Tema 3 (II): Grups abstractes

3.1. En un conjunt $G = \{a, b, c, d, e|f\}$ hi tenim una operació de la qual només en sabem parcialment la seva taula:

	a	b	c	d	e	f
a	b	e	d		a	
b					b	
c	f	a			c	
d					e	
e	a	b	c	d	e	f
f					f	

Completeu la taula, sabent que amb aquesta operació G és un grup.

3.2. En el conjunt $\mathbb{R}^*$ dels nombres reals positius es defineix l'operació següent:

$$a \star b = \begin{cases} ab & \text{si } a > 0, \\ a/b & \text{si } a < 0, \end{cases} .$$

Demostreu que aquesta operació defineix una estructura de grup en $\mathbb{R}^*$. És un grup abelià?

3.3. Comproveu que la *diferència simètrica* de conjunts

$$A \triangle B := (A \cup B) \setminus (A \cap B)$$

defineix una estructura de grup commutatiu en el conjunt $\mathcal{P}(X)$ de les parts d'un conjunt X, i digueu quin és l'ordre dels seus elements.

3.4. Sigui n enter, $n \geq 3$ i $\mu_n = \{e^{i2\pi k/n} \mid k = 0, 1, \ldots, n-1\}$ el conjunt de les arrels n-èssimes de 1 en $\mathbb{C}(\simeq \mathbb{R}^2)$. Sigui $D_{2n} = \{f : \mathbb{R}^2 \to \mathbb{R}^2 \mid f \text{ moviment}, f(\mu_n) = \mu_n\}$.

(a) Proveu que si $f \in D_{2n}$, aleshores f és lineal ($f(0) = 0$).

(b) Proveu que si $f \in D_{2n}$, aleshores la matriu de f en les bases canòniques és

$$r_k = \begin{pmatrix} \cos(2\pi k/n) & -\sin(2\pi k/n) \\ \sin(2\pi k/n) & \cos(2\pi k/n) \end{pmatrix} \text{ o } s_k = \begin{pmatrix} \cos(2\pi k/n) & \sin(2\pi k/n) \\ \sin(2\pi k/n) & -\cos(2\pi k/n) \end{pmatrix},$$

per a $k = 0, 1, \ldots, n-1$.

(*c*) Anomemen $r := r_1$ el gir d'angle $2\pi/n$. Anomenem $s := s_0$ la simetria respecte de l'eix x. Comproveu que $r_k = r^k$ és el gir d'angle $2\pi k/n$; que $s_k = r^k s$ és la simetria respecte de la recta per l'origen i de vector director $(\cos(\pi k/n), \sin(\pi k/n)$. Comproveu que $r^k s = s r^{-k}$.

(*d*) Deduïu $D_{2n} = \{r_k, s_k \mid k = 0, 1, \ldots, n-1\} = \{1, r, \ldots, r^{n-1}, s, rs, \ldots, r^{n-1}s\}$ i que té cardinal $2n$. Proveu que D_{2n} amb la composició és un grup. Se l'anomena el **grup diedral**.

(*e*) Identifiqueu el grup diedral D_{2n} amb un subgrup del simètric $\mathcal{S}_n$.

3.5. Demostreu que:

$$\mathrm{ord}(a^{-1}) = \mathrm{ord}(a), \qquad \mathrm{ord}(bab^{-1}) = \mathrm{ord}(a), \qquad \mathrm{ord}(ba) = \mathrm{ord}(ab).$$

3.6. Siguin a, b dos elements qualssevol d'un grup G. Demostreu que els elements ab i ba tenen el mateix ordre.

3.7. Demostreu que el grup additiu del cos $\mathbb{Q}$ no és cíclic.

3.8. Demostreu que tots els elements de $\mathbb{Q}/\mathbb{Z}$ tenen ordre finit, i que hi ha elements d'ordre arbitràriament gran. Demostreu que el conjunt dels elements d'ordre finit de $\mathbb{R}/\mathbb{Z}$ és justament $\mathbb{Q}/\mathbb{Z}$.

3.9. Determineu l'ordre al grup multiplicatiu $\mathbb{C}^*$ d'un complex no nul $z = re^{2\pi it}$ de mòdul r i argument $2\pi t$, en funció de r i t.

3.10. Demostreu que una matriu invertible $A \in \mathrm{GL}_n(\mathbb{C})$ té ordre finit si, i només si, diagonalitza i els seus valors propis són arrels de la unitat. En aquest cas, doneu l'ordre de A en funció dels seus valors propis.

