Estructures algebraiques

Aniol Garcia i Serrano

Setembre 2019

Capítol 1

Grups

1.1 Definicions

Definició 1
Un grup és un conjunt G amb una operació binària[1] *i interna*[2] *que compleix:*

1. $(xy)z = x(yz), \forall x, y, z \in G$ *(associativitat)*
2. $\exists e \in G$ *tal que* $ex = e = xe$ *(existència de l'element neutre)*
3. $\forall x \in G, \exists x'$ *tal que* $xx' = x'x = e$ *(x' s'anomena element simètric d'x)*

Si, a més, compleix

4. $xy = yx$, $\forall x, y \in G$

diem que G és commutatiu o abelià.

Si l'operació de G és el producte, posem 1 per l'element neutre i diem invers (x^{-1}) al simètric. Si l'operació de G és la suma, posem 0 per l'element neutre i diem oposat ($-x$) al simètric).

Proposició
L'element neutre d'un grup G és únic i l'element simètric d'un element x de G també és únic.

Demostració. Si e, e' són elements neutres de G, aleshores $e = ee' = e'$.
Donat $x \in G$, si x', x'' són elements simètrics d'x,

$$x' = x'e = x'(xx'') = (x'x)x'' = ex'' = x''$$

[1] Diem que una operació és binària quan s'opera sobre dos elements
[2] Una operació és interna a un conjunt X quan al operar amb dos elements d'X, el resultat que s'obté també és a X

Exemple

1. *matrius invertiblesn* $\times$ *n amb coeficients a* $\mathbb{R}$ *amb producte de matrius* $= GL(n, \mathbb{R})$
2. $GL(1, \mathbb{R}) = (\mathbb{R} \setminus \{0\}, \cdot)$
3. $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +)$ *i són grups abelians*
4. $(\mathbb{Q} \setminus \{0\}, \cdot), (\{\pm 1\}, \cdot)$ *i són grups abelians*

Proposició

1. $x, y, a \in G,\ xa = ya \implies x = y$ *i, de manera similar,* $ax = ay \implies x = y$
2. $(xy)^{-1} = y^{-1}x^{-1}$

Definició 2

Un subgrup d'un grup G *és un subconjunt* $H \subseteq G$, $H \neq \emptyset$ *tal que*

- $xy \in H \forall x, y \in H$
- H *és un grup amb l'operació de* G

Proposició

Sigui G *un grup i* H *un subconjunt no buit de* G*. Són equivalents:*

1. H *és un grup amb l'operació de* G
2. (a) $e \in H$
   (b) $x, y \in H \implies xy \in H$
   (c) $x \in H \implies x^{-1} \in H$
3. $x, y \in H \implies xy^{-1} \in H$

Demostració.

$\boxed{1 \implies 2}$: És evident per la definició de grup.

$\boxed{2 \implies 3}$: $x, y \in H \overset{(c)}{\implies} x, y^{-1} \in H \overset{(b)}{\implies} xy^{-1} \in H$

$\boxed{3 \implies 1}$: $H \neq \implies \exists x \in H$

$x, x \in H \overset{(3)}{\implies} xx^{-1} \in H \implies e = xx^{-1} \in H$ (hi ha element neutre)

Donat $y \in H$, $e, y \in H \overset{(3)}{\implies} ey^{-1} = y^{-1} \in H$ $(*)$ (hi ha element invers)

Donats $x, y \in H$, $x, y \in H \overset{(*)}{\implies} x, y^{-1} \in H \overset{(3)}{\implies} x(y^{-1})^{-1} = xy \in H$ (el producte és intern i, com que és associatiu a G, a la restricció a H segueix essent associatiu, de manera que H és un grup amb l'operació de G)

Exemple

- *Si* G *és un grup,* $\{e\}$ *és subgrup de* G *i s'anomena subgrup trivial*

- *Ai G és un grup, G és subgrup de G i s'anomena subgrup total*
- *Subgrups de $GL(n,\mathbb{R})$: $\{Id\}, GL(n,\mathbb{Z}$, matrius diagonals inversibles*
- *Subgrups de $(\mathbb{Z},+)$: $2\mathbb{Z} = \{2n | n \in \mathbb{Z}\}, m\mathbb{Z} = \{\gtrdot\ltimes | \ltimes \in \mathbb{Z}\}$*
- *$(\{1,-1\},\cdot), (\mathbb{Z}/n\mathbb{Z},+)$ (només tenen subgrup trivial i total)*

Proposició
Si G és un grup i $\{H_i\}_{i\in I}$ és un conjunt de subgrups de G, aleshores $\bigcap_{i\in I} H_i$ és subgrup de G.

Proposició
Tot subgrup H de $\mathbb{Z}$ és igual a $m\mathbb{Z}$ per a algun $m \geq 0$.

Demostració. Si $H = \{0\}$, aleshores $H = 0\mathbb{Z}$. Si $H \neq 0$, aleshores conté algun $n \neq 0 \implies n$ ó $-n$ és un element de H i és més gran que 0. Sigui m l'element estrictament positiu contingut a H. Aleshores, $m\mathbb{Z} \subset H$. Vegem ara la inclusió contrària. Sigui $n \in H$. Per l'algorisme de la divisió podem escriure $n = mq + r$, amb $0 \leq r < m$. Així, $r = n - mq \in H$ (ja que $n, mq \in H$). Per com hem escollit m, tenim que $r = 0 \implies n = mq \in m\mathbb{Z}$.

Observem que $m_1\mathbb{Z} \cap m_2\mathbb{Z} = mcm(m_1, m_2)$.

1.2 Grups de permutacions

Definició 3
Donat un conjunt X, diem permutació d'X a una aplicació bijectiva d'X a X. El conjunt de les permutacions d'X és un grup amb la composició d'aplicacions i s'anomena S_X.

Per a n enter, $n \geq 1$, anomenem grup simètric de grau n (S_n) al grup de permutacions de $\{1, \cdots, n\}$. Si $\sigma \in S_n$, definim

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$$

Definició 4
Sigui $\sigma \in S_n$ tal que

- $\sigma(k_1) = k_2, \sigma(k_2) = k_3, \dots, \sigma(k_r) = k_1$
- $\sigma(m) = m\ \forall m \in \{1, 2, \dots, n\} \setminus \{k_1, k_2, \dots, k_r\}$

Aleshores anomenem a σ un cicle d'ordre r o un r-cicle i escrivim $\sigma = (k_1, k_2, \dots, k_r)$. Un 2-cicle s'anomena transposició.

Algunes propietats dels cicles són les següents:

- Si $\sigma = (k_1, k_2, \dots, k_r)$, aleshores $\sigma^{-1} = (k_r, \dots, k_2, k_1)$.

- Dos cicles $(k_1, k_2, \ldots, k_r)$, $(l_1, l_2, \ldots, l_s)$ són disjunts si $\{k_1, k_2, \ldots, k_r\}$, $\{l_1, l_2, \ldots, l_s\}$ són conjunts disjunts.

Proposició
Tota permutació de S_n diferent a la identitat és producte de cicles disjunts dos a dos unívocament determinats tret de l'ordre.

Corol·lari
Tota permutació de S_n és producte de transposicions.

Demostració. $(k_1, k_2, \ldots, k_n) = (k_1, k_2)(k_2, k_3)\ldots(k_{n-1}, k_n)$

Lema
Si $a, b, c \in \{1, 2, \ldots, n\}$, tots diferents, aleshores $(a, b)(b, c) = (a, c)(a, b)$.

Demostració.

$$(a, b)(b.c) = (a, b, c)$$
$$(a, c)(a, b) = (a, b, c)$$

Proposició
La identitat no és producte d'un nombre senar de transposicions.

Demostració. Provarem per inducció que la identitat no és producte de $2k + 1$ transposicions.

$\boxed{\text{k=0}}$: Id no és transposició.

$\boxed{\text{k-1} \implies k}$: Suposem que Id no és proucte de $2k+1$ transposicions. Aleshores podem escriure

$$Id = t_1 t_2 = t_{2k-1}$$

amb t_i transposició. Sigui $t_{2k-1} = (a, x)$. Aleshores, $\exists i$ tal que $t_i = (a, y)$ per a algun y. Pel lema anterior, podem suposar que $t_{2k} = (a, y)$. Per hipòtesi d'inducció sabem que $x \neq y$. Llavors, $\exists t_i = (a, z)$ i, altre cop pel lema, podem suposar que $t_{2k-1} = (a, z)$. D'aquesta manera, per la hipòtesi d'inducció, $z \neq x, y$, i així successivament. Totes les transposicions són (a, v) amb totes les v's diferents. Així, és evident que el producte no pot donar identitat.

Corol·lari
Si $t_1, t_2, \ldots, t_r, \tau_1, \tau_2, \ldots, \tau_s$ són transposicions amb $t_1 t_2 \ldots t_r = \tau_1 \tau_2 \ldots \tau_s$, aleshores r i s tenen la mateixa paritat.

Demostració. $t_1 t_2 \ldots t_r \tau_1 \tau_2 \ldots \tau_s = Id \implies r + s$ parell.

Definició 5
La signatura d'una permutació σ és $sg(\sigma) = (-1)^r$, on r és el nombre de factors en una descomposició de σ en producte de transposicions. Direm que una permutació és ***parella*** *quan $sg(\sigma) = 1$ i* ***senar*** *quan $sg(\sigma) = -1$.*

La signatura compleix les propietats següents:

- $sg(\sigma\tau) = sg(\sigma)sg(\tau)$
- $sg(Id) = 1$
- $sg(\sigma^{-1}) = sg(\sigma)$

Proposició
El conjunt de S_n format per les permutacions parelles és un subgrup de S_n. Es diu subgrup alternat i s'escriu A_n.

1.2.1 Morfismes de grups

Definició 6
Si G, G' són grups, una aplicació $f : G \to G'$ és morfisme de grups si $f(xy) = f(x)f(y)\ \forall x, y \in G$.

Proposició
Siguin G, G' grups, $f : G \to G'$ un morfisme de grups, e l'element neutre de G i e' l'element neutre de G', aleshores

1. $f(e) = e'$
2. $f(x^{-1}) = f(x)^{-1} \forall x \in G$

Demostració. 1. $f(e)f(e) = f(ee) = f(e) \implies f(e) = e'$

2. $f(x^{-1})f(x) = f(x^{-1}x) = f(e) = e' \implies f(x^{-1}) = f(x)^{-1}$

Vet aquí alguns exemples de morfismes:

- $det : GL(n, \mathbb{R}) \to (\mathbb{R} \setminus \{0\}, \cdot)$
- $sg : S_n \to (\{\pm 1\}, \cdot)$
- $$\begin{aligned} \mu_m : &\mathbb{Z} \to \mathbb{Z} \qquad\qquad m \in \mathbb{Z} \\ &a \mapsto am \end{aligned}$$

Proposició
Siguin G, G', G'' grups, i $f : G \to G', g : G' \to G''$ morfismes de grups, aleshores $g \circ f$ és un morfisme.

Demostració. Siguin $x, y \in G$. Aleshores, $(g \circ f)(xy) = g(f(xy)) = g(f(x)f(y)) = g(f(x))g(f(y)) = (g \circ f)(x)(g \circ f)(y)$

Definició 7
Sigui $f : G \to G'$ morfisme de grups. Definim:

1. *$Ker(f) = \{x \in G | f(x) = e'\}$*
2. *$Im(f) = \{f(x) | x \in G\}$*
3. *Si H és un subgrup de G definim $f(H) = \{f(x) | x \in H\}$*

Proposició

1. *$Ker(f)$ és subgrup de G.*
2. *$Im(f)$ és subgrup de G'.*
3. *Si H és subgrup de G, $f(H)$ és subgrup de G'.*

Demostració. 1. $f(e) = e' \implies e \in Ker(f) \implies Ker(f) \neq \emptyset$.
$x, y \in Ker(f), f(xy^{-1}) = f(x)f(y^{-1}) = f(x)f(y)^{-1} = e' \implies xy^{-1} \in Ker(f)$

2. Seguint un argument similar a l'anterior.
3. Sigui H un subgrup de G. $x', y' \in f(H) \implies x, y \in H : x' = f(x), y' = f(y)$. Aleshores $x'y'^{-1} = f(x)f(y)^{-1} = f(xy^{-1}) \in f(H)$. A més, podem afirmar que $f(H) \neq \emptyset$, ja que $e \in H \implies f(e) \in f(H)$.

Proposició

Si $f : G \to G'$ és isomorfisme de grups, $f^{-1} : G' \to G$ també ho és.

Demostració. Siguin

$$\begin{aligned} x', y' \in G', f^{-1}(x'y') &= f^{-1}(x')f^{-1}(y') \\ &\Updownarrow \\ x'y' = f(f^{-1}(x'y')) &= f(f^{-1}(x')f^{-1}(y') = f(f^{-1}(x))f(f^{-1}(y)) = x'y' \end{aligned}$$

Definició 8

Diem que dos grups G, G' són isomorfs ($G \simeq G'$) si existeix un isomorfisme $f : G \to G'$.

