Estructures Algebraiques
2017/2018

Carles Falcó i Gandia

Índex

1

Grups

1.1 Grups i subgrups

Definició 1.1.1. Direm que un conjunt G no buit i tancat amb una operació $\cdot : G \times G \to G$ és un grup si compleix:

1. $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ per tot $x, y, z \in G$
2. Existeix $e \in G$ tal que $e \cdot x = x \cdot e = x$ per tot $x \in G$
3. Per tot $x \in G$ existeix $y \in G$ tal que $x \cdot y = y \cdot x = e$

És a dir si l'operació $\cdot$ és associativa, té element neutre, i a més, per cada element de G existeix un element invers.

Definició 1.1.2. Direm que un grup G és abelià si l'operació commuta, ço és si $x \cdot y = y \cdot x$ per tot $x, y \in G$.

Amb això ja es poden provar algunes propietats.

Proposició 1.1.1. *G grup.*

1. *El neutre és únic.*
2. *Per tot $x \in G$ l'invers de x és únic.*

Demostració. 1. Siguin e, e' dos neutres. Tenim $e \cdot e' = e' = e$.

2. Sigui $x \in G$ i x_1, x_2 dos inversos de x, tenim $e = x \cdot x_1 = x \cdot x_2$. I ara fent $x_2 = x_2 \cdot e = x_2 \cdot (x \cdot x_1) = (x_2 \cdot x) \cdot x = x_1 \cdot e = x_1$.

□

Alguns exemples de grups són:

1. $(\mathbb{Z},+),(\mathbb{Q},+),(\mathbb{R},+)$
2. Si K és un cos i E un K-espai vectorial llavors $(E,+)$ és un grup. Igualment $(\mathbb{Z}/n\mathbb{Z},+)$.
3. De no commutatius tenim per exemple el grup simètric $S_n = \{\sigma : \{1,\dots,n\} \to \{1,\dots,n\} |\ \sigma \text{ és bijectiva}\}$ amb la composició $\circ$. $(S_n,\circ)$ no és commutatiu si $n > 2$.
4. També $GL_n(K) = \{A \in M_n(K) | A \text{ és invertible}\}$ amb el producte de matrius $(GL_n(K),\cdot)$ és un grup.
5. Un altre exemple és el grup dièdric D_{2n}. Es correspon amb les simetries d'un polígon regular d'n costats. Està format per $2n$ elements dels quals n són rotacions i n són reflexions.
6. Per últim, si G_i amb $i \in I$ és una família de grups, el producte directe definit com $\prod_{i\in I} G_i$ és també un grup. En efecte definint el producte component a component $(x_i)(y_i) = (x_i y_i)$ el neutre serà $e = (e_i)$ amb e_i neutre de cada grup G_i i l'invers de cada element serà anàlogament $(x_i)^{-1} = (x_i^{-1})$

Quant a la notació referent a l'operació definida sobre el grup distingirem entre la *notació multiplicativa* emprada fins ara, i la *notació additiva*, segons la qual l'operació es denota amb $+$, el neutre pel 0 i als inversos $-x$. Aquesta última s'utilitzarà només quan el grup és abelià.

Veiem més propietats dels grups.

Proposició 1.1.2. *Sigui G un grup amb e neutre, per tot $x, y \in G$:*

1. $e^{-1} = e$
2. $(x^{-1})^{-1} = x$
3. $(xy) = y^{-1}x^{-1}$

Demostració. 1. Òbviament $ee = e$ i multiplicant per l'invers de e ho tenim.

2. Per unicitat i $xx^{-1} = x^{-1}x = e$ tenim $(x^{-1})^{-1} = x$
3. Tenim $xyy^{-1}x^{-1} = xx^{-1} = e$ i també $y^{-1}x^{-1}xy = e$

□

Proposició 1.1.3. *Sigui G un grup, és commutatiu si i només si $(xy) = x^{-1}y^{-1}$ per tot $x, y \in G$.*

Demostració. Cap a la dreta és trivial puix $(xy) = y^{-1}x^{-1}$ i si G és commutatiu tenim $xy = x^{-1}y^{-1}$. Recíprocament si $(xy)^{-1} = x^{-1}y^{-1}$ tenim que $xy = (x^{-1})^{-1}(y^{-1})^{-1} = (y^{-1}x^{-1})^{-1} = yx$ i per tant G és commutatiu. □

Més propietats que són conseqüència immediata del vist fins ara són:

Proposició 1.1.4. *G grup. Aleshores per tot $x, y, z \in G$ es compleix:*

1. $xy = xz \Rightarrow y = z$
2. $yx = zx \Rightarrow y = z$

A partir d'ara G és sempre un grup.

Definició 1.1.3. Sigui $H \subseteq G$ no buit direm que H és un subgrup de G si H amb l'operació restringida a H és un grup. En altres paraules, H és subgrup de G si és tancat per l'operació definida sobre G i a més compleix els 3 axiomes de la definició de grup. S'escriu en aquest cas $H \leq G$.

Definició 1.1.4. G grup. Els subgrups impropis de G són $\{e\}$ i el propi G. Així anomenem subgrups propis a tots els subgrups que no són un d'aquests.

Proposició 1.1.5. *$H \subseteq G$, H no buit és un subgrup de G si i només si per a tot $x, y \in H$ es dóna que $xy^{-1} \in H$.*

Demostració. Si H és un subgrup llavors $x, y \in H$ implica que y^{-1} i per tant $xy^{-1} \in H$. Recíprocament suposant que $xy^{-1} \in H$ per tot $x, y \in H$ tenim que $xx^{-1} = e \in H$. Igualment l'operació continua sent associativa. D'altra banda com que $x, e \in H$, $ex^{-1} = x^{-1} \in H$. I això ens permet veure finalment que H és tancat ja que si $x, y \in H$ llavors $y^{-1} \in H$ i amb això $x(y^{-1})^{-1} = xy \in H$. □

Alguns exemples de subgrups són:

1. Per $(\mathbb{Z}, +)$ fixem $a \in \mathbb{Z}$ i fem $H = (a)$, és a dir, el conjunt dels múltiples de a. Efectivament H és subgrup de $(\mathbb{Z}, +)$, puix donats dos elements de (a) tindrem $\alpha a - \beta a = (\alpha - \beta)a \in (a)$.

2. A $(S_n, \circ)$ tenim el grup alternat $A_n = \{\sigma \in S_n | \sigma \text{ és parell}\}$ és a dir, el conjunt de les permutacions de S_n que descomposen en un nombre parell de transposicions. Veiem que A_n és un subgrup de S_n. Siguin $\sigma, \sigma' \in S_n$ sabem que descomposen segons: $\sigma = \tau_1 \circ \ldots \circ \tau_r$ i $\sigma' = \tau'_1 \circ \ldots \tau'_p$ amb r, p parells. Observem que $(\sigma')^{-1} = (\tau'_1 \circ \ldots \tau'_p)^{-1} = (\tau'_p)^{-1} \circ \ldots \circ (\tau'_1)^{-1}$. Amb això és immediat veure que $\sigma \circ (\sigma')^{-1} = \tau_1 \circ \ldots \circ \tau_r \circ (\tau'_p)^{-1} \circ \ldots \circ (\tau'_1)^{-1} \in A_n$ en tant que descomposa en un nombre $r+p$ parell de transposicions. Observem també que hi ha el mateix nombre de permutacions de S_n que descomposen en un nombre parell de transposicions que de permutacions que ho fan en un nombre senar. Si teníem que $|S_n| = n!$, ara veiem que $|A_n| = \frac{n!}{2}$

3. Donat un grup G, amb element neutre e, s'anomena subgrup trivial a $\{e\}$. Igualment G en si mateix és subgrup de G.

4. Com és habitual la intersecció finita de subgrups forma un subgrup. Tanmateix això no ocorre amb la unió i generalment no és veritat que la unió de subgrups sigui subgrup -la unió no és tancada-.

5. Fent $G = GL_n(K)$, el conjunt $H = \{A \in GL_n(K) | \det(A) = 1\}$ és subgrup de G. Observem que si $A, B \in H$ llavors $\det(AB^{-1}) = \det A \cdot (\det B)^{-1} = 1$.

Definició 1.1.5. Sigui S un subconjunt de G no buit. Definim el subgrup generat per S, $\langle S\rangle$ com el mínim subgrup de G que conté G.

És fàcil arribar a la conclusió que $\langle S\rangle = \bigcap_{S\subseteq H} H$ amb H subgrup de G.

Proposició 1.1.6. *Fixat $g \in G$ llavors $\langle g\rangle = \{\ldots, g^{-2}, g^{-1}, e = g^0, g, g^2, \ldots\}$*

Demostració. S'ha de veure que aquest subconjunt de G és subgrup, puix és clar que és el mínim. Així doncs siguin $x = g^i, y = g^j \in \{\ldots, g^{-2}, g^{-1}, e = g^0, g, g^2, \ldots\}$ tenim que $xy^{-1} = g^i g^j = g^{i-j}$ que està en aquest subconjunt. Per tant és subgrup i tenim $\langle g\rangle = \{\ldots, g^{-2}, g^{-1}, e = g^0, g, g^2, \ldots\}$. □

Definició 1.1.6. Anomenarem ordre de G, $|G|$, al nombre d'elements de G si aquest és finit. En cas contrari direm que té ordre infinit.

Si $g \in G$ llavors l'ordre de g és l'ordre del subgrup que genera: $|g| = |\langle g\rangle|$.

Proposició 1.1.7. *Si $g \in G$, llavors $|g| = n$ si i només si $n = \min\{k \in \mathbb{N} \mid g^k = e\}$. En aquest cas $\langle g\rangle = \{e, g, g^2, \ldots, g^{n-1}\}$.*

Demostració. Cap a l'esquerra és trivial en tant que si $\langle g\rangle = \{e, g, g^2, \ldots, g^{n-1}\}$ tenim $|g| = n$.

Suposant que $|g| = n$ tenim que el conjunt $\langle g\rangle = \{e, g, g^2, \ldots\}$ és finit. Això implica que existeixen $i, j, i > j$ de forma que $g^i = g^j \Leftrightarrow g^{i-j} = e$. Sigui ara $m = \min\{k \in \mathbb{N} \mid g^k = e\}$ hem de veure que efectivament $\langle g\rangle = \{e, g, g^2, \ldots, g^{m-1}\}$. Per això suposem $t > m$ i fent la divisió euclídea $t = mq + r$ amb $0 \leq r < m$ es troba que $g^t = (g^m)^q g^r = g^r$ que pertany a aquest conjunt. I per últim si $g^m = e$ tindrem gg^{m-1} i així tots els elements de la forma

$$g^{-1} = g^{m-1}$$

$$g^{-2} = g^{m-2}$$

$$\ldots$$

també hi són. En particular serà $m = n$. □

El concepte de grup generat per un element indueix de forma natural la següent definició.

Definició 1.1.7. Direm que un grup G és cíclic si existeix $g \in G$ de manera que $G = \langle g\rangle$. En aquest cas g s'anomena generador de G.

Alguns exemples de grups cíclics són:

1. Els enters $(\mathbb{Z}, +)$ ja que $\mathbb{Z} = \langle 1\rangle = \langle -1\rangle$.
2. Igualment $\mathbb{Z}/n\mathbb{Z} = \langle \overline{1}\rangle$.
3. Al grup dièdric $D_{2\cdot 4}$ format per les transformacions que deixen invariant un quadrat al pla trobem el subgrup format per la identitat i les rotacions d'angles $\pi/2, \pi$ i $3\pi/2$. Aquest subgrup és cíclic.

Així doncs observem també que si G és cíclic tot element de G serà de la forma g^i per a g generador de G i cert i. Amb això $g^i g^j = g^j g^i = g^{i+j}$ de manera que G és abelià.

D'altra banda es pot veure que tot subgrup de G és cíclic també. Per això, si $H \leq G$ i $H = \{e\}$ o bé $H = G$ ja ho tenim. En cas contrari, sigui $g^k \in H$ tal que $g^m \notin H$ si $m < k$. Sigui $g^n \in H$ també llavors fent $n = kq + r$ amb $0 \leq r < k$ tenim $g^r = g^{n-kq} = g^n(g^{-k})^q \in H$. Ha de ser $r = 0$, en cas contrari es contradiu la tria de k. Per tant $H = \langle g^k \rangle$.

Una altra propietat dels grups cíclics és que si G és cíclic finit d'ordre n llavors per cada divisor $d|n$ existeix un únic subgrup d'ordre d. Si $d \mid n$ llavors és obvi que $|g^{n/d}| = d$. Sigui $H \leq G$ d'ordre d pel d'abans sabem que és cíclic. Així $H = \langle g^r \rangle$ per cert r. Com que $g^{rd} = g^n = e$ ha de ser $n \mid rd$. Per tant r és de la forma $\lambda n/d$ per cert λ, i en particular $\langle g^r \rangle \subseteq \langle g^{n/d} \rangle$. El fet que $|g^r| = |g^{n/d}|$ implica $H = \langle g^{n/d} \rangle$.

1.2 Teorema de Lagrange

A $\mathbb{Z}$ teníem la relació d'equivalència donada per: $x \equiv y \mod n$ si i només si $y - x$ és múltiple de n. Anàlogament direm que $x \equiv y \mod H$ si i només si $x^{-1}y \in H$.

Proposició 1.2.1. *Si G és un grup i $H \leq G$ aleshores $x \equiv y \mod H$ és d'equivalència.*

Demostració. Com que H és subgrup $e \in H$ i per tant $x^{-1}x = e \in H$, és a dir és reflexiva. Igualment tenim que si $x \equiv y$ és perquè $x^{-1}y \in H$. Així doncs $(x^{-1}y)^{-1} \in H$ i per tant és simètrica. Finalment si tenim $x \equiv y$ i $y \equiv z$ llavors $x^{-1}y \in H$ i $y^{-1}z \in H$. Fent el producte $x^{-1}yy^{-1}z = x^{-1}z$ arribem a $x \equiv z$ i en conseqüència és transitiva.

És a dir, $x \equiv y \mod H$ és d'equivalència. □

Donada aquesta relació d'equivalència les classes d'equivalència vindran donades doncs per:

$$\overline{x} = \{y \in G |\ x^{-1}y \in H\} = \{y \in G |\ y \in xH\}$$

on definim $xH = \{xh \in G |\ h \in H\}$. Observem doncs que $eH = \{eh \in G |\ h \in H\} = H$

Teorema 1.2.1. *(Teorema de Lagrange) Sigui G un grup finit i $H \leq G$. Aleshores $|H|$ divideix $|G|$.*

Demostració. Per això emprarem l'aplicació donada per

$$H \longrightarrow xH$$

$$h \longmapsto xh$$

que és clarament bijectiva amb $x \in G$ fixat. Amb això $|H| = |xH|$. Ara bé, com que la relació és d'equivalència G serà la unió disjunta de totes les classes d'equivalència i per tant:

$$G = \bigcup_{x \in G} xH \Longrightarrow |G| = \sum_{x \in G} |xH| = |G/H||H|$$

puix $|G/H|$ és el nombre de classes d'equivalència. □

A partir d'ara de $|G/H|$ en direm índex $(G : H)$.

Corol·lari 1.2.1. *Tot grup d'ordre primer és cíclic*

Demostració. Suposem $|G| = p$ amb p primer. Sigui $g \in G$ diferent del neutre i $H = \langle g \rangle$ llavors $|H|$ divideix p. Per tant $|H| = p$ i $G = \langle g \rangle$ ja que el fet que $|H| = 1$ implicaria $g = e$. En conseqüència G és cíclic. □

Corol·lari 1.2.2. *Si G té ordre n i $g \in G$ aleshores l'ordre de g divideix n.*

1.3 Subgrups normals i grup quocient

Hem vist que donat un grup G i un subgrup de G H la relació d'equivalència $x \equiv y \mod H$ si i només si $x^{-1}y \in H$ dóna lloc a les classes d'equivalència xH anomenades classes per la esquerra. Anàlogament podríem definir la relació també d'equivalència $x \equiv y \mod H$ si i només si $xy^{-1} \in H$. Aquesta dóna lloc a les anomenades classes per la dreta Hx. Observem doncs que si el grup és finit $|xH| = |H| = |Hx|$. Veiem alguns casos que mostren que $xH = Hx$ no és cert generalment.

1. Sí que ho és si G és abelià òbviament.
2. A S_3 si considerem $H = \langle (1,2) \rangle = \{id, (1,2)\}$ tenim:

$$(1,2,3)H = \{(1,2,3), (1,2,3) \circ (1,2)\} = \{(1,2,3), (1,3)\}$$

$$H(1,2,3) = \{(1,2,3), (1,2) \circ (1,2,3)\} = \{(1,2,3), (2,3)\}$$

Definició 1.3.1. Sigui G un grup, H subgrup de G. Diem que H és normal a G si per a tot $x \in G$ es dóna que $xH = Hx$. Escriurem $H \trianglelefteq G$.

Definició 1.3.2. Direm que un grup G és simple si tots els únics subgrups normals que té són $\{e\}$ o bé tot G, ço és, els seus subgrups impropis.

Proposició 1.3.1. *Donat $H \leq G$ llavors són equivalents:*

1. *$xH = Hx$ per a tot $x \in H$*
2. *$x^{-1}Hx = H$ per a tot $x \in G$*
3. *$x^{-1}Hx \subseteq H$ per a tot $x \in G$*

Demostració. Veiem $1 \Longrightarrow 2$. Fem primer $x^{-1}Hx \subseteq H$. Sigui $x \in G$ i $h \in H$ tenim que $x^{-1}hx = x^{-1}xh' = h' \in H$ per cert $h' \in H$. Fem ara $H \subseteq x^{-1}Hx$. Sigui $h \in H$ llavors per tot $x \in G$ tenim $xh = h'x$ per cert $h' \in H$. Això implica que $h = x^{-1}h'x \in x^{-1}Hx$.

$2 \Rightarrow 3$ ja ho tenim.

I per $3 \Rightarrow 1$ tenim que $xH \subseteq Hx$ ja que si $x \in G$ i $h \in H$, $x^{-1}hx \in H$ i per tant $xh = h'x \in Hx$ per cert $h' \in H$. L'altra inclusió és anàloga. □

Si a, x són elements d'un grup anomenarem a l'element $a^{-1}xa$ el conjugat de x per a.

Alguns exemples de subgrups normals són:

1. Si G és abelià tot subgrup de G és normal.
2. Fent $G = GL_n(K)$ i prenent el subgrup $SL_n(K) = \{A \in GL_n(K) | \, det(A) = 1\}$ observem que donada $A \in SL_n(K)$ i $P \in GL_n(K)$ llavors $\det(P^{-1}AP) = \det(P)^{-1}\det(A)\det(P) = \det(A) = 1$. Per tant $SL_n(K) \trianglelefteq GL_n(K)$.

Definició 1.3.3. Anomenem centre de G al conjunt:

$$Z(G) = \{x \in G | \; xg = gx \text{ per tot } g \in G\}$$

Podem comprovar que $Z(G) \trianglelefteq G$. Efectivament, sigui $x \in G$ i $z \in Z(G)$ tenim que $x^{-1}zx = x^{-1}xz = z \in Z(G)$. Alguns exemples:

1. $Z(S_3) = \{id\}$
2. $Z(GL_2(K)) = \{\lambda \cdot I_2 | \; \lambda \neq 0\}$

Trivialment tenim que si G és commutatiu llavors $Z(G) = G$.

Fem ara $H \trianglelefteq G$ i considerem el conjunt quocient $G/H = \{xH | \; x \in G\}$.

Definició 1.3.4. Definim $\overline{x} \cdot \overline{y} = \overline{xy}$. Equivalentment tenim $(xH)(yH) = (xy)H$.

Proposició 1.3.2. *L'operació és ben definida i G/H amb aquesta és un grup.*

Demostració. Veiem que no depén del representant. Siguin $x_1 \in \overline{x}$ i $y_1 \in \overline{y}$ ens preguntem si $\overline{x_1} \cdot \overline{y_1} = \overline{xy}$, ço és si x_1y_1, xy estan relacionats. Fem doncs $xy(x_1y_1)^{-1} = xyy_1^{-1}x_1^{-1} = xhx_1^{-1}$ amb $h \in H$. Com que H és normal tindrem per certs $h', h'' \in H$ que $xhx_1^{-1} = xx_1^{-1}h' = h''h' \in H$. I per tant l'operació és ben definida.

Veiem ara doncs que G/H és grup. L'operació és associativa per definició. D'altra banda el neutre serà la classe del neutre de G ja que $\overline{e} \cdot \overline{x} = \overline{ex} = \overline{x}$ i $\overline{x} = \overline{ex} = \overline{xe} = \overline{x} \cdot \overline{e}$. Procedint anàlogament pels elements inversos tenim per $x \in G$: $\overline{x} \cdot \overline{x^{-1}} = \overline{xx^{-1}} = \overline{e}$ i $\overline{e} = \overline{x^{-1}x} = \overline{x^{-1}} \cdot \overline{x}$. □

Observem ara que si G és finit $|G/H| = (G : H) = \frac{|G|}{|H|}$.

1.4 Morfismes de grups

Definició 1.4.1. Siguin G_1 i G_2 grups. Una aplicació $f : G_1 \longrightarrow G_2$ és morfisme de grups si per tot $x, y \in G_1$ es dóna $f(xy) = f(x)f(y)$. A més a més si el morfisme:

- f és injectiu, s'anomena monomorfisme.
- f és exhaustiu, s'anomena epimorfisme.

- f és bijectiu, s'anomena isomorfisme.
- $f : G_1 \longrightarrow G_1$, s'anomena endomorfisme.
- és bijectiu i $f : G_1 \longrightarrow G_1$, s'anomena automorfisme.

