LLICENCIATURA DE MATEMÀTIQUES

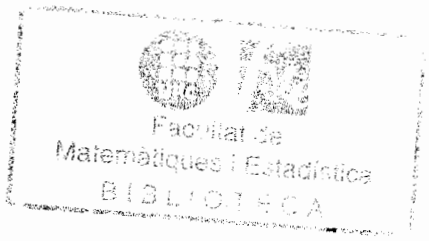
PROBLEMES

ÀLGEBRA ABSTRACTA

Jordi Quer
Anna Rio
Montserrat Vela

Departament de Matemàtica Aplicada 2

Facultat de Matemàtiques i Estadística
UNIVERSITAT POLITÈCNICA DE CATALUNYA



PROBLEMES D'ÀLGEBRA ABSTRACTA (FME) I. TEORIA DE GRUPS

Jordi Quer
Anna Rio
Montserrat Vela

Índex

Presentació

El temari de l'assignatura *Àlgebra Abstracta* que s'imparteix a la Facultat de Matemàtiques i Estadística de la Universitat Politècnica de Catalunya està dividit en tres blocs. El primer es dedica a la teoria de grups, el segon a la teoria d'anells, principalment enfocada a l'estudi d'anells de polinomis, i el tercer a la teoria de cossos i la teoria de Galois.

En aquest llibret es proposa una llista de problemes per a la primera part: una teoria de grups on s'han de tractar tots els conceptes necessaris per entendre en la part final del curs els resultats principals de la teoria de Galois.

Aquests exercicis i problemes es presenten dividits en cinc parts. La primera consta d'alguns exercicis senzills que un estudiant de l'assignatura ha de poder resoldre sense més ajut que uns apunts o un llibre de teoria. En la segona part hem agrupat exercicis relatius a diverses famílies de grups (grups cíclics, grups simètrics, etc.) que apareixeran sovint al llarg del curs. La tercera part conté els problemes pròpiament proposats per a les classes de problemes, és a dir, exercicis que s'han d'intentar resoldre individualment (o en grup) però que ocasionalment requeriran indicacions, suggeriments o guia del professsor. La quarta part inclou problemes que d'alguna manera són una ampliació del temari, conceptes que segurament formarien part de les classes de teoria sinó fos pels habituals problemes de calendari. Finalment, hem decidit incorporar problemes d'examen amb la seva resolució, considerant que aquest és un material prou útil per a la tasca personal que cadascú ha de dur a terme per dominar la matèria i aprovar l'assignatura.

Part 1

Exercicis bàsics

1. Sigui G un grup. Comproveu que l'element neutre de G és únic, que cada element de G té un únic invers i que $(xy)^{-1} = y^{-1}x^{-1}$.

2. Sigui X un conjunt on hi ha una operació associativa, amb element neutre per l'esquerra i tal que tot element té invers per l'esquerra. Demostreu que X, amb aquesta operació, és un grup.

3. Demostreu que el conjunt $\mathcal{P}(E)$ de parts d'un conjunt E, amb l'operació *diferència simètrica*

$$X \Delta Y = (X \cup Y) \setminus (X \cap Y),$$

té estructura de grup abelià.

4. Demostreu que en un grup G, per a qualsevol parell d'elements $x, y \in G$, l'ordre de xy coincideix amb l'ordre de yx .

5. Demostreu que si H és un subgrup de G i $g \in G$, aleshores $g^{-1}Hg$ també és subgrup de G.

6. Sigui G el grup de les bijeccions $f : \mathbb{C} \to \mathbb{C}$. Considereu el subconjunt H format per les bijeccions f tals que

$$|f(z) - f(w)| = |z - w| \qquad \forall z, w \in \mathbb{C}.$$

Demostreu que H és un subgrup de G.

7. Sigui $H = \{a/b \in \mathbb{Q}^* \mid a \equiv b \equiv 1 \pmod 2\}$. Demostreu que H és un subgrup de $\mathbb{Q}^*$.

8. Si $a, b \in \mathbb{R}$, amb $a \neq 0$, denotem $f_{a,b} : \mathbb{R} \to \mathbb{R}$ la trasformació afí $f_{a,b}(x) = ax + b$.

   (a) Calculeu $f_{a,b} \circ f_{c,d}$ i $f_{a,b}^{-1}$. Proveu que el conjunt A de les transformacions afins té estructura de grup amb la composició.

   (b) Considereu el subconjunt $H = \{f_{1,x} \mid x \in \mathbb{R}\}$. Demostreu que és un subgrup normal de A.

   (c) Demostreu que la classe lateral $f_{a,b}H$ només depèn de a. Proveu que A/H és isomorf a $\mathbb{R}^*$.

9. Demostreu que la funció exponencial estableix un isomorfisme entre el grup additiu $(\mathbb{R}, +)$ i el grup multiplicatiu $(\mathbb{R}^*, \cdot)$.

10. Sigui $\omega \in \mathbb{C}$ una arrel cúbica primitiva de la unitat. Demostreu que les matrius

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \omega & 0 \\ 0 & \omega^2 \end{pmatrix} \begin{pmatrix} \omega^2 & 0 \\ 0 & \omega \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & \omega^2 \\ \omega & 0 \end{pmatrix} \begin{pmatrix} 0 & \omega \\ \omega^2 & 0 \end{pmatrix}$$

    formen un grup amb la multiplicació. Establiu un isomorfisme entre aquest grup i el grup simètric $\mathfrak{S}_3$.

Part 2

Famílies de grups

Grups cíclics

1. Siguin G un grup cíclic amb generador x i H un subgrup de G. Demostreu que H és cíclic amb generador x^k on k és el mínim del conjunt $\{m \in \mathbb{N} : x^m \in H\}$. Quin és l'ordre de H?

2. Siguin $a, b \in \mathbb{Z}$. Demostreu que:

   (a) $\langle a, b\rangle = \langle \text{mcd}(a, b)\rangle$.

   (b) $\langle a\rangle \subseteq \langle b\rangle \iff b \mid a$.

   (c) $\langle a\rangle \cap \langle b\rangle = \langle \text{mcm}(a, b)\rangle$.

3. Demostreu que

   (a) Els subconjunts $n\mathbb{Z}$ són tots els subgrups de $\mathbb{Z}$.

   (b) Tot grup cíclic és isomorf a $\mathbb{Z}$ o a $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ per a algun $n > 0$.

   (c) Tot subgrup i tot quocient d'un grup cíclic és cíclic.

   (d) Per a cada enter $d \mid n$, el grup $\mathbb{Z}_n$ (i, per tant, tot grup cíclic d'ordre n) té exactament un subgrup d'ordre d.

   (e) $\mathbb{Z}_n \times \mathbb{Z}_m \simeq \mathbb{Z}_{nm}$ si, i només si, $\text{mcd}(n, m) = 1$.

   (f) El grup $\mathbb{Z}$ té dos generadors, 1 i -1. El grup $\mathbb{Z}_n$ té $\varphi(n)$ generadors.

   (g) El grup $\text{Aut}\,\mathbb{Z}$ és isomorf a $\mathbb{Z}/2\mathbb{Z}$ i $\text{Aut}\,\mathbb{Z}_n$ és isomorf a $\mathbb{Z}_n^*$.

4. Doneu un exemple de grup no cíclic tal que tots els seus subgrups propis siguin cíclics.

Grups simètrics

5. Considerem el conjunt $\mathfrak{S}_n$ de les aplicacions bijectives del conjunt $I_n = \{1, 2, \ldots, n\}$ en si mateix. Els elements de $\mathfrak{S}_n$ s'anomenen *permutacions*. Proveu que amb la composició de funcions $\mathfrak{S}_n$ és un grup, que té ordre $n!$ i que, si $n \geq 3$, no és abelià.

   Si $A = \{a_1, a_2, \ldots, a_r\} \subseteq I_n$ escriurem $\sigma = (a_1, a_2, \ldots, a_r)$ l'element de $\mathfrak{S}_n$ definit per $\sigma(a_i) = a_{i+1}$ per a $1 \leq i < r$, $\sigma(a_r) = a_1$ i σ deixa fixos els elements de I_n que no són de A. Un element d'aquest tipus s'anomena *cicle de longitud* r o *r-cicle*. Dos cicles $(a_1, a_2, \ldots, a_r)$ i $(b_1, b_2, \ldots, b_s)$ són *disjunts* si $\{a_1, a_2, \ldots, a_r\} \cap \{b_1, b_2, \ldots, b_s\} = \emptyset$. Demostreu que un r-cicle té ordre r, que cicles disjunts commuten i que l'ordre d'un producte de cicles disjunts és el mínim comú múltiple de les seves longituds.

