Definició i exemples

Un *grup* és un conjunt G juntament amb unes operació $(\cdot)$ que compleix les propietats:

- Associativa: $g\cdot(g'\cdot g'')=(g\cdot g')\cdot g''$ $\quad\forall g,g',g''\in G$.
- Existeix un element e, que anomenarem *element neutre*, tal que

$$g\cdot e=e\cdot g=g \qquad \forall g\in G$$

- Per a cada $g\in G$ hi un element, que anomenarem l'*invers de* g i denotarem per g^{-1}, tal que

$$g\cdot g^{-1}=g^{-1}\cdot g=e \qquad \forall g,g^{-1}\in G$$

Si es compleix també la propietat commutativa:

$$g\cdot g'=g'\cdot g \qquad \forall g,g'\in G$$

direm que el *grup* és *commutatiu* o *abelià*. En aquest cas l'operació es denota sovint per $+$, l'element neutre per 0 (i es diu *zero*) i l'element invers $-g$ (i es diu l'*oposat* de g).

Quan indiquem l'operació $(\cdot)$, notació multiplicativa, l'element neutre s'acostuma a dir *unitat* i a escriure 1. Amb aquesta notació multiplicativa és costum suprimir el punt que indica l'operació i escriure simplement gg' per indicar $g\cdot g'$.

Permutacions

Sigui $A=\{a_1,\ldots,a_n\}$ un conjunt amb n elements. Una *permutació de* A és una aplicació bijectiva

$$\sigma: A\to A$$

La composició de permutacions és, clarament, una permutació. A més a més es compleixen les propietats:

- Associativa: $\sigma\circ(\rho\circ\tau)=(\sigma\circ\rho)\circ\tau$ $\quad\forall\sigma,\rho,\tau$
- Hi ha una permutació I tal que: $\sigma\circ I=I\circ\sigma=\sigma$ $\quad\forall\sigma$
- Per a cada permutació σ hi ha una permutació σ^{-1} tal que $\sigma\circ\sigma^{-1}=I=\sigma^{-1}\circ\sigma$. σ^{-1} és l'aplicació inversa de σ.

El conjunt de permutacions de $\{1,\ldots,n\}$ el designarem per S_n.

Proposició 2.1 *Si* $n\geq 3$, S_n *no és commutatiu.*

Un element j es diu *fix* per una permutació σ si $\sigma(j)=j$. Si j no és fix, formem la successió

$$j,\sigma(j),\sigma^2(j),\ldots,\sigma^r(j),\ldots$$

on $\sigma^2=\sigma\circ\sigma$ i, en general, $\sigma^r=\sigma\circ\sigma^{r-1}$. Com que $\{1,2,\ldots,n\}$ és finit, en algun moment un element $\sigma^k(j)$ coincidirà amb un dels anteriors. El primer element que torna a sortir és precisament el j: en efecte, si $\sigma^k(j)=\sigma^h(j)$ amb $h<k$, per ser σ bijectiva,

$$\sigma^k(j)=\sigma^h(j)\Rightarrow\sigma^{k-1}(j)=\sigma^{h-1}(j)\Rightarrow\ldots\Rightarrow\sigma^{k-h}(j)=j\,;$$

és a dir, j hauria sortit ja.

Siguin, doncs,

$$j,\sigma(j),\ldots,\sigma^{r-1}(j)$$

diferents i $\sigma^r(j)=j$. Direm que la permutació σ és un *cicle d'ordre* r si deixa fixos tots els elements que no apareixen en la successió anterior. Escriurem aleshores

$$\sigma=\left(j,\sigma(j),\sigma^2(j),\ldots,\sigma^{r-1}(j)\right)$$

Proposició 2.2 *Tota permutació és producte de cicles.*

Els cicles d'ordre 2 es diuen *transposicions*.

Proposició 2.3 *Tot cicle és producte de transposicions.*

La identitat I, i per tant qualsevol permutació, es pot posar de moltes maneres com a producte de transposicions. Anem a veure, però, que el nombre de transposicions en aquests productes té sempre la mateixa paritat.

Proposició 2.4 *La permutació identitat no es pot posar com a producte d'un nombre senar de transposicions.*

Corol·lari 2.5 *Si $\sigma=\tau_p\circ\ldots\circ\tau_1=\rho_q\circ\ldots\circ\rho_1$ són dues descomposicions de la permutació σ com a producte de transposicions, aleshores p i q són de la mateixa paritat.*

Una permutació es diu *parella* si descompon en un nombre parell de transposicions; una permutació es diu *senar* si descompon en un nombre senar.

