x$

Demostració

Diem $E_1 = \mathbb{Z}_p$. Suposem que totes les arrels de $x^{p^m} - x$ dins de E_1 són $\alpha_1 = 0, \alpha_2, \ldots, \alpha_{n_1}$ (poden ser repetides). Aleshores,

$$x^{p^m} - x = x(x - \alpha_2)\cdots(x - \alpha_{n_1}) f_1(x)$$

per un únic polinomi mònic $f_1(x) \in E_1[x]$. Diem $i_1(x)$ a un qualsevol dels factors irreductibles de $f_1(x)$ dins de $E_1[x]$. Construïm $E_2 = E_1[x]/(i_1(x))$.

Ara suposem que totes les arrels de $x^{p^m} - x$ dins de E_2 són $\alpha_1 = 0, \alpha_2, \ldots, \alpha_{n_1}, \ldots, \alpha_{n_2}$ (amb repeticions si cal). Necessàriament, $n_2 > n_1$ per la manera com hem construït E_2. A més, com que E_2 és un cos, $n_2 \leq \text{grau}(x^{p^m} - x) = p^m$. Així,

$$n_1 < n_2 \leq p^m.$$

Mentres $n_i < p^m$ podem repetir el procediment. És a dir, considerem l'únic polinomi mònic $f_2(x) \in E_2[x]$ tal que

$$x^{p^m} - x = x(x - \alpha_2)\cdots(x - \alpha_{n_2}) f_2(x).$$

Diem $i_2(x)$ a un qualsevol dels factors irreductibles de $f_2(x)$ dins de $E_2[x]$ i construïm $E_3 = E_2[x]/(i_2(x))$. Ara totes les arrels de $x^{p^m} - x$ dins de E_3 seran $\alpha_1 = 0, \alpha_2, \ldots, \alpha_{n_1}, \ldots, \alpha_{n_2}, \ldots, \alpha_{n_3}$ amb

$$n_1 < n_2 < n_3 \leq p^m.$$

En algun moment n_i coincidirà amb p^m i, en aquest moment, E_i contindrà totes les arrels de $x^{p^m} - x$. □

Existència d'un cos amb les arrels de $x^{p^m} - x$

Definició

Donat un cos F i un polinomi $f(x) = \sum_{i=0}^{d} a_i x^i \in F[x]$, definim la **derivada formal** de $f(x)$ com

$$f'(x) = \sum_{i=1}^{d} i a_i x^{i-1}.$$

Exercici 6

Comproveu les següents propietats:

- $(f(x)g(x))' = f(x)'g(x) + f(x)g'(x)$,
- $(f(g(x)))' = f'(g(x))g'(x)$.

Existència d'un cos amb les arrels de $x^{p^m} - x$

Lema 13

Si una extensió E de F conté totes les arrels de $f(x) \in F[x]$, aleshores totes les arrels en E són diferents si i només si $\text{mcd}(f(x), f'(x)) = 1$.

Demostració

Si $f(x)$ tingués una arrel múltiple α, aleshores $f(x) = (x-\alpha)^2 g(x)$ amb $g(x)$ un polinomi de grau dos menys que el grau de $f(x)$. Aleshores $f'(x) = 2(x-\alpha)g(x) + (x-\alpha)^2 g'(x)$. Observem que en aquest cas $(x-\alpha)$ divideix tant $f(x)$ com $f'(x)$ i, per tant, $\text{mcd}(f(x), f'(x)) \neq 1$. *Recíprocament, si* $\text{mcd}(f(x), f'(x)) \neq 1$, *el polinomi $r(x) = \text{mcd}(f(x), f'(x)) \neq 1$ també tindrà totes les arrels a E. Sigui α una arrel de $r(x)$. Escrivim $f(x) = (x-\alpha)h(x)$ amb $h(x)$ un polinomi de grau un menys que el grau de $f(x)$. Tindrem $f'(x) = h(x) + (x-\alpha)h'(x)$, d'on deduïm que $(x-\alpha)$ ha de dividir $h(x)$ i, per tant, α és una arrel múltiple de $f(x)$.* □

Existència d'un cos amb les arrels de $x^{p^m} - x$

El lema següent és una conseqüència del Lema 12, el Lema 13, i el fet que la derivada formal de $x^{p^m} - x$ és -1 a $\mathbb{Z}_p$.

Lema 14

Per tot enter positiu m existeix una extensió de $\mathbb{Z}_p$ que conté totes les arrels de $x^{p^m} - x$ i totes elles són diferents.

Existència d'un cos finit de p^m elements

Teorema 4: Existència de cossos finits

Per tot enter positiu m existeix un cos finit de cardinal p^m.