6. Demostreu que tota permutació es pot escriure, de manera única llevat de l'ordre, com a producte de cicles disjunts on apareixen tots els elements de $\{1, 2, \ldots, n\}$.

   Es diu que $\sigma \in \mathfrak{S}_n$ es de tipus $[n_1, \ldots, n_k]$ si la seva descomposició està formada per k cicles disjunts de longituds $n_1, \ldots, n_k$. Demostreu que la conjugació conserva el tipus i que dues permutacions del mateix tipus sempre són conjugades. Quants elements té la classe de conjugació d'un k-cicle a $\mathfrak{S}_n$?

7. Un cicle de longitud 2 s'anomena *transposició*. Demostreu que tota permutació es pot escriure com a producte de transposicions i que si $\sigma_1 \cdots \sigma_r$ i $\tau_1 \cdots \tau_s$ són dues descomposicions de la mateixa permutació com a producte de transposicions, llavors r i s són de la mateixa paritat.

8. Demostreu que els subconjunts següents generen $\mathfrak{S}_n$.

   (a) Les transposicions $(1, i)$.

   (b) Les transposicions $(i, i+1)$.

   (c) El cicle $(1, 2, \ldots, n)$ i la transposició $(1, 2)$.

   (d) El cicle $(1, 2, \ldots, n)$ i una transposició $(i, i+1)$.

9. Comproveu que, en general, un n-cicle i una transposició no tenen perquè generar tot $\mathfrak{S}_n$ i trobeu les condicions en que això passa.

Grups alternats

10. Una permutació es diu *parella* o *senar* segons que descompongui en un nombre parell o senar de transposicions.

    Es defineix l'aplicació *signe*, $\operatorname{sgn} : \mathfrak{S}_n \to \{\pm 1\}$, posant $\operatorname{sgn}(\sigma) = +1$ si σ és parella i $\operatorname{sgn}(\sigma) = -1$ si σ és senar. Comproveu que es tracta d'un homomorfisme de grups.

    El nucli de sgn, format per les permutacions parelles, s'anomena *grup alternat* i es denota per $\mathfrak{A}_n$. Demostreu que el grup alternat és l'únic subgrup d'índex 2 de $\mathfrak{S}_n$.

11. Demostreu que els 3-cicles generen el grup alternat i que, de fet, n'hi ha prou amb els 3-cicles del tipus $(1, i, j)$ i fins i tot només amb els del tipus $(1, 2, i)$.

Grups diedrals

12. Sigui $n \geq 3$. El grup *diedral* n-èssim és el grup de les isometries del pla que deixen fix un n-agon regular. Es denota D_{2n} (o D_n).

    Aquest grup està generat per dos elements, r i s, on r és una rotació d'angle $2\pi/n$ al voltant del centre del polígon i s una simetria respecte una recta que uneixi el centre del polígon amb un dels vèrtexs.

    Demostreu que tot element de D_{2n} s'escriu de manera única com un producte $r^x s^y$ amb $x \in \mathbb{Z}_n$ i $y \in \mathbb{Z}_2$ i calculeu el resultat d'operar dos elements escrits d'aquesta manera.

13. Identifiqueu el grup diedral D_{2n} com a subgrup de $\mathfrak{S}_n$.

14. Siguin a, b elements d'ordre 2 a un grup G tals que ab te ordre $n \geq 3$. Demostreu que $\langle a, b \rangle$ és isomorf al grup diedral D_{2n}.

15. Trobeu el reticle de subgrups de D_8. Observeu que encara que el grup no és abelià tots els seus subgrups propis són abelians.

16. Calculeu l'ordre de tots els elements del grup diedral D_{2n}. Si n és un nombre primer, calculeu-ne els subgrups i digueu quins són normals.

Grups de matrius

17. Siguin K un cos i $\mathrm{GL}_2(K)$ el conjunt de les matrius 2×2 a coeficients en K que tenen determinant diferent de zero.

    (a) Demostreu que $\mathrm{GL}_2(K)$, amb el producte de matrius, és un grup no abelià.

    (b) Demostreu que si $A \in \mathrm{GL}_2(K)$ commuta amb tots els elements de $GL_2(K)$, aleshores $A = a\,\mathrm{Id}$ per a algun $a \in K^*$. És a dir, els elements del centre de $\mathrm{GL}_2(K)$ són les homotècies i, per tant, $Z(\mathrm{GL}_2(K))$ és un grup isomorf al grup multiplicatiu de K.

    (c) Si K és un cos finit de cardinal q, aleshores
    $$|\mathrm{GL}_2(K)| = (q^2-1)(q^2-q)\,.$$

18. Siguin K un cos i $G = \mathrm{GL}_2(K)$.

    (a) Demostreu que el *grup especial lineal* $\mathrm{SL}_2(K)$, format per les matrius de G amb determinant 1, és un subgrup normal de G.

    (b) Demostreu que el *grup ortogonal* $\mathrm{O}_2(K)$, format per les matrius $A \in G$ tals que $AA^t = \mathrm{Id}$, és un subgrup de G.

    (c) Proveu que el *grup especial ortogonal* $\mathrm{SO}_2(K) = \mathrm{O}_2(K) \cap \mathrm{SL}_2(K)$ és un subgrup de G. Estabiu un isomorfisme entre $\mathrm{SO}_2(\mathbb{R})$ i
    $$\left\{ \begin{pmatrix} \cos\alpha & \sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} \mid 0 \le \alpha < 2\pi \right\}.$$

19. (*Grup de Lorentz*) Demostreu que
    $$\left\{ A_v = \frac{1}{\sqrt{1-v^2}} \begin{pmatrix} 1 & -v \\ -v & 1 \end{pmatrix} \mid v \in (-1,1) \right\}$$
    és un subgrup de $\mathrm{GL}_2(\mathbb{R})$.

    Indicació: $A_{v_1} A_{v_2} = A_{v_3}$ amb $v_3 = (v_1+v_2)/(1+v_1v_2)$.

20. Sigui $\Gamma = \mathrm{SL}_2(\mathbb{Z})$ el grup de les matrius 2×2 a coeficients enters i determinant 1. Siguin
    $$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad U = ST.$$
    Calculeu l'ordre d'aquests tres elements i demostreu que $\Gamma = \langle S, T \rangle = \langle S, U \rangle$.

Part 3

Exercicis de classe

1. Demostreu que el grup additiu $(\mathbb{Q}, +)$ i el grup multiplicatiu $(\mathbb{Q}^*, \cdot)$ no són isomorfs.

2. Sigui G un grup i $x \in G$ un element d'ordre n. Demostreu que $\operatorname{ord}(x^{-1}) = n$ i que si $k \in \mathbb{N}$, llavors $\operatorname{ord}(x^k) = n/\gcd(n, k)$.

3. Sigui H un subgrup d'un grup G. Comproveu que les condicions següents són equivalents:

   (a) H és normal a G.

   (b) $\forall a \in G, \quad aH \subseteq Ha$.

   (c) $\forall a \in G, \quad aHa^{-1} \subseteq H$.

   (d) $\forall a \in G, \quad aHa^{-1} = H$.

   (e) Existeix un homomorfisme $G \to G_1$ amb nucli H.

4. Sigui $f : G_1 \to G_2$ un homomorfisme de grups. Comproveu que si H_1 és subgrup de G_1, $f(H_1)$ ho és de G_2 i que si H_2 és subgrup de G_2, $f^{-1}(H_2)$ ho és de G_1. Comproveu, a més, que si H_2 és normal a G_2, $f^{-1}(H_2)$ ho és a G_1 però que, en canvi, si H_1 és normal a G_1 llavors $f(H_1)$ no té perquè ser-ho a G_2 i l'únic que es pot assegurar és que és normal a $\operatorname{Im} f$.

5. Comproveu que $\operatorname{Inn} G = \{\gamma_a : x \mapsto axa^{-1} \mid a \in G\}$ és un subgrup normal de $\operatorname{Aut} G$.

6. Siguin H i K subgrups d'un grup G. Demostreu que:

(a) El conjunt HK és un subgrup de G si, i només si, $HK = KH$.

(b) Si H és normal a G aleshores HK és un subgrup de G.

(c) Si H i K són normals a G, HK també ho és.

7. Sigui H un subgrup del grup G.

   (a) Demostreu que l'índex per l'esquerra, $|G/H|$, és igual que l'índex per la dreta, $|H\backslash G|$.