Alguns exemples de morfismes de grups són:

1. $id : G \longrightarrow G$ automorfisme. Igualment són morfismes les aplicacions lineals entre espais vectorials.
2. Fixat $a \in \mathbb{Z}$,
$$f : \mathbb{Z} \longrightarrow \mathbb{Z}$$
$$x \longmapsto ax$$
és morfisme ja que: $a(x+y) = ax + ay$. A més a més tot morfisme de grups a $\mathbb{Z}$ és d'aquesta forma.
3. La projecció canònica
$$\pi : Z \longrightarrow \mathbb{Z}/n\mathbb{Z}$$
$$x \longmapsto \overline{x}$$
és epimorfisme.
4. L'aplicació determinant també és morfisme de grups puix $\det(AB) = \det(A)\det(B)$.
5. La conjugació. Donat G grup i fixat $a \in G$ considerem: $f_a : G \longrightarrow G$ donada per $f_a(x) = a^{-1}xa$. Efectivament és morfisme en tant que $f_a(xy) = a^{-1}xya = a^{-1}xaa^{-1}ya = f_a(x)f_a(y)$. Igualment és injectiu ja que el fet que $f_a(x) = f_a(y)$ és equivalent a $a^{-1}xa = a^{-1}ya \Leftrightarrow aa^{-1}xaa^{-1} = aa^{-1}yaa^{-1} \Leftrightarrow x = y$. Per veure que és exhaustiva donat $b \in G$ només hem de considerar $f_a(aba^{-1}) = a^{-1}ba^{-1}a = b$. Tenim doncs que f_a és automorfisme.

Dues propietats elementals dels morfismes de grups són:

1. Si $f : G_1 \longrightarrow G_2$ i $g : G_2 \longrightarrow G_3$ són morfismes de grup llavors $g \circ f$ també ho és.
2. Si $f : G_1 \longrightarrow G_2$ és isomorfisme llavors $f^{-1} : G_2 \longrightarrow G_1$ és isomorfisme i $(f^{-1})^{-1} = f$.

En general si dos grups tenen propietats estructurals diferents no poden ser isomorfs.

Proposició 1.4.1. *Sigui $f : G_1 \longrightarrow G_2$ un morfisme de grups llavors:*

1. *$f(e_1) = e_2$ amb e_1, e_2 element neutres de G_1, G_2 respectivament.*
2. *Si $x \in G_1$ llavors $f(x^{-1}) = (f(x))^{-1}$*

Demostració. Per veure 1 tenim $f(e_1e_1) = f(e_1)f(e_1) = f(e_1)$ i amb això $f(e_1) = f(e_1)f(e_1)(f(e_1))^{-1} = f(e_1)(f(e_1))^{-1} = e_2$.

D'altra banda per 2 es troba que, $f(xx^{-1}) = f(x)(f(x))^{-1} = f(e) = e$ i anàlogament per l'altra banda, la qual cosa implica que $f(x^{-1}) = (f(x))^{-1}$. □

Definició 1.4.2. Sigui f un morfisme $G_1 \longrightarrow G_2$.

Definim el nucli de f com $\ker(f) = \{x \in G_1 |\ f(x) = e_2\}$.

Definim la imatge de f com $\mathrm{Im}(f) = \{f(x) |\ x \in G_1\}$.

Proposició 1.4.2. *Sigui $f : G_1 \longrightarrow G_2$ un morfisme de grups. El nucli de f és un subgrup normal de G_1 i la imatge de f és un subgrup de G_2.*

Demostració. Veiem que $\ker(f) \leq G_1$. Siguin $x, y \in G_1$ tenim que $f(xy^{-1}) = f(x)f(y^{-1}) = f(x)f(y)^{-1} = e_2e_2 = e_2$ i per tant $xy^{-1} \in \ker(f)$ que és un subgrup. Veiem ara $\ker(f) \trianglelefteq G_1$. Sigui $k \in \ker(f)$ i $x \in G$ fem $f(x^{-1}kx) = f(x^{-1})f(k)f(x) = f(x^{-1})f(x) = f(x^{-1}x) = f(e_1) = e_2$ i per tant $x^{-1}kx \in \ker(f)$.

Veiem ara que $\mathrm{Im}(f) \leq G_2$. Siguin $f(x), f(y) \in \mathrm{Im}(f)$ fem $f(x)f(y)^{-1} = f(x)f(y^{-1}) = f(xy^{-1}) \in \mathrm{Im}(f)$ ja que G_1 és grup. □

Proposició 1.4.3. *Sigui $f : G_1 \longrightarrow G_2$ un morfisme de grups. Aleshores:*

1. *f és injectiu si i només si* $\ker(f) = \{e_1\}$.
2. *f és exhaustiu si i només si* $\mathrm{Im}(f) = G_2$.

Demostració. 2 és la definició d'exhaustivitat.

Per veure 1 suposem primer que f és injectiu. Sigui $x \in \ker(f)$ llavors $f(e_1) = f(x) = e_2$ i per tant $e_1 = x$. Recíprocament, si suposem que $\ker(f) = e_1$ i que $f(x) = f(y)$ tenim doncs $f(xy^{-1}) = f(x)f(y^{-1}) = f(x)f(y)^{-1} = f(y)f(y)^{-1} = e_2$. Així doncs ha de ser $xy^{-1} = e_1 \Leftrightarrow x = y$ i f és injectiu. □

Proposició 1.4.4. *Sigui $f : G_1 \longrightarrow G_2$ un morfisme de grups. Aleshores:*

1. *Si $H \leq G_1$ llavors $f(H) \leq G_2$.*
2. *Si $K \leq G_2$ llavors $f^{-1}(K) \leq G_2$.*
3. *Si f és epimorfisme i $H \trianglelefteq G_1$ llavors $f(H) \trianglelefteq G_2$.*

Demostració. Veiem 1. Siguin $f(x), f(y) \in f(H)$ llavors $f(x)f(y)^{-1} = f(x)f(y^{-1}) = f(xy^{-1}) \in f(H)$ ja que H és subgrup.

Per veure 2 posem $D = f^{-1}(K) = \{x \in G_1 |\ f(x) \in K\}$. Siguin $x, y \in D$ fem $f(xy^{-1}) = f(x)f(y)^{-1} \in K$. Per tant $xy^{-1} \in D$.

A 3 ja sabem que $f(H) \leq G$. Sigui $f(h) \in f(H)$ i sigui $y \in G_2$ com que f és epimorfisme existeix $x \in G_1$ tal que $f(x) = y$. Així $y^{-1}f(h)y = f(x)^{-1}f(h)f(x) = f(x^{-1})f(h)f(x) = f(x^{-1}hx)$ que pertany a $f(H)$ en tant que per ser subgrup normal H, $x^{-1}hx$ pertany a H. □

Teorema 1.4.1. *Sigui $f : G_1 \longrightarrow G_2$ un morfisme de grups. Aleshores $G_1/\ker(f) \cong \mathrm{Im}(f)$. En particular si f és epimorfisme tindrem $G_1/\ker(f) \cong G_2$.*

Demostració. Definim $\tilde{f} : G_1/\ker(f) \longrightarrow G_2$ donada per $\tilde{f}(\overline{x}) = f(x)$ per tot $x \in G_1$.

Veiem primerament que és ben definida, és a dir que $x \equiv y$ implica $f(x) = f(y)$. Si x, y estan relacionats llavors $\overline{x} = \overline{y} \Leftrightarrow y \in x\ker(f)$. Així doncs tenim que existeix $k \in \ker(f)$ tal que $y = xk$. D'aquesta manera $f(y) = f(xk) = f(x)f(k) = f(x)$ ja que $k \in \ker(f)$.

Veiem a continuació que es tracta d'un morfisme de grups. Per això fem $\tilde{f}(\overline{xy}) = f(xy) = f(x)f(y) = \tilde{f}(x)\tilde{f}(y)$.

És injectiva. Suposem $\tilde{f}(\overline{x}) = \tilde{f}(\overline{y}) \Leftrightarrow f(x) = f(y) \Leftrightarrow f(x)f(y)^{-1} = f(y)f(y)^{-1} = e_2 \Leftrightarrow f(xy^{-1}) = e_2$. Amb això $xy^{-1} \in \ker(f) \Leftrightarrow \overline{x} = \overline{y}$.

A més a més és exhaustiva ja que $\mathrm{Im}(\tilde{f}) = \mathrm{Im}(f)$.

En conseqüència tenim:

$$G_1/\ker(f) \cong \mathrm{Im}(f)$$

□

Teorema 1.4.2. *(Teorema de classificació de grups cíclics) Sigui G un grup cíclic. Si $|G|$ és infinit, llavors $G \cong \mathbb{Z}$; si $|G| = n$, llavors $G \cong \mathbb{Z}/n\mathbb{Z}$.*

Demostració. Posem $G =< g >$ per $g \in G$ generador.

Si G té ordre infinit considerem

$$f : \mathbb{Z} \longrightarrow G$$

$$t \longmapsto g^t$$

que és clarament bijectiva. Veiem que és isomorfisme de grups fent $f(t_1 + t_2) = g^{t_1+t_2} = g^{t_1}g^{t_2} = f(t_1)f(t_2)$. Per tant $\mathbb{Z} \cong G$.

Si ara $|G| = n$ és finit considerem

$$\tilde{f} : \mathbb{Z}/n\mathbb{Z} \longrightarrow G$$

$$\overline{t} \longmapsto g^t$$

És ben definida en tant que si $\overline{t} = \overline{l}$ llavors $t - l = \alpha n$ i així $\tilde{f}(\overline{l}) = g^l = g^{t-\alpha n} = g^t g^{n^{(-\alpha)}} = g^t = \tilde{f}(t)$. A més és morfisme de grups puix $\tilde{f}(\overline{t_1 + t_2}) = g^{t_1+t_2}$ igual que abans. D'altra banda és òbviament exhaustiva i és injectiva ja que si $\tilde{f}(\overline{t_1}) = \tilde{f}(\overline{t_2}) \Leftrightarrow g^{t_1} = g^{t_2} \Leftrightarrow g^{t_1-t_2} = e$ i amb això $t_1 - t_2 = \alpha n \Leftrightarrow \overline{t_1} = \overline{t_2}$. Per tant és un isomorfisme de grups i $\mathbb{Z}/n\mathbb{Z} \cong G$. □

1.4.1 Tres teoremes d'isomorfia

Teorema 1.4.3. *(Primer teorema d'isomorfia) Sigui $f : G_1 \longrightarrow G_2$ epimorfisme de grups. Aleshores:*

1. $G_1/\ker(f) \cong G_2$
2. *L'aplicació $\varphi : \{H \leq G_1 |\ \ker(f) \leq H\} \longrightarrow \{$subgrups de $G_2\}$ donada per $\varphi(H) = f(H)$ és bijectiva.*

3. *L'aplicació* $\varphi : \{H \trianglelefteq G_1 |\ \ker(f) \leq H\} \longrightarrow \{$*subgrups normals de* $G_2\}$ *donada per* $\varphi(H) = f(H)$ *és bijectiva.*

Demostració. La demostració de 1 ja l'hem feta.

Per veure 2 primer comprovem que φ és ben definida. Hem de veure doncs que la imatge de $H \leq G_1$ tal que el nucli hi està contingut és un subgrup de G_2. Siguin $x, y \in H$ fem $f(x)f(y)^{-1} = f(xy^{-1}) \in f(H)$ ja que $xy^{-1} \in H$. Per tant $f(H) \leq G_2$.

Veiem ara que és injectiva. Suposem $f(H) = f(H')$. Hem de veure que $H = H'$. Sigui $h \in H$ llavors $f(h) \in f(H')$ per hipòtesi. Així $f(h) = f(h')$ per cert $h' \in H'$. Ara $f((h')^{-1}h) = e$ de manera que $(h')^{-1}h \in \ker(f) \leq H' \Leftrightarrow h'h \in \ker(f) \Leftrightarrow h \in H'$. Tenim $H \subseteq H'$ i anàlogament $H' \subseteq H$. Per tant, és injectiva.

Veiem ara que és exhaustiva. Sigui K del conjunt d'arribada fem $H = f^{-1}(K)$. Si $x \in \ker(f)$ llavors $f(x) = e \in K$ i $x \in f^{-1}(K)$.

Per tant és φ és bijectiva.

Per veure 3 només hem de comprovar que φ envia un subgrup normal a un subgrup normal. Sigui $H \trianglelefteq G_1$ tal que $\ker(f) \in G_1$ i sigui $x \in G_1$ i $h \in H$ fem $f(x)^{-1}f(h)f(x) = f(x^{-1}hx) \in f(H)$ ja que H és normal. En conseqüència $f(H)$ és normal. □

Corol·lari 1.4.1. *Sigui* G *un grup i* H *un subgrup normal de* G*. Aleshores la correspondència* $K \to \pi(K) = K/H$ *és una bijecció entre els subgrups de* G *que contenen* H *i els subgrups* G/H *i també entre els subgrups normals de* G *que contenen* H *i els subgrups normals de* G/H*. És a dir, els subgrups de* G/H *són de la forma* K/H *amb* K *subgrup de* G*.*

També podem considerar productes de subgrups. Per exemple a $\mathbb{Z}$ donats $(n), (m)$ sabem que $(n) + (m) = (d)$ on $d = \text{mcd}(m, n)$. O donat un espai vectorial sobre un cos i dos subespais, la suma dels dos subespais també és un producte de subgrups. Però, el resultat no és sempre un subgrup.

Un exemple que mostra això és el producte dels subgrups de S_3, $H = \{\text{id}, (1,2)\}$ i $K = \{\text{id}, (1,3)\}$. Tenim doncs $H \cdot K = \{\text{id}, (1,2), (1,3), (1,3,2)\}$ i com que $|H \cdot K| = 4$ no divideix 6, $H \cdot K$ no pot ser subgrup de S_3. Això planteja la pregunta de quan el producte de subgrups dóna lloc a un subgrup.

Proposició 1.4.5. *Sigui* G *grup,* H *i* K *subgrups de* G*. Si* $K \trianglelefteq G$*, aleshores* $H \cdot K$ *és un subgrup de* G *i a més és el mínim subgrup de* G *que conté* H *i* K*.*

Demostració. Siguin $x, y \in H \cdot K$ escriurem $x = hk$ i $y = h'k'$ amb $h, h' \in H$ i $k, k' \in K$. Així doncs fent $xy^{-1} = hk(h'k')^{-1} = h(k(k')^{-1})(h')^{-1}$ com que K és normal i $(k(k')^{-1}) \in K$ tindrem $xy^{-1} = (h(h')^{-1})k'' \in H \cdot K$ per cert $k'' \in K$. Per tant $H \cdot K$ és subgrup de G. □

Proposició 1.4.6. *Sigui* G *grup,* H *i* K *subgrups de* G*. Si* $K \trianglelefteq G$ *i* $H \trianglelefteq G$*, aleshores* $H \cdot K$ *és un subgrup normal de* G

Teorema 1.4.4. *(Segon teorema d'isomorfia) Sigui* G *un grup,* H, K *subgrups de* G *amb* $K \trianglelefteq G$*. Aleshores:*

$$H \cdot K/K \cong H/H \cap K$$

Observem primerament que $H \cdot K$ és subgrup de G ja que $K \trianglelefteq G$ i K és normal a $H \cdot K$ en tant que és normal a tot G. Sabem que $H \cap K \leq H$, veiem que $H \cap K$ és normal a H. Sigui $h \in H$ i $x \in H \cap K$ en particular $x \in K$. Aleshores $h^{-1}xh = h^{-1}hx' = x' \in K$ per cert $x' \in K$. Però $h^{-1}xh \in H$ amb la qual cosa $h^{-1}xh \in H \cap K$ i $H \cap K \trianglelefteq H$.

Observem també que si G és abelià podem escriure en notació additiva:

$$H + K/K \cong H/H \cap K$$

Demostració. Definim:

$$f : H \cdot K \longrightarrow H/H \cap K$$

$$x = hk \longmapsto \overline{h}$$

Veiem primerament que està ben definida. Suposem que $h_1k_1 = h_2k_2$. Així $h_1k_1 = h_2k_2 \Leftrightarrow h_2^{-1}h_1 = k_2k_1^{-1} \in H \cap K \Rightarrow \overline{h_1} = \overline{h_2}$ a $H/H \cap K$.

f és exhaustiva ja que una antiimatge per $\overline{h}$ és $h = he$.

f és morfisme de grups ja que si $x = hk$ i $y = h'k'$ llavors $xy = h(kh')k' = hh'k''k'$ per cert $k'' \in K$ puix K és normal i així $f(xy) = f(hh'k''k') = \overline{hh'} = \overline{h} \cdot \overline{h'} = f(x)f(y)$.

Veiem ara que $\ker(f) = K$. Sigui $k \in K$ llavors $f(k) = f(ek) = \overline{e}$ i per tant $k \in \ker(f)$, ço és $K \subseteq \ker(f)$. Sigui ara $x \in \ker(f)$ llavors $f(x) = \overline{e}$ i $x = hk$ per $h \in H$ i $k \in K$. Com que $f(x) = f(hk) = \overline{h}$ tenim que $eh = h \in H \cap K$ de manera que $h \in K$ i $x \in K$. Així $\ker(f) \subseteq K$, $\ker(f) = K$ i pel primer teorema d'isomorfia tenim el resultat. □

Teorema 1.4.5. *(Tercer teorema d'isomorfia) Sigui G un grup i H, K subgrups normals de G amb $K \leq H$. Aleshores:*

$$G/H \cong (G/K)/(H/K)$$

Observem en aquest cas que com que $K \trianglelefteq G$ serà també $K \trianglelefteq H$. D'altra banda com que $H \trianglelefteq G$ tindrem que donats $g \in G$ i $h \in H$ llavors $hg = gh'$ per cert $h' \in H$. Així $(hK)(gK) = (hg)K = (gh')K$ i també serà $H/K \trianglelefteq G/K$ i per tant té sentit l'enunciat.

Demostració. Considerem l'aplicació

$$f : G/K \longrightarrow G/H$$

$$gK \longmapsto gH$$

És ben definida ja que $K \leq H$ i evidentment és epimorfisme pel mateix motiu. Veiem que $\ker(f) = H/K$. Sigui $h \in H$ tenim que $f(hK) = hH = eH = \overline{e}$ de manera que $hK \in \ker(f)$. Sigui ara $xK \in \ker(f)$ tenim que $f(xK) = xH$ amb la qual cosa ha de ser $x \in H$ i per tant $xK \in H/K$. Pel primer teorema d'isomorfia tenim el resultat. □

1.4.2 Un teorema de representació

Considerem ara un conjunt X no buit. Sigui $S_X = \{\sigma |\ \sigma$ és bijectiva$\}$.Evidentment S_X és un grup amb la composició. A més si X és finit tenim $S_X = S_n$.

Teorema 1.4.6. *(Teorema de Cayley) Sigui G un grup. Aleshores G és isomorf a un subgrup de S_G. En particular si G té n elements, G és isomorf a un subgrup de S_n.*

Demostració. Definim:

$$\varphi : G \longrightarrow S_G$$
$$g \longmapsto l_g$$

on

$$l_g : G \longrightarrow G$$
$$x \longmapsto gx$$

és bijectiva. Veiem que φ és morfisme de grups.

D'una banda tenim $l_{g_1g_2}(x) = g_1g_2x$ i d'altra $(l_{g_1} \circ l_{g_2})(x) = l_{g_1}(g_2x) = g_1g_2x$. D'aquesta forma tenim $l_{g_1g_2} = \varphi(g_1g_2) = \varphi(g_1)\varphi(g_2) = l_{g_1} \circ l_{g_2}$.

Veiem que φ és injectiva. Suposem $\varphi(g_1) = \varphi(g_2) \Leftrightarrow l_{g_1} = l_{g_2} \Leftrightarrow g_1x = g_2x \quad \forall x \in G$. En particular $g_1e = g_1 = g_2e = g_2$. Per tant φ és injectiva i llavors $\ker(f) = \{e\}$.

En conseqüència $G \cong \mathrm{Im}(\varphi) \leq S_G$. □

1.5 Sobre els subgrups d'un grup finit. Els teoremes de Sylow

1.5.1 Accions d'un grup sobre un conjunt

Definició 1.5.1. Sigui G un grup i X un conjunt no buit. Una acció de G sobre X és una aplicació

$$\varphi : G \times X \longrightarrow X$$
$$(g, x) \longmapsto gx$$

que compleix:

1. $\varphi(e, x) = ex = x$ per tot $x \in X$.
2. $(g_1g_2)x = g_1(g_2x)$ per tot $g_1, g_2 \in G, x \in X$. Equivalentment $(g_1g_2x) = \varphi(g_1, \varphi(g_2, x))$ per tot $g_1, g_2 \in G, x \in X$.

Alguns exemples d'accions són:

1. X conjunt no buit. Denotem $S_X = \{\sigma : X \to X | \ \sigma \text{ és bijectiva}\}$. Aleshores S_X actua sobre X amb $\sigma x = \sigma(x)$.
2. Sigui $G = \mathbb{Z}$ i $X = \mathbb{Z}/n\mathbb{Z}$. Si $g \in \mathbb{Z}, \overline{x} \in \mathbb{Z}/n\mathbb{Z}$ llavors $g\overline{x} = \overline{g + x}$ és una acció.
3. G grup i $X = G$. Si $g \in G, x \in X$ llavors l'operació del grup $gx = g \cdot x$ és una acció.
4. Sota les mateixes condicions podem definir l'acció per conjugació i si $g \in G, x \in X$ llavors $gx = gxg^{-1}$ és una acció.