Sigui G un grup i sigui $x \in G$. Definim

$$\begin{aligned} \varphi_x \colon G &\to G' \\ y &\mapsto xyx^{-1} \end{aligned}$$

(xyx^{-1} s'anomena conjugat d'y per x) Aleshores $_x$ és morfisme.

Demostració.

$$\begin{aligned} y, z \in G, \varphi_x(yz) &= x(yz)x^{-1} \\ &= (xyx^{-1})(xzx^{-1}) \\ &=_x (y)\varphi_x(z) \end{aligned}$$

$\varphi_x^{-1} = \varphi_{x^{-1}} \implies \varphi$ automorfisme. H subgrup de G, $xHx^{-1} := \varphi_x(H)$ és subgrup de G. Es diu subgrup conjugat de H per x.

Proposició
$f\colon G \to G'$ morfisme de grups és injectiu $\iff Ker(f) = \{e\}$

Demostració.

$\boxed{\implies}$ $x \in G, f(x) = e' = f(e) \implies x = e$ tenim doncs que $Ker(f) = \{e\}$

$\boxed{\impliedby}$ $x, y \in G$ tal que $f(x) = f(y) \implies f(x)f(y)^{-1} = f(y)f(y)^{-1} \implies f(x)f(y)^{-1} = e' \implies xy^{-1} \in Ker(f) = \{e\} \implies xy^{-1} = e \implies x = y$, de manes que la funció és injectiva.

Definició 9
Si G és un grup, anomenem ***ordre*** *de G al cardinal de G com a conjunt i l'escribim $|G|$. Exemples: $|S_n| = n!$, $|{}^{\mathbb{Z}}/_{m\mathbb{Z}}| = m$, $|\mathbb{Z}| = \infty$.*

Donats un grup G i un subgrup H, definim a G les relacions D i E per

$$xDy \iff x^{-1}y \in H,\ xEy \iff xy^{-1} \in H$$

Proposició
D i E són relacions d'equivalència.

Demostració.

Reflexiva: $xEx \iff xx^{-1} = e \in H$

Simètrica: $xEy \implies yx^{-1} \in H \implies (yx^{-1})^{-1} = xy^{-1} \in H \implies yEx$

Refexiva: $\left.\begin{array}{l} xEy \implies yx^{-1} \in H \\ yEz \implies zy^{-1} \in H \end{array}\right\} \implies (zy^{-1})(yx^{-1}) = zx^{-1} \in H \implies xEz$

$xDy \iff x^{-1}y = h \in H \implies y = xh$, així que la classe d'$x$ per D és $\{xh\colon h \in H\} = xH$. De manera similar, $xEy \iff yx^{-1} = h \in H \implies y = hx$, i la classe d'$x$ per E és $\{hx\colon h \in E\} = Hx$. Anomenem ${}^{G}/_{D}$, ${}^{G}/_{E}$ conjunts quocients de G per H per la dreta i per l'esquerra.

$$\begin{aligned} H &\to xH \\ h &\mapsto xh \end{aligned}$$

$$\begin{aligned} H &\to Hx \\ h &\mapsto hx \end{aligned}$$

són bijeccions.

Observem que $x \in xH \implies y = xh \implies y^{-1} = h^{-1}x^{-1} \in Hx^{-1}$. L'aplicació bijectiva

$$\begin{aligned} G &\to G \\ y &\mapsto y^{-1} \end{aligned}$$

dóna una bijecció entre ${}^{G}/_{D}$ i ${}^{G}/_{E}$.

Exemples:

- Si G és abelià, $D = E$.
- Donat $S_3 = \{Id, t_3 = (1,2), t_2 = (1,3), t_1 = (2,3), c_1 = (1,2,3), c_2 = (1,3,2)\}$, sigui $H = \{Id, t_3\}$.

Classes per la dreta: $IdH = H$, $t_2H = \{Idt_2, t_2t_3\} = \{t_2, c_1\}$, $t_1H = \{t_1Id, t_1t_3\} = \{t_1, c_2\}$

Classes per l'esquerra: $HId = H$, $Ht_2 = \{Idt_2, t_3t_2\} = \{t_2, c_2\}$, $Ht_1 = \{Idt_1, t_3t_1\} = \{t_1, c_1\}$

Definició 10
Diem índex del subgrup H en el grup G (escrit com $[G\colon H]$ el cardinal del conjunt quocient ${}^{G}/_{D}$.

1.2.2 Teorema de Lagrange

Teorema
Donats un grup G i un subgrup H el grup G és finit $\iff$ H i $[G\colon H]$ són finits. En aquest cas, $|G| = |H|[G\colon H]$.

Demostració.

$\boxed{\Longrightarrow}$ $H \subset G \implies H\text{finit}, [G\colon H]$ finit.

$\boxed{\Longleftarrow}$ $|G| = |H|[G\colon H]$.

Corol·lari
Si G és finit, $|H|$ i $[G\colon H]$ són divisors de $|G|$

Definició 11
Sigui T una relació d'equivalència definida en un grup G. Diem que T és compatible amb l'operació de G si per a qualssevol $x, y, x', y' \in G$ es compleix

$$\left.\begin{matrix} xTx' \\ yTy' \end{matrix}\right\} \implies xyTx'y'$$

Proposició
Si T és relació compatible amb l'operació de G, a ${}^{G}/_{T}$ definim $[x][y] = [xy]$. El producte està ben definit i ${}^{G}/_{T}$ és grup amb aquest producte.

Demostració.

$(xy)z = x(yz)$ a $G \implies ([x][y])[z] = [(xy)z] = [x(yz)] = [x]([y][z])$

$[e]$ és element neutre de ${}^{G}/_{T}$

$[x^{-1}]$ és l'invers d'$[x]$ a ${}^{G}/_{T}$

Proposició
Sigui G un grup, H un subgrup de G i D, E les relacions d'equivalència definides a partir d'H. Els enunciats següents són equivalents:

1. $xH = Hx$, $\forall x \in G$
2. $xHx^{-1} = H$, $\forall x \in G$
3. $xHx^{-1} \subset H$, $\forall x \in G$
4. *D és compatible amb l'operació de G*
5. *E és compatible amb l'operació de G*

Demostració. $\boxed{1 \iff 2}$ $h \in H$ i $xH = Hx \implies hx = h'x$ amb $h' \in H$. Aleshores $xhx^{-1} = (h'x)x^{-1} = h'(xx^{-1}) = h'e = h' \in H$. Tenim doncs que $xHx^{-1} \subset H$, $\forall x \in G$. Vegem ara la inclusió cap a l'altra banda. $x \in G \implies x^{-1} \in G$ i tenim que $x^{-1}Hx \subset H$. Aleshores $x \in H$, $x(x^{-1}hx)x^{-1} \subset xHx^{-1} \implies H \subset xHx^{-1}$.

$\boxed{2 \implies 3}$ Evident.

$\boxed{3 \implies 1}$ Sabem que $xHx^{-1} \subset H$. $\forall x \in G, \forall h \in H$, $xhx^{-1} = h' \implies xh = h'x$ per un cert $h' \in H \implies xH \subset Hx$ $\forall x \in G$, $\forall h \in H$, $x^{-1}hx = h' \implies hx = xh'$ per un cert $h' \in H \implies Hx \subset xH$

$\boxed{1 \implies 4}$ Volem veure que $x, y, x', y' \in G$ es compleix que

$$\left.\begin{matrix} xDx' \\ yDy' \end{matrix}\right\} \implies xyDx'y'$$

$$\left.\begin{matrix} xDx' \iff x' = xh_1 \text{ amb } h_1 \in H \\ yDy' \iff y' = yh_2 \text{ amb } h_2 \in H \end{matrix}\right\} \implies x'y' = x(h_1y)h_2 = x(yh_1)h2 = xy(h_1h_2) \implies xyDx'y'$$

$\boxed{4 \implies 3}$ Donats $x \in G$ i $h \in H$, colem veure que $xhx^{-1} \in H$

$$\left.\begin{matrix} hxDx \\ x^{-1}Dx^{-1} \end{matrix}\right\} \implies xhx^{-1}Dx^{-1}x^{-1} \implies xhx^{-1} \in H$$

Definició 12
Un subgrup H de G es diu normal si compleix una de les condicions de la proposició anterior. Ho escrivim $H \triangleleft G$. Si $H \triangleleft G$, posem ${}^{G}/_{H} = {}^{G}/_{D} = {}^{G}/_{E}$ amb el producte de classes li diem grup quocient de G per H

Proposició
Si $f\colon G \to G'$ és morfisme de grups, $Ker(f)$ és subgrup normal de G.

Demostració. $x \in G$, $y \in Ker(f)$. Volem veure que $xyx^{-1} \in Ker(f)$.

$$f(xyx^{-1}) = f(x)f(y)f(x)^{-1} = f(x)e'f(x') = f(x)f(x)^{-1} = e'$$

1.2.3 Teorema d'isomorfia

Siguin G, G' grups, $f\colon G \to G'$ morfismes de grups. Sigui H subgrup normal de G. Diem que f factoritza a través de ${}^{G}\!/_{H}$ si existeix un morfisme $\overline{f}\colon {}^{G}\!/_{H} \to G'$ tal que el següent diagrama és commutatiu: és a dir, $f = \bar{f} \circ \pi$.

Proposició
Siguin G, G' grups, $f\colon G \to G'$ morfisme de grups, H subgrup normal de G. Aleshores f factoritza a través de ${}^{G}\!/_{H}$ sii $H \subset Ker(f)$.

Demostració. Suposem que G factoritza a través de ${}^{G}\!/_{H}$

$$h,\ f(h) = \bar{f}(\pi(h)) = \bar{f}(\bar{e}) = e' \implies H \subset Ker(f)$$

amb e' la classe de l'element neutre a ${}^{G}\!/_{H}$.
Suposem $H \subset Ker(f)$. Aleshores $\bar{f}([x]) = \bar{f}(\pi(x)) = f(x)$ és la única manera de definir $\bar{f}$ per tal que compleixi $f = \bar{f} \circ \pi$. Aleshores, està f ben definida? És a dir, $[x] = [y] \overset{?}{\implies} f(x) = f(y)$

$$[x] = [y] \implies y = xh \implies f(y) = f(x)f(h) = f(x)$$

I és $\bar{f}$ morfisme de grups?

$$\bar{f}([x][y]) = \bar{f}([xy]) = f(xy) = f(x)f(y) = \bar{f}([x])\bar{f}([y])$$

Primer teorema d'isomorfia

Si G, G' són grups i $f\colon G \to G'$ un morfisme de grups, aleshores f factoritza a través de ${}^{G}\!/_{kerf}$ i tenim $f = i \circ \tilde{f} \circ \pi$ on $\tilde{f}\colon {}^{G}\!/_{Kerf} \to Imf$ és isomorfisme de grups, $\pi\colon G \to {}^{G}\!/_{kerf}$ el morfisme de pas al quocient i $i\colon Imf \to G$ és inclusió

Demostració. Per la proposició anterior, f factoritza a través de ${}^{G}\!/_{Kerf}$ i existeix $\tilde{f}{}^{G}\!/_{kerf} \to G'$ tal que $f = \tilde{f} \circ \pi$. A més, $\bar{f}([x]) = f(x)$ pera a $x \in G$. Per tant, $Imf = Im\bar{f}$.

$${}^{G}\!/_{kerf} \xrightarrow{\tilde{f}} Imf = Im\bar{f} \longrightarrow G'$$

I tenim que $\tilde{f}$ és exhaustiva per definició i $\tilde{f}$ és infectiva si i només si $\bar{f}$ injectiva. Però

$$\bar{f}([x]) = e' \implies f(x) = e' \implies x \in Kerf \implies [x] = [e] \implies \bar{f}\text{injectiu}$$

Aleshores $f = \bar{f} \circ \pi = i \circ \tilde{f} \circ \pi$.

1.2.4 Ordre d'un element d'un grup

Definició 13
Sigui $x \in G$, $n \in \mathbb{Z}$. Definim

$$x^n = \begin{cases} x \cdot \overset{n}{\ldots} \cdot & si\ n > 0 \\ e & si\ n = 0 \\ (x \cdot \overset{|n|}{\ldots} \cdot x)^{-1} & si\ n < 0 \end{cases}$$

Donat $x \in G$, definim també l'aplicació

$$\begin{aligned} f_x \colon \mathbb{Z} &\longrightarrow \mathbb{G} \\ n &\longmapsto x^n \end{aligned}$$

Aleshores $x^{n_1+n_2} = x^{n_1} \cdot x^{n_2} \implies f_x$ és morfisme de grups. $Ker f_x$ és subgrup de $\mathbb{Z} \implies Ker f_x = m\mathbb{Z}$ per a algun enter ≥ 0. Si $m > 0$ diem que x té ***ordre*** *m i si $m = 0$, direm que x té ordre infinit. Si $ordx = m$, finit, $Im f_x = \{x^n | n \in \mathbb{Z} = \{e, x, x^2, \ldots, x^{m-1}\}\}$ és subgrup de G. El denotem per $< x >$ i l'anomenem subgrup generat per x. Pel teorema d'isomorfia, $< X > \simeq {}^{\mathbb{Z}}\!/_{m\mathbb{Z}}$. En canvi, si $ordx = 0, Im f_x = \{x^m | m \in \mathbb{Z}\}$ és subgrup de G i isomorf a $\mathbb{Z}$ pel teorema de l'isomorfia. Finalment, $| < x > | = ordx \implies ordx$ divideix a $|G|$.*

1.2.5 Grups cíclics

Definició 14
Diem que un grup és cíclic si $\exists x \in G$ tal que $< x >= G$. De manera equivalent, podem dir que un grup és cíclic si existeix $x \in G$ tal que $ordx = |G|$. Escribim C_n per referir-nos al grup ciclíc d'ordre n.