Demostració

Pel Lema 14 existeix una extensió E de $\mathbb{Z}_p$ que conté totes les arrels de $x^{p^m} - x$ i totes elles són diferents. Considerem el conjunt $A \subseteq E$ de totes les arrels de $x^{p^m} - x$. Com que sabem que són diferents i el grau de $x^{p^m} - x$ és p^m podem afirmar que el cardinal de A és exactament p^m. Vegem que A és un subcòs de E (i, per tant, és un cos). Suposem que $a, b \in A$, aleshores hem de comprovar que $a+b, a-b, ab, a^{-1}$ són arrels de $x^{p^m} - x$. En efecte,

- $(a+b)^{p^m} - (a+b) = a^{p^m} + b^{p^m} - a - b = (a^{p^m} - a) + (b^{p^m} - b) = 0,$
- $(a-b)^{p^m} - (a-b) = a^{p^m} - b^{p^m} - a + b = (a^{p^m} - a) - (b^{p^m} - b) = 0,$
- $(ab)^{p^m} - (ab) = a^{p^m} b^{p^m} - ab = ab - ab = 0,$
- $(a^{-1})^{p^m} - a^{-1} = (a^{p^m})^{-1} - a^{-1} = a^{-1} - a^{-1} = 0.$

□

Factorització del polinomi $x^{p^m} - x$

Lema 15

En un cos finit F de p^m elements, els seus p^m elements són exactament les arrels de $x^{p^m} - x$. És a dir,

$$\prod_{\alpha \in F} (x - \alpha) = x^{p^m} - x$$

Demostració

Com que els p^m elements de F són arrels de $x^{p^m} - x$ tenim que $\prod_{\alpha \in F}(x - \alpha)$ divideix $x^{p^m} - x$. Però com que tots dos polinomis són mònics i tenen el mateix grau, han de coincidir. □

En particular, totes les arrels de $x^{p^m} - x$ dins de F són diferents.

Factorització del polinomi $x^{p^m} - x$

Exercici 7

Demostreu que els factors irreductibles de la descomposició de $x^{p^m} - x$ dins de $\mathbb{Z}_p[x]$ són tots diferents.

Exercici 8

Demostreu que si $f(x) \in \mathbb{Z}_p[x]$ és irreductible a $\mathbb{Z}_p[x]$, aleshores $f(x)$ ha de dividir $x^{p^{\text{grau}(f)}} - x$.

Factorització del polinomi $x^{p^m} - x$

Exercici 9

Sigui F un cos finit de p^m elements. Si $\gamma \in F$ definim $C_\gamma = \{\gamma, \gamma^p, \gamma^{p^2}, \ldots, \gamma^{p^{s-1}}\}$ on s és el mínim enter positiu tal que $\gamma^{p^s} = \gamma$.

- Qui són C_0 i C_1?
- Demostreu que si $\gamma' \notin C_\gamma$, aleshores $C_\gamma \cap C_{\gamma'} = \varnothing$.
- Demostreu que existeix un subconjunt $\Gamma(F) = \{\gamma_1, \ldots, \gamma_r\} \subseteq F$ tal que F és la unió disjunta de $C_{\gamma_1}, \ldots, C_{\gamma_r}$.
- Demostreu que

$$x^{p^m} - x = \prod_{\gamma \in \Gamma(F)} m_\gamma(x).$$

Factorització del polinomi $x^{p^m} - x$

Exercici 10

Demostreu que en un cos finit F de p^m elements,

- $\prod_{\alpha \in F \setminus \{0\}} \alpha = -1$
- Si $p^m \neq 2$, $\sum_{\alpha \in F \setminus \{0\}} \alpha = 0$

Unicitat del cos finit de p^m elements

Teorema 5: Unicitat del cos finit de p^m elements

Tots els cossos finits del mateix cardinal són isomorfs.

Demostració

Suposem que E i F són dos cossos finits amb el mateix cardinal. Pel Teorema 1 sabem que aquest cardinal és p^m per algun primer p i algun enter positiu m. Pel Teorema 2 sabem que E té un element primitiu que anomenem ξ. Com que ξ és primitiu, el grau del seu polinomi mínim és m. Per l'Exercici 9 sabem que el polinomi mínim de ξ coincidirà amb el polinomi mínim d'algun element $\zeta \in F$. Sabem que $\{1, \xi, \xi^2, \ldots, \xi^{m-1}\}$ és una $\mathbb{Z}_p$-base de E mentres que $\{1, \zeta, \zeta^2, \ldots, \zeta^{m-1}\}$ és una $\mathbb{Z}_p$-base de F i que, per tot exponent i, les coordenades de ξ^i en la base $\{1, \xi, \xi^2, \ldots, \xi^{m-1}\}$ coincidiran amb les coordenades de ζ^i en la base $\{1, \zeta, \zeta^2, \ldots, \zeta^{m-1}\}$. Aquestes coordenades les denotem $(\lambda_0^i, \ldots, \lambda_{m-1}^i)$. Recíprocament diem que

$$i = \log(\lambda_0^i + \lambda_1^i \xi + \cdots + \lambda_{m-1}^i \xi^{m-1}) = \log(\lambda_0^i + \lambda_1^i \zeta + \cdots + \lambda_{m-1}^i \zeta^{m-1}).$$

□

Unicitat del cos finit de p^m elements

Teorema 5: Unicitat del cos finit de p^m elements

Tots els cossos finits del mateix cardinal són isomorfs.

Demostració

Definim l'aplicació $f : E \to F$ que assigna $0 \in E$ a $0 \in F$ i que per tot $i > 0$ assigna $f(\xi^i) = \zeta^i$. Vegem que és un isomorfisme.

$$
\begin{aligned}
f(\xi^i + \xi^j) &= f\big((\lambda_0^i + \lambda_1^i \xi + \cdots + \lambda_{m-1}^i \xi^{m-1}) + (\lambda_0^j + \lambda_1^j \xi + \cdots + \lambda_{m-1}^j \xi^{m-1}) \big) \\
&= f\big((\lambda_0^i + \lambda_0^j)1 + (\lambda_1^i + \lambda_1^j)\xi + \cdots + (\lambda_{m-1}^i + \lambda_{m-1}^j)\xi^{m-1} \big) \\
&= f\big(\xi^{\log((\lambda_0^i+\lambda_0^j)1+\cdots+(\lambda_{m-1}^i+\lambda_{m-1}^j)\xi^{m-1})}\big) \\
&= \zeta^{\log((\lambda_0^i+\lambda_0^j)1+\cdots+(\lambda_{m-1}^i+\lambda_{m-1}^j)\zeta^{m-1})} \\
&= (\lambda_0^i + \lambda_0^j)1 + \cdots + (\lambda_{m-1}^i + \lambda_{m-1}^j)\zeta^{m-1} \\
&= (\lambda_0^i + \lambda_1^i \zeta + \cdots + \lambda_{m-1}^i \zeta^{m-1}) + (\lambda_0^j + \lambda_1^j \zeta + \cdots + \lambda_{m-1}^j \zeta^{m-1}) \\
&= \zeta^i + \zeta^j = f(\xi^i) + f(\xi^j).
\end{aligned}
$$

□

Unicitat del cos finit de p^m elements

Teorema 5: Unicitat del cos finit de p^m elements

Tots els cossos finits del mateix cardinal són isomorfs.

Demostració

De la mateixa manera podem provar que $f(\xi^i - \xi^j) = f(\xi^i) - f(\xi^j)$.
D'altra banda,

$$\begin{aligned} f(\xi^i\xi^j) &= f(\xi^{i+j}) \\ &= \zeta^{i+j} \\ &= \zeta^i\zeta^j \\ &= f(\xi^i)f(\xi^j), \end{aligned} \qquad \begin{aligned} f((\xi^i)^{-1}) &= f(\xi^{p^m-1-i}) \\ &= \zeta^{p^m-1-i} \\ &= (\zeta^i)^{-1} \\ &= (f(\xi^i))^{-1}. \end{aligned}$$

□

Unicitat del cos finit de p^m elements

Pel teorema anterior, donada una potència de primer p^m podem escriure $\mathbb{F}_{p^m}$ per denotar *l'únic* cos finit de p^m elements.

Exercici 11

Construïu $\mathbb{F}_9$ utilitzant dos polinomis generadors diferents.

- Doneu les taules d'equivalències potencial polinòmica en ambdós casos.
- Expliciteu l'isomorfisme que existeix entre els dos cossos.

Unicitat del cos finit de p^m elements

Exercici 12

Pel que hem dit, el cos finit $\{a, e, i, o\}$ que té taula de sumes i de producte

$+$	a	e	i	o
a	o	i	e	a
e	i	o	a	e
i	e	a	o	i
o	a	e	i	o

$*$	a	e	i	o
a	e	i	a	o
e	i	a	e	o
i	a	e	i	o
o	o	o	o	o

ha de ser isomorf a $\mathbb{F}_4$. Construïu $\mathbb{F}_4$ a partir del seu cos primer i un polinomi generador i doneu la correspondència entre els elements obtinguts en aquesta construcció i els elements $\{a, e, i, o\}$.

Solució de l'Exercici 1

Sigui a un element de l'anell i sigui 0 el neutre per l'operació $\oplus$. Tenim

$$0 \otimes a = (0 \oplus 0) \otimes a = (0 \otimes a) \oplus (0 \otimes a).$$

Si ara sumem l'oposat de $0 \otimes a$ a banda i banda de la igualtat obtenim que

$$0 = 0 \otimes a,$$

com volíem veure.

Torna a l'exercici (p.7)

Solució de l'Exercici 2

Sigui a un element de l'anell i sigui 0 el neutre per l'operació $\oplus$. Tenim

$$0 \otimes a = (0 \oplus 0) \otimes a = (0 \otimes a) \oplus (0 \otimes a).$$

Si ara sumem l'oposat de $0 \otimes a$ a banda i banda de la igualtat obtenim que

$$0 = 0 \otimes a,$$

com volíem veure.

Torna a l'exercici (p.11)