

TEORIA DE GRUPS: 303 EXERCICIS RESOLTS

Olga Lavila Vidal

Departament de Matemàtiques
i Informàtica

TEORIA DE GRUPS: 303 EXERCICIS RESOLTS

Olga Lavila Vidal

Departament de Matemàtiques
i Informàtica

Índex

PRÒLEG	7
CAPÍTOL 1. Llista d'exercicis.....	9
1.1 Grups. Subgrups	16
1.2 Subgrups normals. Grup quocient	21
1.3 Morfismes de grups.....	21
1.4 Grups lliures. Presentacions	28
1.5 Producte directe i semidirecte de grups	29
1.6 Grups abelians	34
1.7 Grups resolubles	35
1.8 Accions d'un grup sobre un conjunt	38
1.9 Teoremes de Sylow	44
1.10 Aplicacions	48
CAPÍTOL 2. Grups. Subgrups.....	55
CAPÍTOL 3. Subgrups normals. Grup quocient.....	79
CAPÍTOL 4. Morfismes de grups	103
CAPÍTOL 5. Grups lliures. Presentacions	127
CAPÍTOL 6. Producte directe i semidirecte de grups	133
CAPÍTOL 7. Grups abelians.....	157
CAPÍTOL 8. Grups resolubles.....	161
CAPÍTOL 9. Accions d'un grup sobre un conjunt.....	171
CAPÍTOL 10. Teoremes de Sylow	195
CAPÍTOL 11. Aplicacions.....	213
BIBLIOGRAFIA	269

Aquest text docent recull una col·lecció d'exercicis resolts de teoria de grups, que forma part del temari de l'assignatura Estructures Algebraiques del Grau de Matemàtiques de la Facultat de Matemàtiques i Informàtica de la Universitat de Barcelona.

El programa actual de l'assignatura comprèn tres hores de teoria, una de problemes i una de laboratoris per setmana, al llarg d'un semestre. Les classes de problemes i laboratoris tenen la finalitat principal d'ajudar a comprendre la teoria aplicant-la a la resolució de problemes. El professor dona a la classe de teoria una sèrie d'explicacions conceptuals i metodològiques que l'estudiant ha de posar en pràctica posteriorment mitjançant la resolució d'exercicis, tant a l'aula com, sobretot, en forma de treball individual. L'objectiu d'aquest text docent és proporcionar a l'estudiant una eina de consulta i de treball que li permeti completar de manera autònoma els exercicis. Alguns dels problemes proposats es corresponen amb els mateixos que es treballen a les classes pràctiques. També s'incorporen exercicis d'exàmens i exercicis que amplien el focus a resultats que estenen els propis de l'assignatura, així com la teoria de l'assignatura en forma d'exercicis guiats. Tots aquests exercicis es resolen de manera detallada.

La col·lecció de problemes cobreix i amplia el temari de l'assignatura i pressuposa que l'estudiant té coneixements d'àlgebra lineal i de geometria lineal. Unes excel·lents referències de la teoria de l'assignatura són els apunts *Estructures Algebraiques 20-21* de Teresa Crespo, *Estructures Algebraiques 20-21* d'Artur Travesa, i el llibre *Abstract Algebra* de D.S. Dummit i R.M. Foote.

Molts dels membres de la Facultat de Matemàtiques i Informàtica han col·laborat al llarg del temps en la docència de l'assignatura i han participat tant en el desenvolupament dels programes en el context dels diferents plans d'estudis com en la preparació de les llistes d'exercicis. A tots ells, vull fer-los arribar el meu agraïment.

Santa Coloma de Queralt, 2022

LLISTA D'EXERCICIS

1.1. Grups. Subgrups

Definició 1.1. Un grup és un conjunt G no buit amb una operació binària interna

$$\begin{aligned} G \times G &\longrightarrow G \\ (x, y) &\longmapsto xy \end{aligned}$$

que compleix:

- a) Propietat associativa: $(xy)z = x(yz)$, per a qualssevol $x, y, z \in G$.
- b) Element neutre: existeix $e \in G$ tal que $ex = xe = x$, per a tot $x \in G$.
- c) Element simètric: per a tot $x \in G$, existeix $x' \in G$ tal que $x'x = xx' = e$.

Direm que G és un grup *abelià* si, a més, l'operació compleix la propietat commutativa, és a dir, $xy = yx$, per a qualssevol $x, y \in G$.

Aquesta operació a G es pot escriure amb símbols diferents: xy , $x + y$, $x * y$, $x \circ y$, etcètera. Si l'operació de G és un producte, l'element neutre s'escriu 1 i l'element simètric de x es diu l'*invers* de x i s'escriu x^{-1} . Si l'operació de G és una suma, l'element neutre s'escriu 0 i l'element simètric de x es diu l'*oposat* de x i s'escriu $-x$.

Exercici 1.1. Sigui G un grup. Proveu que:

- a) L'element neutre és únic.
- b) El simètric d'un element és únic.

Exercici 1.2. Sigui G un conjunt dotat d'una operació binària interna $(x, y) \mapsto xy$ associativa que compleix:

- a) Existeix $e \in G$ tal que $ex = x$, per a tot $x \in G$.
- b) Per a tot $x \in G$, existeix $x' \in G$ tal que $x'x = e$.