Proposició
Tot grup cíclic infinit és isomorf a $\mathbb{Z}$ i tot grup cíclic d'ordre m és isomorf a ${}^{\mathbb{Z}}\!/_{m\mathbb{Z}}$. Per tant, dos grups cíclics del mateix ordre són isomorfs entre ells.

Demostració. Si $G =< x >$,

$$\begin{aligned} f_x \colon \mathbb{Z} &\longrightarrow \mathbb{G} \\ n &\longmapsto x^n \end{aligned}$$

és morfisme exhaustiu.
Si G té ordre infinit, f_x és injectiva $\implies \mathbb{Z} \simeq G$ pel teorema d'isomorfia.
SI G té ordre $m > 0$, $Ker f_x = m\mathbb{Z} \implies {}^{\mathbb{Z}}\!/_{m\mathbb{Z}} \simeq G$

Definició 15
Sigui G un grup i sigui $\subseteq G$ un subconjunt qualsevol. Definim

$$< S >= \bigcap_{\substack{H \text{ subgrup de } G \\ S \subseteq H}} H$$

Observació
$< S >$ *és subgrup*

Observació
$S =, < 0 >=_{H \ grup} H = \{e\}$

Proposició

$$< S >= \{x_1^{n_1} \cdot x_2^{n_2} \cdot, \ldots, x_r^{n_r} \mid \{x_1, x_2, \ldots, x_r\} \subseteq S,\ n_1, \ldots, n_r \in \mathbb{Z},\ r \in \mathbb{N}\}$$

Demostració. Sigui $H_0 = \{x_1^{n_1}, x_2^{n_2}, \ldots, x_r^{n_r} \mid \{x_1, x_2, \ldots, x_r\} \subseteq S,\ n_1, \ldots, n_r \in \mathbb{Z},\ r \in \mathbb{N}\}$

- $S \subseteq H_0$: Sigui $x \in S \implies x = x_i^{n_i} \in H_0$
- H_0 és subgrup de G $(a, b \in H_0 \implies ab^{-1} \in H_0)$. Siguin $a, b \in H_0$.

  $$a = x_1^{n_1} \cdot \ldots \cdot x_r^{n_r}, b = y_1^{m_1} \cdot \ldots \cdot y_l^{n_l}$$

  amb $r, l \in \mathbb{N},\ n_1, \ldots, n_r, m_1, \ldots, m_l \in \mathbb{Z},\ \{x_1, \ldots, x_r\}, \{y_1, \ldots, y_l\} \subseteq S$. Aleshores $b^{-1} = y_l^{-m_l} \cdot \ldots \cdot y_1^{-m_1}$ i, per tant, $ab^{-1} = x_1^{n_1} \cdot \ldots \cdot x_r^{n_r} \cdot y_l^{-m_l} \cdot \ldots \cdot y_1^{-m_1} \in H_0$, ja que $n_1, \ldots, n_r, m_1, \ldots, m_l \in \mathbb{Z}$ i $\{x_1, \ldots, x_r\}, \{y_1, \ldots, y_l\} \subseteq S$. Aleshores $\bigcap_{\substack{H \text{ subespai} \\ S \subset H}} H \subseteq H_0$.

Per veure que són iguals: Sigui H subgrup, $S \subset H \implies \forall x_1, , x_r \in S,\ \forall n_1, \ldots, n_r \in \mathbb{Z},\ x_1^{n_1} \cdot \ldots \cdot x_r^{n_r} \in H \implies H_0 \subset H$ i, aleshores, $H_0 =< S >$.

Definició 16
Un grup G és finitament generat si $\subseteq G$ finit tal que $< S >= G$.

Observació
Si G és finit, $G =< G >$ és conjunt generador.

Proposició
Si $f \colon G \to G'$ és un morfisme de grups i $S \subseteq H$,

$$< f(S) >= f(< S >)$$

Demostració. Fent servir la proposició anterior:

$$< S >= \{x_1^{n_1} \cdot x_2^{n_2} \cdot, \ldots, x_r^{n_r} \mid \{x_1, x_2, \ldots, x_r\} \subseteq S,\ n_1, \ldots, n_r \in \mathbb{Z},\ r \in \mathbb{N}\}$$

$$f(< S >) = \{f(x_1^{n_1} \cdot x_2^{n_2} \cdot, \ldots, x_r^{n_r}) \mid \{x_1, x_2, \ldots, x_r\} \subseteq S,\ n_1, \ldots, n_r \in \mathbb{Z},\ r \in \mathbb{N}\}$$

$$= \{f(x_1^{n_1}) \cdot f(x_2^{n_2}) \cdot, \ldots, f(x_r^{n_r}) \mid \{x_1, x_2, \ldots, x_r\} \subseteq S,\ n_1, \ldots, n_r \in \mathbb{Z},\ r \in \mathbb{N}\}$$

$$= \{y_1^{n_1} \cdot y_2^{n_2} \cdot, \ldots, y_r^{n_r} \mid \{y_1, y_2, \ldots, y_r\} \subseteq f(S),\ n_1, \ldots, n_r \in \mathbb{Z},\ r \in \mathbb{N} =< f(S) >\}$$

Proposició
Si $\forall g \in G, gSg^{-1} \subseteq < S > \implies < S > \lhd G$

Demostració. $< S > \triangleleft G \implies g < S > g^{-1} \subseteq S \ \forall g in G$ i $\forall x_i \in S \implies gx_ig^{-1} \in S$. Aleshores

$$gx_i^2g^{-1} = (gx_ig^{-1})(gx_ig^{-1} \in < S > \implies gx_i^{n_i}g^{-1} \in < S > \forall n_i \in \mathbb{Z}$$

i

$$gx_1^{n_1}x_2^{n_2}g^{-1})(gx_1^{n_1}g^{-1})(gx_2^{n_2}g^{-1} \in < S >$$

Conclusió: $gx_1^{n_1} \dots x_r^{n_r}g^{-1} \in < S >$.
Així, $\forall x_1 \dots x_r, \forall n_1 \cdots n_r \implies g < S > g^{-1} \subseteq < S >$ i aleshores $< S > \triangleleft G$.

1.2.6 Producte de grups

Si $(G, \cdot), (G', \cdot')$ són dos grups, el producte cartesià

$$G \times G' = \{(g, g') \mid g \in G, g', \in G'\}$$

li podem donar una estructura de grup definint

$$(g, g') \cdot_p (h, h') \colon = (g \cdot h, g' \cdot h')$$

Proposició
$(G \times G', \cdot_p)$ és un grup amb element neutre (e, e') i l'invers de (g, h) serà (g^{-1}, h^{-1}).

Proposició
Si H_1 i H_2 són subespais de G i es compleix

i) $H_1 \cap H_2 = \{e\}$

ii) $H_1 \cdot H_2 = G$

iii) $h_1h_2 = h_2h_1 \ \forall h_1 \in H_1 \ \forall h_2 \in H_2$

aleshores

$$\begin{aligned} \phi \colon H_1 \times H_2 &\longrightarrow G \\ (h_1, h_2) &\longmapsto h_1h_2 \end{aligned}$$

Demostració. Surt directa de les tres condicions de la hipòtesi.

Definició 17
Si es compleixen les condicions de la proposició anterior anterior, G es dirà producte directe (o intern) de H_1 i H_2.

Proposició
Si G_1 i G_2 són grups cíclics d'ordre n_1 i n_2 respectivament $\implies$ $G_1 \times G_2$ és cíclic $\iff mcd(n_1, n_2) = 1$.

Demostració. $|G_1 \times G_2| = n_1 \cdot n_2$

$\boxed{\Longrightarrow}$: $mcd(n_1, n_2) > 1 \implies$ cap element de $G_1 \times G_2$ tindrà ordre $n_1 n_2 \implies$ $G_1 \times G_2$ no pot ser cíclic.

$\boxed{\Longleftarrow}$: Si $G_1 =< x_1 >$, $G_2 =< x_2 >$ volem veure que $G_1 \times G_2 =< (x_1^\alpha x_2^\alpha) >$.$\alpha \in \mathbb{N}$. $G_1 \times G_2 = \{(x_1^a, x_2^b) \mid a \in \{0, 1, \ldots, n_1 - 1\}, b \in \{0, 1, \ldots, n_2 - 1\}\}$.

$$\left.\begin{array}{l} \alpha \equiv a \bmod n_1 \\ \alpha \equiv b \bmod n_2 \end{array}\right\}$$

Pel teorema xinès del residu, el sistema té solució $\forall a, b$ si $mcd(n_1, n_2) = 1$

1.2.7 Grups definits per generadors i relacions

Sigui G un grup generat pel conjunt finit $S = \{x_1, \ldots, x_n\}$. Una relació entre $x_1, \ldots, x_n$ és una igualtat

$$x_1^{k_1} \cdot c_2^{k_2} \cdot \ldots \cdot c_n^{k_n} = e$$

Si S és un conjunt de generadors del grup G i R un conjunt de relacions entre els elements de S, diem que G està definit pel conjunt S de generadors i el conjunt R de relacions si totes les relacions entre els elements de S es dedueixen de les d'R. Si $G =< S/R >$ podem triar una manera única d'escriure els elements de G i podem escriure el producte d'elements de G en aquesta forma.

1.2.8 Grups resolubles

Un grup finit es diu resoluble si existeix una cadena finita de subgrups

$$\{e\} = G_0 \subset G_1 \subset \ldots \subset G_n = G \text{ (torre de subgrups)}$$

tal que

i) $G_i \triangleleft G_{i+1} \; \forall i \in 0, \ldots, n-1$

ii) ${}^{G_{i+1}}\!/_{G_i}$ és abelià

Si compleix i s'anomena torre normal i si compleix i i ii, s'anomena torre abeliana.

Tot grup abelià és resoluble i $\{e\} \subset G$ és torre abeliana.

Proposició

- *Tot subgrup d'un grup resoluble és resoluble.*
- *Tot quocient d'un grup resoluble per un subgrup normal és resoluble.*
- *Si G és grup i H és subgrup normal, aleshores H i ${}^{G}\!/_{H}$ resolubles $\implies$ G resoluble.*

1.2.9 Grups simples

Un grup G es diu simple si no té subgrups normals diferents de G i $\{e\}$.

Proposició
Un grup no trivial és simple i resoluble $\iff$ *és cíclic d'ordre primer.*

Demostració.

$\boxed{\Longleftarrow}$ G cíclic d'ordre p primer $\implies$ $\{e\}$ i G són els únics subgrups de G $\implies$ G és simple.

$$\left.\begin{array}{l} \{e\} \subset G \text{ torre abeliana} \implies G \text{ resoluble} \\ G \text{ cíclic abelià} \end{array}\right\} \implies G \text{ resoluble}$$

$\boxed{\Longrightarrow}$ Suposem G simple i resoluble $\implies$ $\{e\} \subset G$ única torre abeliana possible per a G $\implies$ G abelià $\implies$ tots els subgrups són normals $\overset{G \text{ simple}}{\implies}$ els únics subgrups de G són $\{e\}$ i G.

$$G \neq \{e\} \implies \exists x \in G, x \neq e \text{ tal que } < x >= G \implies G \text{ cíclic}$$

Si $n = |G|$ no fos primer, per a cada divisor d de n, G tindria un subgrup d'ordre d. Si n no és primer, $\exists d | n, d \neq 1, d \neq n \implies G$ tindria un subgrup $p \neq \{e\}$ i $p \neq G$. CONTRADICCIÓ amb G simple $\implies |G|$ primer.

Proposició
El grup alternat A_n *és simple per a tot* $n \neq 4$.

Demostració. Veure exercici 52.

Corol·lari
El grup simètric S_n, $n \geq 5$, *no és resoluble.*

Demostració. Si S_n fos resoluble, A_n ho seria. Però A_n és simple $\implies$ A_n cíclic d'ordre primer.

$$n \geq 5, |A_n| = \frac{n!}{2} = 3 \cdot 4 \cdot \ldots \cdot n \text{ no és primer: CONTRADICCIÓ}$$

Per tant, S_n, $n \geq 5$ no ésresoluble.