Assignem a les permutacions parelles del signe "+" i a les permutacions senars del signe "-". Anomenarem *aplicació signe* l'aplicació

$$\varepsilon:S_n\to\{+1,-1\}$$

tal que

$\varepsilon(\sigma)=+1$ si σ és parell
$\varepsilon(\sigma)=-1$ si σ és senar,

Es compleix

$$\varepsilon(I)=1, \qquad \varepsilon(\sigma\circ\tau)=\varepsilon(\sigma)\cdot\varepsilon(\tau)$$

En particular, per (2.3), si $(a_1,\ldots,a_n)$ és un cicle d'ordre m,

$$\varepsilon(a_1,\ldots,a_n)=(-1)^{m-1}$$

Subgrups

Sigui S un subconjunt no buit d'un grup G. Si compleix que

(1) per a tot parell $g,g'\in S$, $gg'\in S$,

l'operació de G dóna lloc a una operació a S, que anomenarem "l'operació induïda" per la de G. Ens interessen els subconjunts S de G que compleixen (1) i que amb l'operació induïda siguin un grup al seu torn. D'aquests subconjunts en direm "subgrups".

Suposem, doncs, que S compleix (1) i té, per tant, una operació induïda. Aquesta operació serà automàticament associativa (per ser-ho la de G); si té un element neutre $e'\in S$.

$$\forall g\in S \qquad e'g=g;$$

multiplicant a la dreta per l'invers de g (a G), obtenim $e'=e$. És a dir, si S té element neutre, aquest ha d'ésser el mateix element neutre e de G. De manera semblant es veu que si un element g de S té invers per l'operació induïda a S, aquest ha de coincidir amb l'invers g^{-1} que g té a G. Per tant, les condicions que ha de complir S per a ésser un grup són:

- $e\in S$.
- $g\in S\Rightarrow g^{-1}\in S$.

La primera d'aquestes dues condicions és conseqüència de la segona i de (1). Hem justificat així la definició següent de subgrup:

Un subconjunt S, no buit, d'un grup G direm que és un *subgrup de* G, si compleix

1. $g,g'\in S\Rightarrow gg'\in S$,
2. $g\in S\Rightarrow g^{-1}\in S$.

De fet aquestes dues condicions es poden sintetitzar en una:

Proposició 3.1 *Un subconjunt* $S \neq 0$ *d'un grup* G *és un subgrup de* G si i només si compleix

$$g', g \in S \Rightarrow g'g^{-1} \in S$$

Donat un subconjunt S d'un grup G, anomenarem *subgrup generat per* S el "més petit" subgrup de G que conté S. El designarem per (S). Aquí, "més petit" vol dir que (S) està contingut en qualsevol altre subgrup que contingui S.

Homomorfismes

Siguin G i G' dos grups. Una aplicació

$$f : G \to G'$$

es diu un *homomorfisme* (o *morfisme*) *de grups. Siguin* e *i* e' *els elements neutres de* G *i* G' *respectivament. Aleshores*,

a) $f(e) = e'$,
b) $f(g^{-1}) = (f(g))^{-1}$, $\forall g \in G$.

Proposició 4.2 *Si* $f : G \to G'$ *i* $h : G' \to G''$ *són dos homomorfismes de grups, aleshores* $h \circ f : G \to G''$ *és també un hommorfisme.*

Un homomorfisme injectiu es diu un *monomorfisme*; un morfisme exhaustiu es diu un *epimorfisme*; un morfismebijectiu es diu un *isomorfisme*; si $f : G \to G'$ és un isomorfisme, direm que G i G' són *isomorfs* i escriurem $G \cong G'$.

Dos grups isomorfs tenen les mateixes propietats, "els mateixos subgrups", etc.

Anomenarem *nucli d'un homomorfisme* $f : G \to G'$

$$\text{Nuc } f = \{g \in G \mid f(g) = e'\}.$$

Anomenarem *imatge d'un homomorfisme* f

$$\text{Im } f = \{g' \in G' \mid \exists g \in G, f(g) = g'\}.$$

És fàcil comprovar que $\text{Nuc } f$ és un subgrup de G i $\text{Im } f$ és un subgrup de G'.

Proposició 4.3 *Sigui* $f : G \to G'$ *un homomorfisme de grups.*

a) f *és injectiva si i només si* $\text{Nuc } f = \{e\}$.
b) f *és exhaustiva si i només si* $\text{Im } f = G'$.

Grup quocient. Subgrups normals

Recordem que els quocients $\mathbf{Z}/(m)$ estaven definits a partir de la relació d'equivalència: $a \equiv b \Leftrightarrow a - b \in (m)$.

I. $g_1 \sim g_2 \Leftrightarrow g_1 \cdot g_2^{-1} \in H$
II. $g_1 \approx g_2 \Leftrightarrow g_2^{-1} \cdot g_1 \in H$.