   (b) Sigui K un subgrup de G que conté H. Comproveu la multiplicativitat dels índexos: $[G : H] = [G : K] \cdot [K : H]$.

8. Siguin H i K subgrups d'un grup G. El conjunt HK no sempre és un grup, però, com que és una reunió de classes laterals per l'esquerra de K, podem definir $[HK : K]$ com el cardinal d'aquest conjunt de classes laterals. Comproveu les fórmules següents

   (a) $|HK||H \cap K| = |H| \cdot |K|$.

   (b) $[HK : K] = [H : H \cap K]$.

9. Siguin G un grup i H un subgrup de G. Demostreu que $[G : N_G(H)]$ és igual al nombre de conjugats de H.

10. Siguin H i K subgrups de G. Demostreu que

$$[G : H \cap K] \leq [G : H] \cdot [G : K] .$$

    En particular, la intersecció de subgrups d'índex finit té índex finit (*lema de Poincaré*).

11. Demostreu que si un grup G té un subgrup propi d'índex finit, també té un subgrup normal propi d'índex finit.

12. Sigui $n \geq 5$. Siguin $H \subseteq K \subseteq \mathfrak{S}_n$ subgrups amb H normal a K i quocient K/H abelià. Demostreu que si K conté tots els 3-cicles, H també els conté. En particular, $\mathfrak{A}_n$ no té subgrups normals propis amb quocient abelià.

13. Sigui H un subgrup de $Z(G)$. Proveu que si G/H és cíclic, G és abelià.

14. Sigui A un grup abelià finit. Demostreu que si l'ordre de A es divideix per un primer p, aleshores existeixen elements a A d'ordre p.

15. Siguin a i b elements d'un grup que commuten entre si. Siguin $n = \operatorname{ord} a$, $m = \operatorname{ord} b$ i $M = [n, m]$. Aleshores

    (a) $\operatorname{ord} ab$ divideix M i si $(m, n) = 1$, $\operatorname{ord} ab = M$.

    (b) Existeix al grup un element d'ordre M.

16. Siguin a i b elements d'un grup G. El *commutador* de a i b és

$$[a, b] = aba^{-1}b^{-1}.$$

    S'anomena així perquè $ab = [a, b]\, ba$. Si $S, T \subseteq G$ són subconjunts, posem

$$[S, T] = \langle [a, b] \mid a \in S, b \in T \rangle .$$

    El subgrup $G' = [G, G]$ es diu el *grup derivat* de G. Comproveu que:

    (a) G' és un subgrup normal de G amb quocient G/G' abelià.

    (b) Tot homomorfisme $G \to A$ en un grup abelià factoritza a través de G/G'.

    (c) G' és el més petit subgrup normal de G amb quocient abelià.

17. Trobeu el subgrup derivat d'un grup diedral D_{2n}. Identifiqueu el grup D_{2n}/D'_{2n}.

18. Considerem la cadena de grups derivats

$$G^{(0)} = G,\ G^{(1)} = G', \ldots,\ G^{(i+1)} = G^{(i)\prime}, \ldots$$

    Demostreu que G és resoluble si, i només si, $G^{(n)} = 1$ per a algun n.

19. Calculeu totes les sèries de composició possibles per als grups diedrals i simètrics.

20. Demostreu que si H i K són subgrups resolubles de G amb $H \subseteq N_G(K)$, aleshores el grup HK és resoluble.

21. *Lema de Burnside.* Sigui G un grup finit operant a un conjunt finit X. Per a cada $a \in G$ diguem n_a al nombre de punts fixos per a; és a dir, $n_a = \#\{x \in X \mid ax = x\}$. Demostreu que

$$|G\backslash X| = \frac{1}{|G|} \sum_{a \in G} n_a.$$

    Indicació: compteu el nombre de parells $(a, x) \in G \times X$ tals que $ax = x$.

22. Sigui H un subgrup de G. Comproveu que l'acció de G per traslació sobre el conjunt de les classes per l'esquerra G/H és transitiva. Suposem que G opera transitivament sobre un conjunt X. Demostreu que hi ha un subgrup $H \subseteq G$ i una bijecció $(G/H) \to X$ que és un isomorfisme de G-conjunts. Per tant; totes les accions transitives són, essencialment, accions per traslació sobre classes laterals.

23. Sigui p el més petit nombre primer que divideix l'ordre d'un grup G. Demostreu que tot subgrup d'índex p a G és normal.

24. Sigui G un grup d'ordre p^2, p primer. Demostreu que G és abelià.

25. Sigui G un grup finit. Demostreu que G és un p-grup si, i només si, tots els seus elements tenen ordre una potència de p. Proveu també que G és un p-grup si, i només si, tots els seus subgrups propis són p-grups.

26. Donat un p-grup H i un p-grup de Sylow P, considereu l'acció per traslació de H sobre el conjunt de classes laterals per l'esquerra G/P. A partir d'aquesta acció demostreu que H està contingut en algun dels conjugats de P.

27. Demostreu que un grup és producte directe dels seus subgrups de Sylow si, i només si, tots aquests subgrups són normals.

28. Sigui G un grup d'ordre pq, amb p i q primers diferents. Demostreu que G és resoluble.

29. Sigui G un grup d'ordre pqr, amb p, q i r primers diferents. Demostreu que G és resoluble.

Part 4

Exercicis d'ampliació del temari

Producte directe

1. Siguin $H_1, \ldots, H_k$ subgrups d'un grup G. Comproveu que els tres blocs de condicions següents són equivalents:

   (a) L'aplicació $(a_1, \ldots, a_k) \mapsto a_1 \cdots a_k$ és un isomorfisme de grups $H_1 \times \cdots \times H_k \to G$.

   (b) i. Els elements de diferents H_i commuten: si $a \in H_i, b \in H_j$ amb $i \neq j$, llavors $ab = ba$.
   ii. $H_1 \cdots H_k = G$.
   iii. $H_i \cap \prod_{i \neq j} H_j = 1$.

   (c) i. Cada H_i és normal a G.
   ii. Tot element de G s'escriu, de manera única, com a producte $a_1 \cdots a_k$ amb $a_i \in H_i$.

   En aquest cas es diu que G és el *producte directe* (intern) dels seus subgrups H_i. Naturalment, tot producte directe extern d'una familia de grups $G_1, \ldots, G_k$ es pot veure com el producte directe intern d'una familia de subgrups, quins?

2. Sigui $G = \prod_{i \in I} G_i$ el producte directe d'una familia arbitrària de grups. Per a cada $i \in I$ sigui $p_i : G \to G_i$ l'homomorfisme projecció sobre la i-èssima coordenada. Si K és un grup i $\{f_i : K \to G_i\}_{i \in I}$ és una col.lecció d'homomorfismes, demostreu que existeix un únic homomorfisme $f : K \to G$ tal que $p_i f = f_i$ per a tot $i \in I$.

Suma directa

3. Sigui $\{A_i\}_{i\in I}$ una família de grups abelians. La *suma directa* (externa) d'aquests grups és el subgrup A del producte directe format pels elements que tenen només un nombre finit de coordenades no trivials. Denotem la suma directa per $\oplus_{i\in I} A_i$. Naturalment, si la família és finita, llavors $A_1 \oplus \cdots \oplus A_k = A_1 \times \cdots \times A_k$.

   Sigui $t_i : A_i \to A$ l'homomorfisme que envia $a \in A_i$ a l'element que té a a la coordenada i-èssima i 0 a les demés. Si B és un grup abelià i $f_i : A_i \to B$, demostreu que existeix un únic homomorfisme $f : A \to B$ tal que $ft_i = f_i$ per tot i.

4. Sigui $\{A_i\}_{i\in I}$ una família no necessàriament finita de subgrups d'un grup abelià A. Definiu la *suma directa interna* d'aquests grups i caracteritzeu en termes dels subgrups el fet que A sigui igual a aquesta suma directa interna.

Producte semidirecte

5. Siguin G_1 i G_2 dos grups i $\phi : G_2 \to \operatorname{Aut} G_1$ un homomorfisme de grups. Fem servir la notació ${}^b a$ per indicar $\phi(b)(a)$. Sobre el producte cartesià $G_1 \times G_2$ definim l'operació

$$(a_1, b_1)(a_2, b_2) = (a_1 {}^{b_1} a_2, b_1 b_2).$$

   (a) Demostreu que $G_1 \times G_2$ amb l'operació definida té estructura de grup. Aquest grup s'anomena *producte semidirecte* de G_1 i G_2 (respecte ϕ) i s'escriu $G_1 \rtimes_\phi G_2$.