Proveu que G amb aquesta operació és grup, el seu element neutre és e i el simètric de x és x' .

Definició 1.2. Un anell (*commutatiu amb unitat*) és una terna $(A, +, \cdot)$, on $A \neq \emptyset$ és un conjunt dotat de dues operacions binàries internes: $(x, y) \mapsto x + y$, anomenada suma, i $(x, y) \mapsto xy$, anomenada producte, de manera que $(A, +)$ és un grup commutatiu, $(A, \cdot)$ satisfà la propietat associativa, la propietat commutativa i $1 \in A$ és el neutre, i es compleix la propietat distributiva del producte respecte de la suma: $x(y + z) = xy + xz$. Exemples d'anells són $\mathbb{Z}$, $\mathbb{Z}/m\mathbb{Z}$, per a qualsevol enter m , i $A[X_1, \dots, X_n]$, per a qualsevol anell A i indeterminades $X_1, \dots, X_n$.

Un anell commutatiu amb unitat en què tot element no zero té invers es diu *cos*. Exemples de cossos són $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ i $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, per a un primer p .

Notarem indistintament $\mathbb{Z}/n\mathbb{Z}$ i $\mathbb{Z}_n$, per a $n \geq 1$ enter. Si p és un nombre primer, notarem $\mathbb{F}_p$ quan pensem en $\mathbb{Z}/p\mathbb{Z}$ com a cos.

Exercici 1.3. Determineu si els conjunts següents amb les operacions que s'indiquen són grups o no.

- El conjunt dels nombres naturals $\mathbb{N}$ amb la suma.
- El conjunt dels nombres enters $\mathbb{Z}$ amb la suma; el mateix conjunt, però amb el producte.
- El conjunt dels nombres racionals $\mathbb{Q}$ amb la suma; el mateix conjunt, però amb el producte.
- El conjunt $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$ amb el producte.
- El conjunt $S^1 = \{z \in \mathbb{C} : |z| = 1\}$ amb el producte en $\mathbb{C}$.
- El conjunt dels polinomis $P_n = \{p(x) \in \mathbb{R}[x] : \text{gr}(p(x)) \leq n\}$ amb la suma habitual; el mateix conjunt, però amb el producte habitual.
- El conjunt dels endomorfismes $\text{End}(E) = \{f : E \rightarrow E \text{ aplicacions lineals}\}$ amb la suma; el mateix conjunt, però amb la composició, on E és un espai vectorial sobre un cos K .
- El conjunt dels automorfismes de E , és a dir, dels endomorfismes bijectius de E , que denotarem per $\text{Aut}(E)$, amb la composició, on $E \neq 0$ és un espai vectorial sobre un cos K .
- El conjunt $M(n, K)$ de matrius quadrades d'ordre n amb coeficients en un cos K amb la suma; el mateix conjunt, però amb el producte.
- El conjunt $\text{GL}(n, K) = \{A \in M(n, K) : \det(A) \neq 0\}$ de matrius quadrades d'ordre n invertibles amb coeficients en un cos K amb el producte de matrius.

Exercici 1.4. Sigui $(A, \cdot)$ un conjunt amb una operació interna que compleix la propietat associativa i té un element neutre e . Sigui A^* el subconjunt de A format pels elements de A que tenen invers. Proveu que $(A^*, \cdot)$ és un grup.

Exercici 1.5. A $(\mathbb{Z}, +)$ definim l'operació binària següent: $x * y = x + y + 1$. Proveu que $(\mathbb{Z}, *)$ és un grup abelià. Penseu com es pot generalitzar aquesta operació.

Exercici 1.6. Demostreu que si es compleix $x^2 = e$ per a tots els elements x d'un grup G , aleshores G és un grup abelià.

Exercici 1.7. Siguin X un conjunt i $P(X) = \{A : A \subseteq X\}$ el conjunt de les seves parts. Donats $A, B \in P(X)$, definim la *diferència simètrica* de A i B com:

$$A + B := (A \setminus B) \cup (B \setminus A)$$

Proveu que $(P(X), +)$ és un grup abelià. Aquest grup s'anomena el *grup de Boole de X* i es denota per $\mathcal{B}(X)$.

Definició 1.3. Siguin G un grup i H un subconjunt no buit de G . Diem que H és un *subgrup* de G si H és un grup amb l'operació de G .

Exercici 1.8. Siguin G un grup i H un subconjunt no buit de G . Proveu que són equivalents:

- H és un subgrup de G .
- H compleix les propietats següents:
 - $e \in H$,
 - Per a qualssevol $x, y \in H$, es compleix que $xy \in H$,
 - Per a qualsevol $x \in H$, es compleix que $x^{-1} \in H$.
- Per a qualssevol $x, y \in H$, es compleix que $xy^{-1} \in H$.

Exercici 1.9. Sigui H un subconjunt finit i no buit d'un grup G . Proveu que H és subgrup de G si, i només si, $xy \in H$, per a tot $x, y \in H$. És cert l'enunciat si H no és finit?

Exercici 1.10. Sigui G un grup. Proveu que:

- a) G i $\{e\}$ són subgrups de G .
- b) Si H_1, H_2 són subgrups de G , aleshores $H_1 \cap H_2$ és un subgrup de G .
- c) Si $\{H_i\}_{i \in I}$ és una família de subgrups de G , aleshores $\bigcap_{i \in I} H_i$ és un subgrup de G .