Les classes d'equivalència per la relació II són

$$\{g\} = \{g_1 \in G \mid g_1 \approx g\} = \{g_1 \in G \mid g_1 = gh, h \in H\}$$

Direm que H és un *subgrup normal* si és un subgrup que compleix la igualtat

$$\boxed{gHg^{-1} = H}, \ \forall g \in G$$

Observem que $gHg^{-1} = H$ equival a

$$gH = Hg \ , \ \forall g \in G$$

és a dir, si H és normal, les classes per a les dues relacions I i II coincideixen, i, per tant, els conjunts quocients també, $H \setminus G = G/H$. Naturalment, en aquest cas, l'operació de G/H també està ben definida i coincideix amb la de $H \setminus G$.

Proposició 5.1 *Un subgrup H és normal si i només si és nucli d'un homomorfisme.*

$A_n = \text{Nuc}\ \varepsilon$ és diu el *grup alternat d'ordre* n.

Teorema 5.2 (d'isomorfisme) *Sigui $f : G \to G'$ un homomorfisme de grups; aleshores*

$$\boxed{G/\text{Nuc}\ f \cong \text{Im}\ f}$$

Producte directe de grups

Es diu que un grup G és *producte directe* dels seus subgrups H_1 i H_2 si

a) H_1 i H_2 són subgrups normals de G;

b) $H_1 \bigcap H_2 = \{e\}$ (on e és l'element neutre de G);

c) $G = \{h_1 h_2 \mid h_1 \in H_1, h_2 \in H_2\}$.

Proposició 6.1 *G és producte directe dels seus subgrups H_1 i H_2 si i només si*

1. *tot $g \in G$ s'expressa de manera única com a producte $g = h_1 h_2$ amb $h_1 \in H_1$ i $h_2 \in H_2$;*
2. *$h_1 h_2 = h_2 h_1$, $\forall h_1 \in H_1$, $\forall h_2 \in H_2$.*

Siguin ara G_1 i G_2 dos grups (poden ésser el mateix) . *Anomenarem producte directe de* G_1 i G_2 el conjunt $G_1 \times G_2$ juntament amb l'operació

$$(g_1, g_2)(g_1', g_2') = (g_1 g_1', g_2' g_2') \qquad \forall g_1, g_1' \in G_1,\ \forall g_2, g_2' \in G_2 .$$

Proposició 6.2 *Sigui $G_1 \times G_2$ el producte directe de grups G_1 i G_2. Existeixen dos subgrups de $G_1 \times G_2$, G_1' i G_2', isomorfs a G_1 i G_2 respectivament, tals que $G_1 \times G_2$ és el producte directe de G_1' i G_2'.*

Tot element $(g_1, g_2) \in G_1 \times G_2$ es pot posar com

$$(g_1, g_2) = (g_1, e)(e, g_2)$$

Grups cíclics

Un grup G es diu *cíclic* si està generat per un element g (que es diu un *generador* de G). Escriurem

$$G = (g).$$

Tal com hem vist a l'apartat 3, el subgrup generat per g està format per g, g^{-1} i productes d'aquests elements: $g^n, (g^{-1})^n$. Fent servir la notació $g^0 = e, g^{-n} = (g^{-1})^n$, tenim, doncs,

$$\boxed{(g) = \{g^n \mid n \in \mathbf{Z}\}}$$

Proposició 7.1 *Tot grup cíclic és isomorf a* $\mathbf{Z}$ *o a un* $\mathbf{Z}/(m)$.

Proposició 7.2 *Tot subgrup d'un grup cíclic és cíclic.*

Grups finits

Anomenarem *ordre d'un grup finit* G el nombre dels seus elements, i el denotarem per $|G|$. Observem que si G és cíclic aquest ordre coincideix amb el definit a l'apartat anterior.

Anomenarem *ordre d'un element* $g \in G$ l'ordre del subgrup cíclic generat per g.

Proposició 8.1 *Si S és un subgrup del grup finit G, $|S|$ divideix $|G|$.*

Corol·lari 8.2 *L'ordre d'un element divideix l'ordre del grup.*

Corol·lari 8.3 *Si $|G| = p$ és primer, G és un grup cíclic d'ordre p.*

Proposició 8.4 *Només hi ha dos grups d'ordre 4: $\mathbf{Z}/(4)$ i $\mathbf{Z}/(2)\times\mathbf{Z}/(2)$. Ambdós són commutatius.*

Proposició 8.5 *Tot subgrup S d'un grup G d'índex 2 és normal.*

Proposició 8.6 *Si tots els elements d'un grup G són d'ordre 2, G és un grup commutatiu.*

Proposició 8.7 *Només hi ha dos grups d'ordre 6: un de commutatiu, $\mathbf{Z}/(6)$, i un de no commutatiu, S_3.*

Es coneixen tots els grups commutatius amb un nombre finit de generadors.

Teorema 8.8 (d'estructura dels grups commutatius) *Tot grup commutatiu G amb un nombre finit de generadors és producte directe d'un nombre finit de grups $\mathbf{Z}$ i $\mathbf{Z}/(m)$.*