   (b) Considereu el cas $G_1 = \mathbb{Z}_n$, $G_2 = \mathbb{Z}_2$ i ϕ l'homomorfisme que envia el generador de $\mathbb{Z}_2$ a l'automorfisme de $\mathbb{Z}_n$ donat per $a \mapsto -a$. Demostreu que el producte semidirecte $\mathbb{Z}_n \rtimes_\phi \mathbb{Z}_2$ és isomorf al grup diedral D_{2n}.

   (c) Considereu el cas $G_1 = A$ un grup abelià, $G_2 = \mathbb{Z}_2$ i ϕ l'homomorfisme que envia el generador de $\mathbb{Z}_2$ a l'automorfisme de A donat per $a \mapsto -a$. Calculeu explícitament la cadena de derivats del grup $A \rtimes_\phi \mathbb{Z}_2$ i demostreu que aquest grup és resoluble.

L'exponent

6. L'*exponent* d'un grup és el menor n tal que $a^n = 1$ per a tot $a \in G$, o és ∞ si no hi ha cap n en aquestes condicions. Comproveu que:
   (a) Tot grup finit té exponent finit, que divideix l'ordre del grup.
   (b) Hi ha grups infinits amb exponent finit.
   (c) Tot grup abelià finit té elements d'ordre igual al seu exponent.

Torsió

7. Sigui A un grup abelià. Els elements *de torsió* de A són els que tenen ordre finit. Per a cada $n \geq 1$, definim la n-torsió per
$$A[n] = \{a \in A \mid na = 0\}.$$
Per a cada primer p, definim la p-component com
$$A(p) = \{a \in A \mid \exists r \geq 1,\ p^r a = 0\}.$$
Demostreu que:
   (a) La torsió, la n-torsió i les p-components són subgrups de A.
   (b) Si $n = n_1 \cdots n_k$ i $(n_i, n_j) = 1$ per a tot i, j, aleshores $A[n]$ és la suma directa dels $A[n_i]$.
   (c) El subgrup de torsió de A és la suma directa de les p-components.

8. Considereu els grups $\mathbb{R}/\mathbb{Z}$ i $S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$. La funció exponencial estableix un isomorfisme entre l'un i l'altre. Trobeu-ne els subgrups de torsió, els de n-torsió i les p-components.

Sèries de composició

9. Siguin K un cos i T el subgrup de $\mathrm{GL}_n(K)$ format per les matrius triangulars superiors. Sigui N el conjunt de les matrius $n \times n$ que són triangulars superiors i, a més, tenen zeros a la diagonal. Posem $U_k = 1_n + N^k$, on 1_n denota la matriu identitat. Comproveu que $T \supseteq U_1 \supseteq U_2 \supseteq \cdots \supseteq U_n = 1$ és una sèrie abeliana per al grup T; per tant, T és resoluble. Quan $K = \mathbb{F}_q$ és un cos finit, trobeu una sèrie de composició de T.

Accions

10. A la categoria dels G-conjunts, definiu el concepte de G-subconjunt, G-homomorfisme i producte de G-conjunts. Què us sembla que hauria de ser un G-conjunt simple?

11. Sigui G un grup operant a un conjunt X. Una relació d'equivalència $\sim$ a X es diu *compatible* amb l'acció de G si $x \sim y \Rightarrow ax \sim ay$. En tal cas, tenim una acció natural de G sobre el conjunt de classes d'equivalència $X/\sim$. L'acció de G sobre X es diu *primitiva* si les úniques relacions d'equivalència compatibles amb l'acció són la trivial (dos elements sempre estan relacionats) i la d'igualtat.

    Demostreu que una acció transitiva és primitiva si, i només si, l'estabilitzador G_x d'un element qualsevol és un subgrup propi maximal de G.

12. Demostreu que si $|X|$ és un nombre primer tota acció transitiva d'un grup sobre X és primitiva.

13. Una acció es diu *k-transitiva* si donats $x_1, \ldots, x_k$ i $y_1, \ldots, y_k$, dos conjunts de k elements diferents de X, existeix un element $a \in G$ tal que $ax_1 = y_1, \ldots, ax_k = y_k$.

    (a) És clar que $\mathfrak{S}_n$ opera n-transitivament sobre el conjunt $\{1, \ldots, n\}$. Quin és el grau de transitivitat de $\mathfrak{A}_n$?

    (b) Demostreu que tota acció 2-transitiva és primitiva.

14. Sigui $\mathbb{F}_q$ un cos finit. Considerem l'acció de $\mathrm{PSL}_2(\mathbb{F}_q)$ sobre la recta projectiva $\mathbf{P}^1(\mathbb{F}_q) = \mathbb{F}_q \cup \{\infty\}$ per transformacions lineals fraccionàries

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{F}_q),\ z \in \mathbf{P}^1(\mathbb{F}_q), \qquad \gamma z = \frac{az+b}{cz+d}.$$

    Demostreu que aquesta acció és fidel, transitiva i primitiva.

Part 5

Problemes d'examen resolts

Enunciat 1 Sigui G un grup abelià finit no cíclic. Demostreu que G té un subgrup isomorf a $\mathbb{Z}_p \times \mathbb{Z}_p$, per a algun primer p.

Resolució 1 Un grup abelià finit és producte directe de grups cíclics. Existeixen, doncs, enters $n_1,\ n_2, \ldots,\ n_r$ tals que

$$G \simeq \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_r}.$$

Sabem que $r > 1$ i que $n_1,\ n_2, \ldots,\ n_r$ no són coprimers dos a dos, ja que en cas contrari G seria cíclic. Siguin i, j tals que $(n_i, n_j) \neq 1$ i sigui p un primer que divideixi aquest màxim comú divisor. Tant $\mathbb{Z}_{n_i}$ com $\mathbb{Z}_{n_j}$ tenen un subgrup d'ordre p, és a dir, isomorf a $\mathbb{Z}_p$. Aleshores, la imatge de

$$\mathbb{Z}_p \times \mathbb{Z}_p \hookrightarrow \mathbb{Z}_{n_i} \times \mathbb{Z}_{n_j} \hookrightarrow \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_r} \simeq G$$

és un subgrup de G isomorf a $\mathbb{Z}_p \times \mathbb{Z}_p$.

Enunciat 2 (a) Sigui G un grup. Un subgrup H de G es diu *característic* si és invariant per tots els automorfismes de G, és a dir, si $\phi(H) = H$ per a tot $\phi \in \mathrm{Aut}(G)$. Demostreu que si H és característic, llavors H és normal.

(b) Demostreu que $Z(G)$ i G' són subgrups característics de G.

(c) Proveu que $H \triangleleft K$ i $K \triangleleft G \not\Rightarrow H \triangleleft G$. Demostreu que si afegim la hipòtesi que H és característic a K, llavors la implicació és certa.

Resolució 2 (a) Si H és característic a G, en particular és invariant pels automorfismes interns de G, és a dir, H és normal a G.

(b) Cal veure $\phi(Z(G)) = Z(G)$ i $\phi(G') = G'$ per a tot $\phi \in \mathrm{Aut}(G)$. Però, de fet, n'hi ha prou amb les inclusions $\phi(Z(G)) \subseteq Z(G)$ i $\phi(G') \subseteq G'$ perquè podem raonar amb l'automorfisme invers. Siguin $x \in Z(G)$ i $z \in G$. Atès que ϕ és un automorfisme, existeix $y \in G$ tal que $z = \phi(y)$. Llavors, $\phi(x)z = \phi(x)\phi(y) = \phi(xy) = \phi(yx) = \phi(y)\phi(x) = z\phi(x)$. Per tant, $\phi(x) \in Z(G)$.
Per veure que $\phi(G') \subseteq G'$ només cal veure que la imatge d'un commutador és un commutador. Efectivament, tenim que $\phi([a,b]) = \phi(aba^{-1}b^{-1}) = \phi(a)\phi(b)\phi(a)^{-1}\phi(b)^{-1} = [\phi(a), \phi(b)]$.