Exercici 1.11. Proveu que:

- a) Per a cada $m \in \mathbb{Z}$, $m\mathbb{Z} := \{mn : n \in \mathbb{Z}\}$ és un subgrup de $(\mathbb{Z}, +)$.
- b) Si H és un subgrup de $(\mathbb{Z}, +)$, aleshores $H = m\mathbb{Z}$, per a un cert $m \in \mathbb{Z}$.

Exercici 1.12. Sigui K un cos. Considerem:

$$\begin{aligned} \text{GL}(n, K) &:= \{M \in \text{M}(n, K) : \det(M) \neq 0\} && \text{grup lineal} \\ \text{SL}(n, K) &:= \{M \in \text{GL}(n, K) : \det(M) = 1\} && \text{grup especial lineal} \\ \text{O}(n, K) &:= \{M \in \text{GL}(n, K) : M^t M = \text{Id}\} && \text{grup ortogonal} \\ \text{SO}(n, K) &:= \{M \in \text{O}(n, K) : \det(M) = 1\} && \text{grup especial ortogonal} \end{aligned}$$

- a) Demostreu que $\text{GL}(n, K)$ és un grup amb la multiplicació de matrius.
- b) Demostreu que $\text{SL}(n, K)$ i $\text{O}(n, K)$ són subgrups del grup $\text{GL}(n, K)$.
- c) Demostreu que $\text{SO}(n, K)$ és un subgrup de $\text{O}(n, K)$.

Exercici 1.13.

$$\begin{aligned} \text{GL}(n, A) &:= \{M \in \text{M}(n, A) : \det(M) \in A^*\} && \text{grup lineal} \\ \text{SL}(n, A) &:= \{M \in \text{GL}(n, A) : \det(M) = 1\} && \text{grup especial lineal} \\ \text{O}(n, A) &:= \{M \in \text{GL}(n, A) : M^t M = \text{Id}\} && \text{grup ortogonal} \\ \text{SO}(n, A) &:= \{M \in \text{O}(n, A) : \det(M) = 1\} && \text{grup especial ortogonal} \end{aligned}$$

- a) Demostreu que $\text{GL}(n, A)$ és un grup amb la multiplicació de matrius.
- b) Demostreu que $\text{SL}(n, A)$ i $\text{O}(n, A)$ són subgrups del grup $\text{GL}(n, A)$.
- c) Demostreu que $\text{SO}(n, A)$ és un subgrup de $\text{O}(n, A)$.

Exercici 1.14. Considerem el grup $G := \text{GL}(2, \mathbb{F}_2)$. Escriviu els elements de G i la taula del producte de G . És G abelià?

Exercici 1.15. Demostreu que, donat un cos K , el grup $\text{SO}(2, K)$ és abelià. Demostreu que, en canvi, el grup $\text{SO}(n, K)$, per a $n \geq 3$, no ho és.

Exercici 1.16. Demostreu que, per a $n \geq 2$, el subconjunt de $\text{GL}(n, \mathbb{Z})$ format per les matrius simètriques no és un subgrup de $\text{GL}(n, \mathbb{Z})$. El subconjunt de $\text{M}(n, \mathbb{Z})$ format per les matrius simètriques és un subgrup de $\text{M}(n, \mathbb{Z})$?

Exercici 1.17. Siguin H i K subgrups d'un grup G . Definim el producte de H i K com el conjunt $HK := \{hk : h \in H, k \in K\}$. Demostreu que HK és subgrup de G si, i només si, $HK = KH$.

Exercici 1.18. Siguin H, K, I subgrups d'un grup G tals que $I \subseteq HK$. Proveu que aleshores $I \subseteq HK \cap KH$. Doneu una condició necessària i suficient perquè el conjunt $HK \cap KH$ sigui subgrup del grup G .

Exercici 1.19. Siguin H i K subgrups finits d'un grup G . Proveu que el cardinal de HK és:

$$|HK| = \frac{|H||K|}{|H \cap K|}$$

Exercici 1.20. (Regla de Dedekind) Siguin G un grup i H, K, F subgrups de G tals que $F \subseteq K$. Aleshores $(H \cap K)F = HF \cap K$.

Definició 1.4. Sigui G un grup. Diem que G és *finit* si el seu cardinal és finit i, en aquest cas, es defineix l'*ordre* de G , que indiquem per $|G|$, com el nombre d'elements de G .

Definició 1.5. Siguin G un grup i $x \in G$ un element. Per a un enter $n \in \mathbb{Z}$, escrivim:

$$x^n := \begin{cases} x \cdots x & \text{si } n > 0 \\ e & \text{si } n = 0 \\ x^{-1} \cdots x^{-1} & \text{si } n < 0 \end{cases}$$

Escrivim $\langle x \rangle := \{x^n : n \in \mathbb{Z}\}$. Definim l'*ordre* de x , $\text{ord}(x)$, com $\text{ord}(x) := |\langle x \rangle|$. Un grup G s'anomena *cíclic* si existeix un element $x \in G$ tal que $G = \langle x \rangle$. A vegades notarem C_n per indicar un grup cíclic d'ordre n .