3.11. Sigui A un grup commutatiu. Siguin $a, b \in A$ elements d'ordres $\mathrm{ord}(a) = m$ i $\mathrm{ord}(b) = n$, respectivament. Sigui $[m, n]$ el mínim comú múltiple i (m, n) el màxim comú divisor. Demostreu que:

1. $\mathrm{ord}(ab)$ divideix $[m, n]$, però en general no són iguals;
2. si $(m, n) = 1$ aleshores $\mathrm{ord}(ab) = [m, n] = mn$;
3. el grup conté algun element d'ordre $[m, n]$ (que no sempre és ab).
   Indicació: demostreu primer, fent servir la descomposició en primers, que existeixen divisors $m_0 \mid m$ i $n_0 \mid n$ tals que $(m_0, n_0) = 1$ i $[m_0, n_0] = [m, n]$.

Usant l'últim apartat demostre que tot subgrup finit del grup multiplicatiu d'un cos és cíclic.

3.12. Al grup $\mathrm{SL}_2(\mathbb{Z})$ calculeu els ordres dels tres elements següents:

$$U = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}, \qquad S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \qquad T = US = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

i traieu conclusions sobre la finitud dels ordres d'elements i del seu producte.

3.13. Sigui f un homomorfisme de grups. Demostreu que si $\mathrm{ord}(a) = n$ és finit aleshores l'ordre de $f(a)$ divideix n. Si a té ordre infinit, què es pot dir de l'ordre de $f(a)$?

3.14. Determineu tots els homomorfismes $C \to G$ d'un grup cíclic C en un grup G.

3.15. Sigui G = un grup en el que se qualsevol parella d'elements $a, b \in G$ satisfan $(ab)^2 = a^2b^2$. Demostreu que G és abelià.

3.16. Sigui $G = \{a_1, \ldots, a_n\}$ un grup abelià finit i sigui $x = a_1 \cdots a_n$. Demostreu que $x^2 = e$. Doneu un exemple en el qual $x = e$ directament, i un altre en el qual $x \neq e$.

3.17. (*Teorema de Wilson*) Apliqueu l'exercici anterior al grup $(\mathbb{Z}/pZ)^*$ per demostrar que si p és un nombre primer, llavors:

$$(p-1)! \equiv -1 \pmod{p}.$$

Demostreu que el recíproc també és cert: si se satisfà la congruència anterior, llavors p és primer.

3.18. Demostreu que un grup G és abelià si, i només si, l'aplicació $f : G \to G$ donada per $f(x) = x^2$ és un morfisme de grups. Demostreu que en aquest cas, f és un isomorfisme.

3.19. Demostreu que, tot i que els grups additiu $\mathbb{R}$ és isomorf al grup multiplicatiu $\mathbb{R}^*_{>0}$, el grup additiu $\mathbb{Q}$ no és isomorf al grup multiplicatiu $\mathbb{Q}^*_{>0}$.

3.20. Demostreu que un grup G en que tot element no trivial té ordre 2 és abelià i, si és finit, és isomorf a $(\mathbb{Z}/2\mathbb{Z})^n$.

3.21. Sigui $Q = \langle \imath, \jmath \rangle$ el subgrup de $\mathrm{GL}_2(\mathbb{C})$ generat per les matrius $\imath = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ i $\jmath = \left(\begin{smallmatrix} i & 0 \\ 0 & -i \end{smallmatrix}\right)$. Demostreu que els cinc grups Q, $D_{2\cdot 4}$, $\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ i $(\mathbb{Z}/2\mathbb{Z})^3$ són grups d'ordre 8 no isomorfs entre ells. Demostreu que tot grup G d'ordre 8 és isomorf a un dels cinc donats. Per fer-ho vegeu que si G no conté elements d'ordre 8 i conté un element a d'ordre 4, aleshores:

1. si $b \notin \langle a \rangle$ és $G = \langle a \rangle \sqcup b\langle a \rangle$ i $ab = ba$ o bé $ab = ba^3$;
2. si $ab = ba$ el grup G és isomorf a $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$;
3. si $ab = b^3a$ el grup G és isomorf a Q o a $D_{2\cdot 4}$ segons que b tingui ordre 4 o 2.

Deduïu quins són els grups d'ordre $n \leq 8$.