(c) Prenem com a grup G el grup simètric $\mathfrak{S}_4$ i com a subgrups $K = V_4 = \{\mathrm{Id}, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$ i $H = \{\mathrm{Id}, (1,2)(3,4)\}$. Aleshores $K \lhd G$, perquè la conjugació conserva el tipus d'una permutació i K conté tots els productes de transposicions disjuntes; $H \lhd K$, perquè K és abelià; però H no és normal a G ja que, per exemple, conjugant $(1,2)(3,4)$ per $(1,2,3)$ obtenim un element que no pertany a H.
Suposem que H és característic a K i $K \lhd G$. Sigui γ_g un automorfisme intern de G. Com que K és normal a G, $\gamma_g(K) = K$; és a dir, γ_g indueix un automorfisme de K. Per hipòtesi, H és invariant pels automorfismes de K, de manera que $\gamma_g(H) = H$. Per consegüent, H és normal a G.

Enunciat 3 Sigui $p > 3$ un nombre primer.

(a) Proveu que $-\mathrm{Id}$ és un commutador de $\mathrm{GL}_2(\mathbb{F}_p)$.

(b) Utilitzeu el fet que $\mathrm{PSL}_2(\mathbb{F}_p) = \mathrm{SL}_2(\mathbb{F}_p)/\{\pm \mathrm{Id}\}$ és simple per demostrar que el derivat de $\mathrm{GL}_2(\mathbb{F}_p)$ és $\mathrm{SL}_2(\mathbb{F}_p)$.

Resolució 3 (a) Prenem les matrius de $\mathrm{GL}_2(\mathbb{F}_p)$

$$A = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

i tenim $[A, B] = -\mathrm{Id}$.

(b) Atès que els commutadors tenen determinant 1, el derivat de $\mathrm{GL}_2(\mathbb{F}_p)$ està contingut a $\mathrm{SL}_2(\mathbb{F}_p)$. A l'apartat anterior hem

vist que aquest derivat conté $\{\pm \mathrm{Id}\}$. Així doncs,

$$\{\pm \mathrm{Id}\} \subseteq \mathrm{GL}_2(\mathbb{F}_p)' \subseteq \mathrm{SL}_2(\mathbb{F}_p)$$

i $\mathrm{GL}_2(\mathbb{F}_p)'$ és un subgrup normal de $\mathrm{SL}_2(\mathbb{F}_p)$.
D'altra banda, com que els únics subgrups normals del grup $\mathrm{PSL}_2(\mathbb{F}_p)$ són el trivial i el total, una de les inclusions anteriors ha d'ésser una igualtat. Només cal provar que $\mathrm{GL}_2(\mathbb{F}_p)'$ no és $\{\pm \mathrm{Id}\}$.
Per exemple, si prenem

$$A = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad B = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix},$$

tenim

$$[A, B] = \begin{pmatrix} -1 & 0 \\ 2 & -1 \end{pmatrix},$$

que no pertany a $\{\pm \mathrm{Id}\}$.
També podem raonar que si el derivat fos $\{\pm \mathrm{Id}\}$ llavors el quocient $\mathrm{GL}_2(\mathbb{F}_p)/\{\pm \mathrm{Id}\}$ seria abelià i $\mathrm{PSL}_2(\mathbb{F}_p)$, que n'és un subgrup, també ho seria. Però aquest és simple de cardinal no primer.

Enunciat 4 Sigui X un conjunt de cardinal 3 on el el grup simètric $\mathfrak{S}_4$ opera transitivament. Demostreu que els estabilitzadors dels elements de X són els 2−subgrups de Sylow de $\mathfrak{S}_4$. Vegeu que són diedrals i que la seva intersecció és un grup isomorf a $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Resolució 4 Sigui $x \in X$. Atès que l'acció de $G = \mathfrak{S}_4$ sobre X és transitiva, tenim $3 = |X| = |Gx| = [G : G_x]$. Per tant, $|G_x| = 8$, que és la màxima potència de 2 que divideix $|G|$. Així doncs, G_x és un 2-subgrup de Sylow de G.

Com que tots els elements estan a la mateixa òrbita, el conjunt d'estabilitzadors és el conjunt de conjugats de G_x. També, el conjunt de 2−subgrups de Sylow és el conjunt de conjugats d'un qualsevol d'ells, per exemple G_x. Observem que aquest conjunt té cardinal 1 o 3.

El subgrup de G generat per $(1, 2, 3, 4)$ i $(1, 3)$, és isomorf a D_8. Com que té ordre 8, és un 2-subgrup de Sylow. Atès que la conjugació és un isomorfisme, tots els 2-subgrups de Sylow de G i,

consegüentment, tots els estabilitzadors G_x, són isomorfs al grup diedral D_8. A més a més, el nombre de 2-subgrups de Sylow és 3, ja que $\langle (1,2,3,4),(1,3)\rangle$ no és normal a $\mathfrak{S}_4$.

El subgrup V_4, format per la identitat i els tres productes de transposicions disjuntes, és un 2-subgrup normal de G i, per tant, està inclòs a tots els 2-subgrups de Sylow de G; és a dir, $V_4 \subseteq \cap_{x\in X} G_x \subseteq G_x$. Per cardinals, una de les inclusions ha d'ésser una igualtat. Si ho fos la segona, resultaria que $\mathfrak{S}_4$ té un únic 2-subgrup de Sylow, cosa que és falsa. Per tant, $\cap_{x\in X} G_x = V_4 \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$.

Enunciat 5 Siguin G un grup abelià finit i $P = \prod_{x\in G} x$.

(a) Demostreu que $G_2 = \{x \in G \mid x^2 = 1\}$ és un subgrup de G d'ordre potència de 2.

(b) Demostreu que $P = \prod_{x\in G_2} x$. Deduïu que si $|G|$ és senar llavors $P = 1$.

(c) Considereu el cas $G = (\mathbb{Z}/p\mathbb{Z})^*$, amb $p > 2$ primer, i proveu que $(p-1)! \equiv -1 \pmod{p}$.

(d) Siguin $a \in G$ un element d'ordre 2 i $\pi : G \to G/\langle a\rangle$ el morfisme canònic. Demostreu que $\pi(P) = 1$.

(e) Proveu que si G té almenys dos elements d'ordre 2, llavors $P = 1$.

Resolució 5 (a) G_2 és un subgrup de G ja que

$$(xy)^2 = x^2y^2 = 1, \quad (x^{-1})^2 = (x^2)^{-1} = 1.$$

El seu ordre és potència de 2 perquè si existís un primer $p > 2$ que dividís l'ordre de G_2, llavors G_2 tindria un element d'ordre p, cosa que no pot ser perquè els elements de G_2 són d'ordre 1 o 2.

(b) Si $x \notin G_2$ llavors $x^{-1} \neq x$, de manera que en el producte $\prod_{x\notin G_2} x$ cada element està acompanyat del seu invers. Per tant, aquest producte és 1 i $P = \prod_{x\in G_2} x$. Si $|G|$ és senar, no hi ha elements d'ordre 2. Aleshores $G_2 = \{1\}$ i $P = 1$.

(c) Si prenem $G = (\mathbb{Z}/p\mathbb{Z})^*$, els seus elements són $1, \ldots, p-1$ i

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

D'altra banda, les úniques solucions de $X^2 = 1$ al cos $\mathbb{Z}/p\mathbb{Z}$ són ± 1 (l'anell $\mathbb{Z}/p\mathbb{Z}[X]$ és euclidià, el polinomi $X^2 - 1$ factoritza com $(X-1)(X+1)$). Per l'apartat anterior,

$$P = -1 \pmod{p}.$$

(d) Sigui $x_1, \ldots, x_k$ un sistema de representants del grup $\overline{G} = G/\langle a \rangle$. Els elements de G són

$$x_1, x_1 a, \ldots, x_k, x_k a$$

i els de $\overline{G}$ són

$$\pi(x_1), \ldots, \pi(x_k).$$

Aleshores,

$$\pi(P) = \pi\left(\prod_i (x_i^2 a)\right) = \prod_i \pi(x_i)^2,$$

ja que $\pi(a) = 1$. Així doncs,

$$\pi(P) = \prod_{y \in \overline{G}} y^2 = \prod_{y \in \overline{G}_2} y^2 = 1.$$

(e) Hem vist que si a és un element d'ordre 2, llavors $\pi(P) = 1$, és a dir, $P \in \{1, a\}$. Si hi ha dos elements d'ordre 2 diferents, aleshores l'única possibilitat és $P = 1$.

Enunciat 6 (a) Trobeu tots els 3−subgrups de Sylow de $S_4 \times \mathbb{Z}/3\mathbb{Z}$.

(b) Demostreu que no hi ha cap grup simple d'ordre 72.