Exercici 1.21. Siguin G un grup i $x \in G$.

- Proveu que $\langle x \rangle$ és un subgrup de G . Diem que $\langle x \rangle$ és el *subgrup de G generat per x* .
- Proveu que $\langle x \rangle$ és finit si, i només si, existeix un enter $n > 0$ tal que $x^n = e$. En aquest cas, $|\langle x \rangle| \leq n$.
- Proveu que $\text{ord}(x) = n$ si, i només si, $n > 0$, $x^n = e$ i, per a qualsevol enter m tal que $x^m = e$, aleshores $n \mid m$.
- Si $\text{ord}(x) = n$, proveu que $\text{ord}(x^m) = n/\text{mcd}(n, m)$.
- Si $\text{ord}(x) = n$, proveu que x^m genera $\langle x \rangle$ si, i només si, $(n, m) = 1$. Deduïu que, aleshores, el nombre de generadors del grup $\langle x \rangle$ és $\varphi(n) = \#\{m : 1 \leq m \leq n : (m, n) = 1\}$.

Exercici 1.22. Sigui G un grup cíclic d'ordre n .

- Proveu que qualsevol subgrup de G és cíclic i el seu ordre divideix n .
- Proveu que per a cada $d \mid n$, existeix un únic subgrup G_d de G d'ordre d .

Exercici 1.23. Per a $n \in \mathbb{Z}$, $n \geq 1$, es defineix la *funció d'Euler* φ en n com:

$$\varphi(n) := \#\{m \in \mathbb{Z} : 1 \leq m \leq n, \text{mcd}(n, m) = 1\}$$

- Proveu que si G és un grup cíclic d'ordre n , aleshores, per a cada $d \mid n$, existeixen exactament $\varphi(d)$ elements d'ordre d en G .
- Deduïu que $\sum_{d \mid n} \varphi(d) = n$.

Definició 1.6. Sigui G un grup i $x, x' \in G$. Diem que x i x' són *conjugats* si existeix un element $y \in G$ tal que $yxy^{-1} = x'$. El conjunt d'elements conjugats de $x \in G$ s'escriu $\text{Cl}(x) := \{yxy^{-1} : y \in G\} \subseteq G$ i s'anomena *classe de conjugació de x* . Si H és un subgrup de G i $x \in H$, s'anomena *classe de conjugació de x en H* el conjunt $\text{Cl}_H(x) := \{yxy^{-1} : y \in H\} \subseteq H$. Per al grup G , notarem indistintament $\text{Cl}(x)$ i $\text{Cl}_G(x)$.

Exercici 1.24. Sigui G un grup. Proveu que G és abelià si, i només si, $\text{Cl}(x) = \{x\}$, per a tot $x \in G$.

Exercici 1.25. Sigui a, b dos elements d'un grup G . Proveu que $\text{ord}(bab^{-1}) = \text{ord}(a)$ i que $\text{ord}(ab) = \text{ord}(ba)$. Deduïu que dos elements conjugats tenen el mateix ordre.

Exercici 1.26. Sigui n un enter. Proveu que $\mathbb{Z}/n\mathbb{Z}$ és un grup cíclic d'ordre n .

Exercici 1.27. Sigui G un grup no trivial. Proveu que si els únics subgrups de G són el trivial i el total, aleshores G és un grup finit d'ordre primer.

Exercici 1.28. Sigui $\mu_n = \{z \in \mathbb{C} : z^n = 1\}$ el conjunt de les arrels n -èsimes de la unitat complexes. Demostreu que μ_n amb el producte de $\mathbb{C}$ és un grup cíclic.

Exercici 1.29. Sigui p, q nombres primers diferents i $r, s \geq 1$ nombres enters.

- Determineu quants elements del grup $\mathbb{Z}/p\mathbb{Z}$ el generen.
- Determineu quants elements del grup $\mathbb{Z}/p^r\mathbb{Z}$ el generen.
- Determineu quants elements del grup $\mathbb{Z}/p^r q^s\mathbb{Z}$ el generen.

Definició 1.7. Sigui G un grup i $S \subseteq G$ un subconjunt. Definim el *subgrup de G generat per S* , que escriurem $\langle S \rangle$, com la intersecció de tots els subgrups de G que contenen S . Si H és un subgrup de G i $H = \langle S \rangle$, direm que S és un *conjunt (o sistema) de generadors de H* . Si $S = \emptyset$, $\langle S \rangle = \{e\}$.

Exercici 1.30. Sigui G un grup i $S \subseteq G$ un subconjunt no buit. Aleshores $\langle S \rangle$ és el subgrup més petit de G que conté S ; és a dir, $\langle S \rangle$ és un subgrup de G i, per a qualsevol subgrup H de G tal que $S \subseteq H$, aleshores $\langle S \rangle \subseteq H$.

Exercici 1.31. Sigui G un grup i $S \subseteq G$ un subconjunt no buit. Proveu que:

$$\langle S \rangle = \{x_1^{n_1} \cdots x_r^{n_r} : r \in \mathbb{Z}_{>0}, x_1, \dots, x_r \in S, n_1, \dots, n_r \in \mathbb{Z}\}$$

Exercici 1.32. (*El grup dels quaternions*) Sigui Q_8 el subgrup de $\text{GL}(2, \mathbb{C})$ generat per les matrius

$$\text{Id} := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, i := \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, j := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, k := \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

- Demostreu que Q_8 és un grup d'ordre 8 tal que Id és l'element neutre i es compleixen les igualtats $i^4 = \text{Id}$, $i^2 = j^2$ i $ij = ji^3$.
- Calculeu l'ordre de cadascun dels elements de Q_8 .