1.2.10 Accions d'un grup sobre un conjunt

Definició 18
Sigui G *un grup,* S *un conjunt. Una aplicació*

$$\begin{aligned} \rho \colon G \times S &\longrightarrow S \\ (g, s) &\longmapsto g \cdot s \end{aligned}$$

és una acció de G *sobre* S *si compleix:*

1) $e \cdot s = s,\ \forall s \in S$

2) $(g \cdot h)s = g(h \cdot s),\ \forall g, h \in G,\ \forall s \in S.$

Si tenim una acció de G en S, donat $g \in G$ fixat,

$$\begin{aligned} \rho_g \colon S &\longrightarrow S \\ s &\longmapsto g \cdot s \end{aligned}$$

és bijectiva amb inversa $\rho_{g^{-1}}$: $(\rho_{g^{-1}}\rho_g)(s) = g^{-1}(gs) \overset{(2)}{=} (g^{-1}g)s = es = s$. També tenim que

$$\begin{aligned} \phi \colon G &\longrightarrow Permutacions(S) \\ g &\longmapsto \rho_g \end{aligned}$$

és morfisme de grups: $\phi(gh) = \rho_{gh} \overset{?}{=} \rho_g \circ \rho_h = \phi(g) \circ \phi(h)$. Efectivament, $\rho_{gh}(s) = (gh)s = g(hs) = \rho_g(hs) = \rho_g(\rho_h(s)) = (\rho_g \circ \rho_h)(s),\ \forall s \in S$.

Si tenim G grup, S subconjunt i un morfisme de grups $\phi \colon G \to Permutacions(S)$, definim

$$\begin{aligned} \rho \colon G \times S &\longrightarrow S \\ (g, s) &\longmapsto \phi(g)(s) \end{aligned}$$

i aleshores ρ és acció de G en S.

Definició 19
Donada una acció ρ d'un grup G sobre un conjunt S, per a $s \in S$ fixat, definim

$$\begin{aligned} G &\longrightarrow S \\ g &\longmapsto g \cdot s \end{aligned}$$

L'imatge d'aquesta aplicació es diu ***òrbita*** *de s. $Gs = \{g \cdot s \mid g \in G\}$. Un punt $s \in S$ es diu fix per l'acció si $Gs = \{s\}$.*

Proposició
Donada una acció ρ de G sobre S, si fixem $s \in S$, $E(s) = \{g \in G \mid g \cdot s = s\}$ és un subgrup de G, que anomenarem ***estabilitzador*** *de s.*

Demostració.

- $e \cdot s = s \implies e \in E(s)$
- $g_1, g_1 \in E(s) \implies (g_1 \cdot g_2) \cdot s = g_1(g_2 \cdot s) = g_1 s = s \implies g_1 \cdot g_2 \in E(s)$.
- $g \in E(s) \implies g \cdot s = g \implies g^{-1}(g \cdot s) = g^{-1} \cdot s \implies g^{-1} \in E(s)$.

Definició 20
Diem que s és un punt fix quan $E(s) = G$.

Proposició
Donat $s \in S$, l'aplicació $G \to S$, $g \mapsto g \cdot s$ indueix una bijecció entre les classes per la dreta de G i $E(s)$ i l'òrbita Gs. Si G és finit, $|G \cdot S| \cdot |E(s)| = |G|$.

Demostració. La imatge de f és Gs. $g_1, g_2 \in G, f(g_1) = f(g_2) \implies g_1 \cdot s = g_2 \cdot s \implies g_2^{-1}(g_1 \cdot s) = f_2^{-1}(g_2 \cdot s) \implies (g_2^{-1}g_1) \cdot s = sg_2^{-1}g_1 \in E(s) \implies g_1 \in g_2E(s)$,.

Definició 21
Definim el nucli d'una acció ρ com el nucli del morfisme ϕ associat.

Equació de les òrbites

Si S és finit, S_0 conjunt de punts fixes

$$|S| = |S_0| + \sum_{i=1}^{r} |O_i|$$

a,b $\{O_1, \ldots, O_r\}$ és el conjunt de les òrbites amb més d'un element. Aleshores

$$|S| = |S_0| + \sum_{i=1}^{r} [G\colon E(x_i)] \text{ amb } x_i \in O_i$$

Sigui G un grup, $G \times G \to G$ l'acció de G sobre G tal que $(g, h) \mapsto ghg^{-1}$ (anomenada acció per conjugació). L'òrbita d'$h \in G$ per aquesta acció s'anomena la classe de conjugació d'h. Aleshores, h és fix $\iff h \in Z(G)$. $E(h) = \{g \in G \mid gh = hg\} = Z_G(h)$ centralitzador de h en G.

Proposició (Equació de les classes)
Si G és grup finit,

$$|G| = |Z_G(G)| + \sum_{i=1}^{r} [G\colon Z_G(x_i)]$$

on $\{x_1, \ldots, x_r\}$ és el conjunt dels representants de classes de conjugació de G amb més d'un element.

Definició 22
Si p és un nombre primer, un p-grup és un grup d'ordre p^r amb $r \geq 1$.

Proposició (Congruència dels punts fixes)
Si G és un p-grup que opera sobre un conjunt finit S,

$$|S| \equiv |S_0| \pmod{p}$$

Proposició
$|S| - |S_0| = \sum_{i=1}^{r} [G\colon E(x_i)]$ *i* $[G\colon E(x_i)] \geq 1$. $[G\colon E(x_i)] \mid |G| = p^r \implies$ $[G\colon E(x_i)]$ *múltiple de* $p \sum_{i=1}^{r} [G\colon E(x_i)]$ *és múltiple de* p.

Corol·lari
Si G és p-grup, $Z(G)$ és no trivial.

Demostració. Considerem l'acció de G sobre G per conjugació:

$$|G| \equiv |Z(G)| \pmod{p}$$

$$\left.\begin{array}{l} |G| \text{ i } |Z(G)| \text{ divisibles per } p \\ |Z(G)| \geq 1 \end{array}\right\} \implies |Z(G)| > 1$$

Si G és grup, H és subgrup

$$\begin{aligned} H \times {}^{G}\!/_{D_H} &\longrightarrow {}^{G}\!/_{D_H} \\ (h, gH) &\longmapsto (hg)H \end{aligned}$$

és acció.

$$\begin{aligned} gH \text{ és fix} &\iff hgH = gH && \forall h \in H \\ &\iff g^{-1}hgH = H && \forall h \in H \\ &\iff g^{-1}hg \in H && \forall h \in H \\ &\iff g \in N_G(H) && \text{normalitzador de H en G} \end{aligned}$$

H subgrup de G, $N_G(H) = \{g \in G \mid gHg^{-1} \subset H\}$ és subgrup de G i aleshores $H \triangleleft N_G(H)$.

Proposició (Congruència del normalitzador)
Si G és p-grup, H subgrup de G, $[N_G(H)\colon H] \equiv [G\colon H] \bmod p$

Demostració. Considerem $H \times {}^{G}\!/_{D_H} \to {}^{G}\!/_{D_H}$. ${}^{G}\!/_{D_H}$ té cardinal $[G\colon H]$, i el cardinal dels punts fixes és $[N_G(H)\colon H]$.

Teorema (Teorema de Cauchy)
Sigui G un grup finit d'ordre n i p un nombre primer que divideix a n. Aleshores G té un element d'ordre p (que genera un subgrup d'ordre p).

Demostració. Sigui $S = \{(x_1, \ldots, x_p) \in G \times \overset{(p)}{\ldots} \times G \mid x_1 x_2 \ldots x_p = e\}$ i

$$\begin{aligned} {}^{\mathbb{Z}}\!/_{p\mathbb{Z}} \times S &\longrightarrow S \\ (k, (x_1, \ldots, x_p)) &\longmapsto (x_{k+1}, \ldots, x_{k+p}) \end{aligned}$$

amb els índex de les x mòdul p. Aleshores el conjunt dels punts fixes $S_0 = \{(x, \ldots, x) \mid x^p = e\} = x \in G \mid x^p = e$. Com que $|S| = n^{p-1}$ és divisible per p, per la congruència de punts fixes, , el cardinal del conjunt S_0 de punts fixes és divisible per p, de manera que $|S_0| > 1$. Aleshores, $\exists x \in G,\ x \neq e$ amb $x^p = e$.

1.2.11 Teoremes de Sylow

Definició 23
Sigui G un grup finit i p un enter primer que divideix $|G|$. Els subgrups de G amb ordre la màxima potència de p que divideix G es diuen p-subgrups de Sylow de G.

Teorema (Primer teorema de Sylow)
Sigui G un grup finit, p un nombre primer tal que p^r divideix $|G|$ per a algun enter $r > 0$. Aleshores existeixen subgrups $H_1, H_2, \ldots, H_r$ de G tals que $|H_i| = p^i,\ 1 \leq i \leq r,\ H_i \triangleleft H_{i+1},\ 1 \leq i \leq r-1$.

Corol·lari
Si G és subgrup finit, p primer tal que $p \mid |G|$, aleshores existeixen p subgrups de Sylow de G.

Corol·lari
Tot p-grup és resoluble.

Demostració. Tenim $|G| = p^r$ amb $r \geq 1$. Aleshores $\{e\} \subset H_1 \subset \ldots \subset H_r = G$ és torre normal i $|{}^{H_{i+1}}\!/_{H_i}| = \frac{p^{i+1}}{p^i} = p \implies {}^{H_{i+1}}\!/_{H_i}$ és cíclic $\implies {}^{H_{i+1}}\!/_{H_i}$ és abelià.

Demostració. Demostració del primer teorema de Sylow

Teorema (Segon teorema de Sylow)
Sigui G un grup finit, H un p-subgrup de G i S un p-subgrup de Sylow de G. Aleshores existeix $x \in G$ tal que $H \subset xSx^{-1}$. En particular, dos p-subgrups de Sylow de G són conjugats.

Demostració. Demostració del segon teorema de Sylow

Corol·lari
G té un únic p-subgrup de Sylow $S \iff G$ té un p-subgrup de Sylow normal.

Teorema (Tercer teorema de Sylow)
Sigui G un grup finit i p primer dividint $|G|$. Sigui n_p el nombre de p-subgrups de Sylow de G. Aleshores es compleix:

1. *$n_p = [G\colon N_G(S_p)]$ per a tot S_p p-subgrup de Sylow de G.*
2. *$n_p \mid [G\colon S_p]$ per a tot p-subgrup de Sylow S_p de G.*
3. *$n_p \equiv 1 \pmod{p}$*

Demostració. Demostració del tercer teorema de Sylow

1.3 Grups abelians finitament generats

A partir d'ara tractarem amb grups abelians amb l'operació suma.

Definició 24
Sigui $(A,+)$ un grup abelià. Sigui $n \in \mathbb{Z}$, $a \in A$. Definim

$$na = \begin{cases} a + \overset{n}{\ldots} + a & n > 0 \\ 0 & n = 0 \\ -(a + \overset{n}{\ldots} + a) & n < 0 \end{cases}$$

Definició 25
Si $\cdot e_1, \ldots, e_r$ són elements de $(A,+)$, diem que són $\mathbb{Z}$-linealment independents si $n_1e_1, \ldots, n_re_r = 0 n_1 = \ldots = n_r = 0$, amb $n_1, \ldots, n_r \in \mathbb{Z}$. Diem que $(e_1, \ldots, e_r)$ és base de A si són linealment independents i generen A.

Proposició
Si $e_1, \ldots, e_r$ és base de A, tot element d'A s'escriu en la forma $n_1e_1 + \ldots + n_re_r$, amb $n_1, \ldots, n_r$ únics.

Definició 26
Un grup abelià finitament generat es diu lliure si és isomorf a $\mathbb{Z} \times \overset{r}{\ldots} \times \mathbb{Z}$ amb la suma definida per $(a_1, \ldots, a_r) + (b_1, \ldots, b_r) = (a_1 + b_1, \ldots, a_r + b_r)$ (suma terme a terme) $(\mathbb{Z} \oplus \overset{r}{\ldots} \oplus \mathbb{Z})$.

Proposició
Un grup abelià finitament generat és lliure si i només si té una base.

Demostració. A $\mathbb{Z} \oplus \overset{n}{\ldots} \oplus \mathbb{Z}$, $e_1 = (1,0,\ldots,0), e_2 = (0,1,\ldots,0), \ldots, e_r = (0,0,\ldots,1)$ és base. Aleshores si considerem $\varphi\colon \mathbb{Z} \oplus \overset{n}{\ldots} \oplus \mathbb{Z} \xrightarrow{\sim} A$, tenim que $(\varphi(e_1), \ldots, \varphi(e_r))$ és base de A. Si $(v_1, \ldots, v_r)$ és base d'A,

$$\begin{aligned} \mathbb{Z} \oplus \overset{n}{\ldots} \oplus \mathbb{Z} &\longrightarrow A \\ n_1e_1 + \ldots + n_re_r &\longmapsto n_1v_1 + \ldots + n_rv_r \end{aligned}$$

és morfisme.

Proposició
Ai un grup abelià A té una base de r elements, totes les bases de A tenen r elements.

Definició 27
Tots els elements d'ordre finit d'un grup abelià A s'anomenen també elements de torsió i formen un subgrup d'A que anomenem subgrup de torsió d'A, i l'escribim com $F(A)$. Diem que A és lliure de torsió si $F(A) = \{0\}$.

Subgrup de torsió és subgrup.