Resolució 6 (a) El cardinal de $S_4 \times \mathbb{Z}/3\mathbb{Z}$ és $24 \cdot 3 = 72 = 2^3 3^2$. Per tant, els 3−subgrups de Sylow són d'ordre 9. Pel teorema de Sylow, el nombre d'aquests subgrups és un divisor de 8 congruent amb 1 mòdul 3. Pot ser 1 o 4. D'altra banda, els cicles de longitud 3 generen subgrups d'ordre 3 de S_4 i si H és un subgrup de S_4, llavors $H \times \mathbb{Z}/3\mathbb{Z}$ és un subgrup de $S_4 \times \mathbb{Z}/3\mathbb{Z}$. Els subgrups cíclics d'ordre 3 de S_4 són

$$\begin{aligned} H_1 &= \{\mathrm{Id}, (1,2,3), (1,3,2)\} \\ H_2 &= \{\mathrm{Id}, (1,2,4), (1,4,2)\} \\ H_3 &= \{\mathrm{Id}, (1,3,4), (1,4,3)\} \\ H_4 &= \{\mathrm{Id}, (2,3,4), (2,4,3)\}. \end{aligned}$$

Així doncs, els 3−subgrups de Sylow que busquem són $H_i \times \mathbb{Z}/3\mathbb{Z}$, per a $i = 1, 2, 3, 4$. (Tots ells són isomorfs a $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$)

(b) Raonant com abans, si G té ordre 72 el nombre de 3−subgrups de Sylow és 1 o 4. Si hi ha un únic 3−subgrup de Sylow, aquest és un subgrup normal de G, diferent de 1 i G, ja que té ordre 9. Per tant, G no és simple.
Si hi ha quatre 3−subgrups de Sylow, aleshores G opera (transitivament) per conjugació en el conjunt d'aquests subgrups. Tenim doncs, un morfisme $G \to S_4$. El nucli d'aquest morfisme és un subgrup normal de G, diferent de 1 perquè $|G| > 24$ i diferent de G perquè l'acció no és la trivial. Per tant, G no és simple. (El subgrup normal que hem descrit és la intersecció dels quatre 3−subgrups de Sylow de G, que coincideix amb $\cap_{g \in G} gHg^{-1}$, on H és un qualsevol d'aquests subgrups).

Enunciat 7 Sigui $A = \{1, 2, 4\} \subset \mathbb{Z}/7\mathbb{Z}$. Definim

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mid a, d \in A,\ b \in \mathbb{Z}/7\mathbb{Z} \right\}.$$

(a) Demostreu que A és un subgrup del grup multiplicatiu $(\mathbb{Z}/7\mathbb{Z})^*$ i que G és un subgrup del grup lineal $\mathrm{GL}_2(\mathbb{Z}/7\mathbb{Z})$.

(b) És G abelià? És simple? És resoluble? (Justifiqueu les respostes).

(c) Trobeu explícitament un p-subgrup de Sylow de G per a cada p.

(d) Doneu una sèrie de composició de G.

Resolució 7 (a) El conjunt A és $\{x^2 \mid x \in (\mathbb{Z}/7\mathbb{Z})^*\}$, que òbviament és un subgrup de $(\mathbb{Z}/7\mathbb{Z})^*$, ja que $x^2y^2 = (xy)^2$ i $(x^2)^{-1} = (x^{-1})^2$. De tota manera, és igualment senzill comprovar directament que A és tancat pel producte i per inversos.
Les matrius de G tenen determinant no nul, atès que

$$\det \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = ad \in A.$$

A més, formen un subgrup del grup lineal, ja que

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix} = \begin{pmatrix} aa' & ab' + bd' \\ 0 & dd' \end{pmatrix} \in G,$$

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}^{-1} = \begin{pmatrix} a^{-1} & -b(ad)^{-1} \\ 0 & d^{-1} \end{pmatrix} \in G.$$

(b) El grup G no és abelià, ja que, per exemple,

$$\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 3 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 3 \\ 0 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 5 \\ 0 & 2 \end{pmatrix}.$$

Atès que $a, d \in A$ i $b \in \mathbb{Z}/7\mathbb{Z}$, el cardinal de G és $3 \cdot 3 \cdot 7 = 63$. El nombre de 7-subgrups de Sylow de G divideix 9 i és congruent amb 1 mòdul 7. Hi ha, per tant, un únic 7-subgrup de Sylow, que és normal a G. El grup G no és simple.
Si posem H per indicar el subgrup normal esmentat, tenim una successió exacta $1 \to H \to G \to G/H \to 1$. Atès que el grup H té ordre 7, es tracta d'un grup cíclic i, per tant, resoluble. El grup quocient G/H té cardinal $9 = 3^2$, per tant és abelià i també resoluble. Llavors, G és resoluble, ja que és extensió d'un grup resoluble per un grup resoluble.

(c) Si

$$H = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mid b \in \mathbb{Z}/7\mathbb{Z} \right\},\ K = \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \mid a, d \in A \right\},$$

tenim que $H \simeq \mathbb{Z}/7\mathbb{Z}$ és un 7-subgrup de Sylow i $K \simeq A \times A \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ és un 3-subgrup de Sylow.

(d) Tenim la torre normal abeliana $G \supset H \supset \{1\}$, que no és una sèrie de composició perquè el quocient G/H no és simple. Intercalarem entre H i G un subgrup d'ordre 21. Observem que qualsevol subgrup de G d'ordre 21 és normal, perquè és d'índex 3, el més petit primer que divideix l'ordre de G. Per exemple, podem prendre

$$\begin{aligned} H_1 &= G \cap \mathrm{SL}_2(\mathbb{Z}/7\mathbb{Z}) = \{M \in G \mid \det M = 1\} = \\ &= \left\{ \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \mid a \in A, b \in \mathbb{Z}/7\mathbb{Z} \right\}, \end{aligned}$$

o bé

$$H_1 = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mid a \in A, b \in \mathbb{Z}/7\mathbb{Z} \right\}$$

(en ambdós casos és senzill raonar directament que són subgrups normals). Llavors la torre normal $G \supset H_1 \supset H \supset \{1\}$ tè quocients isomorfs a $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/7\mathbb{Z}$ i es tracta d'una sèrie de composició.

Enunciat 8 Siguin A un anell (commutatiu) i $G = GL_2(A)$ el grup de les matrius 2×2 amb coeficients a A i determinant invertible. Sigui H el subconjunt de G format per les matrius triangulars superiors. Demostreu que H és un subgrup de G, que en general no és abelià però que sempre és resoluble.

Resolució 8 Els elements de H són les matrius $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in G$. Atès que

$$\begin{pmatrix} a_1 & b_1 \\ 0 & c_1 \end{pmatrix}\begin{pmatrix} a_2 & b_2 \\ 0 & c_2 \end{pmatrix} = \begin{pmatrix} a_1a_2 & a_1b_2 + b_1c_2 \\ 0 & c_1c_2 \end{pmatrix},$$

el producte és tancat en H. D'altra banda,

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}^{-1} = \begin{pmatrix} c(ac)^{-1} & -b(ac)^{-1} \\ 0 & a(ac)^{-1} \end{pmatrix}$$

i també la inversió és tancada en H. Per tant, H és un subgrup de G.

Per provar que en general H no és abelià, es poden donar exemples molt diversos. Com a mostra,

$$\begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix},$$

$$\begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$$

són diferents si A és un anell on $2 \neq -2$.

Finalment, provem que H és resoluble veient que té un quocient resoluble amb nucli resoluble. Val a dir que hi han altres possibilitats igualment correctes.

Considerem l'aplicació $\varphi : H \to A^* \times A^*$ definida per

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mapsto (a, c).$$

(Observem que $ac \in A^* \iff a \in A^*$ i $c \in A^*$.) Per la fórmula del producte de matrius triangulars superiors, φ és un morfisme de grups. A més, és epimorfisme: per exemple, la matriu diagonal $< a, c >$ és una antiimatge del parell (a, c). El grup $A^* \times A^*$ és abelià i, per tant, resoluble; de manera que ja hem trobat un quocient resoluble.

El nucli de φ està format per les matrius $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$, amb $b \in A$. O bé directament, observant que dues d'aquestes matrius commuten, o bé mostrant que

$$\begin{array}{ccc} \ker\varphi & \longrightarrow & A \\ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} & \mapsto & b \end{array}$$

és un isomorfisme, s'obté que $\ker\varphi$ és abelià i, per consegüent, resoluble. La cadena $H \supset \ker\varphi \supset \{1\}$ és una torre normal abeliana de H.

Enunciat 9 Demostreu (sense utilitzar el teorema de Feit-Thompson) que les dues condicions següents són equivalents:

(a) tot grup d'ordre senar és resoluble

(b) els únics grups simples d'ordre senar són els d'ordre primer.

Resolució 9 Suposem (a). Aleshores,

$$\begin{array}{lll} G \text{ simple d'ordre senar} & \Rightarrow & G \text{ resoluble simple} \\ & \Rightarrow & G \text{ abelià simple} \\ & \Rightarrow & G \text{ d'ordre primer} \end{array}$$

Suposem (b). Aleshores, si G és un grup d'ordre senar, considerem una sèrie de composició de G. Els quocients seran grups simples d'ordre senar, per tant, grups d'ordre primer ($\Rightarrow$ cíclics $\Rightarrow$ abelians). Així doncs, G és resoluble.

Enunciat 10 Sigui $G = \{x \in \mathbb{Q} : 0 \leq x < 1\}$.

(a) Demostreu que G amb l'operació

$$x \oplus y = \begin{cases} x+y & \text{si } 0 \leq x+y < 1 \\ x+y-1 & \text{si } x+y \geq 1 \end{cases}$$

és un grup abelià d'ordre infinit.

(b) Demostreu que tots els elements de G tenen ordre finit.

(c) Demostreu que $(G, \oplus)$ és isomorf a $(\mathbb{Q}/\mathbb{Z}, +)$

Resolució 10 (a) Està clar que l'operació és interna. L'associativitat es pot comprovar de la manera següent:

$$\begin{aligned} (x \oplus y) \oplus z &= \left\{ \begin{array}{ll} x+y+z & \text{si } 0 \leq x+y+z < 1 \\ x+y+z-1 & \text{si } 1 \leq x+y+z < 2 \\ x+y+z-2 & \text{si } x+y+z \geq 2 \end{array} \right\} \\ &= x \oplus (y \oplus z) \end{aligned}$$

L'element neutre és $e = 0$, ja que $x \oplus 0 = 0 \oplus x = x$ per a tot $x \in G$. Finalment, l'oposat de 0 és 0 i l'oposat d'un element $x \in G - \{0\}$ és $1 - x$, que pertany a G i compleix $x \oplus (1-x) = (1-x) \oplus x = 0$. Per tant, $(G, \oplus)$ és un grup. De la definició de l'operació també resulta obvi que és commutativa (la suma de nombres racionals ho és), és a dir, que aquest grup és abelià. Una justificació senzilla de què té infinits elements: $1/n$ pertany a G per a tot nombre natural $n \geq 1$.

(b) Si $x \in G - \{0\}$, podem escriure $x = r/n$, amb r i n enters positius i $r < n$. Aleshores,

$$x = \overbrace{\frac{1}{n} \oplus \cdots \oplus \frac{1}{n}}^{r}$$

i per veure que x té ordre finit només cal veure que $1/n$ té ordre finit. Atès que

$$\overbrace{\frac{1}{n} \oplus \cdots \oplus \frac{1}{n}}^{n} = \frac{n-1}{n} \oplus \frac{1}{n} = 0\,,$$

aquest element té ordre finit. (De fet, l'ordre és exactament n)

(c) Considerem l'aplicació $\varphi : G \to \mathbb{Q}/\mathbb{Z}$ definida per $\varphi(x) = \bar{x}$. Aleshores,

$$\varphi(x \oplus y) = \left\{ \begin{array}{c} \overline{x+y} \\ \\ \overline{x+y-1} \end{array} \right\} = \overline{x+y} = \bar{x} + \bar{y} = \varphi(x) + \varphi(y)$$

i φ és morfisme de grups. D'altra banda,

$$\varphi(x) = \bar{0} \Rightarrow \bar{x} = \bar{0} \Rightarrow x \in \mathbb{Z}.$$

Atès que $0 \leq x < 1$, l'única possibilitat és $x = 0$; de manera que φ és injectiva. Considerem ara un element $\bar{q} \in \mathbb{Q}/\mathbb{Z}$. Si $n \in \mathbb{Z}$ és la part entera de q, aleshores $n \leq q < n+1$ i l'element $x = q - n$ és antiimatge de $\bar{q}$ en G. Així doncs, φ és exhaustiva.

Enunciat 11 (a) Demostreu que si G és un grup finit simple i H és un subgrup propi de G, aleshores $|G|$ divideix $[G : H]!$

(b) Demostreu que si p és primer, tot grup d'ordre $4p$ és resoluble.

(c) Demostreu que si p és primer, tot grup d'ordre $4p^2$ és resoluble.

Resolució 11 (a) Considerem l'acció per translació sobre les classes laterals G/H:

$$(g, xH) \to gxH.$$

Això ens proporciona un morfisme $T : G \to S_{[G:H]}$. El nucli és la intersecció dels conjugats de H i està, doncs, contingut a H. En conseqüència, és subgrup normal propi. Atès que G és simple, deduim que el nucli és trivial. Així, T és monomorfisme i G és isomorf a la seva imatge, que és subgrup de $S_{[G:H]}$. En definitiva, $|G|$ divideix $[G : H]!$.

(b) Sigui G un grup d'ordre $4p$. Si $p = 2$, es tracta d'un $2-$grup i és resoluble. Suposem $p > 2$. El grup G té un $2-$Sylow, de cardinal 4, i un $p-$Sylow, de cardinal p. Si G fos simple, per l'apartat anterior, tindríem $4p \mid 4!$ i $4p \mid p!$. La primera condició només es pot donar si $p = 3$, però llavors $12 \nmid 3!$. Així doncs, G té un subgrup normal propi H. Llavors

$$\begin{array}{rcl} |H| & = & 2,\ 4,\ p,\ 2p \\ [G:H] & = & 2p,\ p,\ 4,\ 2 \end{array}$$

Si veiem que tots els grups d'aquests cardinals són resolubles tindrem una successió exacta

$$1 \to H \to G \to G/H \to 1$$

amb H i G/H resolubles, la qual cosa implica G resoluble.
Els grups de cardinals $2, 4, p$ són abelians i, per tant, resolubles. Els grups de cardinal $2p$ tenen cardinal producte de dos primers diferents i són, per tant, resolubles.

(c) Sigui G un grup d'ordre $4p^2$. Si $p = 2$, es tracta d'un $p-$grup i és resoluble. Suposem $p \neq 2$ i considerem un $p-$Sylow de G. Si G fos simple, pel primer apartat, $|G|$ dividiria 4!. Aleshores tindríem $p^2|6$, que no pot ser. Per tant, G té un subgrup H normal propi no trivial. Considerem la successió exacta

$$1 \to H \to G \to G/H$$

Si veiem que H i G/H són resolubles haurem acabat. Els cardinals d'aquests dos grups tenen les possibilitats següents: $2, 4, p, 2p, 4p, p^2$, i $2p^2$. Tots els grups d'ordre $2, 4, p$ o p^2 són abelians i, per tant, resolubles. Els grups d'ordre $2p$ són del tipus pq i, per tant, resolubles. En l'apartat anterior hem vist que els grups de cardinal $4p$ són resolubles.
Sigui K un grup de cardinal $2p^2$. El nombre de $p-$Sylows és divisor de 2 i congruent amb 1 mòdul p. Per tant, hi ha un únic $p-$Sylow K_p, que és normal. Aquest té cardinal p^2 i és, doncs, resoluble. El quocient K/K_p té ordre 2 i també és resoluble. Per tant, K és resoluble.

Enunciat 12 Siguin G un grup finit, H un subgrup normal de G i p un nombre primer. Si n_p indica el nombre de $p-$subgrups de Sylow, demostreu que

$$n_p(G/H) \leq n_p(G)$$

Resolució 12 Sigui $|G| = p^r n$ amb $p \nmid n$. Sigui $|H| = p^s n'$ amb $p \nmid n'$. Aleshores, $|G/H| = p^{r-s}(n/n')$.
Considerem un $p-$Sylow de G/H. Tindrà cardinal p^{r-s}. Per la correspondència bijectiva, serà K/H amb K subgrup de G que

conté H. El cardinal de K serà $p^r n'$. Sigui K' un $p-$Sylow de K. Atès que el seu cardinal és p^r, serà també un $p-$Sylow de G.
Amb tot això hem definit una aplicació

$$K/H \to K'$$

entre $p-$Sylows de G/H i $p-$Sylows de G. Si veiem que és injectiva, haurem acabat.
Suposem que $K_1' = K_2'$. Aleshores, $K_1 \cap K_2$ serà múltiple de p^r. A més, del fet que $H \subseteq K_1 \cap K_2$ deduim que és múltiple de $p^s n'$. En conseqüència, serà múltiple del mcm, que és $p^r n'$. Llavors, $K_1 = K_1 \cap K_2 = K_2$

Alternativa 1: Demostrar primer que si P és un $p-$Sylow de G, llavors $\bar{P} = PH/H$ és $p-$Sylow de G/H. Raonar a continuació que l'aplicació $gPg^{-1} \to \bar{g}\bar{P}\bar{g}^{-1}$ entre conjugats de P i conjugats de $\bar{P}$ és exhaustiva. Finalment usar que $n_p(G)$ =nombre de conjugats de P.