Exercici 1.33. Es defineix el grup *diedral* D_{2n} com el grup de desplaçaments del pla que deixen invariant un polígon regular de n costats.

- Descriu els elements de D_{2n} i digueu quants n'hi ha.
- Siguin ρ una rotació d'angle $2\pi/n$ centrada en el centre de simetria del polígon, i σ una simetria axial respecte d'un dels radis del polígon. Proveu que es compleixen les igualtats $\rho^n = \text{Id}$, $\sigma^2 = \text{Id}$ i $\sigma\rho\sigma = \rho^{-1}$.
- Proveu que $D_{2n} = \langle \rho, \sigma \rangle$ i $D_{2n} = \{\text{Id}, \rho, \dots, \rho^{n-1}, \sigma, \rho\sigma, \dots, \rho^{n-1}\sigma\}$. Observeu que D_{2n} queda determinat pels generadors ρ, σ i les relacions $\rho^n = \text{Id}$, $\sigma^2 = \text{Id}$ i $\sigma\rho\sigma = \rho^{-1}$.

Definició 1.8. Donat un conjunt X , una *permutació* de X és una aplicació bijectiva de X en X i S_X és el conjunt format per totes les permutacions de X . En el cas $X = \{1, 2, \dots, n\}$, per a $n \geq 1$ un enter, escriurem $S_X = S_n$ i diem que S_n és el *grup simètric de n elements*. Per donar una permutació concreta $\sigma \in S_n$, cal dir qui és la imatge de cada un dels elements $1, 2, \dots, n$. Una manera útil de fer-ho és escrivint aquests elements en una fila i, sota de cada un, la seva imatge:

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

Donades les permutacions $\sigma, \tau \in S_n$, escriurem indistintament $\sigma \circ \tau$ i $\sigma\tau$. Diem que un element $i \in \{1, \dots, n\}$ és *fix* per una permutació $\sigma \in S_n$ si $\sigma(i) = i$.

Exercici 1.34. Proveu que S_n amb la composició és un grup d'ordre $n!$.

Definició 1.9. Donats r elements $i_1, \dots, i_r \in \{1, 2, \dots, n\}$, diferents dos a dos, designem per $(i_1, \dots, i_r)$ la permutació σ de S_n tal que $\sigma(i_1) = i_2$, $\sigma(i_2) = i_3$, ..., $\sigma(i_{r-1}) = i_r$, $\sigma(i_r) = i_1$ i $\sigma(i) = i$, per a qualsevol $i \notin \{i_1, \dots, i_r\}$; és a dir, si $\{i_{r+1}, \dots, i_n\} = \{1, 2, \dots, n\} \setminus \{i_1, \dots, i_r\}$,

$$(i_1, \dots, i_r) = \begin{pmatrix} i_1 & i_2 & \dots & i_{r-1} & i_r & i_{r+1} & \dots & i_n \\ i_2 & i_3 & \dots & i_r & i_1 & i_{r+1} & \dots & i_n \end{pmatrix}$$

Un *cicle d'ordre r* de S_n és una permutació de la forma $(i_1, \dots, i_r)$. Un cicle d'ordre 2 s'anomena *transposició*.

Dos cicles $(i_1, \dots, i_r)$ i $(j_1, \dots, j_s)$ s'anomenen *disjunts* si ho són els conjunts $\{i_1, \dots, i_r\}$ i $\{j_1, \dots, j_s\}$. Clarament dos cicles disjunts commuten entre ells.

Exercici 1.35. Proveu que S_n és commutatiu si, i només si, $n = 1, 2$.

Exercici 1.36. Proveu que:

- Qualsevol permutació de S_n diferent de la identitat s'escriu com a producte de cicles disjunts, determinats de manera única llevat de l'ordre.
- Qualsevol permutació de S_n s'escriu com a producte de transposicions.

Exercici 1.37. Proveu que:

- La permutació identitat només es pot escriure com a producte d'un nombre parell de transposicions. (Indicació: escriu la identitat com a producte de transposicions de la forma $(1, i)$, per a $i > 1$.)
- Si $\sigma = \tau_1 \circ \dots \circ \tau_r = \rho_1 \circ \dots \circ \rho_s$, on τ_i, ρ_i són transposicions, aleshores $r \equiv s \pmod{2}$.

Definició 1.10. Una permutació es diu *parella* si descompon com a producte d'un nombre parell de transposicions i *senar* si descompon com a producte d'un nombre senar de transposicions. Observem que aquesta definició té sentit gràcies a l'exercici 1.37. Anomenem *aplicació signe* l'aplicació:

$$\begin{aligned} \epsilon : S_n &\longrightarrow \{1, -1\} \\ \sigma &\longmapsto \epsilon(\sigma) = \begin{cases} 1 & \text{si } \sigma \text{ és parella} \\ -1 & \text{si } \sigma \text{ és senar} \end{cases} \end{aligned}$$

Observem que si $\sigma = (a_1, \dots, a_r)$ és un r -cicle, aleshores podem escriure σ com a producte de $r - 1$ transposicions com $\sigma = (a_1, a_2) \cdots (a_{r-1}, a_r)$ i, per tant, $\epsilon(\sigma) = (-1)^{r-1}$. En particular, les transposicions tenen signe -1 .