- a, b de torsió $\implies na = 0,\ mb = 0 nm(a + b) = 0$
- a de torsió $\implies na = 0 \implies n(-a) = 0$

Proposició
A es lliure de torsió $\iff$ A és lliure

Proposició
Tot grup abelià finitament generat és suma directa d'un grup abelià lliure i d'un grup finit.

1.3.1 Estructura dels grups abelians finits

Si A és un grup abelià finit, existeixen un nombre natural s i enters natural $d_1, d_2, \ldots, d_s$ amb $d_j \mid d_{j+1}$, $1 \leq j \leq s-1$ tal que $A = F_1 \oplus F_2 \oplus \ldots \oplus F_s$, amb F_j grup cíclic d'ordre d_j, $1 \leq j \leq s$. Per tant, $|A| = d_1 \times d_2 \times \ldots \times d_s$. $d_1, d_2, \ldots, d_s$ es diuen factors invariants del grup A.

Proposició
Sigui A un grup abelià finit, $|A| = p_1^{k_1} \ldots p_l^{k_l}$, amb $p_1, \ldots, p_l$ nombres primers diferents dos a dos. Aleshores existeixen enters positius s_i, $1 \leq i \leq l$, i $k_{i1} \geq k_{i2} \geq \ldots \geq k_{is_i}$ tals que

$$A = \bigoplus_{i=1}^{l} \Big(\bigoplus_{1 \leq j \leq s_i} F_{ij} \Big)$$

on F_{ij} és grup cíclic d'ordre $p_i^{k_{ij}}$. A més, $p_1, \ldots, p_l$ i els seus exponents k_{ij} estan determinats per A. Els enters $p_i^{k_{ij}}$ es diuen divisors elementals de A.

Capítol 2

Anells

2.1 Definicions

Definició 28
Un anell és un conjunt A amb dues operacions:

1. *Una operació $+$ binària i interna tal que $(A,+)$ és un grup abelià.*
2. *Una operació que escrivim com a producte, binària i interna, complint:*
   - *És associativa: $(ab)c = a(bc)$, $\forall a,b,c \in A$*
   - *És distributiva respecte la suma: $a(b+c) = ab+ac$ i $(b+c)a = ba+ca$, $\forall a,b,c \in A$*

Si el producte és commutatiu, direm que A és anell commutatiu. Si existeix element neutre pel producte de A, diem que A és anell unitari. Posem per 1 l'element neutre del producte en A.

Proposició
Ai A és anell, $a0 = 0$, $0a = 0$, $\forall a \in A$.

Demostració. $a0 + a0 = a(0+0) = a0 \implies a0 = 0$

Definició 29
Donat un anell A, un subanell de A és un subconjunt B d'A tal que:

1. *$(B,+)$ és subgrup d'$(A,+)$*
2. *$b_1, b_2 \in B \implies b_1 b_2 \in B$, $\forall b_1, b_2 \in A$*

Si B és un subanell de A, aleshores B és anell amb les operacions d'A. Si A és unitari, diem subanell de A un subanell que contingui 1.

Definició 30
Un element d'un anell A, $a \neq 0$, s'anomena divisor de zero si $\exists b \in A$: $ba = 0$.

Definició 31
Un anell A es diu domini d'integritat si no té divisors de zero.

A domini d'integritat $\iff [ab = 0 \implies a = 0 \vee b = 0] \iff [a \neq 0 \wedge b \neq 0 \implies ab \neq 0]$. Si A és domini d'integritat, $ab = ac \wedge a \neq 0 b = c$.

A partir d'ara, si no s'indica el contrari, suposarem tots els anells commutatius i unitaris

Definició 32
Un element d'un anell A és invertible si $\exists b \in A \mid ab = 1$. Diem que b és l'invers de a. Escrivim per A^* el conjunt dels elements invertibles de A. A^* amb el producte d'A és un grup.

Definició 33
UN cos és una anell no trivial en què tot element no nul és invertible. Aleshores, si K és un cos, $K^* = K \setminus \{0\}$.

Proposició
Si un element a d'un anell A és invertible, aleshores no és divisor de zero. En particular, tot cos és domini d'integritat.

Demostració. $ab = 0 \implies a^{-1}(ab) = a^{-1}0 = 0$, i $a^{-1}(ab) = b$, de manera que l'única possibilitat és que $b = 0$.

Proposició
Ai A és domini d'integritat, $A[x]$ és domini d'integritat.

Demostració. $P(x), Q(x) \in A[x]$ no nuls:

$$P(x) = a_n x^n + a_{n-1}x^{n-1} + \dots \text{ amb } a_n \neq 0$$
$$Q(x) = b_m x^m + b_{m-1}x^{m-1} + \dots \text{ amb } b_m \neq 0$$

Aleshores $P(x)Q(x) = a_n b_m x^{n+m} +$ sumands de grau $< n + m$, amb $a_n b_m \neq 0$. A més, $gr(PQ) = gr(P) + gr(Q)$.

Definició 34
Donat un anell A, un ideal de A és un subconjunt I de A que compleix:

1. *$(I, +)$ és subgrup de $(A, +)$*
2. *$\forall x \in I$, $\forall a \in A$, $ax \in I$*

Proposició
Tot ideal de $\mathbb{Z}$ és (m) per a algun m enter ≥ 0.

Demostració. I ideal de $\mathbb{Z} \implies (I, +)$ és subgrup de $(\mathbb{Z}, +)$, i com que tot subgrup de $\mathbb{Z}$ és isomorf a $m\mathbb{Z}$, aleshores $I = (m)$ i (m) és ideal.

Un anell d'ideals principals és un anell tots els ideals dels qual són principals. Un domini d'ideals principals (DIP) és un domini d'integritat que és anell d'ideals principals.

Proposició
Si K és un cos, $K[x]$ és domini d'ideals principals.

Demostració. Tenim que K cos $\implies$ K domini d'integritat $\implies$ $K[x]$ domini d'integritat. Sigui I ideal de $K[x]$. Si $I = 0 = (0)$. Si $I \neq 0 \implies I$ conté polinomis no nuls, és a dir, de graus > 0. Sigui P un polinomi de grau mínim entre els elements no nuls de I. Sigui $Q \in I$, fem divisió de Q entre P: $Q = PC + R$ amb $R = 0$ o $gr(R) < gr(P)$. $\implies R = Q - PC \in I$. Si $R \neq 0, gr(R) < gr(P)$ contradiu P de grau mínim. $R = 0 \implies Q = PC \in (P)$. Hem provat $I \subset (P)$. En l'altra direcció, simplement tenim que $P \in I \implies (P) \subset I$.

Definició 35
Si A anell, $a, b \in A$, diem que a divideix b, $a \mid b$, si $\exists c \in A \mid b = ac$. Tenim $a \mid b \iff b \in (a)$.

Operacions amb ideals

Si A és anell, $\{I_j\}_{j\in J}$ família d'ideals de A, $\bigcap_{j\in J} I_j$ és ideal de A. Si S és subconjunt de l'anell A, diem ideal generat per S a la intersecció de tots els ideals de A que contenen S. L'escribim (S). Si $S =, (S) = \{0\}$.

Proposició
Si S és un subconjunt no buit de l'anell A,

$$(S) = \{b_1a_1 + b_2a_2 + \cdots + a_rb_r \mid a_1, \ldots, a_r \in S,\ b_1, \ldots, b_r \in A,\ r \in \mathbb{N}\}$$

Donats I, J ideals de A, $I + J = \{x + y \mid x \in I, y \in J\}$ és ideal de A generat per $I \cup J$. S'anomena ideal sima de I i J. Si $\{I_j\}_{j\in J}$ és un conjunt d'ideals de A, l'ideal suma $\sum_{j\in J} I_j$ és l'ideal generat per $\bigcup_{j\in J} I_j$

Proposició
Si $\{I_j\}_{j\in J}$ és conjunt d'ideals de A,

$$\sum_{j\in J} I_j = \{a_1 + \ldots + a_k \mid k \in \mathbb{N},\ j_1, \ldots, j_k \in J,\ a_l \in I_l\}$$

Si I, J són ideals de l'anell A, IJ és l'anell generat per $\{xy \mid x \in I,\ y \in J\}$. Tenim

$$IJ = \{x_1y_1 + \ldots + x_ky_k \mid k \in \mathbb{N},\ x_i \in I,\ y_i \in J,\ 1 \leq i \leq k\}$$

Si $I_1, \ldots I_r$ són ideals de A, $I_1 \ldots I_r$ és l'ideal generat per $\{x_1 \cdot \cdots \cdot x_r \mid x_i \in I_i,\ 1 \leq i \leq r\}$. Tenim

$$I_1 \ldots I_r = \{x_1^1 \ldots x_r^1 + x_1^2 \ldots x_r^2 + \ldots + x_1^k \ldots x_r^k \mid k \in \mathbb{N},\ x_i^j \in I_i,\ 1 \leq i \leq r,\ 1 \leq j \leq k\}$$

Sempre tenim que, si I, J ideals, $IJ \subset I \cap J$, que $I^2, I^3, \ldots$ ideals i que $I \supset I^2 \supset I^3 \ldots$.

Anel quocient

Si I és ideal de A, $(I,+)$ és subgrup de $(A,+)$ i és commutatiu (tot subgrup és normal, ja que és $(A,+)$ abelià (?)). Tenim que ${}^{A}/_{I}$ té estructura de grup amb la suma definida per

$$[a]+[b]=[a+b]$$

Definim el producte a ${}^{A}/_{I}$ per

$$[a][b]=[ab]$$

Vegem que està ben definit:

$$[a']=[a] \implies a'=a+x,\ x\in I$$

$$[b']=[b] \implies b'=b+y,\ y\in I$$

$$a'b'=(a+x)(b+y)=ab+xb+ay+xy \implies [a'b']=[ab]$$

ja que $xb, ay, xy \in I$ i aleshores la seva suma també.

El producte és associatiu, distributiu respecte la suma , commutatiu i l'element unitat és [1]. ${}^{A}/_{I}$ amb la suma i el producte definits es diu anell quocient de l'anell A per l'ideal I

Morfismes d'anells

Si A,B són anells, una aplicació $f\colon A\to B$ és morfisme d'anells si compleix:

1. $f(a+a')=f(a)+f(a')$, $\forall a,a'\in A$
2. $f(aa')=f(a)f(a')$, $\forall a,a'\in A$
3. $f(1_A)=1_B$

Si $f\colon A\to B$ és morfisme, $Ker(f)=\{a\in A \mid f(a)=0_B\}$ i $Ker(f)=\{0\} \iff f$ injectiva. f morfisme d'anells $\implies f(0_A)=0_B$ i $f(-a)=-f(a)$. Si $a\in A$ és invertible $\implies aa^{-1}=1_A \implies f(a)f(a^{-1})=f(1_A)=f(1_B) \implies f(a)$ invertible i $f(a)^{-1}=f(a^{-1})$.

Proposició
A anell, I ideal de A,

$$\begin{aligned}\pi\colon A &\longrightarrow {}^{A}/_{I}\\ a &\longmapsto [a]\end{aligned}$$

és morfisme d'anells.

Proposició
Si $f\colon A\to B$ és morfisme d'anells, $Ker(f)$ és ideal de A i $Im(f)$ és subanell de B.

Demostració. $a \in A$, $x \in Ker f$, $f(ax) = f(a)f(x) = f(a)0_B = 0_B \implies ax \in Ker f$. $b, b' \in Im f \implies b = f(a)$, $b' = f(a') \implies bb' = f(a)f(a') = f(aa') \in Im f$.

Definició 36
Si $f\colon A \to B$ morfisme d'anells, I ideal de A, diem que f factoritza a través de ${}^{A}/_{I}$ si $\exists \bar{f}\colon {}^{A}/_{I} \to B$ morfisme d'anells tal que $f = \bar{f} \circ \pi$, on $\pi\colon A \to {}^{A}/_{I}$

(Afegir diagrama commutatiu)

Proposició
f factoritza a través de ${}^{A}/_{I} \iff I \subset Ker f$

Demostració. Sabem que si $I \subset Ker f$, existeix $\bar{f}\colon {}^{A}/_{I} \to B$ morfisme de $({}^{A}/_{I}, +)$ en $(B, +)$ tal que $f = \bar{f} \circ \pi$. A més $\bar{f}([a]) = f(a)$. Queda veure que $\bar{f}$ és morfisme d'anells:

$$\bar{f}([a][a']) = \bar{f}([aa']) = f(aa') = f(a)f(a') = \bar{f}([a])\bar{f}([a])$$

$$\bar{f}([1]) = f(1) = 1$$

Si existeix $\bar{f}$ tal que $f = \bar{f} \circ \pi$, aleshores $I \subset Ker f$.

Teorema (Teorema d'isomorfia)
Si $f\colon A \to B$ és morfisme d'anells, aleshores f factoritza a través de ${}^{A}/_{Ker f}$ i tenim $f = i \circ \tilde{f} \circ \pi$, (Afegir diagrama) on $\pi\colon A \to {}^{A}/_{Ker f}$ morfisme de pas al quocient, $\tilde{f}\colon {}^{A}/_{Ker f} \to Im f$ és isomorfisme i $i\colon Im f \to B$ és la inclusió.