Definició 1.5.2. Si G actua sobre X diem que X és un G-conjunt.

Suposarem ara que X és un G-conjunt i introduïm la següent relació. Si $x_1, x_2 \in X$ diem que $x_1 \sim x_2$ si i només si existeix $g \in G$ tal que $x_2 = gx_1$.

Proposició 1.5.1. *La relació $\sim$ és d'equivalència*

Demostració. És reflexiva en tant que prenent el neutre de G tenim $x_1 = ex_1 = x_1$. Igualment si $x_1 \sim x_2$ existeix $g \in G$ tal que $x_1 = gx_2$. Com que $g^{-1} \in G$, podem fer actuar g^{-1} de manera que $g^{-1}x_1 = g^{-1}(gx_2) = (g^{-1}g)x_2 = ex_2 = x_2$ i tenim $x_2 \sim x_1$. Per últim és transitiva ja que si $x_1 = g_1x_2$ i $x_2 = g_2x_3$ aleshores $x_1 = g_1(g_2x_3) = (g_1g_2)x_3$ i per tant $x_1 \sim x_3$. □

Definició 1.5.3. Sigui $x \in X$. Anomenem òrbita de x a la classe d'equivalència $\overline{x}$ sota aquesta relació, és a dir:

$$\mathcal{O}(x) = \overline{x} = \{x' \in X |\ x' = gx \text{ per cert } g \in G\}$$

Igualment, anomenem estabilitzador de x al conjunt:

$$G_x = \{g \in G |\ gx = x\}$$

Proposició 1.5.2. *G_x és un subgrup de G.*

Demostració. $e \in G_x$ ja que $ex = e$ per definició.

Suposem $g_1, g_2 \in G_x$. Aleshores $(g_1g_2)x = g_1(g_2x) = g_1x = x$.

Sigui ara $g \in G$ hem de veure que $g^{-1} \in G_x$. Tenim que $gx = x \Leftrightarrow g^{-1}(gx) = g^{-1}x \Leftrightarrow (g^{-1}g)x = g^{-1}x \Leftrightarrow ex = x = g^{-1}x$ i per tant $g^{-1} \in G_x$. En conseqüència $G_x \leq G$. □

Observem ara que $\mathcal{O}(x) = Gx$ que no és el mateix que l'estabilitzador G_x.

Proposició 1.5.3. *Suposem G i X finits. Sigui $x \in X$. Aleshores $|Gx| = |\mathcal{O}(x)| = (G : G_x)$ amb l'índex del conjunt quocient $G/G_x = \{gG_x |\ g \in G\}$.*

Demostració. Considerem l'aplicació:

$$f : G/G_x \longrightarrow \mathcal{O}(x) = Gx$$

$$\overline{g} = gG_x \longmapsto gx$$

Veiem que està ben definida. Suposem $g' \in gG_x$, llavors $g' = gg''$ per un cert $g'' \in G_x$. I tenim $g'x = (gg'')x = g(g''x) = gx$.

Veiem ara qeu f és injectiva. Suposem $gx = g'x \Leftrightarrow g^{-1}gx = g^{-1}g'x \Leftrightarrow x = (g^{-1}g')x$. Per tant tenim que $g^{-1}g' \in G_x$ i en conseqüència $\overline{g} = \overline{g'}$.

D'altra banda f és clarament exhaustiva ja que una antiimatge s'obté prenent classe de l'element de $\mathcal{O}(x)$ en qüestió. □

Posem un exemple. Suposem $X = G$ finit i l'acció donada per la conjugació $gx = gxg^{-1}$. Així doncs $\mathcal{O}(x) = \{x\} \Leftrightarrow gx = x \quad \forall g \Leftrightarrow gxg^{-1} = x \quad \forall g \Leftrightarrow gx = xg \quad \forall g$. És a dir, si $x \in Z(G)$

Generalment, $G_x = \{g \in G |\ gx = x\} = \{g \in G |\ gxg^{-1} = x \Leftrightarrow gx = xg\}$ s'anomena el *centralitzador* de x a G, $C_G(x)$.

Sigui ara G finit i X finit amb X un G-conjunt. Considerem les òrbites dels elements de X. Suposem que en tenim r, $\mathcal{O}(x_1), \mathcal{O}(x_2), \ldots, \mathcal{O}(x_r)$, diferents 2 a 2. Tenim doncs $|X| = |\mathcal{O}(x_1)| + |\mathcal{O}(x_2)| + \ldots + |\mathcal{O}(x_r)|$. Algunes d'aquestes poden tenir un sol element. Suposant que són les $0 \leq s \leq r$ primeres:

$$|X| = s + \sum_{i=s+1}^{r} |\mathcal{O}(x_i)|$$

Com que acabem de veure que $\mathcal{O}(x) = \{x\} \Leftrightarrow Gx = x$ amb x fix pels elements de G podem definir:

$$X_G = \{x \in X |\ gx = x \text{ per tot } g \in G\} \subseteq X$$

Per tant per la proposició anterior tenim l'*equació de les òrbites*:

$$|X| = |X_G| + \sum_{i=s+1}^{r} |\mathcal{O}(x_i)| = |X_G| + \sum_{i=s+1}^{r} (G : G_{x_i})$$

En particular per l'acció donada per la conjugació tenim: $X_G = Z(G)$ i així:

$$|X| = |G| = |Z(G)| + \sum_{i=s+1}^{r} (G : C_G(x_i))$$

Definició 1.5.4. Sigui p un primer. Direm que G és un p-grup si $|G| = p^n$ amb $n \geq 1$.

Proposició 1.5.4. *Sigui G un p-grup i X un G-conjunt finit. Aleshores:*

$$|X| \equiv |X_G| \mod p$$

Demostració. Tenim $(G : G_{x_i}) || |G|$ amb la qual cosa $(G : G_{x_i}) = p^t$ per a $t \geq 1$. En conseqència $|X| - |X_G|$ és múltiple de p per l'equació de les òrbites. □

Proposició 1.5.5. *Si G és un p-grup, aleshores $Z(G)$ no és trivial. En particular com que $Z(G) \trianglelefteq G$, G no és simple.*

Demostració. $|G| - |Z(G)|$ és múltiple de p per l'equació de les òrbites i $|G| = p^n$ amb $n \geq 1$. Per tant $|Z(G)|$ és múltiple de p i no és 0. En conseqüència $Z(G)$ no és trivial. □

Corol·lari 1.5.1. *Si p és primer i G és un grup amb p^2 elements llavors G és abelià.*

Demostració. Considerem $Z(G) \neq \{e\}$ per la proposició anterior. Pel teorema de Lagrange $|Z(G)||p^2 \Rightarrow |Z(G)| = p$ o bé $|Z(G)| = p^2$.

Si $|Z(G)| = p^2$ i ja ho tenim.

Si $|Z(G)| = p$ fem $G/Z(G)$ que té ordre p. Com que p és primer tindrem $G/Z(G) = \langle \overline{g} \rangle$ per cert $g \in G$. Aleshores si $x \in G$, $\overline{x} = \overline{g}^r$ per cert $r \Rightarrow x \in g^r Z(G) \Leftrightarrow x = g^r z$ per $z \in Z(G)$. Sigui ara $y \in G$ pel mateix raonament tindrem $y = g^s z'$ amb $z' \in Z(G)$ i així $xy = g^r z g^s z' = g^s z' g^r z = yx$.

□

Corol·lari 1.5.2. *Hi ha només dos grups d'ordre p^2 amb p primer (tret d'isomorfisme).*

Demostració. Sigui G un grup d'ordre p^2. Sigui $g \in G$ diferent del neutre $|g| > 1$. Pel teorema de Lagrange $|g| \mid p^2$. Així:

- Si $|g| = p^2$ tenim $\langle g \rangle = G$ i pel teorema de classificació dels grups cíclics
$$G \cong \mathbb{Z}/p^2\mathbb{Z}$$
- Suposem doncs que G no és cíclic. Amb això si $x \neq e$ tindrem $|x| = p$. Llavors $\langle x \rangle \leq G$ i podem prendre $y \in G, y \neq e, y \notin \langle x \rangle$ de forma que $|y| = p$ igualment. Observem doncs que $\langle x \rangle \cap \langle y \rangle = \{e\}$ ja que l'ordre del grup intersecció és 1 o p pel teorema de Lagrange. Per la tria de b ha de ser 1. Considerem l'aplicació
$$\varphi : \langle x \rangle \times \langle y \rangle \longrightarrow G$$
$$(a, b) \longmapsto ab$$
Com que G és abelià, φ és morfisme. D'altra banda, és injectiu ja que la intersecció $\langle x \rangle \cap \langle y \rangle$ només conté el neutre. I com que ambdos grups tenen el mateix ordre p^2 són isomorfs.

  Pel teorema de classificació de grups cíclics novament tenim que $\langle x \rangle$ i $\langle y \rangle$ són isomorfs a $\mathbb{Z}/p\mathbb{Z}$. Amb això
$$G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$$

□

Teorema 1.5.1. *(Teorema de Cauchy per grups abelians) Sigui G un grup abelià i finit i p un primer tal que $p||G|$. Aleshores G conté algun element d'ordre p.*

Demostració. Ho fem per inducció sobre $|G|$. Si $|G| = 2$ llavors G és cíclic i per tant té un element d'ordre 2.

Si G és cíclic llavors existeix un element x d'ordre $|G|$. Com que $p \mid |G|$ considerem $x^{|G|/p}$ que té ordre p i hem acabat.

Si G no és cíclic considerem $x \in G$. Si $p \mid |x|$ llavors per hipòtesi d'inducció existeix un element de $\langle x \rangle$ d'ordre p. Suposem doncs $p \nmid |x| = s$. Considerem $G/\langle x \rangle$ que és grup d'ordre menor que $|G|$ per ser G abelià i per tant $\langle x \rangle \trianglelefteq G$. Per hipòtesi d'inducció existeix un element $\overline{y} \in G/\langle x \rangle$ d'ordre p, és a dir $(\overline{y})^p = \overline{e}$. Així $y^p \in \langle x \rangle$ que té ordre s. Conseqüentment $e = (y^p)^s = (y^s)^p \Rightarrow |y^s| \mid p$. Com que p és primer, si $|y^s| = 1$, llavors $y^s = e \Rightarrow \overline{y}^s = e$ a $G/\langle x \rangle$. Amb això hauria de ser $p \mid s$ la qual cosa és una contradicció. Ha de ser doncs $|y^s| = p$.

□

Definició 1.5.5. Sigui G un grup finit i p un primer tal que $p||G|$. Si $|G| = p^n \cdot m$ amb $p \nmid m$ aleshores diem que $P \leq G$ és un p-subgrup de Sylow de G si $|P| = p^n$.

Alguns exemples de p-subgrups de Sylow són:

1. Si G és un p-grup, G ja és un p-subgrup de Sylow de G.
2. Sigui $G = \mathbb{Z}/12\mathbb{Z}$. Tenim $12 = 2^2 \cdot 3$. Així doncs $\langle \overline{4} \rangle$ té ordre 3 i és un 3-subgrup de Sylow. Igualment $\langle \overline{3} \rangle$ és un 2-subgrup de Sylow.

1.5.2 Sobre l'existència de p-subgrups de Sylow

Teorema 1.5.2. *(Primer teorema de Sylow) Sigui G un grup finit, p primer tal que $p||G|$. Aleshores G conté algun p-subgrup de Sylow.*

Demostració. Ho fem per inducció sobre $|G|$. Si $|G| = 2$ llavors $2|2$ i G ja és un 2-subgrup de Sylow de G.

Ara distingim dos casos:

1. Suposem que $p \mid Z(G)$. Pel teorema de Cauchy per grups abelians existeix $x \in Z(G)$ d'ordre p. Considerant $N = \langle x \rangle \leq Z(G)$ tenim que òbviament $N \trianglelefteq G$. El grup quocient G/N té ordre:
$$|G/N| = \frac{|G|}{|N|} = \frac{p^n m}{p} = p^{n-1}m$$
.
Ara per hipòtesi d'inducció G/N conté un subgrup P' d'ordre p^{n-1}. Considerant ara
$$\pi : G \longrightarrow G/N$$
epimorfisme fem $P = \pi^{-1}(P')$ tindrem $|P/N| = |P'| = p^{n-1} \Rightarrow |P| = |N|p^{n-1} = p^n$
2. Suposem $p \nmid |Z(G)|$. Considerem doncs l'equació de les classes de conjugació:
$$|G| = p^n m = |Z(G)| + \sum_{i=s+1}^{r} (G : C_G(x_i))$$
amb $(G : C_G(x_i)) \geq 2$.
Com que $|G| = |C_G(x_i)|(G : C_G(x_i)) \Rightarrow (G : C_G(x_i)) \mid |G|$. Així $(G : C_G(x_i)) \geq 2 \Rightarrow |C_G(x_i)| < |G|$. Com que $p \nmid (G : C_G(x_i)) \Rightarrow p^n \mid |C_G(x_i)|$. Tenim doncs que $C_G(x_i)$ és un subgrup d'ordre menor que $|G|, p^n \mid C_G(x_i) \Rightarrow C_G(x_i)$ conté un p-subgrup de Sylow per hipòtesi d'inducció. Aquest mateix és un p-subgrup de Sylow de G.

□

Teorema 1.5.3. *(Teorema de Cauchy) Sigui G d'ordre finit i p primer tal que $p||G|$. Aleshores G conté algun element d'ordre p.*

Demostració. $|G| = p^n m, p \nmid m$. Pel 1r teorema de Sylow G conté algun p-subgrup de Sylow. Sigui P un i $x \in P$ diferent del neutre. Com que $|x| \mid |P| = p^n \Rightarrow |x| = p^t$ per cert $t \geq 1$. L'element $x^{p^{t-1}}$ té ordre p. □

1.5.3 Relació entre dos p-subgrups de Sylow

Teorema 1.5.4. *(Segon teorema de Sylow) Sigui G un grup finit i p un primer tal que $p||G|$. Aleshores si P_1 i P_2 són p-subgrups de Sylow de G, existeix $g \in G$ tal que $gP_2g^{-1} = P_1$.*

En altres paraules el que ens diu el teorema és que dos p-subgrups de Sylow són un conjugat de l'altre. Així doncs, si P és un p-subgrup de Sylow, $\forall g \in G$, gPg^{-1} és també un p-subgrup de Sylow. Observem també que G tindrà a P com a únic subgrup de Sylow si i només si $P \trianglelefteq G$.

Demostració. Considerem $X = \{xP_1|\ x \in G\}$ les classes per l'esquerra de P_1. Fem actuar P_2 sobre X segons: $y \in P_2, y(xP_1) = (yx)P_1$. L'acció és ben definida en tant que si $xP_1 = x_1P_1$ llavors $(yx)^{-1}yx_1 = x^{-1}y^{-1}yx_1 = x^{-1}x_1 \in P_1$ i així $(yx)P_1 = (yx_1)P_1$. D'altra banda $e(xP_1) = (ex)P_1 = xP_1$ i també $y_1(y_2(xP_1)) = y_1((y_2x)P_1) = ((y_1y_2)x)P_1 = (y_1y_2)(xP_1)$. Per tant X és un P_2-conjunt.

D'aquesta manera sabem que $|X_{P_2}| \equiv |X| \mod p$ però també $|X| = (G : P_1) = \frac{p^n m}{p^n} = m$, que no és divisible per p. Això implica $|X_{P_2}| \neq 0 \Rightarrow \exists xP_1 \in X$ fix per P_2.

En conseqüència $y(xP_1) = (yx)P_1 = xP_1 \forall y \in P_2 \Leftrightarrow x^{-1}yx \in P_1 \forall y \in P_2 \Leftrightarrow x^{-1}P_2x \leq P_1$. Com que ambdós tenen p^n elements $x^{-1}P_2x = P_1$ i $g = x^{-1}$. □

1.5.4 Sobre el nombre de p-subgrups de Sylow d'un grup

Definició 1.5.6. Sigui G un grup i H un subgrup de G. El normalitzador de H a G és:

$$N_G(H) = \{x \in G|\ xHx^{-1} = H\}$$

Teorema 1.5.5. *(Tercer teorema de Sylow) Sigui G finit, p primer de manera que $p||G| = p^n \cdot m$ amb $p \nmid m$. Aleshores si n_p és el nombre de p-subgrups de Sylow de G, $n_p \equiv 1 \mod p$ i $n_p||G| = p^n \cdot m$. En particular $n_p \mid m$.*

Demostració. Fixem p primer i P un p-subgrup de Sylow de G. Considerem $X = \{T|\ T$ és p-subgrup de Sylow de $G\}$. Amb l'acció donada per $xT = xTx^{-1}, x \in P$, X és un P-conjunt. En efecte, és una acció ja que compleix que $eT = eTe^{-1} = T$ i $x(yT) = x(yTy^{-1}) = (xy)T(xy)^{-1} = (xy)T$.

Considerem com sempre $X_P = \{T \in X|\ xTx^{-1} = T, \forall x \in P\}$. Evidentment $P \in X_P$. Sigui $T \in X_P$ llavors $xTx^{-1} = T, \forall x \in P \Rightarrow P \leq N_G(T)$ i també $T \leq N_G(T)$. És a dir P i T són p-subgrups de Sylow de $N_G(T)$. Pel 2n teorema de Sylow P i T són conjugats dins $N_G(T)$, ço és, existeix $y \in N_G(T)$ tal que $P = yTy^{-1}$. En conseqüència $X_P = \{P\}$.

Ara bé P és un p-grup $\Rightarrow |X| \equiv |X_P| = 1 \mod p$. Per tant $n_p = |X| \equiv 1 \mod p$.

Fem ara actuar G sobre X segons $gP = gPg^{-1}, g \in G$. Pel 2n teorema de Sylow $\mathcal{O}(P) = \{gPg^{-1}|\ g \in G\} = X$. Ara $|X| = n_p = |\mathcal{O}(P)|\ |\ |G|$ però pel que hem vist abans $p \nmid n_p \Rightarrow n_p \mid m$. □

Corol·lari 1.5.3. *Suposem $|G| = pq$ amb p i q primers $p < q$. Aleshores $n_q = 1$ i per tant el q-subgrup de Sylow de G és normal. (G no és simple).*

Demostració. $n_q \equiv 1 \mod q \Rightarrow n_q = 1 + \alpha q$ per cert α. Ara $n_q \mid p \Rightarrow n_q = 1$ o bé $n_q = p$, que no pot ser per ser $p < q$. Aleshores $n_q = 1$ i pel 2n teorema de Sylow, l'únic que hi ha és normal a G. □

1.6 Classificació de grups abelians

Teorema 1.6.1. *Si A_n és el grup alternat d'n elements i $n \geq 5$ aleshores A_n és simple.*

Teorema 1.6.2. *(Teorema de Feit-Thompson) Si G és un grup finit no abelià simple llavors G té ordre parell.*

Proposició 1.6.1. *Suposem que G és un grup abelià finit. Siguin H_1 i H_2 subgrups de G d'ordres primers. Considerem $H = H_1 \cdot H_2$:*

1. *Tot element $h \in H$ s'escriu de forma única com $h = h_1 h_2$ amb $h_1 \in H_1$ i $h_2 \in H_2$.*
2. *$H \cong H_1 \times H_2$*

Demostració. 1. Observem que $H_1 \cap H_2$ és subgrup de H_1 i de H_2. Pel teorema de Lagrange $|H_1 \cap H_2| \mid |H_1|$ i $|H_1 \cap H_2| \mid |H_2|$. Per tant ha de ser $H_1 \cap H_2 = \{e\}$.

Així suposant que $h = h_1 h_2 = h_1' h_2' \in H$ tenim $(h_1')^{-1} h_1 = h_2' h_2^{-1} \in H_1 \cap H_2 \Rightarrow h_1 = h_1', h_2 = h_2'$.

2. Considerem ara

$$\varphi : H \longrightarrow H_1 \times H_2$$
$$h_1 h_2 \longmapsto (h_1, h_2)$$

φ és ben definida per l'apartat anterior. Evidentment és epimorfisme per ser G abelià. I a més φ és injectiu en tant que $h_1 h_2 = ee$ implica per l'apartat anterior també $h_1 = h_2 = e$ i per tant $\ker(f) = \{e\}$. En conseqüència φ és isomorfisme i

$$H \cong H_1 \times H_2$$

□

Proposició 1.6.2. *Suposem que G és un grup abelià finit. Siguin $H_1, \ldots, H_r$ subgrups de G d'ordres coprimers. Considerem $H = H_1 \cdot \ldots \cdot H_r$. Aleshores $H \cong H_1 \times \ldots \times H_r$.*

Demostració. Per inducció a partir de l'anterior. □

Teorema 1.6.3. *Suposem que G és un grup abelià finit $|G| = p_1^{n_1} \ldots p_r^{n_r}$ amb els p_i primers diferents. Aleshores si $P_1, \ldots, P_r$ són els subgrups de Sylow de G:*

$$G \cong P_1 \times \ldots \times P_r$$

Cada P_i és un grup abelià d'ordre potència d'un primer.

Demostració. Posem $H = P_1 \cdot \ldots \cdot P_r$ de forma que $H \leq G, |H| = p_1^{n_1} \ldots p_r^{n_r} = |G| \Rightarrow H = G$. Conseqüentment:

$$G \cong P_1 \times \ldots \times P_r$$

□

Teorema 1.6.4. *Si G és un grup abelià finit aleshores:*

$$G \cong \mathbb{Z}/p_1^{n_1}\mathbb{Z} \times \ldots \times \mathbb{Z}/p_r^{n_r}\mathbb{Z}$$

on els p_i són primers no necessàriament diferents. A més la descomposició és única tret de l'ordre dels factors.