Exercici 1.38. Siguin $\sigma, \tau \in S_9$ les permutacions següents:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 9 & 1 & 8 & 7 & 6 & 3 & 4 & 5 \end{pmatrix} \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 1 & 3 & 5 & 8 & 2 & 9 & 6 & 4 \end{pmatrix}$$

- Calculeu $\sigma\tau$ i $\tau\sigma$.
- Descomponen σ i τ com a producte de cicles disjunts, i també com a producte de transposicions; calculeu les seves signatures.
- Calculeu σ^{2021} .

Exercici 1.39. Considereu els subgrups $H = \langle (1, 2) \rangle$ i $K = \langle (1, 3) \rangle$ del grup simètric S_3 . Proveu que HK no és un subgrup de S_3 .

Exercici 1.40. a) Demostreu que, donada una permutació $\rho \in S_n$ i donats elements $a_1, \dots, a_r \in \{1, \dots, n\}$, llavors

$$\rho(a_1, \dots, a_r)\rho^{-1} = (\rho(a_1), \dots, \rho(a_r))$$

- Demostreu que, donats dos cicles σ_1 i σ_2 de S_n del mateix ordre, existeix una permutació $\rho \in S_n$ tal que $\rho\sigma_1\rho^{-1} = \sigma_2$.
- Sigui $\sigma = \sigma_1 \cdots \sigma_k \in S_n$, on $\sigma_1, \dots, \sigma_k$ són cicles disjunts dos a dos. Per a qualsevol permutació ρ de S_n , proveu que $\rho\sigma\rho^{-1}$ és producte de k cicles disjunts, amb ordres iguals als de $\sigma_1, \dots, \sigma_k$.
- Siguin $\sigma_1, \dots, \sigma_k \in S_n$ cicles disjunts dos a dos, i també $\tau_1, \dots, \tau_k \in S_n$ cicles disjunts dos a dos. Posem $\sigma := \sigma_1 \cdots \sigma_k$ i $\tau := \tau_1 \cdots \tau_k$. Demostreu que si, per a $1 \leq i \leq k$, l'ordre del cicle σ_i coincideix amb l'ordre del cicle τ_i , aleshores existeix una permutació $\rho \in S_n$ tal que $\rho\sigma\rho^{-1} = \tau$.

Exercici 1.41. Determineu la signatura i l'ordre de totes les permutacions de S_3 . Determineu tots els subgrups de S_3 .

Exercici 1.42. Demostreu que S_n admet els sistemes de generadors següents:

- $(1, 2), (1, 3), \dots, (1, n)$.
- $(1, 2), (2, 3), \dots, (n-1, n)$.
- $(1, 2, \dots, n), (1, 2)$.

Exercici 1.43. Sigui A_n el conjunt de permutacions parelles de S_n , per a $n \geq 2$. Demostreu que:

- a) S_n té el mateix nombre de permutacions parelles que de permutacions senars.
- b) A_n és un subgrup de S_n .

Definició 1.11. Si designem per A_n el conjunt de totes les permutacions parelles de S_n , aleshores A_n és un subgrup de S_n que s'anomena *grup alternat*.

Exercici 1.44. Proveu que, per a $n \geq 3$, A_n admet els conjunts de generadors següents:

- a) El conjunt de tots els 3-cicles.
- b) El conjunt de 3-cicles de la forma $(1, i, j)$, amb $1 < i < j \leq n$.
- c) El conjunt de 3-cicles de la forma $(1, 2, k)$, amb $2 < k \leq n$.

1.2. Subgrups normals. Grup quocient

Exercici 1.1. (Classes laterals per l'esquerra) Sigui H un subgrup d'un grup G . Definim entre els elements de G la relació següent:

$$g \sim g' \Leftrightarrow g \in g'H$$

- a) Proveu que $\sim$ defineix una relació d'equivalència en G . Escriurem $G/H := G/\sim$ i direm que és el conjunt de *classes laterals per l'esquerra de G mòdul H* . Si G/H és finit, escriurem $[G : H] := |G/H|$ i direm que és l'*índex de H en G* .
- b) Per a un element $g \in G$, escriurem $[g]$ per a la classe de g . Proveu que $[g] = gH$.
- c) Si G és finit, proveu que $|H|$ divideix $|G|$ i $[G : H] = |G|/|H|$.
- d) Definim en G/H l'operació següent: $[g][g'] = [gg']$. Proveu que està ben definida si, i només si, $ghg^{-1} \in H$, per a qualssevol $h \in H$, $g \in G$. Aleshores G/H té estructura de grup amb aquesta operació.