Demostració. $\bar{f}$ injectiu: $\bar{f}([a]) = 0 \implies f(a) = 0 \implies a \in Ker f \implies [a] = [0]$. $f([a]) = \bar{f}([a])$. $\bar{f}([a]) = f(a) \implies Im\bar{f} = Im f \implies \tilde{f}$ exhaustiva.

Definició 37
Sigui A un anell. Un ideal primer de A és un ideal propi I de A tal que si $a, b \in A$, $ab = I \implies a \in I$ o bé $b \in I$.

Proposició
I ideal pirmer de $A \iff {}^{A}/_{I}$ és domini d'integritat.

Demostració. $a \in I \iff [a] = [0] \in {}^{A}/_{I}$

Definició 38
Sigui A un anell. Un ideal maximal de A és un ideal I de A propi tal que si J és ideal de A, $I \subset J \subset A \implies J = I$ o $J = A$. De manera equivalent, si no existeix J ideal de A amb IJA

Proposició
Sigui I un ideal propi de A. Aleshores, I és maximal $\iff {}^{A}/_{I}$ és cos.

Demostració. $\boxed{\Longrightarrow}$ $[a] \neq [0] \in {}^{A}/_{I} \implies a \notin I \implies II + (a) \implies I + (a) = A \implies 1 \in I + (a) \implies 1 = x + ya$, amb $x \in I$, $y \in A \implies [1] = [y][a] \implies [a]$ invertible $\implies {}^{A}/_{I}$ és cos.

$\boxed{\Longleftarrow}$ Si ${}^{A}/_{I}$ és cos, sigui J ideal de A amb $IJ \subset A$. Com que IJ, $\exists a \in J \backslash I \implies [a] \neq [0] \implies \exists [b] \in {}^{A}/_{I}$ tal que $[a][b] = [1] \implies ab - 1 = x$ per a alguna $x \in I \implies 1 = ab - x \in J$, ja que $ab \in J$, $x \in I \subset J$. Si $z \in A$, $z = z \cdot 1 \in J$. Per tant, $A \subset J \implies A = J$ i, aleshores, I és maximal.

Proposició
Tot ideal maximal és primer.

Demostració. I maximal $\implies {}^{A}/_{I}$ és cos $\implies {}^{A}/_{I}$ domini d'integritat $\implies I$ és primer.

Definició 39
Sigui S un conjunt ordenat.Diem que un element $a \in S$ es diu màxim si $a \geq x$ $\forall x \in S$ i mínim si $a \leq x$ $\forall x \in S$. Si existeix mínim és únic, anàlogament amb màxim. Un element m es diu maximal si $\forall x \in S$, $m \leq x \implies x = m$, i minimal si $\forall x \in S$, $m \geq x \implies x = m$.

Si S és un conjunt ordenat i T un subconjunt, una cota superior de T en S és un element b de S tal que $x \leq x$ $\forall x \in T$.

Direm que S està ordenat inductivament si tot subconjunt de S totalment ordenat té cota superior.

Lema (Lema de Zorn)
Sigui S un conjunt no buit ordenat inductivament. Aleshores existeix un element maximal de a S.

Demostració. $S = \{J \mid J \text{ ideal propi de } A \wedge I \subset J\}$ ordenat amb la inclusió. $I \in S \implies S \neq$. Sigui T un subconjunt totalment ordenat de S, $M = \bigcup_{J \in T} J$. M ideal, $a, b \in M \implies a \in J_1, b \in J_2$ per a alguns $J_1, J_2 \in T$.

$$T \text{ totalment ordenat} \implies \begin{cases} J_1 \subset J_2 \implies a, b \in J_2 \implies a + b \in J_2 \subset M \\ J_2 \subset J_1 \implies a, b \in J_1 \implies a + b \in J_1 \subset M \end{cases}$$

$a \in M, b \in A \implies A \in J$ per a algun $J \in T \implies ba \in J \subset M$ Amb aquestes dues afirmacions, podem veure que M és ideal de A i $I \subset M$.

Ara cal veure si M és ideal propi: Si $M = A \implies 1 \in J$ per a algun $J \in T \implies a \in A \implies a = a \cdot 1 \in J \implies J = A$ contradicció.

I si $M \in S$ i és cota superior de T: Pel lema de Zorn, S té element maximal. Per tant, A té algun ideal maximal M.

Corol·lari
Tot anell té almenys un ideal maximal.

Demostració. Ideal propi $I = (0)$.

Cos de fraccions d'un domini

A domini, $A \times (A \setminus \{0\}) = \{(a,b) \mid a,b \in A, b \neq 0\}$. Definim la relació d'equivalència $\sim$ en $A \times (A \setminus \{0\})$ com

$$(a,b) \sim (c,d) \iff ad = bc \qquad (\frac{a}{b} = \frac{c}{d} \iff ad = bc)$$

Comprovem que és relació d'equivalència:

Reflexiva: $(a,b) \sim (a,b) \iff ab = ab$

Simètrica: si $(a,b) \sim (c,d) \iff ad = bc \iff da = cb \iff (c,d) \sim (a,b)$

Transitiva: Si $c \neq 0$

$$\begin{cases} (a,b) \sim (c,d) \\ (c,d) \sim (e,f) \end{cases} \iff \begin{cases} ad = bc \\ cf = de \end{cases} \implies adcf = bcde \implies acf = bce \implies af = be \implies (a,b) \sim (e,f)$$

Si $c = 0$,

$$\left.\begin{array}{l} ad = bc = 0 \implies a = 0 \\ cb = de = 0 \implies d = 0 \end{array}\right\} \implies af = be = 0$$

Aquesta relació indueix particions en $A \times (A \setminus \{0\})$: $K(A) = {}^{A \times (A \setminus \{0\})}/_{\sim} = \{[(a,b)], a,b \in A, b \neq 0\}$

Definició 40
$\frac{a}{b} = [(a,b)] = \{(c,d) \mid d \neq 0, ad = bc\}$

Aleshores $K(A)\{\frac{a}{b} : a \in A, b \in A \setminus \{0\}\}$ Definim una suma i un producte en $K(A)$ de la següent manera:

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

i

$$\frac{a}{b} \cdot_k \frac{c}{d} = \frac{ac}{bd}$$

Comprovem que estan ben definides: Tenim $\frac{a}{b} = \frac{a'}{b'}$ i $\frac{c}{d} = \frac{c'}{d'} \implies ab' = a'b$ i $cd' = c'd$.
Aleshores $\frac{ad+bc}{bd} = \frac{a'd'+b'c'}{b'd'} \iff (ad + bc)b'd' = (a'd' + b'c')bd \iff adb'd' + bcb'd' = a'd'bd + b'c'bd \iff a'vdd' + bc'b'd = a'd'bd + b'c'bd$. I, partint del mateix, $\frac{ac}{bd} = \frac{a'c'}{b'd'} \iff acb'd' = a'c'bd \iff a'bc'd = a'c'bd$

Proposició
$(k(A), +_k, \cdot_k)$ és in cos

Demostració.

- $+_k$ i $\cdot_k$ són operacions internes

Neutre $\frac{0}{1}$: $\frac{a}{b} + \frac{0}{1} = \frac{a \cdot 1 + 0 \cdot b}{b \cdot 1} = \frac{a}{b}$

Oposat $\frac{-a}{b}$ o $\frac{a}{-b}$: $\frac{a}{b}+\left(\frac{-a}{b}\right)=\frac{ab+(-a)b}{b\cdot b}=\frac{0}{b^2}=\frac{0}{1}$

Neutre del producte $\frac{1}{1}=\frac{b}{b}$ amb $b\neq 0$

Commutativitat :

1. $\frac{a}{b}+_k\frac{c}{d}=\frac{c}{d}+_k\frac{a}{b}$
2. $\frac{a}{b}\cdot_k\frac{c}{d}=\frac{c}{d}\cdot_k\frac{a}{b}$

Associativitat : $\left(\frac{a}{b}+_k\frac{c}{d}\right)\cdot_k\frac{e}{f}=\frac{ad+bc}{bd}\cdot_k\frac{e}{f}=\frac{ade+bce}{bdf}=\frac{ade}{bdf}+_k\frac{bce}{bdf}=\frac{ae}{bf}+_k\frac{ce}{df}=\frac{a}{b}\cdot\frac{e}{f}+\frac{c}{e}\cdot\frac{e}{f}$

Tenim que és anell commutatiu. Vegem que tot $\frac{a}{b}\neq\frac{0}{1}$ té inversa en $k(A)$:$\frac{a}{b}\cdot\frac{b}{a}=\frac{1}{1}$.

Proposició

$$f\colon A\longrightarrow k(A)$$
$$a\longmapsto\frac{a}{1}$$

és morfisme d'anells.

Demostració. Hem de veure:

$\boxed{f(a+b)=f(a)+_k f(b)}$: $f(a+b)=\frac{a+b}{1}=\frac{a1+b1}{1\cdot 1}=\frac{a}{1}+_k\frac{b}{1}=f(a)+_k f(b)$

$\boxed{f(ab)=f(a)\cdot f(b)}$: $f(ab)=\frac{ab}{1}=\frac{a\cdot b}{1\cdot 1}=f(a)\cdot_k f(b)$

$\boxed{f(1)=\frac{1}{1}}$: Evident

i que f és monomorfisme (injectiva) $\iff$ $ker(f)=\{0\}$: $a\in Ker(f)\implies f(a)=\frac{a}{1}=\frac{0}{1}$ i $\frac{a}{1}=\frac{0}{1}\iff a\cdot 1=0\cdot 1\implies a=0$

Teorema
*Suposem que $g\colon A\to L$ un morfisme d'anells, L un cos. Aleshores existeix $\tilde{g}\colon k(A)\to L$ morfisme d'anells tal que $g=\tilde{g}\circ f$, amb la f definida a la proposició anterior. (**Afegir diagrama commutatiu**)*

Demostració. Tenim que

$$\tilde{g}\left(\frac{a}{b}\right)=\tilde{g}\left(\frac{a}{1}\cdot\frac{1}{b}\right)=\tilde{g}\left(\frac{a}{1}\right)\cdot\tilde{g}\left(\frac{1}{b}\right)$$

$$\tilde{g}\left(\frac{a}{1}\right)=(\tilde{g}\circ f)(a)=g(a)$$

$$\tilde{g}\left(\frac{1}{b}\right)=\tilde{g}\left(\left(\frac{b}{1}\right)^{-1}\right)=\left(\tilde{g}\left(\frac{b}{1}\right)\right)^{-1}=(g(b))^{-1}$$

De manera que podem definir

$$\tilde{g}\left(\frac{a}{b}\right) = g(a) \cdot g(b)^1$$

Amb aquesta definició, tenim que $\tilde{g} \circ f = g$. Vegem ara que $\tilde{g}\colon k(A) \to L$ és morfisme d'anells:

1. $\tilde{g}\left(\frac{a}{b} +_k \frac{c}{d}\right) = \tilde{g}\left(\frac{a}{b}\right) + \tilde{g}\left(\frac{c}{d}\right)$ i
   $\tilde{g}\left(\frac{a}{b} +_k \frac{c}{d}\right) = \tilde{g}\left(\frac{ad+bc}{bd}\right) = g(ad+bc) \times g(b)^{-1} \times g(d)^{-1} = g(a)g(d)g(b)^{-1}g(d)^{-1} +$
   $g(b)g(c)g(b)^{-1}g(d)^{-1} = \tilde{g}\left(\frac{a}{b}\right) + \tilde{g}\left(\frac{c}{d}\right)$

2. $\tilde{g}\left(\frac{a}{b} \cdot_k \frac{c}{d}\right) = \tilde{g}\left(\frac{a}{b}\right) \cdot \tilde{g}\left(\frac{c}{d}\right)$ i
   $\tilde{g}\left(\frac{a}{b} \cdot_k \frac{c}{d}\right) = \tilde{g}\left(\frac{ac}{bd}\right) = g(ac)g(bd)^{-1} = g(a)g(c)g(b)^{-1}g(d)^{-1} = (g(a)g(b)^{-1})(g(c)g(d)^{-1}) =$
   $\tilde{g}\left(\frac{a}{b}\right) \cdot \tilde{g}\left(\frac{c}{d}\right)$

3. $\tilde{g}\left(\frac{1}{1}\right) = \tilde{g}(f(1)) = g(1) = 1_L$ (Última igualtat deguda a morfisme d'anells).

Factorialitat

Definició 41
*Dos elements a, b d'un anell A es diuen **associats** si $b = ua$ amb u un element invertible de A. Si això passa, diem que $a \sim b$.*

Proposició
Sigui A un anell, $a, b \in A$. Tenim que $a \sim b \implies a \mid b \wedge b \mid a$. Si a o b no són divisors de 0, aleshores $a \mid b \wedge b \mid a \implies a \mid b$.