Proposició 1.6.3. *$\mathbb{Z}/(m \cdot n)\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ si i només si m i n són coprimers.*

2

Anells

2.1 Anells i subanells

Definició 2.1.1. Direm que un conjunt R no buit i tancat amb dues operacions $+$ i $\cdot$ és un anell si compleix:

1. $(R, +)$ és un grup commutatiu.
2. El producte $\cdot$ compleix:
   i. $\forall x, y \in R$ es dóna que $x \cdot y \in R$
   ii. Propietat associativa, $\forall x, y, z \in R$ tenim $x \cdot (y \cdot z) = (x \cdot y) \cdot z$
   iii. Existència d'element neutre, 1 tal que $\forall x \in R$, $1 \cdot x = x \cdot 1 = x$
   iv. Propietat distributiva, $\forall x, y, z \in R$ tenim $x \cdot (y + z) = x \cdot y + x \cdot z$ i també $(y + z) \cdot x = y \cdot x + z \cdot x$

Si el producte és a més commutatiu, ço és, $x \cdot y = y \cdot x$ $\forall x, y \in R$, aleshores l'anell s'anomena commutatiu.

A partir d'ara R representa un anell. Pel que fa a la notació, emprarem notació additiva per $(R, +)$. Així el neutre per la suma és 0 i els inversos per la suma són donat $a \in R$, $-a$.

Proposició 2.1.1. *El neutre multiplicatiu* 1 *de* R *és únic.*

Demostració. Siguin $1, 1'$ neutres multiplicatius de R llavors $1 = 1 \cdot 1' = 1'$. □

Proposició 2.1.2. *Siguin* $a, b \in R$. *Aleshores:*

1. $-(-a) = a$
2. $0a = a0 = 0$
3. $(-a)b = a(-b) = -(ab)$
4. $(-a)(-b) = ab$
5. $-1(a) = -a$

Demostració. 1. Ja ho tenim de grups.

2. Tenim $0 + 0 = 0$ i així $0a = (0 + 0)a = 0a + 0a$. Sumant $-0a$ tenim $0a = 0$. Anàlogament $a0 = 0$.
3. Fem $0 = (a - a)b = ab + (-a)b$. Per tant $-(ab) = (-a)b$ i igualment tenim $-(ab) = a(-b)$.
4. A partir de l'anterior observem que $(-a)(-b) = -(a(-b)) = -(-(ab)) = ab$.
5. Anàlogament $-1(a) = -(1a) = -a$.

□

Alguns exemples d'anells són:

1. $\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ i l'anell de polinomis $K[x]$.
2. Les matrius $M_n(\mathbb{Q})$ amb la suma i el producte de matrius habituals. És tracta d'un anell no commutatiu com ja sabem.
3. Si G és un grup abelià llavors:

$$\mathrm{End}(G) = \{f : G \longrightarrow G \mid f \text{ és morfisme}\}$$

amb la composició $f \cdot g = f \circ g$ i

$$f + g : G \longrightarrow G$$
$$x \longmapsto f(x) + g(x)$$

és un anell.

Definició 2.1.2. Sigui $S \subseteq R$ no buit. Direm que S és un subanell si $1_R \in S$ i amb les operacions de R restringides a S, S és un grup amb la suma i és tancat pel producte.

Seguint els exemples d'abans ara tindriem:

$$\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$$

o també

$$\mathbb{Z} \subseteq K[x]$$

Definició 2.1.3. Diem que $x \in R$ és invertible si existeix $y \in R$ tal que $xy = yx = 1$. El denotem $y = x^{-1}$.

Proposició 2.1.3. *Si $x \in R$ és invertible llavors aquest invers és únic.*

Demostració. Suposem $y, z \in R$ dos inversos de x. Aleshores $y = y1 = y(xz) = (yx)z = 1z = z$. □

Definició 2.1.4.

$$U(R) = \{x \in R \,|\, x \text{ és invertible}\}$$

.

Proposició 2.1.4. *$U(R)$ és un grup amb el producte*

Demostració. Siguin $x, y \in U(R)$. Sabem que x és invertible i per tant xy^{-1} també ho és. □

Per exemple $U(\mathbb{Z}) = \{1, -1\}$ i $U(\mathbb{Q}) = \mathbb{Q} \setminus \{0\}$. A $\mathbb{Z}/n\mathbb{Z}$ tenim que $U(\mathbb{Z}/n\mathbb{Z}) = \{\overline{a} \,|\, \text{mcd}(a, n) = 1\}$. Veiem-ho. Suposem $\overline{a}$ invertible, és a dir, existeix $\overline{b}$ tal que $\overline{ab} = \overline{1}$. Això vol dir que $ab - 1 = \lambda n \Leftrightarrow ab - \lambda n = 1$ la qual cosa implica que $\text{mcd}(a, n) = 1$. Si ara tenim $\overline{a}$ tal que $\text{mcd}(a, n) = 1$ llavors per la identitat de Bézout existeixen α, β tals que $\alpha a + \beta n = 1$. Prenent classes tenim $\overline{a\alpha} = \overline{1}$ i $\overline{a}$ és invertible.

Definició 2.1.5. Direm que un anell commutatiu R és un cos si $U(R) = R \setminus \{0\}$. Si $U(R) = R \setminus \{0\}$ i R no és commutatiu diem que R és un anell de divisió.

2.2 Ideals

Considerarem anells commutatius, és a dir, $xy = yx \; \forall x, y \in R$.

Definició 2.2.1. Diem que un subconjunt no buit I de R és un ideal de R si amb la suma $+$, I és un subgrup de R i a més $rx \in I \; \forall r \in R, \forall x \in I$.

Definició 2.2.2. Diem que un ideal I de R és principal, si està generat per un sol element.

Tenint el compte el que hem vist a grups podem enunciar la següent proposició.

Proposició 2.2.1. *$I \subseteq R$ no buit és un ideal si i només si:*

1. $\forall x, y \in I \quad x - y \in I$
2. $\forall r \in R, \; \forall x \in I \quad rx \in I$.

Alguns exemples d'ideals són doncs:

1. Els ideals de R $I = \{0\}$ i $I = R$.
2. Fixat un element $a \in R$, els múltiples de a $(a) = aR = Ra = \{ra \,|\, r \in R\}$ és un ideal ja que $ra - sa = (r - s)a \in (a)$ i $s(ra) = (sr)a \in (a)$.

3. Si $R = \mathbb{Z}$ aleshores tot ideal de R és principal. Sigui I un ideal de R llavors I és subgrup de R amb la suma, que és cíclic $\Rightarrow$ I és cíclic. Així $I = n\mathbb{Z} = (n)$ per cert $n \in \mathbb{Z}$.

4. El mateix ocorre si fem $R = K[x]$. Si I és un ideal de R i $I = \{0\}$ llavors $I = (0)$. Suposem doncs que $I \neq \{0\}$. Sigui ara $f(x) \in R$ diferent de 0 tal que $\text{grau}(f(x)) = \min\{g(x) \in K[x] \,|\, g(x) \in I\}$. Veiem doncs que $f(x)$ ja genera I.

   Sigui $g(x) \in I$ fem $g(x) = f(x)q(x) + r(x)$ amb $\text{grau}(r(x)) < \text{grau}(f(x))$ o $r(x) = 0$. Ara $r(x) = g(x) - f(x)q(x) \in I$ ja que ambdós polinomis són de I. Ha de ser doncs $r(x) = 0$ i $I = (f(x))$.

Proposició 2.2.2. *R és un cos si i només si els únics ideals de R són (0) i R.*

Demostració. Suposem R cos. Si I és diferent de (0) i sigui $a \in I$ diferent de 0 a té invers $a^{-1} \in R$. Així $aa^{-1} = 1 \in I$. Sigui ara $r \in R$ $r = r1$ amb la qual cosa $r \in I$ i com que per definició $I \subseteq R$ tenim $I = R$.

Si els únics ideals de R són (0) i R posem per $a \in R$, $a \neq 0$, $I = (a)$. Hem de veure que $U(R) \supseteq R$. Aleshores $(a) = aR = R$ i en particular $1 \in (a)$ Per tant existeix $b \in R$ tal que $ab = 1$ i a és invertible. En particular R és invertible □

Proposició 2.2.3. *Siguin I, J ideals de R. Aleshores:*

1. *$I + J = \{x + y \,|\, x \in I, y \in J\}$ és un ideal de R.*
2. *$I \cap J$ és ideal de R.*
3. *$IJ = \{\sum_i x_i y_i \,|\, x_i \in I, y_i \in J\}$ és un ideal de R i a més $IJ \subseteq I \cap J$.*

Demostració.

1. Sabem que $I + J \leq R$. SiguiN $x \in I, y \in J, r \in R$ llavors $r(x + y) = rx + ry \in I + J$ evidentment.
2. Sabem que $I \cap J \leq R$. Sigui $x \in I \cap J, r \in R$ aleshores $rx \in I$ i $rx \in J$ per ser I, J ideals.
3. $IJ \leq R$. És ideal pel mateix motiu que als casos anteriors. Així sigui $z \in IJ$ tenim que $z = \sum_i x_i y_i$ per $x_i \in I$ i $y_i \in J$. Ara bé com que I és ideal per tot i tenim que $x_i y_i \in I$. Igualment com que J és ideal per tot i tenim $x_i y_i \in J$. En particular $z \in I \cap J$.

□

Fent ara $R = \mathbb{Z}$ i donats dos ideals I, J de R tenim que $I = (a), J = (b)$ per certs a i b. Veiem que $I + J = (a) + (b) = (d)$ amb $d = \text{mcd}(a, b)$.

Així doncs tenim que $a = a'd$ i $b = b'd$ per certs a', b'. D'aquesta forma $d = \alpha a + \beta b = \alpha a'd + \beta b'd = (\alpha a' + \beta b')d$ i per tant $(a) + (b) \subseteq (d)$. Però, per la identitat de Bézout tenim $d = \alpha' a + \beta' b$ per certs α', β'. Així $(d) \subseteq (a) + (b)$.

Igualment podem veure que $(a) \cap (b) = (m)$ amb $m = \text{mcm}(a, b)$. Com que $m = \lambda a = \mu b$ tenim òbviament $(m) \subseteq (a) \cap (b)$. D'altra banda si $x \in (a) \cap (b)$ ha de ser múltiple de a i de b. En particular és múltiple del mínim comú múltiple i $x \in (m)$.

Per últim $(a)(b) = \{\alpha_1 ab + \ldots + \alpha_n ab\} = \{(\alpha_1 + \ldots \alpha_n)ab\} = (ab)$

2.3 Anell quocient

Considerarem el grup additiu $(R, +)$ i un ideal I de R. Com que R és abelià I és normal a R. Considerarem doncs el grup quocient R/I amb $\overline{x} + \overline{y} = \overline{x + y}$.

Proposició 2.3.1. *Amb el producte $\overline{x} \cdot \overline{y} = \overline{xy}$ R/I és un anell.*

Demostració. Veiem que el producte és ben definit. Suposem que $\overline{x_1} = \overline{x_2}$ i $\overline{y_1} = \overline{y_2}$. Així doncs $x_1y_1 - x_2y_2 = x_1y_1 - x_1y_2 + x_1y_2 - x_2y_2 = x_1(y_1 - y_2) + y_2(x_1 - x_2) \in I$ ja que $(y_1 - y_2), (x_1 - x_2) \in I$. Així $\overline{x_1y_1} = \overline{x_2y_2}$.

Només queda comprovar les propietats referents al producte. Així $\overline{1}$ és el neutre multiplicatiu de R/I i l'associativitat i la distributivitat són conseqüència de les propietats corresponents sobre R i de la definició del producte a R/I. □

Com a exemple podem considerar $\mathbb{Z}/n\mathbb{Z}$.

Proposició 2.3.2. *$\mathbb{Z}/n\mathbb{Z}$ és cos si i només si n és primer.*

2.4 Morfismes d'anells

Definició 2.4.1. Si R, S són anells direm que $f : R \longrightarrow S$ és un morfisme d'anells si:

1. $f : R \longrightarrow S$ és morfisme de grups amb la suma.
2. $f(xy) = f(x)f(y)$ $\forall x, y \in R$
3. $f(1_R) = f(1_S)$.

A més a més si el morfisme:

- f és injectiu, s'anomena monomorfisme.
- f és exhaustiu, s'anomena epimorfisme.
- f és bijectiu, s'anomena isomorfisme. En aquest cas diem que R i S són isomorfs i escrivim $R \cong S$.
- $f : R \longrightarrow R$, s'anomena endomorfisme.
- és bijectiu i $f : R \longrightarrow R$, s'anomena automorfisme.

Proposició 2.4.1. *Sigui $f : R \longrightarrow S$ un morfisme d'anells. Aleshores:*

1. $f(0) = 0$
2. $f(-x) = -x \quad \forall x \in R$

Demostració. En particular f és morfisme de grups amb $+$. □

Definició 2.4.2. Sigui $f : R \longrightarrow S$ un morfisme d'anells. Aleshores:

$$\ker(f) = \{x \in R \,|\, f(x) = 0\}$$
$$\mathrm{Im}(f) = \{f(x) \,|\, x \in R\}$$

Proposició 2.4.2. *Sigui $f : R \longrightarrow S$ un morfisme d'anells. Aleshores:*

1. $\ker(f)$ *és un ideal de R i a més* $\ker(f) = \{0\}$ *si i només si f és monomorfisme.*
2. $\mathrm{Im}(f)$ *és subanell de S. Evidentment* $\mathrm{Im}(f)$ *si i només si f és epimorfisme.*

Demostració. 1. Sabem que $\ker(f) \trianglelefteq R$ i a més si $x \in \ker(f)$ i $r \in R$ llavors $f(rx) = f(r)f(x) = f(r)0 = 0$ i per tant $rx \in \ker(f)$, és a dir $\ker(f)$ és un ideal de R.

Ara si $\ker(f) = \{0\}$ suposem $f(x) = f(y)$. Sumant $-f(y)$ tenim $0 = f(x) - f(y) = f(x - y)$ amb la qual cosa $x - y \in \ker(f)$ i $x = y$. Si f és monomorfisme, sigui $x \in \ker(f)$ tenim $f(x) = 0$ i $f(0) = 0$ per ser morfisme de grups amb la suma. Per tant $x = 0$.

2. Sabem que $\mathrm{Im}(f) \leq R$. Siguin $f(x), f(y) \in \mathrm{Im}(f)$ llavors $f(x)f(y) = f(xy) \in \mathrm{Im}(f)$ i és tancat pel producte. Com que $1_S = f(1_R) \in \mathrm{Im}(f)$ $\mathrm{Im}(f)$ és subanell de S

□

Proposició 2.4.3. *Sigui $f : R \longrightarrow S$ un morfisme d'anells. Aleshores:*

1. *J ideal de $S \Rightarrow f^{-1}(J) = \{x \in R \,|\, f(x) \in J\}$ és un ideal de R.*
2. *f epimorfisme i I ideal de $R \Rightarrow f(I)$ és un ideal de S.*
3. *Si R' és un subanell de $R \Rightarrow f(R')$ és un subanell de S.*
4. *S' subanell de $S\Rightarrow f^{-1}(S')$ és un subanell de R.*

Com a exemples podem considerar:

1. I ideal de R. La projecció canònica $\pi : R \longrightarrow R/I$ donada per $\pi(x) = \overline{x}$ és un epimorfisme d'anells.
2. El morfisme avaluació. Sigui K un cos i $a \in K$, considerem $K[x]$. Aleshores l'aplicació:
$$\psi_a : K[x] \longrightarrow K$$
$$f(x) \longmapsto f(a)$$
és un morfisme d'anells. El seu nucli conté els polinomis que tenen a com a arrel. Així $\ker(\psi_a) = \{f(x) \,|\, f(a) = 0\}$ és un ideal de $K[x]$.

Proposició 2.4.4. *Siguin R, S, T anells i $f : R \longrightarrow S$, $g : S \longrightarrow T$ morfismes d'anells llavors:*

1. *$g \circ f : R \longrightarrow S \longrightarrow T$ és un morfisme d'anells.*
2. *Si f és isomorfisme llavors $f^{-1} : S \longrightarrow R$ és un isomorfisme d'anells.*

2.4.1 Tres teoremes d'isomorfia

Teorema 2.4.1. *(Primer teorema d'isomorfia) Sigui $f : R \longrightarrow S$ un morfisme d'anells. Aleshores*

$$\begin{aligned} \tilde{f} : R/\ker(f) &\longrightarrow \mathrm{Im}(f) \\ \overline{x} &\longmapsto f(x) \end{aligned}$$

és un isomorfisme. En particular $R/\ker(f) \cong \mathrm{Im}(f)$.

Demostració. Sabem que $\tilde{f}$ és ben definida i que és isomorfisme de grups. Només hem de veure que és morfisme d'anells d'acord amb

$$\tilde{f}(\overline{x} \cdot \overline{y}) = \tilde{f}(\overline{xy}) = f(xy) = f(x)f(y) = \tilde{f}(\overline{x})\tilde{f}(\overline{y})$$

□

Teorema 2.4.2. *Sigui $f : R \longrightarrow S$ epimorfisme d'anells. Aleshores l'aplicació*

$$\begin{aligned} \varphi : \{J \text{ ideal de } R \mid \ker(f) \subseteq J\} &\longrightarrow \{\text{ideals de } S\} \\ J &\longmapsto f(J) \end{aligned}$$

és bijectiva.

En particular si I és ideal de R, els ideals de R/I són de la forma $\pi(J) = J/I$ on J és un ideal de R que conté I.

Proposició 2.4.5. *Els ideals de $\mathbb{Z}/n\mathbb{Z}$ són els generats pels divisors de n.*

Demostració. Pel 1r teorema d'isomorfia hi ha una bijecció entre ideals de $\mathbb{Z}$ que contenen (n) i ideals de $\mathbb{Z}/n\mathbb{Z}$. Veurem més endavant que tot ideal de $\mathbb{Z}$ és principal. D'aquesta manera els ideals de $\mathbb{Z}/n\mathbb{Z}$ són de la forma $(\overline{a})$ amb $(n) \subseteq (a)$. En altres paraules, els ideals de $\mathbb{Z}/n\mathbb{Z}$ són els generats per $\overline{a}$ tal que $a \mid n$. □

Teorema 2.4.3. *(Segon teorema d'isomofia) Siguin I, J ideals de R, aleshores:*

$$(I + J)/I \cong J/(I \cap J)$$

on aquest isomorfisme és un isomorfisme de grups que conserva el producte.

En aquest cas l'isomorfisme no és d'anells ja que malgrat que $I + J$ és ideal de R, $I, J \subseteq I + J$ i $I \cap J$ és ideal de R no podem assegurar que aquests continguin l'unitat de l'anell.

Demostració. Sabem que existeix un isomorfisme de grups. Només s'ha de veure que aquest mateix conserva el producte. □

Teorema 2.4.4. *(Tercer teorema d'isomorfia) Siguin I, J ideals de R tals que $I \subseteq J$. Aleshores hi ha un isomorfisme d'anells de manera que:*

$$(R/I)/(J/I) \cong R/J$$

Sabem pel primer teorema que $J/I = \pi(J)$ és un ideal de R/I, de manera que té sentit l'enunciat.

Demostració. El mateix isomorfisme que per grups funciona. □

2.5 Característica d'un anell

Definició 2.5.1. Diem que un anell R té característica $n > 0$ si n és el mínim tal que $1 + 1 + \overset{n)}{\ldots} + 1 = n \cdot 1 = 0$ a R. Si aquest no existeix, diem que R té característica zero. Escriurem $\mathrm{ch}(R) = n$ o bé $\mathrm{ch}(R) = 0$.

Evidentment tindrem $\mathrm{ch}(\mathbb{Z}) = \mathrm{ch}(\mathbb{Q}) = 0$ i també $\mathrm{ch}(\mathbb{Z}/n\mathbb{Z}) = n$.

Proposició 2.5.1. *Sigui $f : \mathbb{Z} \longrightarrow R$ l'aplicació tal que $f(a) = 1_R + 1_R + \overset{a)}{\ldots} + 1_R = a \cdot 1_R$. Aleshores f és morfisme d'anells i $\ker(f) = (n)$ amb $n = \mathrm{ch}(R)$. En particular si f és injectiva $\mathrm{ch}(R) = 0$.*

Demostració. És morfisme de grups en tant que $f(a + b) = (a + b) \cdot 1_R = f(a) + f(b)$. I compleix igualment que $f(1) = 1 \cdot 1_R = 1_R$ i que $f(a \cdot b) = (a \cdot b) \cdot 1_R = f(a)f(b)$. Suposem doncs $\mathrm{ch}(R) = n$. Llavors és evident que com que $\ker(f)$ és cíclic haurà d'estar generat pel mínim enter que compleix $n \cdot 1_R = 0$, ço és $\ker(f) = (n)$.

□

Corol·lari 2.5.1. *Si $\mathrm{ch}(R) = 0$ llavors $\mathbb{Z}$ és isomorf a un subanell de R. Si pel contrari, $\mathrm{ch}(R) = n$, aleshores $\mathbb{Z}/n\mathbb{Z}$ és isomorf a un subanell de R.*

Demostració. Si $\mathrm{ch}(R) = 0$ aleshores

$$f : \mathbb{Z} \longrightarrow R$$

$$1 \longmapsto 1_R$$

és injectiva, bijectiva sobre la imatge. Tenim doncs $\mathbb{Z} \cong \mathrm{Im}(f)$ subanell de R.

Si $\mathrm{ch}(R) = n$, llavors

$$f : \mathbb{Z} \longrightarrow R$$

$$1 \longmapsto 1_R$$

té $\ker(f) = (n)$ i pel primer teorema d'isomorfia $\mathbb{Z}/n\mathbb{Z} \cong \mathrm{Im}(f)$ subanell de R. □

Corol·lari 2.5.2. *Sigui K un cos. Si $\mathrm{ch}(K) = 0$ aleshores K conté un subcos isomorf a $\mathbb{Q}$. Si $\mathrm{ch}(K) = p$ amb p primer aleshores K conté algun subcos isomorf a $\mathbb{Z}/p\mathbb{Z}$.*

Demostració. Suposem $\mathrm{ch}(K) = 0$. Considerant f de la proposició anterior podem veure que si $b \in K$ llavors el seu invers també és dins de K Ara considerem

$$\phi : \mathbb{Q} \longrightarrow K$$

donada per $\phi(\frac{a}{b}) = ab^{-1} \in K$. L'aplicació és ben definida ja que $\frac{a}{b} = \frac{c}{d}$ si i només si $ad = cb$. Per ser K cos ϕ és compleix $\phi(\frac{a}{b}\frac{c}{d}) = \phi(\frac{a}{b})\phi(\frac{c}{d})$ i a més $\phi(1) = 1_K$. D'altra banda es comprova fàcilment que es morfisme de grups. Tenim doncs un morfisme de cossos, veiem que és injectiu. Si considerem $\ker(\phi)$ ideal de $\mathbb{Q}$ haurà de ser $\ker(\phi) = \mathbb{Q}$ o $\ker(\phi) = (0)$. Haurà de ser $\ker(\phi) = (0)$ i tenim ϕ injectiva amb la qual cosa $\mathbb{Q}$ és contingut a K. □

Proposició 2.5.2. *Sigui K un cos. Aleshores* $\mathrm{ch}(K) = 0$ *o bé* $\mathrm{ch}(K) = p$ *primer.*

Demostració. Suposem $\mathrm{ch}(K) = n \neq 0$. Aleshores $1+\overset{n)}{\dots}+1 = 0$ a K. Si n no és primer llavors $n = n_1 n_2$ amb $1 < n_1, n_2 < n$. Tenim.

$$(1+\overset{n_1)}{\dots}+1)(1+\overset{n_2)}{\dots}+1) = n_1 n_2 1_K = 1+\overset{n)}{\dots}+1 = 0$$

Hem trobat doncs n_1 i n_2 diferents de zero tals que $n_1 n_2 1_K = 0$. Contradicció. □

2.6 Dominis d'integritat, ideals primers i ideals maximals

En aquesta secció R serà un anell commutatiu i com sempre amb unitat.

Definició 2.6.1. Un element $a \in R$ diferent de 0 és un divisor de zero si existeix $b \in R$ diferent de 0 també tal que $ab = 0$. Així doncs diem que R és un domini d'integritat (DI) si R no té divisors de zero.

Evidentment si K és un cos llavors és un DI. Ja que si suposem $a, b \in K$ diferents de zero tals que $ab = 0$ llavors multiplicant pels inversos tindríem $1 = 0$.

Teorema 2.6.1. *Si R és un DI finit llavors és un cos.*

Demostració. Sigui $a \in R$ fix, diferent de 0. Considerem l'aplicació $f : R \longrightarrow R$ donada per $f(x) = ax$. Com que R és tancat, si R és finit f és exhaustiva. En particular existeix $x \in R$ tal que $ax = 1$ i hem acabat. □

Proposició 2.6.1. *$\mathbb{Z}/n\mathbb{Z}$ és DI si i només si n és primer.*

Definició 2.6.2. Sigui I un ideal de R, $I \neq R$, es diu que és primer si sempre que $ab \in I$ llavors $a \in I$ o bé $b \in I$.

Proposició 2.6.2. *Sigui I un ideal de R, $I \neq R$. Aleshores I és primer si i només si R/I és domini d'integritat.*

Demostració. Suposem I primer i $\overline{a}\overline{b} = 0$ a R/I. Això implica $ab \in I$ i com que és primer un dels dos és de I i per tant 0 a R/I.

Recíprocament si R/I és DI i suposem $ab \in I$ llavors $\overline{a}\overline{b} = 0$ a R/I. En particular algun dels dos és 0 i pertany a I. □

Podem posar exemples d'algunes aplicacions:

1. Si R és anell llavors R és DI si i només si (0) és primer.
2. Els ideals primers de $\mathbb{Z}$ són (0) i (n) amb n primer ja que $\mathbb{Z}/n\mathbb{Z}$ és DI.

Definició 2.6.3. Diem que un ideal M de R és maximal si $M \neq R$ i sempre que $M \subseteq I \subseteq R$ amb I ideal de R es dóna que $I = M$ o bé $I = R$.

Proposició 2.6.3. *Sigui M un ideal de R diferent de R. Aleshores M és maximal si i només si R/M és cos.*

Demostració. R/M és anell. Per tant serà cos si i només si els seus ideals són (0) i R/M. D'altra banda els ideals de R/M són, pel 1r teorema d'isomorfia de la forma I/M amb I ideal de R, és a dir $M \subseteq I$. Tenim doncs M maximal si i només si $I = M$ o $I = R$. Les dues possibilitats impliquen R/M cos. □

Corol·lari 2.6.1. *Si M és un ideal maximal de R llavors és primer.*

Definició 2.6.4. Sigui A un conjunt no buit. Aleshores diem que una relació $\leq$ és d'ordre si compleix:

1. Reflexiva: $a \leq a \; \forall a \in A$
2. Antisimètrica: $a \leq b$ i $b \leq a \Rightarrow a = b \; \forall a, b \in A$
3. Transitiva: $a \leq b, b \leq c \Rightarrow a \leq c \; \forall a, b, c \in A$.

Definició 2.6.5. Sigui A un subconjunt no buit amb una relació d'ordre $\leq$. Aleshores un subconjunt $\mathcal{C} \subseteq A$ és una cadena si donats $a, b \in \mathcal{C}$ llavors $a \leq b$ o $b \leq a$.

Sigui $B \subseteq A$ diem que $a \in A$ és una fita superior de B si $b \leq a$ per a tot $b \in B$.

Diem que $c \in A$ és maximal si sempre que $a \leq b$ llavors $b = a$.

Lema de Zorn. *Sigui A un conjunt no buit amb una relació d'ordre $\leq$. Si tota cadena $\mathcal{C}$ de A té alguna fita superior a A aleshores A té elements maximals.*

Teorema 2.6.2. *R té algun ideal maximal*

Demostració. Considerem el conjunt $A = \{I \,|\, I \text{ ideal de } R, I \neq R\}$.$A$ no és buit ja que (0) hi és. L'ordenem segons la relació $\subseteq$ inclusió de conjunts. És evident que és d'ordre. Veurem que tota cadena de A té una fita superior a A. Prenem $\mathcal{C} \subseteq A$

Considerem

$$J = \bigcup_{I_i \in \mathcal{C}} I_i$$

Si $x, y \in J$ aleshores $x \in I_1$ i $y \in I_2$ per certs $I_1, I_2 \in \mathcal{C}$. Suposem $I_1 \subseteq I_2 \Rightarrow x, y \in I_2 \Leftrightarrow x - y \in I_2$. Això implica $x - y \in J$. Ara si $x \in J$ i $r \in R$ seguint el mateix raonament tenim $rx \in J$ i J és ideal de R.

Veiem que J és fita superior de $\mathcal{C}$. Primer veurem que J és de A. Suposem $J = R \Rightarrow 1 \in J \Rightarrow 1 \in I_i$ per cert i. Això implica $I_i = R$ la qual cosa és una contradicció. Tenim doncs $J \in A$ i $I_i \in J$ per tot $I_i \in \mathcal{C}$. En particular J és fita superior de $\mathcal{C}$ i pel lema de Zorn R té elements maximals. □

De forma similar es pot demostrar el següent teorema

Teorema 2.6.3. *Sigui K un cos. Tot K-espai vectorial té una base.*

2.7 El cos de fraccions d'un domini

Com a exemple podríem construir $\mathbb{Q}$ a partir de $\mathbb{Z}$. Més generalment ho farem per un DI R commutatiu.

Considerem $A = \{(a,b) \in R \times R \,|\, b \neq 0\} = R \times R*$ amb $R* = R \setminus \{0\}$. Definim a A la relació $(a,b) \sim (c,d) \Leftrightarrow ad = bc$. És fàcil veure que $\sim$ és d'equivalència. Evidentment $(a,b) \sim (a,b)$. D'altra banda si $(a,b) \sim (c,d)$ llavors $ad = bc \Leftrightarrow cb = da \Leftrightarrow (c,d) \sim (a,b)$. Finalment si $(a,b) \sim (c,d)$ i $(c,d) \sim (e,f)$ tenim $ad = bc$ i $cf = de$. Hem de veure que $af = be$. Tenim $adf = bcf = bde \Leftrightarrow af = be$ per ser R domini.

Considerem doncs el conjunt quocient $A/\sim$ i denotem $\frac{a}{b} = \overline{(a,b)}$. Definim les operacions suma i producte:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$$
$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

Es comprova directament que aquestes operacions són ben definides, ço és, que no depenen del representant escollit.

Igualment es poden comprovar les propietats de cos per $A/\sim$. Escriurem $\mathcal{F} = A/\sim$ per denotar el cos de fraccions de R.

Podem entendre el que acabem de fer d'acord amb:

$$f : R \hookrightarrow \mathcal{F}$$
$$x \mapsto \frac{x}{1}$$

que es tracta d'un morfisme d'anells injectius. Això és perquè:

$$f(x+y) = \frac{x}{1} + \frac{y}{1} = f(x) + f(y)$$
$$f(xy) = \frac{xy}{1} = f(x)f(y)$$
$$f(1) = \frac{1}{1} \in \mathcal{F}$$

Teorema 2.7.1. *Sigui R un DI commutatiu amb 1. Sigui $\mathcal{F}$ el cos de fraccions de R. Sigui K un cos tal que $R \subseteq K$. Aleshores existeix un únic morfisme de cossos $f : \mathcal{F} \longrightarrow K$ tal que $f|_R = \mathrm{id}$. En particular $\mathcal{F} \cong f(K) \subseteq K$.*

Demostració. S'ha de complir que $f(\frac{a}{b}) = f(\frac{a}{1}\frac{1}{b}) = f(a)f(\frac{1}{b}) = af(b)^{-1} = ab^{-1} \in K$. Precisament definim f així, és a dir $f(\frac{a}{b}) = ab^{-1} \in K$. Queda comprovar que f és morfisme de cossos. □

3

Divisibilitat i factorització

En aquesta secció. R serà un DI commutatiu i com sempre amb unitat.

3.1 Primers conceptes, mcd i mcm

Definició 3.1.1. Siguin $a, b \in R$. Diem que a divideix b, $a \mid b$ si existeix $c \in R$ tal que $b = ac$. En aquest cas diem també que b és múltiple de a.

Observem doncs que si $a \in R$ aleshores $n \mid a$ si $n \in U(R)$ ja que $a = n(n^{-1}a)$ i igualment $an \mid a$ en tant que $a = (an)n^{-1}$. Als elements invertibles de R els direm unitats. Així doncs les unitats i an per $n \in U(R)$ són sempre divisors obvis de a.

També si a, b són diferents de 0, $a \mid b$ i $b \mid a$ implica $b = ac$ i $a = bc'$ per certs $c, c' \in R$. Així $b = bc'c \Rightarrow 1 = c'c$. És a dir, a i b només difereixen en una unitat. Recíprocament tenim que si $a = bn$ amb n unitat llavors evidentment $a \mid b$ i $b \mid a$. Ara si $a = 0$ i $0 \mid b$ aleshores $b = 0$.

Definició 3.1.2. Diem que $a, b \in R$ són associats si $a = bu$ amb $u \in U(R)$. Escriurem $a \sim b$.

Proposició 3.1.1. *$\sim$ és d'equivalència*

Demostració. Evidentment $a \sim a$. Igualment si $a = bu$ tenim $b = au^{-1}$. I si $a = bu$ i $b = cu'$ tenim $a = cu'u$ amb $u'u \in U(R)$. □

Observem ara que si $b \mid a$ llavors $a \in (b)$ amb la qual cosa $(a) \subseteq (b)$. Si $a \mid b$ i $b \mid a$ aplicant l'anterior es tenen les dues inclusions i $(a) = (b)$.

Definició 3.1.3. Diem que d és un mcd de a i b i posem $d = \text{mcd}(a, b)$ si:

1. $d \mid a$ i $d \mid b$
2. Si $\exists d' \in R$ tal que $d' \mid a$ i $d' \mid b$ llavors $d' \mid d$.

Diem que m és un mcm de a i b i posem $m = \text{mcm}(a, b)$ si:

1. $a \mid m$ i $b \mid m$
2. Si $\exists m' \in R$ tal que $a \mid m'$ i $b \mid m'$ llavors $m \mid m'$.

No pensem però que per tot $a, b \in R$ existeixen mcm i mcd. Per exemple a $\mathbb{Z}[\sqrt{-3}]$ els elements 2 i $1 + \sqrt{-3}$ tenen mcd però no mcm. Els elements 4 i $2 + 2\sqrt{-3}$ no tenen ni mcd ni mcm.

De fet, en general l'existència de mcm implica que existeix mcd. Suposant que $m = mcm(a, b)$ aleshores tenim $a \mid ab$ i $b \mid ab$. Per definició de mcm tenim $m \mid ab$ i podem considerar $\frac{ab}{m}$. Precisament aquest element és un mcd de a i b. Es pot veure provant que compleix les hipòtesi de mcd. Aquests tampocs han de ser únics i per exemple quan escrivim $d = \text{mcd}(a, b)$ estem dient que d és un mcd de a i b.

Considerant ara $d = \text{mcd}(a, b)$ tenim per definició $d \mid a$ i $d \mid b$ de manera que $(a) \subseteq (d)$ i $(b) \subseteq (d)$. Per tant $(a) + (b) \subseteq (d)$. Generalment aquesta inclusió no és una igualtat. No obstant això a $\mathbb{Z}$ i a $K[x]$ amb K cos la identitat de Bézout ens dóna l'altra inclusió. Com que existeixen $\alpha, \beta \in R$ tals que $d = \alpha a + \beta b$ tenim $d \in (a) + (b)$ i així $(a) + (b) = (d)$.

Més propietats del mcm i del mcd, suposant que existeixen, són:

1. Si $d = \text{mcd}(a, b)$, $m = \text{mcm}(a, b)$ i $u \in U(R)$ llavors $du = \text{mcd}(a, b)$ i $mu = \text{mcm}(a, b)$. Veiem-ho pel mcd. Escriurem $d' = du$. Com que $d \mid a$ i $d \mid b$ existeixen $\alpha, \beta \in R$ tals que $a = \alpha d = \alpha d' u^{-1}$ i $b = \beta d = \beta d' u^{-1}$. Així $d' \mid a, b$. I si $c \mid a$ i $c \mid b$ tenim $c \mid d = d' u^{-1}$. D'aquesta forma per cert c' hom té $d' u'^{-1} = cc' \Leftrightarrow d' = cc' u$ i $c \mid d'$ i d' és mcd de a i b.
2. Si d, d' són mcd de a i b aleshores $d \sim d'$. Si els dos són diferents de 0 tenim $d \mid d'$ i $d' \mid d$ i per tant $d \sim d'$. Si un dels dos és zero llavors $a = b = 0$.
3. $\text{mcd}(a, 0) = a$ i $\text{mcm}(a, 0) = 0$.
4. Si d és un mcd de a i b podem escriure $a = a'd$ i $b = b'd$. Així doncs $\text{mcd}(a', b') = 1$. Evidentment 1 divideix els dos. Suposem ara $c \mid a'$ i $c \mid b'$. Aleshores existeixen $\alpha, \beta \in R$ tals que $a' = \alpha c$ i $b' = \beta c$. Per tant $a = a'd = \alpha cd$ i $b = b'd = \beta cd$ de manera que cd divideix a i b. Per definició de d, $ca \mid d$ i d és de la forma $d = \gamma cd \Leftrightarrow 1 = \gamma c$ per cert γ.
5. $c \in R$ també com a i b. Suposant que $\text{mcd}(ca, cb)$ i $\text{mcd}(a, b)$ existeixen tenim $\text{mcd}(ca, cb) = c \cdot \text{mcd}(a, b)$. Veiem-ho.
   - Si $a = 0$ tenim $\text{mcd}(0, cb) = cb = c \cdot \text{mcd}(0, b) = cb$.
   - Si $b = 0$ tenim $\text{mcd}(ca, 0) = ca = c \cdot \text{mcd}(a, 0) = ca$.
   - Si $c = 0$ tenim $\text{mcd}(0, 0) = 0 = 0 \cdot \text{mcd}(0, 0) = 0$.

Suposant a, b, c diferents de 0 escrivim $d = \mathrm{mcd}(a, b)$ i $d' = \mathrm{mcd}(ca, cb)$. Així $cd \mid ca$ i $cd \mid cb$ de manera que $cd \mid d' \Leftrightarrow d' = \gamma cd$ per cert γ. També existeixen α, β tals que $ca = \alpha d'$ i $cb = \beta d'$. Escrivint com sempre $a = a'd$ i $b = b'd$ tenim $ca = ca'd = \alpha d' = \alpha\gamma cd \Leftrightarrow a' = \gamma c \Leftrightarrow \gamma \mid a'$ i anàlogament per cb tenim $\gamma \mid b'$. Conseqüentment tindrem $\gamma \mid 1$ i γ és invertible. Així doncs $d' \sim cd$ i cd és mcd de ca, cb.

6. Suposant a, b diferents de 0, suposem que m és un mcm de a i b. Si $ab = mc$ per cert $c \in R$ aleshores c és un mcd de a i b. Tenim $a \mid m$ i $b \mid m$ de manera que per certs α, β tenim $m = \alpha a = \beta b$. Llavors

$$ab = mc = \alpha ac \Rightarrow c \mid b$$

$$ab = mc = \beta bc \Rightarrow c \mid a$$

Suposem ara $e \mid a$ i $e \mid b$. Escrivint $a = \alpha' e$ i $b = \beta' e$ podem considerar $\alpha'\beta' e = \gamma m$ ja que $\alpha'\beta' e$ és múltiple de a i b i en particular de m. Així $ab = \alpha'\beta' ee = \gamma me = mc \Leftrightarrow \gamma e = c \Leftrightarrow e \mid c$ com volíem veure.

Proposició 3.1.2. *Existeix* mcd *per a tots $a, b \in R$ si i només si existeix mcm per a tots $a, b \in R$*

Proposició 3.1.3. *Si el* mcd *existeix és associatiu. És a dir, si $a, b, c \in R$ aleshores:*

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

Lema d'Euclides. *Suposem que el* mcd *existeix per tota parella d'elements. Si $n \mid ab$ i $\mathrm{mcd}(n, a) = 1$ llavors $n \mid b$.*

3.2 Primers i irreductibles. Dominis de factorització única

R continua sent un DI commutatiu i com sempre amb unitat.

Definició 3.2.1. Un element $p \in R$ diferent de 0 no invertible és diu que es primer si sempre que $p \mid ab$ amb $a, b \in R$ llavors $p \mid a$ o $p \mid b$.

Observem que p és primer si i només si (p) és un ideal primer.

Definició 3.2.2. Un element $a \neq 0$ i no invertible es diu que és irreductible o àtom si sempre que $a = bc$ amb $b, c \in R$ llavors b és invertible o c és invertible.

Proposició 3.2.1. *Si p és primer llavors p és irreductible.*

Demostració. Suposem $p = ab$. Com que p és primer $p \mid a$ o $p \mid b$. Suposem sense pèrdua de generalitat $p \mid a \Leftrightarrow a = \alpha p$ per cert α. Aleshores $p = ab = \alpha pb \Rightarrow 1 = \alpha b$ i b és invertible. □

Definició 3.2.3. R és domini de factorització única (DFU) si:

1. Si a és diferent de 0 i no invertible aleshores $a = p_1 \cdot \ldots \cdot p_r$ amb els p_i irreductibles.

2. Si $a = p_1 \cdot \ldots \cdot p_r = q_1 \cdot \ldots \cdot q_s$ llavors $r = s$ i reordenant si cal tenim $p_i \sim q_i$ per tot i.

Proposició 3.2.2. *Siguin $p, q \in R$ primers i $a, b \in R$ irreductibles, aleshores:*

1. *pu és primer per tot $u \in U(R)$.*
2. *au és irreductible per tot $u \in U(R)$.*
3. *$p \mid q$ si i només si $p \sim q$.*
4. *$a \mid b$ si i només si $a \sim b$.*

Teorema 3.2.1. *R és DFU si i només si tot irreductible és primer i tot element a diferent de 0 i no invertible descomposa com a producte d'irreductibles, ço és $a = p_1 \cdot \ldots \cdot p_n$ amb p_i irreductibles.*

Demostració. Suposem R DFU. Hem de veure que tot irreductible és primer. Sigui $p \in R$ irreductible suposem $p \mid ab$. Posem $a = p_1 \cdot \ldots \cdot p_r, b = q_1 \cdot \ldots \cdot q_s$ amb factors irreductibles. La descomposició de ab en irreductibles és $ab = p_1 \cdot \ldots \cdot p_r q_1 \cdot \ldots \cdot q_s$ i també $ab = p\alpha$ per cert $\alpha = \alpha_1 \cdot \ldots \cdot \alpha_t \in R$ amb els α_i irreductibles. Aleshores tenim $p\alpha_1 \cdot \ldots \cdot \alpha_t = p_1 \cdot \ldots \cdot p_r q_1 \cdot \ldots \cdot q_s$. Com que R és DFU tenim $t + 1 = r + s$ i p és associat a algun p_i o q_i. Per tant $p \mid a$ o $p \mid b$.

Recíprocament suposem que es compleixen les dues condicions enunciades. Només hem de veure la unicitat de la descomposició. Sigui $a \in R$ llavors $a = p_1 \cdot \ldots \cdot p_r = q_1 \cdot \ldots \cdot q_s$ amb els p_i i els q_i irreductibles. Ara $p_1 \mid q_1(q_2 \cdot \ldots \cdot q_s)$. Com que p_1 és primer $p_1 \mid q_1$ amb la qual cosa $p_1 \sim q_1$ o bé $p_1 \mid q_2 \cdot \ldots \cdot q_s$. Repetint aquest mateix argument veiem que sense pèrdua de generalitat podem suposar $p_1 \mid q_1$. Així tenim per $u \in U(R)$ que $q_1 = up_1$ i llavors $p_2 \cdot \ldots \cdot p_r = uq_2 \cdot \ldots \cdot q_s$. Repetint aquest procés ens podem trobar davant tres situacions:

- Si $r < s$ llavors $1 = u_1 \cdot \ldots \cdot u_r q_{r+1} \cdot \ldots \cdot q_s \Rightarrow q_{r+1} \cdot \ldots \cdot q_s$ són invertibles. Contradicció.
- Si $s < r$ llavors $u_1 \cdot \ldots \cdot u_s = p_{s+1} \cdot \ldots \cdot p_r \Rightarrow p_{s+1} \cdot \ldots \cdot p_r$ són invertibles. Contradicció.

Ha de ser doncs $r = s$ i tenim per tot i que $p_i \sim q_i$. □

Proposició 3.2.3. *Suposem R DFU. Suposem $a, b \in R$ diferents de 0 i no invertibles. Posem $a = p_1^{\alpha_1} \cdot \ldots \cdot p_r^{\alpha_r}, b = p_1^{\beta_1} \cdot \ldots \cdot p_r^{\beta_r}$ amb els p_i irreductibles, $p_i \neq p_j$ si $i \neq j$ i $\alpha_i, \beta_i \geq 0$. Aleshores $d = \prod_{i=1}^r p_i^{\min(\alpha_i, \beta_i)}$ és un* mcd *de a i b i $m = \prod_{i=1}^r p_i^{\max(\alpha_i, \beta_i)}$ és un* mcm.

Demostració. Ho fem per d. Evidentment $d \mid a$ i $d \mid b$. Sigui $c \in R$ tal que $c \mid a$ i $c \mid b$. Aleshores $c = up_1^{\gamma_1} \cdot \ldots \cdot p_r^{\gamma_r}$ amb $\gamma_i \leq \alpha_i, \beta_i$ i u unitat. Per tant $\gamma_i \leq \min(\alpha_i, \beta_i)$ i $c \mid d$. □

3.2.1 Dominis d'ideals principals i dominis de factorització única

L'objectiu principal d'aquesta part és demostrar que tot domini d'ideals principals és domini de factorització única.

Definició 3.2.4. Diem que R és un domini d'ideals principals (DIP) si tot ideal de R és principal.

Proposició 3.2.4. *Suposem R DIP. Si $I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots$ és una cadena d'ideals de R aleshores existeix n tal que $I_n = I_{n+1} = \ldots$.*

Demostració. Fem $I = \bigcup_i I_i$ que és un ideal ja que cadascun està contingut al següent. Com que R és DIP$\Rightarrow I = (a)$ per cert $a \in R$. Així $a \in I_n$ per cert n i tenim $I = I_n$. □

Proposició 3.2.5. *Si R és un DIP aleshores tot irreductible de R és primer.*

Demostració. Suposem que p és irreductible. Suposem que $p \mid ab$. Si $p \mid a$ ja està. Suposem $p \nmid a$. Considerem doncs $(a) + (p) = (c)$ per cert $c \in R$. Així $p \in (c)$, és a dir $p = ce$ per cert $e \in R$. Per hipòtesi, c és invertible o e és invertible. Si e és invertible llavors $c = pe^{-1} \Rightarrow c \in (p)$ i així $(c) = (p)$. Aleshores $(a) + (p) = (p) \Rightarrow a \in (p) \Rightarrow p \mid a$ la qual cosa és absurda. Llavors c és invertible i $(c) = R$.

D'aquesta manera $(a) + (p) = (1) = R$ existeixen $\alpha, \beta \in R$ tals que $\alpha a + \beta p = 1$. Multiplicant per b hom troba $b = b\alpha a + b\beta p$ i $p \mid b$. □

Teorema 3.2.2. *Si R és DIP aleshores R és DFU.*

Demostració. Sigui $a \neq 0$ i no invertible. Suposem que a no factoritza en irreductibles. En particular a no és irreductible i si $a = a_1 b_1$ llavors a_1 i b_1 no són invertibles. Aleshores a_1 o b_1 no descomponen com a producte d'irreductibles. Suposem a_1 així. Evidentment $(a) \subseteq (a_1)$. A més no es pot donar que $(a_1) \subseteq (a)$ ja que si $a_1 = \alpha a \Rightarrow 1a = \alpha a b_1 \Rightarrow b_1$ invertible.

Repetint aquest argument amb a_1 podem trobar una cadena $(a) \subseteq (a_1) \subseteq (a_2) \subseteq \ldots$ no estacionària, la qual cosa és una contradicció amb el fet que R és DIP. Per tant tot element factoritza com a producte d'irreductibles.

Com que a més en un DIP tot irreductible és primer tenim R DFU. □

Proposició 3.2.6. *Si R és DIP i $a, b \in R$. Aleshores d és un* mcd *de a i b si i només si $(a) + (b) = (d)$.*

Demostració. Suposem que $\mathrm{mcd}(a, b) = d$. Com que R és DIP tenim $(a) + (b) = (d')$ per cert d'. Així doncs $(a), (b) \subseteq (d')$ i tenim $d' \mid a$ i $d' \mid b$. Suposant $c \mid a$ i $c \mid b$ veiem que $d' = \alpha a + \beta b$ per certs $\alpha, \beta \in R$ i per tant $c \mid d' \Rightarrow d'$ és mcd de a i b. D'aquesta manera $d' \sim d$ i tenim $(a) + (b) = (d') = (d)$.

Recíprocament si $(a) + (b) = (d)$ ja hem vist que d és un mcd de a i b. □

Proposició 3.2.7. *Suposem R DFU i $a, b, c \in R$. Aleshores:*

1. $ab = \mathrm{mcd}(a, b)\,\mathrm{mcm}(a, b)$.
2. *Si* $d = \mathrm{mcd}(a, b)$ *i* $a = a'd$ *i* $b = b'd$ *llavors* $\mathrm{mcd}(a', b') \sim 1$.
3. *Si* $a \mid bc$ *i* $\mathrm{mcd}(a, b) = 1$ *llavors* $a \mid c$

Demostració. 1 és immediat a partir de la Proposició 3.2.3. □

Proposició 3.2.8. *Suposem R DIP. Llavors tot ideal $I \neq (0)$ primer de R és maximal.*

Demostració. Suposem J ideal de R tal que $I \subseteq J \subseteq R$. Com que R és DIP existeixen $x, y \in R$ tals que $I = (x) \subseteq (y) = J$. Amb això $x \in (y)$, ço és, existeix $\lambda \in R$ tal que $x = \lambda y$. Però (x) és primer i així si $y \in (x)$ tenim $I = J$ i si $\lambda \in (x)$ tenim per cert $\mu \in R$ que $\lambda = \mu x \Rightarrow x = \mu xy \Leftrightarrow 1 = \mu y$. Això ens diu que y és una unitat i $J = R$. □

Amb això ja tenim que a un DIP un ideal és primer si i només si és maximal.

Proposició 3.2.9. *Sigui R DFU i $a, b, c \in R$ aleshores:*

1. $ab \sim \operatorname{mcm}(a, b) \operatorname{mcd}(a, b)$
2. *Si* $d = \operatorname{mcd}(a, b)$ *i* $a = a'd, b = b'd \Rightarrow \operatorname{mcd}(a', b') \sim 1$
3. *Si* $a \mid bc$ *i* $\operatorname{mcd}(a, b) = 1 \Rightarrow a \mid c$

3.3 Dominis euclidians

Definició 3.3.1. Diem que R DI és un domini euclidià (DE) si existeix una aplicació $d : R \setminus \{0\} \longrightarrow \mathbb{N} \cup \{0\}$ tal que:

1. Si $a, b \in R$ i $b \neq 0$, existeixen $q, r \in R$ tals que $a = bq + r$ on $r = 0$ o $d(r) < d(b)$.
2. $d(a) \leq d(ab)$.

A d se l'anomena funció euclidiana.

Proposició 3.3.1. *Sigui R un DE. Aleshores $d(1) = \min_{x \in R \setminus \{0\}} \{d(x)\}$. A més, si $u \neq 0$, és invertible si i només si $d(1) = d(u)$.*

Demostració. Sigui $x \in R$ diferent de zero fem $d(1) \leq d(x \cdot 1) = d(x)$.

Suposem u invertible. Tenim $d(1) \leq d(u)$. Així doncs $d(u) \leq d(uu^{-1}) = d(1)$ i $d(u) = d(1)$.

Recíprocament si $d(u) = d(1)$ llavors fem $1 = qu + r$ de manera que $d(r) < d(u) = d(1)$ la quial cosa no pot ser. Per tant $r = 0$ i u invertible. □

Proposició 3.3.2. *Si R és DE aleshores R és DIP.*

Demostració. Sigui I un ideal de R diferent de (0) (Si $I = \{0\} = (0)$). Sigui $b \in I$ diferent de 0 tal que $d(b)$ és mínim entre els $d(x)$ per $x \in I, x \neq 0$. Veurem que $I = (b)$. Si $a \in I$ fem $a = bq + r$ amb $r = 0$ o $d(r) < d(b)$. Però $r = a - bq \in I \Rightarrow r = 0$ per la tria de b □

Observem que de moment tenim la següent cadena d'implicacions

$$\text{DE} \Rightarrow \text{DIP} \Rightarrow \text{DFU} \Rightarrow \text{DI}$$

Proposició 3.3.3. *Sigui R DI, suposem que a R hi tenim* mcm *i* mcd. *Si $a = bq + r$ aleshores* $\mathrm{mcd}(a, b) \sim \mathrm{mcd}(b, r)$.

Demostració. Si $c \mid a, b$ llavors $c \mid r = a - bq \Rightarrow c \mid b, r \Rightarrow \mathrm{mcd}(a, b) \mid \mathrm{mcd}(b, r)$.

Si $c \mid b, r \Rightarrow c \mid a = bq + r \Rightarrow c \mid a, b \Rightarrow \mathrm{mcd}(b, r) \mid \mathrm{mcd}(a, b)$. □

Seguint aquesta proposició podem emprar l'algorisme d'Euclides per trobar el màxim comú divisor de dos elements de R. L'únic que hem de fer és fer la divisió euclidiana i anar aplicant el resultat anterior.

3.4 Els enters de Gauss

S'anomena enters de Gauss al subanell de $\mathbb{C}$:

$$\mathbb{Z}[i] = \{a + bi \,|\, a, b \in \mathbb{Z}\}$$

Es tracta d'un domini d'integritat. Considerant l'aplicació norma $N : \mathbb{Z}[i] \longrightarrow \mathbb{N} \cup \{0\}$ donada per $N(a + bi) = a^2 + b^2$ tenim si $z, w \in \mathbb{Z}[i]$:

1. $N(z) \geq 0$
2. $N(z) = 0 \Leftrightarrow z = 0$
3. $N(zw) = N(z)N(w)$

Proposició 3.4.1. $\mathbb{Z}[i]$ *és DE.*

Demostració. Considerarem l'aplicació norma N. Siguin $a, b \in \mathbb{Z}[i]$ amb b diferent de 0. Tindrem $a = a_1 + a_2 i, b = b_1 + b_2 i$. A $\mathbb{C}$ podem considerar.

$$\frac{a}{b} = \frac{a_1 b_1 + a_2 b_2}{b_1^2 + b_2^2} + \frac{a_2 b_1 - b_2 a_1}{b_1^2 + b_2^2} i$$

Així podem prendre $q_1, q_2 \in \mathbb{Z}$ tals que $|\Re(\frac{a}{b}) - q_1| < \frac{1}{2}$ i $|\Im(\frac{a}{b}) - q_2| < \frac{1}{2}$. Observem que no necessàriament seran únics. Fem $q = q_1 + iq_2$.

Sigui ara $r = a - bq$ fem si $r \neq 0$:

$$N(\frac{r}{b}) = N(\frac{a}{b} - q) = (\Re(\frac{a}{b}) - q_1)^2 + (\Im(\frac{a}{b}) - q_2)^2 \leq \frac{1}{4} + \frac{1}{4} = \frac{1}{2} < 1$$

Això implica que $N(r) < N(b)$ de forma que N serveix com a funció euclidiana. □

Amb això sabem que els invertibles a $\mathbb{Z}[i]$ seran aquells u tals que $N(u) = 1$. Tenim $u = a + bi \Rightarrow N(u) = a^2 + b^2 = 1$ i només hi ha quatre possibilitats: $u = \pm 1$ o $u = \pm i$.

3.4.1 Primers a $\mathbb{Z}[i]$

Observem que als enters de Gauss 2 deixa de ser primer com demostra:

$$2 = (1+i)(1-i)$$

Lema 3.4.1. *Sigui $z \in \mathbb{Z}[i]$. Aleshores z és irreductible a $\mathbb{Z}[i]$ si i només si $\overline{z}$ és irreductible a $\mathbb{Z}[i]$*

Demostració. Observem que $\alpha \in \mathbb{Z}[i]$ és unitat si i només el seu conjugat ho és puix tenen la mateixa norma.

Suposem $\overline{z}$ irreductible. Suposant $z = \alpha\beta,\ \alpha, \beta \in \mathbb{Z}[i]$ tenim que o bé α o bé β són unitats perquè per $\overline{z} = \overline{\alpha}\overline{\beta}$ o bé $\overline{\alpha}$ o bé $\overline{\beta}$ ho són. Anàlogament el recíproc. □

Lema 3.4.2. *Sigui $z = a + bi \in \mathbb{Z}[i]$ irreductible amb $a \neq 0$ i $b \neq 0$. Aleshores $z \sim \overline{z}$ si i només si $z = \pm 1 \pm i$.*

Demostració. Suposem primer $z = \pm 1 \pm i$. Llavors si $z = \alpha\beta$ tenim $N(z) = 2 = N(\alpha)N(\beta)$. Hi ha dues possibilitats. Les dues impliquen z irreductible.

Recíprocament, suposem $z \sim \overline{z}$. Com que tenim les unitats de $\mathbb{Z}[i]$ determinades:

- $z = \overline{z} \Rightarrow b = 0 \Rightarrow$ No pot ser.
- $z = -\overline{z} \Rightarrow a = 0 \Rightarrow$ No pot ser.
- $z = i\overline{z} \Rightarrow a = b \Rightarrow z = a(1+i)$.
- $z = -i\overline{z} \Rightarrow a = -b \Rightarrow z = a(1-i)$.

El fet que z sigui irreductible implica el resultat puix a ha de ser unitat. □

Teorema 3.4.1. *Sigui p primer a $\mathbb{Z}$ positiu. Aleshores p és reductible a $\mathbb{Z}[i]$ si i només si $p = a^2 + b^2$.*

Demostració. Suposem que $p = a^2 + b^2$. Aleshores $p = (a+bi)(a-bi)$ amb $a, b \neq 0$ ja que p és primer. Per tant p és reductible.

Recíprocament, suposem que p és reductible. Si $p = 2$ llavors tenim $p = 1 + 1$. Suposem $p \neq 2$. Posem $p = zw$ amb z irreductible i w no unitat. Fem $z = a + bi, a, b \in \mathbb{Z}$. Si per exemple $a = 0$ tenim $p = (bi)(c+di) = bci - bd \Rightarrow bc = 0 \Rightarrow p = i - bq \Rightarrow b(-d) = p$ a $\mathbb{Z}$. Això implica contradicció puix o bé $b = 1$ o bé $d = 1$ i ni z ni w són invertibles. Per tant $a \neq 0$.

Si suposem ara $b = 0$ llavors $z = a$ i $p = a(c + di)$. Observem doncs que ha de ser $d = 0$ ja que $p \in \mathbb{Z}$. Però això implica $p = ac$ amb p primer la qual cosa també és una contradicció (raonem igual que abans).

Tenim doncs $z = a + bi$ amb $a, b \neq 0$. Ara com que $p \in \mathbb{Z}$ $p = \overline{p} = zw = \overline{zw}$ i $\overline{z}$ és irreductible per ser-ho també z. Distingim ara dos casos:

- z i $\overline{z}$ són associats $\Rightarrow N(z) = 2$ i $p^2 = N(p) = N(z)N(w) = 2N(w) \Rightarrow 2 \mid p^2 \Rightarrow 2 \mid p \Rightarrow p = 2$ la qual cosa és una contradicció.
- z i $\overline{z}$ no poden ser associats llavors. Per tant són coprimers i tenim $p = zw = \overline{zw} \Rightarrow z \mid \overline{zw} \Rightarrow z \mid \overline{w}$. D'aquesta forma $p = z\overline{z}(c + di) = (a^2 + b^2)(c + di)$. Però com que p és enter i és primer positiu ha de ser $c = 1$ i $d = 0$. Per tant $p = a^2 + b^2$.

□

Teorema 3.4.2. *Sigui $z = a + ib \in \mathbb{Z}[i]$ amb $a \neq 0$ i $b \neq 0$. Aleshores z és irreductible a $\mathbb{Z}[i]$ si i només s $N(z) = a^2 + b^2$ és primer a $\mathbb{Z}$.*

Demostració. Suposem $N(z)$ primer a $\mathbb{Z}$. Si z no és irreductible a $\mathbb{Z}[i]$ llavors $z = \alpha\beta$ amb $\alpha, \beta \in \mathbb{Z}[i]$ no invertibles. Per tant $N(z) = N(\alpha)N(\beta)$ amb $N(\alpha), N(\beta) > 1$ contradiu que p és primer a $\mathbb{Z}$.

Recíprocament suposem z és irreductible. Considerem $\overline{z}$ que també és irreductible. Tenim dos casos:

- Si z i $\overline{z}$ no són primers com que són irreductibles són associats i per tant $N(z) = 2$ és també primer a $\mathbb{Z}$.
- Si z i $\overline{z}$ són coprimers tenim $N(z) = a^2 + b^2 = z\overline{z}$. Suposem $N(z) = rs$ amb $r, s \in \mathbb{Z}$ i $z\overline{z} = rs$. Com que z és irreductible podem suposar $z \mid r$. Posem ara $r = zw \in \mathbb{Z}$. $\overline{r} = r = \overline{zw} \Rightarrow \overline{z} \mid r$ a $\mathbb{Z}[i]$ i igualment $\overline{z} \mid zw \Rightarrow \overline{z} \mid w \Rightarrow w = \overline{z}w'$ per cert w'. D'aquesta manera $r = z\overline{z}(w') = (a^2 + b^2)w' \in \mathbb{Z}$. Tenim també $N(z) = a^2 + b^2 = (a^2 + b^2)w's$. Fem $w' = c + di$ i així $r = (a^2 + b^2)w'$. Ha de ser doncs $w' = c \in \mathbb{Z}$ i $d = 0$. Finalment $a^2 + b^2 = (a^2 + b^2)cs \Rightarrow cs = 1 \Rightarrow s = 1$ i hem acabat.

□

Proposició 3.4.2. *(Congruència de Wilson) Sigui p primer a $\mathbb{Z}$. Llavors*

$$(p-1)! \equiv -1 \mod p$$

Teorema 3.4.3. *Sigui p primer de $\mathbb{Z}$. Aleshores p és irreductible a $\mathbb{Z}[i]$ si i només si $p \equiv 3 \mod 4$*

Demostració. Suposem $p \equiv 3 \mod 4$. Si p no és irreductible a $\mathbb{Z}[i]$ llavors $p = a^2 + b^2$ amb a, b enters. A $\mathbb{Z}/(4)$ tenim $\overline{p} = \overline{a}^2 + \overline{b}^2$. Cap combinació d'elements a $\mathbb{Z}/(4)$ dóna el resultat $\Rightarrow p$ ha de ser irreductible.

Recíprocament suposem p irreductible. Estudiem les possibilitats:

- $p \equiv 0 \mod 4 \Rightarrow 4 \mid p$ que és una contradicció puix p és primer.
- $p \equiv 2 \mod 4 \Rightarrow p = 2 + 4\alpha \Rightarrow 2(1 + 2\alpha) \Rightarrow p = 2$ que és una contradicció ja que 2 és reductible.

- $p \equiv 1 \mod 4$. Veurem que això implica p reductible. Suposem p irreductible. Considerem el grup multiplicatiu $(\mathbb{Z}/(p))^*$ que és cíclic. Per tant i tenint en compte que $4 \mid p-1$ tindrem que existeix un element n d'ordre 4. En particular n^2 tindrà ordre 2 i llavors $n^2 \equiv -1 \mod p$ i $p \mid n^2+1$ a $\mathbb{Z}$.

  Amb això $n^2+1 = (n+i)(n-i)$. Com que hem suposat p irreductible, ha de dividir $n+i$ o $n-i$. En qualsevol dels dos casos s'arriba a contradicció amb igualtats del tipus $\pm 1 = p\alpha, \alpha \in \mathbb{Z}$. Per tant p ha de ser reductible.

Ha de ser doncs $p \equiv 3 \mod 4$. □

3.5 Anells de polinomis

En aquest apartat K serà sempre un cos.

Recordem que a $K[x] = \{a_0 + a_1x + \ldots + a_nx^n \mid a_i \in K\}$ tenim la suma i el producte de polinomis donades respectivament per:

$$(a_0 + a_1x + \ldots + a_nx^n) + (b_0 + b_1x + \ldots + b_nx^n) = \sum_{i=0}^{n}(a_i + b_i)x^n$$

$$(a_0 + a_1x + \ldots + a_nx^n)(b_0 + b_1x + \ldots + b_nx^n) = \sum_{k=0}^{m+n}\Big(\sum_{i+j=k} a_ib_j\Big)x^k$$

Podem igualment definir *avaluacions*. Sigui $\alpha \in K$ fix considerem

$$\varphi : K[x] \longrightarrow K$$

$$a_0 + a_1x + \ldots + a_nx^n \longmapsto a_0 + a_1\alpha + \ldots + a_n\alpha^n$$

que evidentment és morfisme d'anells.

Més generalment tenim que si $K \subseteq S$ amb S anell commutatiu i $\alpha \in S$ es fix llavors

$$\varphi : K[x] \longrightarrow S$$

$$f(x) \longmapsto f(\alpha)$$

és morfisme d'anells.

Tenim també la funció grau donada per:

$$\text{grau} : K[x] \longrightarrow \mathbb{N} \cup \{0\}$$

$$a_0 + a_1x + \ldots + a_nx^n \longmapsto n \text{ si } a_n \neq 0$$

En aquest cas sabem que es dóna $\text{grau}(f(x)g(x)) = \text{grau}(f(x)) + \text{grau}(g(x))$.

Algunes propietats de $K[x]$ són:

1. És DI.
2. $U(K[x]) = K \setminus \{0\}$

3. Es compleixen les implicacions DE⇒DIP⇒DFU.

4. Si $f \in K[x]$ i $\text{grau}(f) \geq 1$ llavors f és irreductible si i només si f no descompon en producte $f = f_1 f_2$ amb $\text{grau}(f_1), \text{grau}(f_2) < \text{grau}(f)$.

5. En general la irreductibilitat a $K[x]$ depén de K.

Si ara considerem $R[x]$ amb R DI tenim:

1. $R[x]$ és DI igualment.

2. $U(R[x]) = U(R)$

Proposició 3.5.1. *Si R és DI aleshores els següents enunciats són equivalents:*

1. *R és cos.*

2. *$R[x]$ és DE.*

3. *$R[x]$ és DIP.*

Demostració. Si R és cos llavors $R[x]$ és DE i si $R[x]$ és DE llavors és DIP. Suposem $R[x]$ DIP. Considerem $\psi : R[x] \longrightarrow R$ tal que $\psi(f) = f(0)$ per tot $f \in R[x]$. ψ és evidentment epimorfisme d'anells. D'altra banda veiem també que $\ker(\psi) = (x)$. Pel 1r teorema d'isomorfia tenim:

$$R[x]/\ker(\psi) \cong R[x]/(x) \cong R$$

que és DI. Això implica que (x) és primer. Com que $R[x]$ és DIP tot ideal primer I diferent de (0) és maximal. En particular (x) és maximal a $R[x]$ i $R[x]/(x)$, isomorf a R, és cos. □

Definició 3.5.1. Sigui R DI. Siguin $a_1, \ldots, a_n \in R$ diem que d és un mcd de $a_1, \ldots, a_n$ si:

1. $d \mid a_1, \ldots, a_n$

2. $c \mid a_1, \ldots, a_n \Rightarrow c \mid d$

Proposició 3.5.2. *Sigui R DI, $a_1, \ldots, a_n \in R$. Suposant que tota parella té* mcd *llavors:*

1. $\text{mcd}(a_1, \ldots, a_n) = \text{mcd}(\text{mcd}(a_1, \ldots, a_{n-1}), a_n)$

2. *Si $d = \text{mcd}(a_1, \ldots, a_n)$ i posem $a_i = a_i' d$ com sempre aleshores* $\text{mcd}(a_1', \ldots, a_n') \sim 1$.

A partir d'ara en aquesta secció R serà un DFU.

Definició 3.5.2. Sigui $f(x) = a_0 + a_1 x + \ldots + a_n x^n \in R[x]$ direm que el contingut de f és $c(f) = \text{mcd}(a_0, a_1, \ldots, a_n)$. Diem que f és primitiu si $c(f) \sim 1$.

Lema 3.5.1. *Si $f \in R[x]$ aleshores $f = c(f) f^*$ amb f^* primitiu. A més si $f = \alpha \tilde{f}$ amb $\alpha \in R$ i $\tilde{f}$ primitiu, tindrem $\alpha \sim c(f)$ i $\tilde{f} \sim f^*$.*

Demostració. Posem $f(x) = \sum_{i=0}^{n} a_i x^i$ i $c(f) = \mathrm{mcd}(a_1, \ldots, a_n)$. Com sempre $a_i = a_i' c(f)$. Treient factor comú tenim la primera part:

$$f(x) = c(f) \sum_{i=0}^{n} a_i' x^n \text{ amb } \sum_{i=0}^{n} a_i' x^n \text{ primitiu.}$$

Ara suposem $f = c(f) \sum_{i=0}^{n} a_i' x^n = \alpha \sum_{j=0}^{m} b_j x^j$. Com que dos polinomis són iguals si i només si els seus coeficients ho són tenim igualtats del tipus $a_i = c(f) a_i' = \alpha b_i$ i a més $m = n$. Així $\mathrm{mcd}(a_1, \ldots, a_n) = c(f) = \mathrm{mcd}(\alpha b_1, \ldots, \alpha b_n) = \alpha \,\mathrm{mcd}(b_1, \ldots, b_n) \Rightarrow c(f) \sim \alpha$ ja que $\sum_{i=0}^{m} b_j x^j$ és primitiu. D'altra banda tenim $f = \alpha \tilde{f} = c(f) f^*$ i pel que acabem de veure també tenim $\tilde{f} \sim f^*$. □

Lema de Gauss. *Siguin $f, g \in R[x]$ primitius. Aleshores $h = fg$ és primitiu.*

Demostració. Suposem h no primitiu. Aleshores existeix $p \in R$ irreductible tal que $p \mid c(h)$. Com que R és DFU, p és primer i per tant (p) és primer. Conseqüentment $R/(p)$ és DI. Sabem que l'aplicació donada per

$$\varphi : R[x] \longrightarrow R/(p)[x]$$

$$\sum_{i=0}^{n} a_i x^i \longmapsto \sum_{i=0}^{n} \overline{a_i} x^i$$

és un morfisme d'anells. Alehsores $\varphi(h) = 0$ ja que $p \mid c(h)$. Així $\varphi(f)\varphi(g) = 0$ i tant $\varphi(f) = 0$ com $\varphi(g) = 0 \Rightarrow p \mid c(f)$ o $p \mid c(g)$ contradiuen el fet que f i g són primitius. □

Corol·lari 3.5.1. *Siguin $f, g \in R[x]$. Aleshores $c(fg) \sim c(f)c(g)$*

Demostració. Posem $f = c(f) f*$ amb f^* primitiu i $g = c(g) g^*$ amb g^* primitiu. Llavors $fg = c(f)c(g) f^* g^* = c(fg)(fg)^*$ amb $(fg)^*$ primitiu. Pel lema de Gauss tenim $c(f)c(g) \sim c(fg)$. □

Teorema 3.5.1. *Sigui $f \in R[x]$ i sigui $\mathcal{F}$ el cos de fraccions de R aleshores són equivalents:*

1. $\mathrm{grau}(f) \geq 1$ *i* f *és irreductible a* $R[x]$.
2. $c(f) \sim 1$ *i* f *irreductible a* $\mathcal{F}[x]$.

Demostració. Suposem primerament $\mathrm{grau}(f) \geq 1$ i f irreductible a $R[x]$. Fem $f = c(f) f^*$ amb f^* primitiu. Com que f és irreductible tindrem per definició $c(f) \in U(R) \Rightarrow c(f) \sim 1$.

Suposem ara $f = gh$ a $\mathcal{F}[x]$. Siguin $a, b \in R$ tals que $ag, bh \in R[x]$ llavors

$$abf = (ag)(bh) \Rightarrow ab \sim c(ag)c(bh)$$

ja que f és primitiu. Amb això podem descomposar f a $R[x]$ d'acord amb $abf = c(ag)c(bh)(ag)^*(bh)^* \Rightarrow f \sim (ag)^*(bh)^*$ on $(ag)^*, (bh)^*$ són primitius.

Suposem $(ag)^*$ invertible $\Rightarrow \mathrm{grau}((ag)^*) = 0$. D'aquesta manera $\mathrm{grau}(g) = \mathrm{grau}(ag) = \mathrm{grau}((ag)^*) = 0 \Rightarrow g$ és invertible a $\mathcal{F} \Rightarrow f$ és irreductible a $\mathcal{F}[x]$. Si $(bh)^*$ tenim el mateix resultat.

Recíprocament suposem f primitiu i irreductible a $\mathcal{F}[x]$. Llavors $f \neq 0$ és no invertible $\Rightarrow$ grau$(f) \geq 1$. Suposem que $f = gh$ és una descomposició a $R[x] \subseteq \mathcal{F}[x] \Rightarrow g$ o h constants. Suposant g constant haurà de ser $g \in R$ i així

$$c(f) = c(g)c(h) = gc(h) = u \text{ amb } u \text{ invertible}$$

Amb això g és invertible a R i f és irreductible a $R[x]$. Si h és una constant procedim anàlogament. □

Teorema 3.5.2. *Si R és un DFU aleshores $R[x]$ és DFU.*

Demostració. Considerem $\mathcal{F}$ el cos de fraccions de R. Sigui $f(x) \in R[x]$ diferent de zero i no inverible.

Si grau$(f) = 0 \Rightarrow f \in R \Rightarrow f$ descompon en irreductibles de forma única a R i hem acabat.

Suposem grau$(f) \geq 1$. Tenim $f = f_1 \dots f_r$ a $\mathbb{F}[x]$ amb els f_i irreductibles a $\mathcal{F}[x]$. Sigui $a_i \in R$ tal que $a_i f_i \in R[x]$ considerem doncs

$$a_1 a_2 \dots a_r f = (a_1 f_1)(a_2 f_2) \dots (a_r f_r)$$

Aleshores

$$(a_1 \dots a_r)c(f)f^* = c(a_1 f_1) \dots c(a_r f_r)(a_1 f_1)^* \dots (a_r f_r)^*$$

amb els * primitius. Sabem doncs que

$$(a_1 \dots a_r)c(f) \sim c(a_1 f_1) \dots c(a_r f_r) \Rightarrow f^* \sim (a_1 f_1)^* \dots (a_r f_r)^*$$

amb els $(a_i f_i)^*$ primitius i irreductibles a $\mathcal{F}[x]$. Per tant seran irreductibles a $R[x] \Rightarrow f*$ irreductible a $R[x]$ pel Lema de Gauss. En particular $c(f) \in R$ que és DFU i una descomposició de f en irreductibles és:

$$f = c(f)f^*$$

prenent les descomposicions de $c(f)$ i f^* en irreductibles.

Veiem que aquesta és única. Per això veurem que tot irreductible de $R[x]$ és primer. Sigui $f \in R[x]$ irreductible. Suposem $f \mid gh$. Si grau$(f) = 0$ llavors $f = a \in R$ i tenim $gh = a\alpha$ per cert $\alpha \in R[x]$. Sabem que $c(h)c(g) \sim ac(\alpha)$ a R i per tant si $a \mid c(f)c(g) \Rightarrow a$ divideix un dels dos. Suposem sense pèrdua de generalitat $a \mid c(g) \Rightarrow a \mid g$ i hem acabat.

Si grau$(f) \geq 1$ com que $\mathcal{F}[x]$ és DFU $\Rightarrow f \mid g$ o $f \mid h$ a $\mathcal{F}[x]$. Suposem novament sense pèrdua de generalitat $f \mid g$ a $\mathcal{F}[x]$. Això implica que $g = fq$ per cert $q \in \mathcal{F}[x]$. Sigui $a \in R$ tal que $aq \in R[x]$ tenim $ag = faq \Rightarrow ac(g) \sim c(f)c(aq) \Rightarrow ac(g) \sim ac(g) \sim c(aq)$ ja que f és irreductible a $R[x]$ i per tant primitiu a $\mathcal{F}[x]$. Escrivint ara

$$ag = fc(aq)(aq)^* = fac(g)(aq)^* \Rightarrow g = fc(g)(aq)^*$$

a $R[x]$. Per tant $f \mid g$ a $R[x]$ i tot irreducctible és primer. □

Teorema 3.5.3. *Suposem R DI. Aleshores són equivalents:*

1. *R és DFU.*

2. $R[x]$ *és DFU.*

3. $R[x_1, \ldots, x_n]$ *és DFU.*

Demostració. Sabem que $(1) \Rightarrow (2), (2) \Rightarrow (3)$. Són conseqüència de l'anterior.

Veiem $(3) \Rightarrow (1)$. Primerament obsevem que $U(R[x]) = U(R)$ ja que R és DI. D'altra banda si $p \in R, p \neq 0$ i no és invertible tindrem que p és irreductible a R si i només si p és irreductible a $R[x]$.

Prenem doncs $a \in R$ no invertible i diferent de zero. Com que $a \in R[x_1, \ldots, x_n]$ tenim que $a = p_1 \ldots p_n$ amb p_i irreductibles a $R[x] \Rightarrow p_i$ irreductibles a R. Veiem que tot irreductible és primer a R. Si $p \in R$ és irreductible suposem $p \mid ab$. Per ser p primer a $R[x_1, \ldots, x_n]$ tenim per exemple $a = p\alpha$ amb $\alpha \in R[x_1, \ldots, x_n] \Rightarrow \alpha \in R \Rightarrow a = p\alpha$ a R[1]. □

3.6 Irreductibilitat

Proposició 3.6.1. *Sigui* K *un cos i* $f \in K[x]$*, aleshores:*

1. $\text{grau}(f) = 1 \Rightarrow f$ *irreductible.*

2. $\text{grau}(f) = 2$ *o* 3 *llavors* f *irreductible si i només si* f *no té arrels a* K*.*

Si un polinomi de grau major a 4 no té arrels generalment no podem dir res. Cal buscar altres arguments.

Proposició 3.6.2. *Sigui* R *un DFU i* $f(x) = \sum_{i=0}^{n} a_i x^i$*. Sigui* $\mathcal{F}$ *el cos de fraccions de* R*. Suposem que* $\frac{a}{b}$ *és arrel de* $f(x)$ *amb* $\text{mcd}(a, b) = 1$*. Aleshores* $a \mid a_0$ *i* $b \mid a_n$*.*

Demostració. Tenim

$$a_0 + a_1 \frac{a}{b} + \ldots + a_n \frac{a^n}{b^n} = 0 \Leftrightarrow b^n a_0 + a_1 a b^{n-1} + \ldots + a_n a^n = 0$$

D'aquesta manera

$$b^n a_0 + \ldots a_{n-1} a^{n-1} b = -a_n a^n$$

i $b \mid a_n a^n \Rightarrow b \mid a_n$. Anàlogament $a \mid a_0$. □

Proposició 3.6.3. *(Criteri modular) Sigui* R *un DFU. Sigui* $f = \sum_{i=0}^{n} a_i x^i \in R[x]$ *primitiu. Sigui* $p \in R$ *irreductible tal que* $p \nmid a_n$*. Aleshores si* $\tilde{f} = \sum_{i=0}^{n} \overline{a_i} x^i \in R/(p)[x]$ *és irreductible* f *és irreductible a* $R[x]$*.*

Demostració. Suposem que $f = gh \in R[x]$. Així $g = \sum_{i=0}^{m} b_i x^i$ i $h = \sum_{i=0}^{t} c_i x^i$. Considerem

$$\varphi : R[x] \longrightarrow R/(p)[x]$$

[1] Pregunta. L'unicitat era clara, si tinguèssim altra descomposició també la tindríem a $R[x_1, \ldots, x_n]$

donat per $\varphi(\sum_{i=0}^n a_i x^i) = \sum_{i=0}^n \overline{a_i} x^i \in R/(p)[x]$. Així doncs $\tilde{f} = \sum_{i=0}^n \overline{a_i} x^i = (\sum_{i=0}^m \overline{b_i} x^i)(\sum_{i=0}^t \overline{c_i} x^i) = \tilde{g}\tilde{h} \Rightarrow \tilde{g}$ o $\tilde{h}$ invertibles a $R/(p)[x]$.

Suposem $\tilde{g}$ invertible. Com que (p) és primer $R/(p)[x]$ és DI i per tant $\tilde{g} \in R/(p)$. Com que $\tilde{f}$ té grau n a $R/(p)[x]$ en tant que $p \nmid a_n$ tenim que necessàriament h ha de tenir grau $n \Rightarrow \text{grau}(g) = 0 \Rightarrow g = b \in R$. Així escrivim $f = bh \Rightarrow c(f) = bc(h) = 1 \Rightarrow b \in U(R)$ i f és irreductible. □

Proposició 3.6.4. *(Criteri d'Eisenstein) Sigui R un DFU. Sigui $f = \sum_{i=0}^n a_i x^i \in R[x], n \geq 1$ primitiu. Suposem que existeix $p \in R$ irreductible tal que $p \mid a_0, p \mid a_1, \ldots p \mid a_{n-1}, p \nmid a_n, p^2 \nmid a_0$. Aleshores f és irreductible a $R[x]$.*

Demostració. Suposem $f = ah$ amb $a \in R$. Llavors $c(f) = ac(h) = 1$ i $a \in U(R)$.

Suposem doncs que $f = gh$ amb $\text{grau}(g), \text{grau}(h) > 0$. Tenim $g = \sum_{i=0}^m b_i x^i$ i $h = \sum_{i=0}^t c_i x^i$ amb $m, t \geq 1$ i $m + t = n$. Quan ho mirem a $R/(p)$ tenim que $\overline{f} = \overline{a_n} x^n = \overline{g}\overline{h}$ i com que $\overline{a_n} = \overline{b_m c_t}$ ha de ser $\overline{b_0} = \overline{c_0} = 0$ i b_0, c_0 són múltiples de p. Hem arribat a contradicció puix $p^2 \mid b_0 c_0 = a_0$.

□

Proposició 3.6.5. *(Criteri d'Eisenstein dual) Sigui R un DFU. Sigui $f = \sum_{i=0}^n a_i x^i \in R[x], n \geq 1$ primitiu. Suposem que existeix $p \in R$ irreductible tal que $p \nmid a_0, p \mid a_1, \ldots p \mid a_{n-1}, p \mid a_n, p^2 \nmid a_n$. Aleshores f és irreductible a $R[x]$.*

Demostració. El mateix argument d'abans funciona. □

Corol·lari 3.6.1. *Sigui R DFU, $\mathcal{F}$ el cos de fraccions de R. Sigui $f = \sum_{i=0}^n a_i x^i \in R[x], n \geq 1$. Suposem que existeix $p \in R$ irreductible tal que $p \mid a_0, p \mid a_1, \ldots p \mid a_{n-1}, p \nmid a_n, p^2 \nmid a_0$. Aleshores f és irreductible a $\mathcal{F}[x]$.*

Demostració. Posem $f = c(f)f^*$. Considerem $f^* \in R[x]$. Aleshores f^* i p compleixen les condicions del criteri d'Eisenstein i f^* és irreductible a $R[x]$. Com que a més $n \geq 1$ tenim f^* és irreductible a $\mathcal{F}[x]$. Finalment com que $c(f) \in R$ tenim $f = c(f)f^*$ irreductible a $\mathcal{F}[x]$. □

4

Cossos finits

4.1 Primers resultats

Observem que si p és primer a $\mathbb{Z}$ llavors (p) és primer $\Rightarrow$ (p) és maximal i $\mathbb{Z}/(p)$ és cos. Raonant de forma similar arribem a la conclusió que si prenem $f = x^2 + x + 1 \in \mathbb{Z}/(2)[x]$ irreductible, aleshores:

$$K = \mathbb{Z}/(2)[x] \big/ (x^2 + x + 1)$$

Si tenim $g \in \mathbb{Z}/(2)[x]$ i fem $g = qf + r$ llavors $\text{grau}(r) < \text{grau}(f) = 2$ i per tant $\overline{g} = \overline{r}$, és a dir, a K només hi ha polinomis de grau 1. Però sabem quins són aquests i si $\alpha = \overline{x}$:

$$K = \{0, 1, \alpha, \alpha + 1\}$$

té 4 elements.

Proposició 4.1.1. *A $\mathbb{Z}/(p)[x]$ amb p primer el grau dels irreductibles no és fitat.*

Demostració. Suposem que els polinomis irreductibles de $\mathbb{Z}/(p)[x]$ tenen grau fitat per n. Suposem que n és la més petita de les fites superiors. Aleshores hi ha un número finit ja que de polinomis de grau $\leq n$ hi ha p^{n+1}. Suposem que $p_1, \ldots, p_t \in \mathbb{Z}/(p)[x]$ són els irreductibles. Considerem:

$$f(x) = p_1(x) \ldots p_t(x) + 1$$

que no és irreductible per tenir grau $> n$. Aleshores algun p_i ha de dividir f i per tant ha de dividir 1. Hem arribat a contradicció. □

Observem doncs que si K és un cos finit, la seua característica és p primer. Aleshores el subcos primer de K és $\mathbb{Z}/(p) \subseteq K$.

A més si F és subcos de K tindrem que F i K tenen la mateixa característica ja que $1_F = 1_K$. Si L és un cos tal que $K \subseteq L$ K i L tenen la mateixa característica.

Proposició 4.1.2. *Siguin K i L cossos tals que $K \subseteq L$. Aleshores L és un K-espai vectorial.*

Demostració. Amb la suma a L, L és un grup abelià. Si $\lambda \in K$ i $a \in L$ és defineix el producte com el producte de L. □

Proposició 4.1.3. *Suposem K cos. Si K té característica p (serà primer), aleshores $|K| = p^n$ per cert n natural. Recíprocament si $|K| = p^n$ llavors K té característica p.*

Demostració. Suposem $\mathrm{ch}(K) = p$. Aleshores $\mathbb{Z}/(p) \subseteq K$ i K és un $\mathbb{Z}/(p)$-espai vectorial de dimensió finita positiva. Posem $\dim(K) = n \Rightarrow K \cong \mathbb{Z}/(p) \overset{n)}{\times} \cdots \times \mathbb{Z}/(p)$. Per tant $|K| = p^n$.

Suposem ara $|K| = p^n$ amb p primer. Tenim que $\mathrm{ch}(K) = q$ primer. Com que $\mathbb{Z}/(q) \subseteq K \Rightarrow |K| = q^m = p^n \Rightarrow p = q$. □

Corol·lari 4.1.1. *Sigui K és un cos finit amb p^n (primer) elements. Sigui F un subcos de K. Aleshores $|F| = p^d$ amb $d \mid n$.*

Demostració. Suposem F subcos de K. Aleshores $\mathrm{ch}(K) = \mathrm{ch}(F) = p$. Així $|F| = p^d$. Aleshores $\mathbb{Z}/(p) \subseteq F \subseteq K$ i K és un F-espai vectorial. Igual que abans tenim $p^n = |K| = |F|^m = (p^d)^m = p^d m \Rightarrow d \mid n$. □

Teorema 4.1.1. *(Teorema de l'element primitiu) Sigui K un cos finit. Aleshores el grup multiplicatiu K^* és cíclic. Anomenarem element primitiu a un generador de K^*.*

Demostració. Com que K és finit tenim $|K| = p^n$ amb p primer. Aleshores si $K^* = K \setminus \{0\} \Rightarrow |K^*| = p^n - 1$. Posem $q = p^n$ i també $p^n - 1 = q - 1 = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ amb els p_i primers diferents.

Considerem els polinomis

$$f_i = x^{\frac{q-1}{p_i}} - 1$$

que com a màxim tenen $\frac{q-1}{p_i}$ arrels a K. En particular existeix algun element $y_i \in K^*$ tal que y_i no és arrel de f_i, és a dir $y_i^{\frac{q-1}{p_i}} \neq 1$. Considerem també

$$x_i = y_i^{\frac{q-1}{p_i^{\alpha_i}}} \in K^*$$

Veurem que l'ordre de x_i a K^* és $p_i^{\alpha_i}$.

Primer observem que

$$x_i^{p_i^{\alpha_i}} = y_i^{q-1} = 1$$

ja que l'ordre de K^* és $q - 1$. Conseqüentment tenim $|x_i| \mid p_i^{\alpha_i} \Rightarrow |x_i| = p_i^{\beta_i},\ \beta_i \leq \alpha_i$.

Suposem $\beta_i < \alpha_i$. Llavors

$$1 = x_i^{p_i^{\beta_i}} = y_i^{\frac{q-1}{p_i^{\alpha_i - \beta_i}}}$$

amb $\alpha_i - \beta_i \geq 1$. Però d'altra banda

$$y_i^{\frac{q-1}{p_i}} = y_i^{\left(\frac{q-1}{p_i^{\alpha_i-\beta_i}}\right)^{\alpha_i-\beta_i-1}} = 1$$

la qual cosa és una contradicció. Ha de ser doncs $\alpha_i = \beta_i$ i $|x_i| = p_i^{\alpha_i}$ a K^*.

Per cada p_i tenim $x_i = y_i^{\frac{q-1}{p_i^{\alpha_i}}}$ tal que $|x_i| = p_i^{\alpha_i}$. Sigui $\beta = x_1 \dots x_r$ els x_i tenen ordres coprimers i per tant $|\beta| = p_1^{\alpha_1} \dots p_r^{\alpha_r} = q - 1$. Hem trobat β element primitiu. □

Recapitulem, fins al moment hem vist que si K és un cos finit llavors $|K| = p^n, p = \mathrm{ch}(K), p$ primer i que el grup multiplicatiu K^* és cíclic. Observem també que si β és un element primitiu de K^* llavors els elements primitius de K^* seran aquells $\gamma \in K^*$ que compleixen: $\mathrm{mcd}(\gamma, |K^*|) = 1$.

Teorema 4.1.2. *Sigui K un cos finit amb característica p primer. Aleshores existeix un polinomi irreductible $f(x) \in \mathbb{Z}/(p)[x]$ de grau n tal que*

$$K \cong \mathbb{Z}/(p)[x]\big/(f(x))$$

Demostració. Sigui $\beta \in K^*$ un element primitiu. Considerem el morfisme avaluació $\varphi : \mathbb{Z}/(p)[x] \longrightarrow K$ donat per $\varphi(x) = \varphi(\beta)$. Sabem que és epimorfisme d'anells ja que K^* és generat per β. Tenim doncs pel 1r teorema d'isomorfia:

$$\mathbb{Z}/(p)[x]\big/\ker(\varphi) \cong K$$

i com que $\ker(\varphi) \neq (0) \Rightarrow \ker(\varphi)$ és maximal. Com que $\mathbb{Z}/(p)[x]$ és DIP tenim $\ker(\varphi) = (f(x))$ amb $f(x)$ irreductible a $\mathbb{Z}/(p)[x]$. □

Si considerem l'extensió de cossos $K \subseteq L$ i $\gamma \in L$ i prenem el morfisme avaluació en γ, $\varphi : K[x] \longrightarrow L$ tenim:

1. φ injectiu. Llavors γ no compleix cap polinomi amb coeficients a K. Diem que γ és transcendent sobre K.

2. Si $\ker(\varphi) \neq (0) \Rightarrow \gamma$ és arrel d'algun polinomi a $K[x]$. Diem que γ és algebraic sobre K. Tenim
$$K[x]\big/\ker(\varphi) \cong \mathrm{Im}(\varphi) \subseteq L$$
Com que $\mathrm{Im}(\varphi)$ és dins d'un cos, que no té divisors de zero és DI. Per tant $\ker(\varphi)$ és primer i en particular maximal per ser diferent de zero i estar contigut a un DIP. En conseqüència $\mathrm{Im}(\varphi)$ és un cos. A més de generadors de $\ker(\varphi)$ mònics només hi ha un. Es denota generalment $\mathrm{Irr}(\gamma, K)$.

Observem que si K és finit llavors té característica p primer i tot element $\gamma \in K$ és algebraic sobre $\mathbb{Z}/(p)$.

4.2 Existència de cossos finits

Primerament suposem que K és un cos amb p^n elements i $a \in K$ diferent de 0. Sabem que $a^{p^n-1} = 1 \Rightarrow a^{p^n} = a$ i també $0^{p^n} = 0$. És a dir, si $a \in K$ a és arrel del polinomi $f = x^{p^n} - x \in \mathbb{Z}/(p)[x]$.

Definició 4.2.1. Siguin $K \subseteq L$ cossos. Sigui $f(x) \in K[x]$. Diem que f descompon a L si hi té totes les arrels, és a dir, $f(x) = (x - \alpha_1) \dots (x - \alpha_r) \in L[x]$ (amb les α_i potser repetides).

Diem que L és un cos de descomposició de f si L és el mínim cos on f descompon. Diem

$$L = K(\alpha_1, \dots, \alpha_r)$$

generat per K i les arrels α_i de f.

Teorema 4.2.1. *(Teorema de Kronecker) Sigui K un cos, $f(x) \in K[x]$. Aleshores existeix un cos L, $K \subseteq L$ tal que f descompon a L.*

Demostració. Suposem $\text{grau}(f) \geq 1$. Sigui $h(x) \in K[x]$ un factor irreductible de $f(x)$. Considerem

$$L_1 = {}^{K[x]}\!/_{(h(x))}$$

Com que h és irreductible és primer i per tant $(h(x))$ és primer i en conseqüència maximal. A L_1 $h(x)$ té una arrel ($\alpha_1 = \overline{x}$) de manera que podem escriure $f(x) = (x - \alpha_1)g_1(x)$ amb $\text{grau}(g_1) < \text{grau}(f)$. Si $g_1(x)$ descompon a $L_1[x]$ ja ho tenim. Si no, repetim el mateix argument formant una cadena $K \subseteq L_1 \subseteq \dots$ que serà finita ja que el grau de f és finit. Per tant, f descompondrà com a producte de factors lineals en un nombre finit de passos. □

Definició 4.2.2. Sigui K un cos i $f(x) = a_0 + a_1x + \ldots + a_nx^n \in K[x]$. Definim la derivada formal de f com $f' = a_1 + 2a_2x + \ldots + na_nx^{n-1} \in K[x]$ on $ia_i = a_i + \overset{i)}{\ldots}. + a_i$ a K.

Algunes propietats són per $f, g \in K[x]$:

1. $(af)' = af'$
2. $(f + g)' = f' + g'$
3. $(fg)' = f'g + fg'$
4. $(f^n)' = nf'f^{n-1}$
5. $f(g(x)) = g'f'(g(x))$

Proposició 4.2.1. *Si K és un cos i $f(x) = a_0 + a_1x + \ldots + a_nx^n \in K[x]$ amb $n \geq 1$ aleshores:*

1. *Si $\text{ch}(K) = 0 \Rightarrow f' \neq 0$*
2. *Si $\text{ch}(K) = p \neq 0$ llavors $f' = 0 \Leftrightarrow p \mid i \; \forall i > 0$ tal que $a_i \neq 0$.*

Demostració. 1. Si $\text{ch}(K) = 0$ llavors $na_n \neq 0 \Rightarrow f' \neq 0$.

2. Si ara $\text{ch}(K) = p \neq 0$ tenim $f' = 0 \Leftrightarrow ia_i = 0 \ \forall i \Leftrightarrow p \mid (ia_i) \Leftrightarrow p \mid i$ ja que si $p \mid a_i \Rightarrow a_i = 0$.

□

Proposició 4.2.2. *Sigui K un cos i $f(x) = a_0 + a_1x + \ldots + a_nx^n \in K[x]$ amb $n \geq 1$. Sigui α arrel de f. Aleshores α és una arrel múltiple de f si i només si α és també arrel de f'.*

Demostració. Suposem α arrel múltiple de f. Llavors en algun cos L $K \subseteq L$ tenim $f = (x-\alpha)^m g(x)$ amb $m \geq 2$. Així $f' = m(x-\alpha)^{m-1}g(x) + (x+\alpha)^m g'(x) \Rightarrow \alpha$ és arrel de f'.

Recíprocament suposem α arrel de f'. Suposem que α no és arrel múltiple de f. Aleshores $f = (x-\alpha)g(x)$ amb $(x-\alpha) \mid g(x)$. D'aquesta forma $f'(x) = g(x) + (x-\alpha)g'$. Però $(x-\alpha) \mid f' \Rightarrow (x-g) \mid g$ la qual cosa és una contradicció. □

Corol·lari 4.2.1. *K cos i $f \in K[x]$. Si $\text{mcd}(f, f') = 1 \Rightarrow f$ no té arrels múltiples. (el recíproc és cert també).*

Demostració. Suposem $\text{mcd}(f, f') = 1$. La identitat de Bézout ens diu que: $g(x)f(x) + h(x)f'(x) = 1$ per certs $g(x), h(x) \in K[x]$ Si f té una arrel múltiple α és arrel de $f'(x) \Rightarrow (x-\alpha) \mid 1$ i arribem a contradicció. □

Teorema 4.2.2. *(Teorema d'existència) Per a tot primer p i natural n existeix un cos amb p^n elements.*

Demostració. Considerem $x^{p^n} - x \in \mathbb{Z}/(p)[x]$. Sigui L un cos de descomposició de $x^{p^n} - x$. Sigui $F = \{a \in L \mid a^{p^n} = a\} \subseteq L$. Veiem que F té p^n elements.

Fent la derivada formal d'aquest polinomi veiem que $\text{mcd}(x^{p^n} - x, -1) = 1$ i per tant no té arrels repetides. En conseqüència $|F| = p^n$. Només hem de veure que és tancat.

Així doncs tenim que si $a, b \in F$ llavors

$$(a+b)^p = a^p + b^p$$

$$(a+b)^{p^2} = a^{p^2} + b^{p^2}$$

i en general

$$(a+b)^{p^n} = a^{p^n} + b^{p^n} = a + b$$

de manera que $a + b \in F$. Igualment $(ab)^{p^n} = a^{p^n}b^{p^n} = ab \Rightarrow ab \in F$. I com que F és dins de L que és cos, F és DI. En particular tot DI finit és cos. □

Corol·lari 4.2.2. *Per a cada n existeix un polinomi irreductible de grau n a $\mathbb{Z}/(p)[x]$.*

Demostració. Sigui K un cos amb p^n elements. Sabem que existeix $f \in \mathbb{Z}/(p)[x]$ irreductible tal que

$$K \cong \mathbb{Z}/(p)[x]\big/(f) \Rightarrow |K| = p^{\text{grau}(f)} = p^n$$

□

4.3 Unicitat dels cossos finits

Proposició 4.3.1. *Sigui $f \in \mathbb{Z}/(p)[x]$ irreductible de grau d. Si n és múltiple de d aleshores $f \mid (x^{p^n} - x)$, és a dir $x^{p^n} - x$ és múltiple de tots els polinomis irreductibles de grau d amb d divisor de n.*

Demostració. Tenim f. Suposem $n = n'd$ amb n' natural. Pel teorema de Kronecker sabem que f té una arrel α en un cos L.

Considerem el morfisme avaluació en α $\varphi : \mathbb{Z}/(p)[x] \longrightarrow L$. Tenim $f \in \ker(\varphi)$ ja que $f(\alpha) = 0$. Com que f és irreductible i estem a un DIP haurà de ser $\ker(\varphi) = (f)$. Així pel 1r teorema d'isomorfia:

$$\mathbb{Z}/(p)[x]\big/_{(f)} \cong \mathrm{Im}(\varphi) \subseteq L$$

Sabem doncs que $\mathrm{Im}(\varphi)$ serà un cos de p^d elements. D'aquesta manera el seu grup multiplicatiu és cíclic i tenim que si $a \in \mathrm{Im}(\varphi) \Rightarrow a^{p^d} = a$. Així $\alpha^{p^d} = \alpha \Rightarrow (\alpha^{p^d})^{p^d} = \alpha^{p^d} = \alpha$ i d'aquesta manera fins a $\alpha^{p^n} = \alpha \Rightarrow \alpha$ també és arrel de $x^{p^n} - x \Rightarrow x^{p^n} - x \in \ker(\varphi)$. És a dir $x^{p^n} - x \in (f)$. □

Teorema 4.3.1. *(Teorema d'unicitat) Si K i F són dos cossos amb p^n elements llavors $F \cong K$.*

Demostració. Suposem que F és el cos de les arrels de $x^{p^n} - x$. D'altra banda sabem que existeix $f \in \mathbb{Z}/(p)[x]$ irreductible de grau n tal que

$$K \cong \mathbb{Z}/(p)[x]\big/_{(f)}$$

Amb això $f \mid (x^{p^n} - x) \Rightarrow f$ té totes les arrels a F. Sigui $a \in F$ una arrel de f i com sempre $\varphi : \mathbb{Z}/(p)[x] \longrightarrow F$ el morfisme avaluació en a. Sabem que $\ker(\varphi) = (f)$ i

$$\mathbb{Z}/(p)[x]\big/_{(f)} \cong \mathrm{Im}(\varphi) \subseteq F \Rightarrow \mathrm{Im}(\varphi) = F$$

ja que tenen el mateix nombre d'elements. □

Teorema 4.3.2. *Sigui K un cos amb p^n elements. Aleshores per cada $d \mid n$ existeix un únic subcos de K amb p^d elements.*

Demostració. Sigui f un polinomi irreductible de grau d, $f \in \mathbb{Z}/(p)[x]$. Com que $f \mid (x^{p^n} - x) \Rightarrow f$ té les arrels a K. La imatge del morfisme avaluació $\varphi : \mathbb{Z}/(p)[x] \longrightarrow K$ per una arrel és un subcos de K i té p^d elements. □

Proposició 4.3.2. *Considerem $x^{p^n} - x, x^{p^d} - x \in \mathbb{Z}/(p)[x]$. Aleshores $x^{p^d} - x \mid x^{p^n} - x$ si i només si $d \mid n$.*

Teorema 4.3.3. *A $\mathbb{Z}/(p)[x]$ tenim $x^{p^n} - x \sim \prod_{f(x)} f(x)$ amb els $f(x)$ irreductibles de grau $d \mid n$.*

Demostració. Com que els diferents f són mònics i irreductibles no són associats i per tant $\prod_{f(x)} f(x) \mid x^{p^n} - x$. Veiem que són iguals.

Sigui ara $\mathbb{F} = \mathbb{F}_{p^n}$ el cos de p^n elements. Sigui α arrel de $x^{p^n} - x$, és a dir, $\alpha \in \mathbb{F}$. Considerant $\varphi : \mathbb{Z}/(p)[x] \longrightarrow \mathbb{F}$ de forma que $\varphi(x) = \alpha$ tenim

$$\mathbb{Z}/(p)[x]\big/_{\ker(\varphi)} \cong \mathrm{Im}(\varphi) \subseteq \mathbb{F}$$

i sabem que $\mathrm{Im}(\varphi)$ és un subcos de $\mathbb{F}$.

A més $|\mathrm{Im}(\varphi)| = p^d$ i $\ker(\varphi) = (f(x))$ amb $f(x)$ irreductible mònic. Així

$$|\mathbb{Z}/(p)[x]\big/_{\ker(f(x))}| = p^{\mathrm{grau}(f(x))} = p^d$$

Ara sabem que $x^{p^n} - 1 = g(x) \prod_{f(x)} f(x)$ per cert $g(x)$. Ara bé, qualsevol arrel α compleix un dels $f(x)$. Per tant g no té cap i és una constant. Tenim doncs $x^{p^n} - x \sim \prod_{f(x)} f(x)$. □

Sigui K un cos amb $\mathrm{ch}(K) = p \neq 0$. Aleshores considerem

$$\phi : K \longrightarrow K$$

donada per $\phi(a) = a^p$. És un morfisme de cossos (injectiu). S'anomena *morfisme de Frobenius*.

Si K és finit ϕ és també exhasutiu.

Teorema 4.3.4. *Sigui $f \in \mathbb{Z}/(p)[x]$ irreductible de grau n. Sigui α una arrel de f en un cos finit K. Aleshores les arrels de f són $\alpha, \alpha^p, \alpha^{p^2}, \ldots, \alpha^{p^{n-1}}$. A més $\alpha^{p^n} = \alpha$.*

Demostració. Veiem que les potències són arrels. Si $f = \sum_{i=0}^n a_i x^i \in \mathbb{Z}/(p)[x]$. D'aquesta manera

$$(\sum_{i=0}^n a_i \alpha^i)^p = 0^p = 0$$

i també

$$0 = f(\alpha)^p = (\sum_{i=0}^n a_i \alpha^i)^p = \sum_{i=0}^n a_i (\alpha^i)^p = f(\alpha^p)$$

de manera que α^p és arrel. Repetint l'argument, les potències esmentades de α són arrels de f.

Veiem que totes les potències de α són diferents. Suposem $\alpha^{p^i} = \alpha^{p^j}, n > i > j$. Considerem K cos finit tal que $\alpha \in K$. Sigui ϕ el morfisme de Frobenius tenim $\alpha^{p^i} = \phi^i(\alpha) = \alpha^{p^j} = \phi^j(\alpha) \Rightarrow \phi^{i-j}(\alpha) = \alpha \Rightarrow \alpha^{p^{i-j}} = \alpha$.

Escrivim $t = i - j$. Aleshores α és arrel del polinomi $x^{p^t} - x \in \mathbb{Z}/(p)[x]$. En conseqüència α és arrel d'un polinomi irreductible de grau s, $g \in \mathbb{Z}/(p)[x]$ tal que $s \mid t$. Però $s < n$ contradiu el fet que α és arrel també d'un polinomi irreductible de grau n. Per tant són totes diferents.

Com que f és irreductible de grau n tenim $f \mid x^{p^n} - x \Rightarrow \alpha$ és arrel de $x^{p^n} - x \Rightarrow \alpha^{p^n} = \alpha$. □

Corol·lari 4.3.1. *Sigui K un cos finit. Sigui $\gamma \in K$. Sigui d el mínim tal que $\gamma^{p^d} = \gamma$. Aleshores:*

$$\mathrm{Irr}(\gamma, \mathbb{Z}/(p)) = (x-\gamma)(x-\gamma^p)(x-\gamma^{p^2})\dots(x-\gamma^{p^{d-1}})$$

Demostració. Els elements de K són les arrels de $x^{p^n} - x \Rightarrow \mathrm{Irr}(\gamma, \mathbb{Z}/(p)) \mid x^{p^n} - x$. Fem $f = \mathrm{Irr}(\gamma, \mathbb{Z}/(p))$. Suposem $\mathrm{grau}(f) = s$. Volem veure que $s = d$. Sabem doncs que $f \mid x^{p^s} - x \Rightarrow \gamma$ és arrel de x^{p^s}. Com que d és el mínim tenim $s = d = \mathrm{grau}(f)$. Les altres arrels són doncs $\gamma, \gamma^p, \dots, \gamma^{p^{d-1}}$. □