Exercici 1.2. (Classes laterals per la dreta) Sigui H un subgrup d'un grup G . Definim entre els elements de G la relació següent:

$$g \equiv g' \Leftrightarrow g \in Hg'$$

- a) Proveu que $\equiv$ defineix una relació d'equivalència en G . Escriurem $H \backslash G := G/\equiv$ i direm que és el conjunt de *classes laterals per la dreta de G mòdul H* . Si $H \backslash G$ és finit, escriurem $[G : H] = |H \backslash G|$ i direm que és l'*índex de H en G* .
- b) Per a un element $g \in G$, escriurem $\overline{g}$ per a la classe de g . Proveu que $\overline{g} = Hg$.
- c) Si G és finit, proveu que $[G : H] = |G|/|H|$.
- d) Definim en $H \backslash G$ l'operació següent: $\overline{g}\overline{g'} = \overline{gg'}$. Proveu que està ben definida si, i només si, $ghg^{-1} \in H$, per a qualssevol $h \in H$, $g \in G$. Aleshores $H \backslash G$ té estructura de grup amb aquesta operació.

Exercici 1.3. (Teorema de Lagrange) Si G és un grup i H és un subgrup de G , aleshores G és finit si, i només si, H i G/H són finits. En aquest cas, $|G| = |H|[G : H]$. En particular, $|H|$ i $[G : H]$ són divisors de $|G|$.

Exercici 1.4. Si G és un grup finit, l'ordre de qualsevol element divideix l'ordre del grup.

Exercici 1.5. Si G és un grup d'ordre primer, aleshores G és un grup cíclic i qualsevol element de G diferent del neutre genera G .

Definició 1.1. Sigui G un grup i $H \subseteq G$ un subgrup. Direm que H és un *subgrup normal* de G , i escriurem $H \triangleleft G$, si $ghg^{-1} \in H$, per a tot $g \in G$, $h \in H$. En aquest cas, G/H té estructura de grup i direm que és el *grup quocient de G per H* . Si G és un grup finit, l'ordre del grup G/H o *índex de H en G* és $[G : H] = |G|/|H|$.

Exercici 1.6. Sigui G un grup. Proveu que:

- a) Els subgrups $\{e\}$ i G són subgrups normals de G .
- b) Si G és un grup abelià, tots els seus subgrups són normals.
- c) Si $\{H_i\}_{i \in I}$ és una família de subgrups normals de G , llavors $\bigcap_{i \in I} H_i$ és un subgrup normal de G .

Exercici 1.7. Sigui G un grup i H un subgrup. Proveu que H és un subgrup normal de G si, i només si, $G/H = H \setminus G$; és a dir, per a qualsevol $g \in G$, $gH = Hg$.

Exercici 1.8. Demostreu que tot subgrup d'índex 2 d'un grup és normal. Dedueu que A_n és un subgrup normal de S_n .

Exercici 1.9. Sigui $D_{2n} = \langle \rho, \sigma : \rho^n = \sigma^2 = \text{Id}, \sigma\rho\sigma = \rho^{-1} \rangle$ el grup diedral de $2n$ elements. Si d és un divisor de n , proveu que $\langle \rho^d \rangle$ és un subgrup normal de D_{2n} .

Exercici 1.10. Sigui G un grup i H un subgrup normal de G . Si G/H és abelià, proveu que tots els subgrups de G que contenen H són normals en G .

Exercici 1.11. Sigui G un grup i $H \subseteq G$ un subgrup d'ordre n . Proveu que:

- a) Per a qualsevol $g \in G$, gHg^{-1} és un subgrup de G d'ordre n .
- b) Si G té un únic subgrup d'ordre n , aleshores H és normal en G .

Definició 1.2. Sigui G un grup. Donats dos subgrups H, H' de G , diem que H i H' són *conjugats en G* si existeix un element $g \in G$ tal que $gHg^{-1} = H'$. El conjunt de subgrups conjugats d'un subgrup H de G s'escriu $\text{Cl}_G(H) := \{gHg^{-1} : g \in G\}$ i s'anomena *classe de conjugació de H en G* .

Exercici 1.12. Sigui K i H subgrups d'un grup G , $H \triangleleft G$. Proveu que HK és un subgrup de G .

Definició 1.3. Un grup G és *simple* si no té subgrups normals diferents de $\{e\}$ i G .

Exercici 1.13. Proveu que els grups d'ordre primer són simples.

Definició 1.4. Donats un grup G i elements $x, y \in G$, es defineix el *commutador de x i y* com $[x, y] := xyx^{-1}y^{-1} \in G$.

Exercici 1.14. Sigui G un grup i $x, y \in G$. Proveu que:

- a) $xy = [x, y]yx$. En particular, x i y commuten si, i només si, $[x, y] = e$.
- b) $[x, y]^{-1} = [y, x]$.

Definició 1.5. Donat un grup G i donats dos subconjunts no buits A i B de G , es defineix el *commutador de A i B* , que escriurem $[A, B]$, com el subgrup de G generat pels elements de la forma $[a, b]$, amb $a \in A$ i $b \in B$; és a dir, $[A, B] := \langle [a, b] : a \in A, b \in B \rangle$. Es defineix el *commutador de G* (o *subgrup derivat de G*) com $G' := [G, G] = \langle [x, y] : x, y \in G \rangle$.

Exercici 1.15. Sigui G un grup. Proveu que:

- a) G és abelià si, i només si, $G' = \{e\}$.
- b) G' és un subgrup normal de G .
- c) G/G' és un grup abelià.
- d) G' és el menor subgrup normal de G tal que G/G' és abelià; és a dir, per a qualsevol subgrup normal $N \triangleleft G$ tal que G/N és abelià, se satisfà que $G' \subseteq N$.
- e) Si $G' \subseteq N$, aleshores $N \triangleleft G$ i G/N és abelià.