Demostració. Suposem que a no és divisor de zero.

$$\left.\begin{array}{l} a \mid b \implies b = ac \\ b \mid a \implies a = bd \end{array}\right\} \implies a = acd \implies a(1-cd) = 0 \implies 1 - cd = 0 \implies cd = 1$$

$$\implies c, d \text{ invertibles} \implies a \sim b$$

Si $a \in A$, els elements invertibles de A i els associats de a són divisors de a ($u \in A^* \implies a = u(u^{-1}a),\ a = u^{-1}(ua)$). Un divisor propi de A és un divisor de a que no és invertible ni associat de a.

Definició 42
Un element a d'un anell A, no nul i no invertible, es diu irreductible si no té divisors propis. Si a no és irreductible, es diu compost.

Definició 43
1. *Siguin $a, b, d \in A$. Direm que d és el màxim comú divisor de a i b si:*

   (a) $d \mid a$ i $d \mid b$.

(b) Si $c \in A$ tal que $c \mid a$ i $c \mid b$. aleshores $c \mid d$.

2. *Sigui $a, b, m \in A$. Direm que m és el mínim cimú múltiple de a i b si:*

   (a) $a \mid m$ i $b \mid m$.

   (b) Si $c \in A$ tal que $a \mid c$ i $b \mid c$, aleshores $m \mid c$.

Si A és domini d'integritat, el màxim comú divisor i el mínim comú múltiple de dos elements són únics tret d'associats.

Dominis Euclidians

Definició 44

Sigui A domini d'integritat. Direm que A és domini euclidià si existeix una aplicació $\delta\colon A \setminus \{0\} \to \mathbb{N}$ tal que

1. *Si $a, b \in A \setminus \{0\}$ i $a \mid b \implies \delta(a) \leq \delta(b)$*

(Divisió entera respecte δ) Si $a, b \in A$, $b \neq 0$, $q, r \in A$ tal que $a = bq + r$ amb $r = 0$ o bé $\delta(r) < \delta(b)$

(A, δ) és domini euclidià.

Proposició

Sigui (A, δ) un domini euclidià. Siguin $a, b \in A \setminus \{0\}$

1. *$a \sim b \implies \delta(a) = \delta(b)$*

2. *Si $a \mid b$ i $\delta(a) = \delta(b)$, aleshores $a \sim b$*

Demostració. 1. $a \sim b \implies a \mid b$ i $b \mid a \implies \delta(a) \leq \delta(b)$ i $\delta(b) \leq \delta(a) \implies \delta(a) = \delta(b)$.

2. Fem la divisió de a entre b, $a = bq + r$ amb $\delta(r) < \delta(b)$ si $r \neq 0$
   a $\mid b \implies b = aa' \implies r = a - bq = a - aa'q = a(1 - a'q) \implies a \mid r \implies \delta(a) < \delta(b)$, que es contradiu amb $\delta(a) = \delta(b)$. Tenim, doncs, $r = 0$ i
   $\left.\begin{array}{l} b \mid a \\ a \mid b \end{array}\right\} \implies a \sim b.$

Corol·lari

Un element $a \in A \setminus \{0\}$ és invertible $\iff \delta(a) = \delta(1)$.

Demostració.

$\boxed{\implies}$: a invertible $\implies a \mid 1 \overset{(1)}{\implies} \delta(a) = \delta(1)$.

$\boxed{\impliedby}$: $\delta(a) = \delta(1)$ i $1 \mid a \overset{(2)}{\implies} a \mid 1 \implies a$ és invertible.

Proposició

Tot domini euclidià és un domini d'ideals principals.

Demostració. Sigui (A, δ) un domini euclidià, I un ideal de A. Si $I = 0 = (0)$. Si $I \neq 0$, sigui $b \in I \setminus \{0\}$ amb $\delta(b)$ mínim entre els valors de δ a $I \setminus \{0\}$. Volem veure que $I = (b)$. La primera inclusió és immediata: $b \in I \implies (b) \subset I$. Vegem la inclusió en l'altre sentit:
Sigui $a \in I$. $\exists q, r \in A$ tal que $a = bq + r$, amb $\delta(r) < \delta(b)$ si $r \neq 0$. Aleshores $r = a - bq \in I$. Si $r \neq 0$, llavors $\delta(r) < \delta(b)$ CONTRADICCIÓ!!! Per tant, $r = 0$, $a = bq \in (b)$ i tenim doncs que $I \subset (b)$.

Normes

Definició 45
Sigui A un anell. Una norma és una aplicació $N\colon A \to \mathbb{Z}$ que compleix:

1. *Si $a \in A$, $N(a) = 0 \iff a = 0$.*
2. *Si $a, b \in A$, $N(ab) = N(a)N(b)$*

Proposició
Si un anell A té norma N, aleshores:

1. *A és domini d'integritat.*
2. *$\delta\colon A \setminus \{0\} \to \mathbb{N}$ definida per $\delta(a) = |N(A)|$ compleix les propietats de l'aplicació δ de la definició de domini euclidià.*
3. *$N(1) = 1$.*
4. *$u \in A^* \implies N(u) = \pm 1$*

Demostració.
1. $ab = 0 \implies N(a)N(b) = N(ab) = N(0) = 0 \implies N(a) = 0 \vee N(b) = 0 \implies a = 0 \vee b = 0 \implies$ és domini d'integritat.
2. $a \mid b \implies b = ac \implies |N(b)| = |N(a)||N(c)|$ amb $|N(c)| \geq 1 \implies |N(a)| \leq |N(b)| \implies \delta(a) \leq \delta(b)$.
3. $1 \cdot 1 = 1 \implies N(1) \cdot N(1) = N(1) \implies N(1) = 1$.
4. $u \in A^* \implies \exists s \in A$ tal que $us = 1 \implies N(u)N(s) = N(1) = 1 \implies N(u) = \pm 1$

Factorització en un domini d'ideals principals

Proposició
Si A és domini d'ideals principals, $d = mcd(a, b) \iff (d) = (a, b)$.

Demostració. Veure exercici 4 de la llista d'anells.

Proposició
Sigui A un domini d'ideals principals, $a \in A$, $a \neq 0$ i a no invertible. Si a no és producte d'elements irreductibles, aleshores existeix una successió $\{a_n\}_{n\in\mathbb{N}}$ d'elements de A tals que a_{n+1} és divisor propi d'a_n per a tot n.

Demostració. Construïm la successió $\{a_n\}$ de manera inductiva amb la propietat addicional següent: a_n no producte d'irreductibles per a tota n. Definim $a_0 = a$. Suposem construïda $\{a_n\}$ fins a $n = k$. a_k no és irreductible $\implies a_k = bc$, amb b, c divisors propis de a_k. Si b i c fossin producte d'irreductibles, a_k també ho seria. Necessàriament b o c no producte d'irreductibles. WLOG suposem que b és l'element que no és producte d'irreductibles. Aleshores, premem $a_{k+1} = b$.

Proposició
Sigui A domini d'ideals principals i $\{a_n\}$ successió d'elements de A tal que tenim la inclusió d'ideals $(a_n) \subset (a_{n+1})$ per a tot n. Aleshores $\exists m \in \mathbb{N}$ tal que $(a_m) = (a_n)$ $\forall n \leq m$.

Demostració. $I = \bigcup_{n\in\mathbb{N}}(a_n)$ és ideal $\implies I = (a)$ per a $a \in A$. Tenim que $a \in (a_m)$ per a algun m. Aleshores, si $n \geq m$, $(a_m) \subset (a_n) \subset I = (a) \subset (a_m) \implies (a_m) = (a_n)$.

Corol·lari
Si A és domini d'ideals principals, $a \in A \setminus \{0\}$, a no invertible, aleshores existeixen elements irreductibles $p_1 \dots p_r$ de A tals que $a = p_1 \dots p_r$.

Demostració. a no producte d'irreductibles: a_{n+1} divisor propi de a_n, $a_{n+1} \mid a_n \iff (a_n)(a_{n+1})$ propi. Això contradiu la proposició anterior.

Definició 46
UN element p d'un domini d'integritat A es diu primer si $p \neq 0$, p no invertible i es compleix que per a $a, b \in A$, $p \mid ab \implies p \mid a \vee pb$,

Proposició
En un domini d'integritat, tot element primer és irreductible.

Demostració. Suposem p primer de A i $p = ab$. Aleshores $p \mid ab \implies p \mid a \vee p \mid b$. Suposem $p \mid a \implies a = pa' \implies p = pa'b \underset{p\neq 0, A domini}{\implies} 1 = a'b \implies b$ és invertible.

Proposició
En un domini d'integritat A, $p \in A$, $p \neq 0$ és primer $\iff$ l'ideal (p) és primer.

Demostració.

$$\begin{array}{ccc} p \mid ab & \iff & ab \in (p) \\ \Downarrow & & \Downarrow \\ p \mid a \vee p \mid b & \iff & a \in (p) \vee b \in (p) \end{array}$$

A més, (p) primer $\implies (p)$ propi $\implies p$ no invertible.

Proposició
Si A és DIP, tot element irreductible de A és primer.

Demostració. Sigui p un element irreductible de A i $p \mid ab$. Suposem pa Tenim $mcd(p, a) = 1 \implies (p, a) = (1) \implies 1 = \lambda p + \mu a$ per a certs $\lambda, \mu \in A \implies b = b\lambda p + \mu ab \implies p \mid b$.

Proposició
Sigui A un domini d'ideals principals. Un element no nul de A és irreductible si i només si l'ideal (p) és maximal. Per tant, en un DIP tots els ideals principals no nuls són maximals.

Demostració. Suposem p irreductible . Suposem $(p) \subset I$ ideal de A, A DIP $\implies I = (a)$, $(p) \subset (a) a \mid p \implies \begin{cases} a \text{ invertible} \implies (p) = A \\ a \text{ associat de } p \implies (a) = p \end{cases} \implies (p)$ maximal. Suposem (p) maximal. Suposem $a \mid p \implies (a) \subset (a) \underset{(p)\text{maximal}}{\implies}$ $\begin{cases} (a) = A \implies a \text{ invertible} \\ (a) = (p) \implies a \text{ associat de } p \end{cases} \implies p$ és irreductible.

Proposició
Sigui a un element no nul, no unitat, d'un domini d'ideals principals A i $a = p_1 \dots p_r$ amb p_i irreductible $1 \leq i \leq r$. Si p és irreductible i $p \mid a$, aleshores p és associat d'algun p_i.

Demostració. $\begin{cases} p \mid a = p_1 \dots p_r \\ p \text{ primer} \end{cases} \implies p \mid p_1$ per a algun índex $i, 1 \leq i \leq r$.
Com p és irreductible i no invertible, p ha de ser associat de p_i.

Proposició
Sigui A un domini d'ideals principals. Si a és un element no nul i no unitat, aleshores existeixen $p_1, \dots, p_r$ elements irreductibles de A tals que $a = p_1 \dots p_r$. A més, si $a = q_1 \dots q_s$ irreductibles tenim $r = s$ i existeix $\sigma \in S_r$ tal que $q_i \sim p_{\sigma(i)}$.

Demostració. Suposem $r \leq s$, $q_1 \dots q_s = p_1 \dots p_r \implies q_i \mid p_1 \dots p_r \implies \exists i$ tal que $q_1 \sim p_i \implies q_1 = u_1 p_i$ amb u_i invertible.
$u_1 p_i q_2 \dots q_s = p_1 \dots p_r$, $\sigma(1) = i$. Reiterant tenim $q_{r+1} \dots q_s = 1 \implies$ els q's restants serien invertibles, CONTRADICCIÓ!!! Per tant $r = s$.

Dominis de factorització única

Definició 47
Un domini d'integritat A es diu domini de factorització única (DFU) si compleix:

1. *Per a tot $a \in A$ no nul i no invertible, existeixen elements irreductibles $p_1 \dots p_r$ de A tals que $a = p_1 \dots p_r$.*
2. *Si $p, p_1, \dots, p_r$ són elements irreductibles de A i $p \mid p_1 \dots p_r$, aleshores p és associat a algun p_i.*

Un domini d'integritat complint 1) *s'anomena domini de factorització. Tot DIP és DFU i tot domini euclidià és DIP i, per tant DFU.*

Proposició
Sigui A un domini de factorització. Aleshores A és un domini de factorització única si i només si tot element irreductible de A és element primer.

Demostració. $\boxed{\Longrightarrow}$: Suposem A DFU, p element irreductible de A, $p \mid ab$. $\begin{cases} \text{si } a = 0 \implies p \mid a \\ \text{si } a = 0 \implies p \mid a \\ \text{si } b = 0 \implies p \mid b \\ \text{si } a \text{ invertible} \implies p \mid b \\ \text{si } b \text{ invertible} \implies p \mid a \end{cases}$

Suposem a i b no nuls i no invertibles: $a = p_1 p_2 \dots p_r$, $b = q_1 q_2 \dots q_s$, amb $p_1, \dots, p_r, q_1, \dots, q_s$ irreductibles de A. $p \mid ab = p_1 \dots p_r q_1 \dots q_s \implies$ $\begin{cases} p \text{ associat de } p_i \text{ per a algun } 1 \leq i \leq r \implies p \mid a \\ q \text{ associat de } q_i \text{ per a algun } 1 \leq i \leq s \implies p \mid b \end{cases}$

$\boxed{\Longleftarrow}$: Suposem que tot irreductible de A és primer. Sigui p irreductible de A, $p_1, \dots, p_r$ irreductibles de A i suposem $p \mid p_1 \dots p_r \overset{p \text{ primer}}{\Longrightarrow} p \mid p_i$ per a algun $1 \leq i \leq r$. Això juntament amb p_i irreductible, impliquen que $p \sim p_i$

Proposició
Els anells $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$ són anells de factorització.

Demostració. Hem de veure que $\forall a \in \mathbb{Z}[\sqrt{d}]$ no nul i no invertible és producte d'irreductibles: A $\mathbb{Z}[\sqrt{d}]$ tenim una norma N i tenim que $(a \in (\mathbb{Z}[\sqrt{d}]^*) \iff N(a) = \pm 1)$ i $(N(a) = 0 \iff a = 0)$. Suposem que a $\mathbb{Z}[\sqrt{d}]$ existeixen elements no nuls no invertibles que són producte d'irreductibles. Sigui a un d'aquests amb $|N(a)|$ màxima. a no irreductible $\implies$ $a = bc$ amb b i c no invertible $\implies$ $N(a) = N(b)N(c) \implies |N(a)| = |N(b)||N(c)|$. Com que $|N(b)| > 1$ i $|N(c)| > 1 \implies \begin{cases} |N(b)| < |N(a)| \implies b \text{ és producte d'irreductibles} \\ |N(c)| < |N(a)| \implies c \text{ és producte d'irreductibles} \end{cases} \implies$ $a = bc$ és producte d'irreductibles. **CONTRADICCIÓ!!!**.

Màxim comú divisor i mínim comú múltiple en un domini de factorització única

Sigui A un domini de factorització única i P un subconjunt de A tal que:

1. Tot element de P és irreductible.
2. Tot element irreductible de A és associat a algun element de P.
3. Dos elements diferents de P no són associats.

P es diu conjunt fonamental d'elements irreductibles.

Proposició
Si A és DFU i P un conjunt fonamental d'elements irreductibles, tot element de A no nul es pot expressar en la forma $a = up_1^{r_1} \dots p_k^{r_k}$ amb

- *u invertible, $k \in \mathbb{Z} \geq 0$*
- *$p_1, \dots, p_k$ elements de P diferents dos a dos*
- *$r_1, \dots, r_k$ enters > 0*

A més, la unitat u, els irreductibles p_i i els enters r_i queden determinats per a de forma única.

Proposició
Si a, b són element de A, DFU, existeixen el màxim comú divisor i el mínim comú múltiple de a i b.

Demostració. $a = up_1^{n_1} \dots p_k^{n_k}$, $a = vp_1^{m_1} \dots p_k^{m_k}$ amb u, v unitaris, p_i irreductibles de P diferents dos a dos, $n_1, \dots, n_r, m_1, \dots, m_r$ enters ≥ 0.

$$k_i = min\{n_i, m_i\},\ d = \prod_{i=1}^{r} p_i^{k_i} \text{ és mcd de } a, b$$

$$l_i = max\{n_i, m_i\},\ d = \prod_{i=1}^{r} p_i^{l_i} \text{ és mcm de } a, b$$

Algorisme d'Euclides

Sigui (A, δ) un domini euclidià.

Lema
Sigui A un domini d'integritat, $a, b, q \in A$. Es compleix la igualtat d'ideals $(a, b) = (a - bq, b)$. Si A és DIP, tenim $mcd(a, b) \sim mcd(a - bq, b)$.

Proposició
Sigui (A, δ) un domini euclidià, $a, b \in A$, $b \neq 0$.Fem successivament les divisions enteres:

$$a = bq + r_1 \ amb\ \delta(r_1) < \delta(b) \vee r_1 = 0 \tag{2.1}$$
$$si\ r_1 = 0 b = r_1 q_2 + r_2 \ amb\ \delta(r_2) < \delta(r_1) \vee r_2 = 0 \tag{2.2}$$
$$si\ r_2 = 0 r_1 = r_2 q_3 + r_3 \ amb\ \delta(r_3) < \delta(r_2) \vee r_3 = 0 \tag{2.3}$$
$$\vdots \tag{2.4}$$

Aleshores $\exists n \in \mathbb{N}$ tal que $r_1 \neq 0, \dots, r_{n-1} \neq 0$ i $r_n = 0$. Es compleix que $mcd(a, b) = r_{n-1}$.

Demostració. $\delta(r_1) > \delta(r_2) > \dots$ és successió decreixent d'enters positius $\implies$ $\exists n \in \mathbb{N}$ amb $r_n = 0$. Pel lema anterior, $mcd(a, b) = mcd(r_1, b) = mcd(r_2, r_1) = \dots = mcd(r_{n-1}, r_n = 0) = r_{n-1}$

Factorialitat dels anells de polinomis

Proposició
Sigui A un domini d'integritat. Són equivalents

(1) A és un cos

(2) $A[x]$ és domini euclidià

(3) $A[x]$ és domini d'ideals principals

Demostració. (1) $\implies$ (2) $\implies$ (3) ja ho hem vist anteriorment. Vegem que (3) $\implies$ 1:

$$\begin{aligned} \phi\colon A[x] &\longrightarrow A \\ P &\longmapsto P(0) \end{aligned}$$

és morfisme d'anells, exhaustiu i $ker\phi = (x)$. Pel teorema d'isomorfia tenim que ${}^{A[x]}\!/_{(x)} \cong A$. x irreductible i $A[x]$ DIP $\implies$ (x) maximal $\implies$ ${}^{A[x]}\!/_{(x)}$ cos $\implies$ A cos. A domini d'integritat $\implies A[x]^* = A^*$

Definició 48
Sigui $f(n) = a_n x^n + \ldots + a_0 \in A[x]$, A DFU. El contingut de f ($c(f)$) és el màxim comú divisor dels coeficients de f, $c(f) = mcd(a_0, a_1, \ldots, a_n)$. Direm que f és primitiu si $c(f)$ és una unitat. $f \in A[x]$, $f = c(f)f^*$, amb f^* primitiu. Si $f = cf^*$, amb $c \in A$, f primitiu, aleshores $c \sim c(f)$ i $f \sim \tilde{f}$.

Lema (Lema de Gauss)
Sigui A un DFU. Aleshores en $A[x]$ el producte de polinomis primitius és primitiu. Més exactament si $f, g \in A[x]$, $c(fg) \sim c(f)c(g)$.

Demostració. Sigui $p \in A$ un element irreductible. Definim $A \xrightarrow{\pi} {}^{A}\!/_{(p)}$. Sigui

$$\begin{aligned} \phi\colon A[x] &\longrightarrow {}^{A}\!/_{(p)}[x] \\ h = a_n x^n + \ldots + a_o &\longmapsto \pi(a_n)x^n + \ldots + \pi(a_0) \end{aligned}$$

A DFU $\implies$ p és primer $\implies$ ${}^{A}\!/_{(p)}$ és domini d'integritat $implies {}^{A}\!/_{(p)}[x]$ és domini d'integritat.
$\phi(h) = 0 \iff p \mid a_i \iff p \mid c(f)$
$f, g \in A[x]$, $\phi(fg) = \phi(f)\phi(g)$, per tant $\phi(fg) = 0 \implies \phi(f) = 0 \vee \phi(g) = 0$.
$p \mid c(fg) \implies p \mid c(f) \vee p \mid c(g)$. Si f, g primirius, fg no primiriu $\implies \exists p$ irreductible amb $p \mid c(fg)$. CONTRADICCIÓ!!!

$$\left.\begin{array}{l} f = c(f)f^*, f^* \text{ primitiu} \\ g = c(g)g^*, g^* \text{ primitiu} \end{array}\right\} \implies fg = c(f)c(g)(f^*g^*) \implies c(f)c(g) \sim c(fg)$$

Corol·lari
Sigui A un DFU, k el cos de fraccions de A i $f \in A[x]$ mònic. Si $f = gq$ a $k[x]$ amb g i h mònics, aleshores g i h són de $A[x]$

Demostració. f mònic $c(f) \sim 1$. Siguin $a, b \in A$ tals que $ag, bh \in A[x]$. Tenim que $abf = (ag)(bh)$ $\left.\begin{array}{rl} ab = c(abf) \sim c(ag)c(bh) & \\ g \text{ mònic} & \implies c(ag) \mid a \\ g \text{ mònic} & \implies c(bh) \mid b \end{array}\right\} \implies c(ag) \sim a \wedge c(bh) \sim b \implies$
$\begin{cases} a \text{ divideix qualsevol coeficient de } ag \implies g \in A[x] \\ b \text{ divideix qualsevol coeficient de } bh \implies h \in A[x] \end{cases}$

Irreductibles de $A[x]$

Si a és element irreductible de A, aleshores també ho és de $A[x]$. Tenim $A[x]^* = A^*$.

Proposició
Sigui A un DFU i sigui $f \in A[x]$. Les condicions següents són equivalents:

1. *$f(x)$ té grau positiu i és irreductible a $A[x]$.*
2. *f és primitiu i és irreductible a $k[x]$ (k el cos de fraccions de A).*

Demostració.

$\boxed{1 \implies 2}$: $\begin{cases} f = c(f)f^* \\ f \text{ irreductible} \end{cases} \implies f$ primitiu. $f = gh$ amb $g, h \in k[x]$ i suposem $gr(h) > 0$. Sigui $a, b \in A$ tals que $ag, bh \in A[x]$, $abf = (ag)(bh)$. $\left.\begin{array}{l} ag = c(ag)g^* \text{ amb } g^* \text{ primitiu} \\ bh = c(bh)h^* \text{ amb } h^* \text{ primitiu} \end{array}\right\} \implies (ag)(bh) = c(ag)c(bh)g^*h^*$, amb g^*h^* primitiu $\implies ab \sim c(ag)c(bh)$ i $f \sim g^*h^* \implies f = ug^*h^* \overset{f \text{ irreductible a } A[x]}{\implies}$ $ug^* \in A[x]^* = A^* \implies gr(g^*) = 0 \implies gr(g) = 0 \implies g \in k \setminus \{0\} = k[x]^*$.

$\boxed{2 \implies 1}$: $f = gh$ amb $g, h \in A[x]$, h de grau positiu $\implies gr(g) = 0 \implies g \in k \cap A[x]$. $f = gh \implies c(f) \sim c(g)c(h) \overset{g \text{ constant}}{\implies} c(f) \sim gc(h) \implies g \mid c(f) \sim 1 \implies g \in A^*$.

Lema
Si $p \in A$ és element primer a A, aleshores és element també primer a $A[x]$.

Demostració. $p \mid fg$ amb $f, g \in A[x]$, $f = a_0 + a_1x + \ldots + a_nx^n$, $g = b_0 + b_1x + \ldots + b_mx^m$ Suposem pf. Sigui i tal que $p \mid a_0, \ldots, p \mid a_{i-1}, pa_i$. El coeficient de x^2 de fg és $b_0a_2 + b_1a_{i-1} + \ldots + b_ia_0 \implies \left.\begin{array}{l} p \mid b_0a_i \\ pa_i \end{array}\right\} \implies p \mid b_0$.
Suposem vist $p \mid b_0, b_1, \ldots, b_{j-1}$ i provem qur $p \mid b_j$: el coeficient de x^{i+j} de fg és $b_0a_{i+j} + \ldots + \_j - 1a_{i+1} + b_ja_i + b_{j+1}a_{i-1} + \ldots + b_{i+j} \implies \left.\begin{array}{l} p \mid b_ja_i \\ pa_i \end{array}\right\} \implies p \mid b_j$, per tant $p \mid g$.

Teorema
Si A és domini de factorització única, aleshores $A[x]$ és domini de factorització única.

Demostració. Provem que $A[x]$ és domini de factorització: Sigui $f \in A[x]$, f no nul i no unitat, $f = c(f)f^*$, f^* primiriu. $c(f) \in A$, $c(f)$ producte d'irreductibles de A que ho són també de $A[x](1)$ a $k[x]$, $f = g_1 \dots_r$ amb $g_i \in k[x]$ irreductible. Siguin a_i tals que $a_i g_i \in A[x]$, $a = \prod_{i=1}^{r} a_i$

$$af = (a_1 g_1) \dots (a_r g_r)$$

$f = c(f)f^*, a_i g_i = c(a_i g_i) g_i^*$, amb f^*, g_i^* primitius. $a = c(f)f^* = c(a_1 g_1) g_1^* \dots c(a_r g_r) g_r^* = c(a_1 g_1) \dots c(a_r g_r) f_1^* \dots f_r^*$ ($f_1^* \dots f_r^*$ primitiu pel lema de Gauss) $\implies$ $f^* \sim g_1^* \dots g_r^*$. g_i irreductible a $k[x]$ $\implies$ $\left.\begin{array}{l} g_i^* \text{ irreductibles a } k[x] \\ g_i^* \text{ primitius} \end{array}\right\} \implies g_i^*$ irreductibles a $A[x]$ $\implies$ f^* és producte d'irreductibles de $A[x](2)$. $(1) + (2) \implies f$ és productie d'irreductibles de $A[x]$