3.22. Sigui G un grup finit i H un subconjunt de G tancat pel producte (si $a, b \in H$, llavors $ab \in H$). Demostreu que H és un subgrup de G. Doneu un contraexemple en el cas que G sigui infinit.

3.23. Proveu que l'índex dels subgrups és multiplicatiu: si $K \subseteq H \subseteq G$, H, K, subgrups de G, aleshores $[G : K] = [G : H][H : K]$.

3.24. Doneu un exemple d'un grup G, un subgrup H d'índex 3 i un element $g \in G$ tal que $g^3 \notin H$.

3.25. Siguin $K \lhd N \lhd G$. Demostreu que si K és l'únic subgrup de N que té ordre $|K|$ aleshores $K \lhd G$. Doneu un exemple en que K no és normal a G i vegeu que no es compleix la hipòtesi anterior.

3.26. Sigui $f : G \to H$ un morfisme de grups i sigui $N \lhd G$ un subgrup normal de G. Demostreu que $f(N) \lhd H$.

3.27. Donat un morfisme de grups, és cert que les antiimatges de subgrups conjugats són subgrups conjugats? i les imatges?

3.28. (*Automorfismes interns*) Sigui G un grup.

1. Comproveu que, per a cada $a \in G$, l'aplicació $\gamma_a(x) = axa^{-1}$ de conjugació per a és un automorfisme de G. S'anomena *automorfisme intern* de G.
2. Sigui $\operatorname{Inn}(G)$ el conjunt dels automorfismes interns. Proveu que formen un subgrup de $\operatorname{Aut}(G)$.
3. Demostreu que $\operatorname{Inn}(G) \lhd \operatorname{Aut}(G)$. El quocient $\operatorname{Aut}(G)/\operatorname{Inn}(G)$ es denota $\operatorname{Out}(G)$.
4. Comproveu que l'aplicació $a \mapsto \gamma_a$ es un homomorfisme $G \to \operatorname{Aut}(G)$. Calculeu el seu nucli i la seva imatge. Què diu el teorema d'isomorfisme?
5. Demostreu que $\operatorname{Inn}(G)$ és isomorf a $G/Z/G$.

3.29. Siguin H i K subgrups normals amb intersecció trivial $H \cap K = \{1\}$. Demostreu que tot element de H commuta amb tot element de K.

3.30. *Producte directe.* Es diu que el grup G és *producte directe* dels seus subgrups H i K si l'aplicació $(h, k) \mapsto hk \colon H \times K \mapsto G$ és un isomorfisme de grups.

Demostreu que això es compleix si, i només si, H i K són tots dos normals, el seu producte és el total: $HK = G$, i tenen intersecció trivial: $H \cap K = \{1\}$.

La definició de producte directe es generalitza a més de dos subgrups de manera natural. Doneu una caracterització en termes dels subgrups anàloga a la donada. Indicació: Inspireu-vos en la suma directa d'espais vectorials.

3.31. Sigui G el grup lliure generat per dos símbols x, y. i considereu el subgrup $H = \langle u = x^2, v = y^2, w = xy \rangle$. Demostreu que H és isomorf al grup lliure generat per u, v, w.

3.32. Demostreu que el grup $G = \langle x, y \mid x^3, y^3, yxyxy \rangle$ és cíclic d'ordre 3.

3.33. Estudieu els grups següents:

a) $G = \langle x, y \mid x^2 = y^2 = e, xyx = yxy \rangle$.
b) $G = \langle x, y \mid x^3 = y^2 = yxyxy = e \rangle$.
c) $G = \langle x, y \mid y^3 = x^2yxy = e \rangle$.

3.34. (*El grup homofònic* En el grup lliure G generat per 26 símbols $\{a, b, c, \ldots, z\}$, diem que dos paraules (elements) són equivalents si es pronuncien igual en anglès. Per exemple, *bee* $\sim$ *be*. El grup quocient de G per aquesta relació s'anomena grup homofónic anglès. Se sap que el grup homofònic anglès és trivial (cf. *Quotients Homophones des Groupes Libres Homophonic Quotients of Free Groups*, J.F. Mestre, R. Schoof, L. Washington, D. Zagier, Experimental Mathematics, Experimental Mathematics, vol. 2, 1993). Se sap també que els grups homofònics francès i alemany són trivials, però en canvi, el grup homofònic coreà és un grup lliure amb dos generadors, i el grup homofònic turc és un grup lliure amb 22 generadors. Estudieu el grup homofònic català.

3.35. Siguin X un conjunt de cardinal n. Doneu un isomorfisme entre el grup $\mathrm{Perm}(X)$ de les permutacions de X i el grup simètric $\mathcal{S}_n$.

3.36. Sigui $n \geq 3$.

(a) Sigui H un grup amb dos generadors ρ i σ tals que compleixen $\mathrm{ord}(\rho) = n$, $\mathrm{ord}(\sigma) = 2$ i $rs = sr^{-1}$. Proveu que $H = \{1, \rho, \ldots, \rho^{n-1}, \sigma, \rho\sigma, \ldots, \rho^{n-1}\sigma\}$ i que el cardinal de H és $2n$. Deduïu que H és isomorf al grup diedral D_{2n}.

(b) Sigui G un grup i a, b elements d'ordre 2 de G tals que ab té ordre finit n. Demostreu que el subgrup $H = \langle a, b \rangle$ és isomorf al grup diedral D_{2n}.

3.37. Demostreu que tot grup d'ordre $2p$, amb p un primer senar, és isomorf a un dels dos grups $\mathbb{Z}/2p\mathbb{Z}$ o D_{2p}.

3.38. Doneu dos subgrups no isomorfs de $\mathcal{S}_9$ d'ordre 14.

3.39. Trobeu tots els subgrups de D_{2p}, D_{6p} i D_{8p}, on p és un primer > 3.

3.40. Sigui G un grup i X un G-conjunt. Sigui $m\colon G \to \mathrm{Perm}(X)$ l'homomorfisme corresponent. Demostreu que:

1. $x \in X$ és un punt fix si, i només si, el seu estabilitzador és tot G;
2. $\ker m$ és la intersecció dels estabilitzadors de tots els elements de x
3. m és injectiu si, i només si, l'acció és fidel.
4. si $|X| > 1$ i l'acció és transitiva m és no trivial.

3.41. Sigui G un grup finit, i $m \mapsto m_g \colon G \to \mathrm{Perm}(G)$ l'homomorfisme corresponent a l'acció per translació de G sobre ell mateix; o sigui, $m_g(a) = ga$ per a tot $a \in G$. Demostreu que:

1. La permutació m_g és senar si, i només si, el subgrup cíclic generat per g té ordre parell i índex senar a G.
   INDICACIÓ: estudieu la descomposició en cicles disjunts de m_g.
2. Si $\mathrm{Im}(m)$ conté alguna permutació senar, aleshores G conté algun subgrup d'índex 2.
3. Tot grup simple (no abelià) d'ordre parell té ordre divisible per 4.

3.42. Demostreu que tot grup G d'ordre $2n$ amb n senar conté un subgrup d'ordre n.
INDICACIÓ: Considereu l'acció $m \colon G \to \mathrm{Perm}(G) \simeq \mathcal{S}_{2n}$ sobre ell mateix per translació i estudieu la imatge d'un element d'ordre 2.

3.43. Sigui p el primer més petit que divideix $|G|$. Demostreu que tot subgrup de $H \subset G$ d'índex p és normal.
INDICACIÓ: Considereu l'acció per translació sobre el conjunt G/H.

3.44. Demostreu que si G és un grup finit simple i H és un subgrup propi, aleshores $|G|$ divideix $[G : H]!$. Deduïu que, per a $n \geq 5$, el grup alternat $\mathcal{A}_n$ no té subgrups d'índex $< n$.

3.45. Sigui p un primer. Demostreu que tot grup d'ordre p^2 és abelià.

3.46. Demostreu que un p-grup té subgrups de tots els ordres que divideixin el seu cardinal. Es dedueix que tot grup finit conté subgrups d'ordre tota potència de primer que divideixi el seu cardinal.

3.47. Demostreu que si tots els subgrups de Sylow d'un grup són normals aleshores el grup és el producte directe d'aquests subgrups de Sylow.

3.48. Calculeu tots els subgrups de Sylow del grup simètric $\mathcal{S}_5$.

3.49. Sigui G un grup simple que conté $k > 1$ p-subgrups de Sylow. Demostreu que G és isomorf a un subgrup de $\mathcal{S}_k$. Deduïu que no hi ha grups simples d'ordres $12, 24, 36, 48, 72, 80$ ni 96.

3.50. Demostreu que tot grup d'ordre 45 o 99 és abelià.

3.51. Demostreu que tot grup d'ordre 1645 és cíclic.

3.52. Demostreu que no existeix cap grup simple que tingui 280 elements.