El grup $G^{ab} = G/G'$ s'anomena *grup abelianitzat de G* .

Exercici 1.16. Trobeu el commutador de S_3 .

Exercici 1.17. Proveu que $S'_n = A_n$, per a qualsevol $n \geq 2$.

Exercici 1.18. Proveu que $A'_n = A_n$, per a qualsevol $n \neq 3, 4$. Determineu el commutador de A_n per a $n = 3, 4$.

Exercici 1.19. Sigui $D_{2n} = \langle \rho, \sigma : \rho^n = \sigma^2 = \text{Id}, \sigma\rho\sigma = \rho^{-1} \rangle$ el grup diedral. Proveu que $D'_{2n} = \langle \rho^2 \rangle$.

Definició 1.6. Donats un grup G i un enter $k \geq 0$, definim per recurrència el *subgrup derivat k -èsim* $G^{(k)}$ de G de la forma següent: $G^{(0)} := G$, $G^{(1)} := G'$, $G^{(2)} := (G')'$ i, en general, $G^{(k+1)} := (G^{(k)})'$.

Exercici 1.20. Sigui G un grup. Proveu que:

- a) $G^{(k)} \triangleleft G^{(k-1)}$, per a qualsevol enter $k \geq 1$.
- b) Si N és un subgrup normal de G , aleshores N' també és un subgrup normal de G .
- c) $G^{(k)} \triangleleft G$, per a qualsevol enter $k \geq 0$.

Exercici 1.21. Sigui G un grup i $H \subseteq G$ un subgrup. Es defineix el *normalitzador de H en G* , que escriurem $N_G(H)$, com $N_G(H) := \{x \in G : xHx^{-1} = H\}$.

- a) Proveu que $N_G(H)$ és un subgrup de G que conté H .
- b) Proveu que $H \triangleleft N_G(H)$.
- c) Proveu que, donat un subgrup K de G , se satisfà que $H \triangleleft K$ si, i només si, $K \subseteq N_G(H)$. Deduiu que $N_G(H)$ és el subgrup més gran de G en el qual H és normal.
- d) Proveu que $H \triangleleft G$ si, i només si, $N_G(H) = G$ si, i només si, $\text{Cl}_G(H) = \{H\}$.
- e) Si K és un subgrup del normalitzador $N_G(H)$, aleshores HK és un grup i H és normal en HK .

Exercici 1.22. Sigui G un grup i N un subgrup normal de G . Si H i K són subgrups de G , aleshores $H \triangleleft K$ implica que $HN \triangleleft KN$.

Exercici 1.23. Sigui G un grup. Definim el *centre* de G com:

$$z(G) := \{x \in G : xy = yx, \text{ per a tot } y \in G\}$$

Proveu que:

- a) $z(G)$ és un subgrup normal de G .
- b) Si H és un subgrup de $z(G)$, H és un subgrup normal de G .

Exercici 1.24. Sigui G un grup i $x \in G$. Es defineix el *centralitzador* de x en G com:

$$z_G(x) := \{y \in G : xy = yx\}$$

Proveu que:

- a) $z_G(x)$ és un subgrup de G .
- b) $x \in z(G)$ si, i només si, $z_G(x) = G$ si, i només si, $\text{Cl}_G(x) = \{x\}$.

Exercici 1.25. Sigui G un grup, H un subgrup de G i $x \in G$.

- a) Proveu que $\#\text{Cl}_G(x) = [G : z_G(x)]$. En particular, el nombre d'elements conjugats de x en G divideix l'ordre de G .
- b) Deduïu que en A_4 no tots els 3-cicles són conjugats.
- c) Proveu que $\#\text{Cl}_G(H) = [G : N_G(H)]$. En particular, el nombre de subgrups conjugats de H en G divideix l'ordre de G .

Exercici 1.26. Sigui G un grup i $z(G)$ el seu centre. Proveu que:

- a) Si H és un subgrup abelià de G tal que $G = z(G)H$, aleshores G és abelià.
- b) Si H és un subgrup de $z(G)$ i G/H és cíclic, aleshores G és abelià.

Exercici 1.27. Sigui K un cos. Demostreu que el centre de $\text{GL}(n, K)$ està format per les matrius de la forma $M = \lambda \text{Id}$, per a algun $\lambda \in K^*$.

Exercici 1.28. Demostreu que si $n \geq 3$, el centre de S_n només conté la identitat.

Exercici 1.29. Sigui G un grup i $H \subseteq G$ un subgrup. Es defineix el *core* de H en G com:

$$\text{core}_G(H) := \bigcap_{g \in G} gHg^{-1}$$

Proveu que:

- a) $\text{core}_G(H)$ és un subgrup normal de G contingut en H .
- b) Si K és un subgrup normal de G contingut en H , aleshores $K \subseteq \text{core}_G(H)$. És a dir, $\text{core}_G(H)$ és el subgrup normal de G més gran contingut en H .

Exercici 1.30. Sigui G un grup i $H \subseteq G$ un subgrup. Es defineix la *clausura normal* de H en G com: