

# Àlgebra Abstracta curs 07/08

## Estructura dels grups abelians finits

Jordi Quer

19 de setembre de 2007

Es recorda que si  $a$  és un element d'ordre  $n$  d'un grup, cada potència  $a^k$  té ordre  $n/\gcd(n, k)$ . En particular, per a cada divisor  $d \mid n$  l'element  $a^{n/d}$  té ordre  $d$ .

**Definició 1** *L'exponent d'un grup  $G$  és el menor enter  $m \geq 1$  tal que  $a^m = 1$  per a tot  $a \in G$  (o infinit, si no hi ha cap enter que compleixi aquesta condició).*

És clar que l'exponent d'un grup és el mínim comú múltiple dels ordres de tots els seus elements i que l'exponent d'un grup finit divideix el seu ordre. Exemples:

- el grup infinit  $(\mathbb{Z}/2\mathbb{Z})^{\mathbb{Z}} = \prod_{n \in \mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$  té exponent 2,
- el grup diedral  $D_{2n}$  té exponent  $[2, n]$ ,
- el grup  $\mathbb{Q}/\mathbb{Z}$ , que té tots els elements d'ordre finit, té exponent  $\infty$ ,
- el grup simètric  $\mathfrak{S}_n$  té exponent  $[2, 3, 4, \dots, n]$ .

**Lema 1** *Siguin  $n$  i  $m$  enters positius. Existeixen divisors  $n_0 \mid n$  i  $m_0 \mid m$  tals que*

$$(n_0, m_0) = 1 \quad i \quad n_0 m_0 = [n, m].$$

PROVA: Siguin  $p_1, \dots, p_k$  tots els divisors primers de  $nm$ . Es pot escriure

$$n = p_1^{r_1} \cdots p_k^{r_k}, \quad m = p_1^{s_1} \cdots p_k^{s_k}, \quad \text{amb } r_i, s_i \geq 0.$$

Siguin

$$n_0 = \prod_{r_i \geq s_i} p_i^{r_i}, \quad m_0 = \prod_{r_i < s_i} p_i^{s_i}.$$

És clar que són divisors de  $n$  i de  $m$  respectivament i que compleixen les propietats que es demanaven.  $\square$

**Lema 2** *En un grup abelià  $A$ , siguin  $a, b$  elements d'ordres  $n$  i  $m$ , respectivament.*

1.  $\text{ord}(ab) \mid [n, m]$ ,
2. si  $(n, m) = 1$  aleshores  $\text{ord}(ab) = nm$ ,
3. A conté algun element d'ordre  $[n, m]$ .

Per tant tot grup abelià finit conté algun element d'ordre igual al seu exponent.

PROVA: 1. Sigui  $r = [n, m]$ . Aleshores  $(ab)^r = a^r b^r = 1$ .  
 2. Si  $(ab)^k = 1$  aleshores  $a^k = b^{-k}$ . Elevant a  $m$  es té

$$a^{mk} = (b^m)^{-k} = 1 \quad \Rightarrow \quad n \mid mk \quad \stackrel{(n,m)=1}{\Rightarrow} \quad n \mid k.$$

Elevant a  $n$  es veu que  $m \mid k$ . Per tant  $nm = [n, m] \mid k$ . Per tant  $nm \mid \text{ord}(ab)$ .

3. Siguin  $n_0, m_0$  com al lema anterior. Aleshores  $a^{n/n_0}$  i  $b^{m/m_0}$  tenen ordres  $n_0$  i  $m_0$ , respectivament. Per l'apartat anterior  $\text{ord}(a^{n/n_0} b^{m/m_0}) = n_0 m_0 = [n, m]$ .  $\square$

**Lema 3** Sigui  $A$  un grup abelià finit,  $a \in A$  un element d'ordre màxim  $d$  i  $\pi: A \rightarrow A/\langle a \rangle$  la projecció canònica.

Tot element del quocient  $A/\langle a \rangle$  té una antiimatge del seu mateix ordre.

PROVA: Recordi's que per a un morfisme de grups  $f$  qualsevol l'ordre de  $f(x)$  divideix l'ordre de  $x$ .

Sigui  $y \in A/\langle a \rangle$  d'ordre  $n$  i sigui  $x \in A$  amb  $\pi(x) = y$ . Aleshores  $\pi(x^n) = 1$  i per tant  $x^n \in \langle a \rangle$ . Sigui  $x^n = a^k$ . Com que  $d$  és l'exponent del grup  $A$ , l'ordre de  $x$  divideix, i com que  $n$  és un divisor de l'ordre de  $x$ , resulta que  $n \mid d$ . Elevant a  $d/n$  es té  $x^d = a^{kd/n} = 1$ . Per tant  $d \mid kd/n \Rightarrow nd \mid kd \Rightarrow n \mid k$ . Sigui  $k = nk_0$ . Aleshores l'element  $xa^{-k_0}$  compleix el que es demana: és també una antiimatge de  $y$ , i per tant té ordre divisible per  $n$ , i  $(xa^{-k_0})^n = x^n a^{-k} = 1$  de manera que el seu ordre és  $n$ .  $\square$

**Teorema 4** Tot grup abelià finit és isomorf a un producte de grups cíclics

$$A \simeq C_{d_1} \times C_{d_2} \times \cdots \times C_{d_r}, \quad \text{amb } d_1 \mid d_2 \mid \cdots \mid d_r.$$

A més, els enters  $d_i$  determinen unívocament la classe d'isomorfisme del grup.

PROVA: Es demostrarà per inducció sobre el cardinal del grup. És obvi si el grup té  $\leq 3$  elements. Suposi's demostrat per a tots els grups de cardinal més petit que el de  $A$ .

Sigui  $a$  un element de  $A$  d'ordre màxim  $d > 1$ . El quocient  $A/\langle a \rangle$  és abelià d'ordre estrictament menor que el de  $A$  i per inducció és isomorf a un producte de  $r$  grups cíclics  $C_{d_i}$ . Siguin  $y_1, \dots, y_r$  elements d'aquest quocient d'ordres  $d_1, \dots, d_r$  corresponents a un tal isomorfisme. Siguin  $x_1, \dots, x_r$  elements de  $A$  antiimatges per la projecció canònica dels mateixos ordres, que existeixen segons el lema anterior. Sigui  $B$  el subgrup de  $A$  generat per tots aquests elements,

$$B = \{x_1^{m_1} \cdots x_r^{m_r} : m_i \in \mathbb{Z}\}.$$

Com que  $x_i^{d_i} = 1$  és clar que el nombre d'elements de  $B$  és  $\leq \prod d_i$ . D'altra banda la restricció  $\pi|_B$  de la projecció  $\pi: A \rightarrow A/\langle a \rangle$  és exhaustiva i el grup quocient  $A/\langle a \rangle$  conté  $\prod d_i$  elements. Per tant  $|B| = \prod d_i = |A/\langle a \rangle|$ .

Es considera el morfisme  $B \times \langle a \rangle \rightarrow A$  definit per  $(b, a^k) = ba^k$ . Per a cada element  $\alpha \in A$  sigui  $\pi(\alpha) = y_1^{m_1} \cdots y_t^{m_t}$  i sigui  $b = x_1^{m_1} \cdots x_t^{m_t}$ . Aleshores  $\pi(\alpha b^{-1}) = 1$  i, per tant  $\alpha b^{-1} = a^k$ , de manera que  $\alpha = ba^k$  i el morfisme anterior és exhaustiu. Com que tots dos grups tenen el mateix cardinal, és bijectiu, i per tant  $A$  és isomorf a

$$B \times \langle a \rangle \simeq C_{d_1} \times C_{d_2} \times \cdots \times C_{d_r} \times C_d.$$

La condició  $d_r \mid d$  és conseqüència del fet que l'ordre de tot element (i  $d_r$  és l'ordre de  $x_r$ ) divideix l'exponent del grup, que és  $d$ .

Abans de veure que la descomposició és única, algunes observacions. Per a tot grup abelià  $A$ ,  $A^n = \{a^n : a \in A\}$  és un subgrup. És clar que  $(A \times B)^n = A^n \times B^n$  i que  $(A \times B)/(A \times B)^n = A/A^n \times B/B^n$ . En el cas cíclic, si  $C_d = \langle a \rangle$  aleshores  $C_d^n$  és el subgrup generat per  $a^n$ , que com que té ordre  $d/(n, d)$  és isomorf al grup  $C_{d/(n, d)}$ . Per tant el quocient  $C_d/C_d^n$  és isomorf a  $C_{(n, d)}$ .

És clar que dos grups isomorfs a un mateix producte de cíclics són isomorfs. Suposi's que un grup  $A$  admet isomorfismes en dos productes de cíclics

$$C_{d_1} \times C_{d_2} \times \cdots \times C_{d_r} \simeq A \simeq C_{e_1} \times C_{e_2} \times \cdots \times C_{e_s}$$

amb  $d_i \mid d_{i+1}$  i  $e_i \mid e_{i+1}$ . Sigui  $p$  un factor primer de  $d_1$ , i per tant un divisor de tots els  $d_i$ . Sigui  $e_k$ , amb  $k \geq 1$ , el primer dels  $e_i$  divisibles per  $p$ . Aleshores  $A/A^p$  és isomorf, d'una banda, a un producte de  $r$  grups  $C_p$ , i de l'altra, al producte de  $s - k + 1$  grups com aquest. Comparant els seus cardinals resulta que  $r = s - k + 1$  i per tant  $s \geq r$ . Fent el mateix amb un factor primer de  $e_1$  es dedueix la desigualtat contrària. Per tant  $s = r$  i  $p$  divideix tant  $d_1$  com  $e_1$ . Aleshores el grup  $A^p$ , que té cardinal estrictament menor que  $A$ , és isomorf a

$$C_{d_1/p} \times \cdots \times C_{d_r/p} \simeq A^p \simeq C_{e_1/p} \times \cdots \times C_{e_r/p},$$

i per hipòtesi d'inducció  $d_i/p = e_i/p$  d'on resulta que  $d_i = e_i$  per a tot  $i$ . □

Recordant l'isomorfisme del teorema xinès del residu  $C_n \times C_m \simeq C_{nm}$  si  $(n, m) = 1$  es veu que tot producte de grups cíclics es pot posar com a producte de grups cíclics d'ordre potència de  $p$ . De grups abelians d'ordre  $p^n$  n'hi ha tants com particions de  $n$ , o sigui com maneres d'escriure  $n = n_1 + n_2 + \cdots + n_r$  amb  $0 < n_1 \leq \cdots \leq n_r$ , a cadascuna de les quals li correspon el grup

$$C_{p^{n_1}} \times C_{p^{n_2}} \times \cdots \times C_{p^{n_r}}.$$

D'aquesta observació es dedueix que el nombre de grups abelians d'ordre  $N = \prod_{i=1}^r p_i^{m_i}$  és el producte  $P(m_1)P(m_2) \cdots P(m_r)$  dels nombres de particions corresponents.