Alternativa 2: Començar igual que abans i després demostrar:

- $N_G(H) \subseteq N_G(PH)$
- $H \subseteq N_G(PH)$
- $N_G(PH)/H \simeq N_{G/H}(PH/H)$

Finalment, usar $n_p(G) = [G : N_G(P)]$

Enunciat 13 Sigui G un grup.

(a) Proveu que si H és un subgrup normal de G, aleshores $G/Z_G(H)$ és isomorf a un subgrup de $\mathrm{Aut}(H)$. Per a quins H és el subgrup trivial?

(b) Proveu que si G és finit i H n'és un subgrup normal de cardinal el més petit primer que divideix $|G|$, aleshores $H \subseteq Z(G)$.

(c) Suposeu que $|G| = pq$ amb p, q primers tals que $p < q$ i $p \nmid q - 1$. Demostreu que G és cíclic.

Resolució 13 (a) Si H és un subgrup normal de G, aleshores per a cada element $g \in G$, la conjugació $h \to ghg^{-1}$ és un automorfisme de H i

l'aplicació

$$\begin{array}{rcl} \varphi : G & \longrightarrow & \mathrm{Aut}(H) \\ g & \mapsto & \gamma_g : h \to ghg^{-1} \end{array}$$

és un morfisme de grups: $\gamma_{g_1 g_2}(h) = g_1 g_2 h g_2^{-1} g_1^{-1} = \gamma_{g_1} \circ \gamma_{g_2}(h)$. El seu nucli està format pels elements $g \in G$ tals que γ_g és la identitat:

$$\begin{array}{rcl} ghg^{-1} & = & h \quad \forall h \in H \\ gh & = & hg \quad \forall h \in H \\ g & \in & Z_G(H) \end{array}$$

Així doncs, $G/Z_G(H) \simeq \mathrm{Im}\,\varphi$ que és un subgrup de $\mathrm{Aut}(H)$. El quocient serà trivial quan $Z_G(H) = G$, és a dir, quan es compleixi $gh = hg$ per a tot $g \in G$ i per a tot $h \in H$. Aquesta condició és equivalent a $H \subseteq Z(G)$.

(b) Suposem que $|H| = p$, el més petit primer que divideix $|G|$. Considerem l'acció per conjugació

$$\begin{array}{rcl} G \times H & \longrightarrow & H \\ (g,h) & \mapsto & ghg^{-1} \end{array}$$

De la fórmula de les òrbites $p = |H| = \sum |\text{òrbita}|$ i del fet que el cardinal de cada òrbita sigui un divisor de $|G|$ (doncs coincideix amb l'índex d'un subgrup d'isotropia) deduïm que només poden donar-se dues possibilitats: o bé hi ha sola una òrbita de cardinal p o bé hi ha p òrbites de cardinal 1. Atès que l'òrbita del neutre $1 \in H$ té un sol element, hem d'estar en el segon cas. Així doncs, tots els punts són fixos: $ghg^{-1} = h$ per a tot $g \in G$ i $h \in H$. Com abans, aquesta situació correspon a $H \subseteq Z(G)$.

(c) Siguin n_p i n_q el nombre de $p-$subgrups de Sylow y de $q-$subgrups de Sylow de G, respectivament.

$$\begin{array}{ll} n_p \mid q & n_p \equiv 1 \bmod p \\ n_q \mid p & n_q \equiv 1 \bmod q \end{array}$$

No pot ser $n_p = q$ perquè $p \nmid q - 1$ i no pot ser $n_q = p$ perquè $p < q$. Per tant, $n_p = 1 = n_q$. Tots els subgrups de Sylow són normals i, en conseqüència, G és producte directe dels Sylows. Aleshores, $G \simeq H_p \times H_q \simeq \mathbf{Z}_p \times \mathbf{Z}_q \simeq \mathbf{Z}_{pq}$ i G és cíclic.

Enunciat 14 Sigui K un subgrup normal d'un grup finit G. Proveu que si P és un p-subgrup de Sylow (per algun primer p) de K, aleshores $G = K\,\mathrm{N}_G(P)$.

Resolució 14 Si $g \in G$, aleshores $gPg^{-1} \subseteq gKg^{-1} = K$ doncs K és normal. Per tant, gPg^{-1} també és un p-subgrup de Sylow de K. De manera que existeix $k \in K$ tal que $kPk^{-1} = gPg^{-1}$. En conseqüència, $P = (k^{-1}g)P(k^{-1}g)^{-1}$; d'on es dedueix que $k^{-1}g \in \mathrm{N}_G(P)$. I arribem a que $g = k(k^{-1}g) \in K\,\mathrm{N}_G(P)$.

Enunciat 15 Considerem el grup dels quaternions

$$H_8 = < a, b \mid a^4 = e, a^2 = b^2, ba = a^{-1}b > .$$

(a) Escriu tots els elements de H_8. Demostra que en té 8.

(b) Calcula l'ordre de tots els elements de H_8. Demostra que H_8

(c) Fes la partició del grup H_8 en classes de conjugació.

(d) Troba tots els subgrups de H_8. Dibuixa el reticle de subgrups. Digues quins són normals.

(e) Troba el derivat de H_8.

(f) Troba el centre de H_8. Prova que $H_8/Z(H_8)$ és abelià, digues quina és la seva estructura i quants subgrups té.

(g) Demostra que H_8 és resoluble.

(h) Demostra que no hi ha cap acció transitiva de H_8 que doni lloc a un monomorfisme $H_8 \hookrightarrow S_4$

Resolució 15 (a) Les dues primeres relacions ens diuen que a i b són d'ordre 4. Aleshores, $a^{-1} = a^3$ i $b^{-1} = b^3$. Els elements de H_8 són paraules $a^{n_1}b^{m_1}a^{n_2}\ldots a^{n_k}b^{m_k}$ amb $n_i, m_i \in \{0,1,2,3\}$. Usant la tercera relació, $ba = a^3b$, podem passar totes les a's cap a l'esquerra i obtenim que els elements de H_8 són de la forma a^nb^m. Atès que són d'ordre 4 i $b^2 = a^2$, tindrem $n \in \{0,1,2,3\}$ i $m \in \{0,1\}$.

$$\begin{aligned} a^{n_1} &= a^{n_2} \Rightarrow n_1 = n_2, \text{ perquè } a \text{ té ordre } 4 \\ a^{n_1} &= a^{n_2}b \text{ no pot ser, perquè tindríem } b = a^{n_1-n_2} \\ a^{n_1}b &= a^{n_2}b \Rightarrow a^{n_1} = a^{n_2} \Rightarrow n_1 = n_2 \end{aligned}$$

Així doncs, $H_8 = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$

(b) Ja hem esmentat abans que a i b són d'ordre 4. Per tant, tenim $\text{ord}(a^2) = 4/(4,2) = 4/2 = 2$ i $\text{ord}(a^3) = 4/(4,3) = 4$. D'altra banda, aplicant reiteradament la tercera relació tenim $ba^n = a^{-n}b$ i llavors,

$$a^n b a^n b = a^n a^{-n} b^2 = b^2 = a^2$$

té ordre 2, de manera que $a^n b$ té ordre 4. En resum,

Element	e	a	a^2	a^3	b	ab	a^2b	a^3b
Ordre	1	4	2	4	4	4	4	4

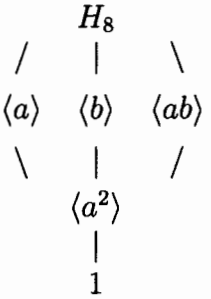
(c) Sabem que elements conjugats tenen el mateix ordre, per tant, d'entrada $[e] = \{e\}$ i $[a^2] = \{a^2\}$. Vegem com es reparteixen els elements d'ordre 4.

$$\begin{aligned} gag^{-1} &= a^n b^m a b^{-m} a^{-n} = a^n a^{-m} b^m b^{-m} a^{-n} = a^{-m} \\ &\Rightarrow [a] = \{a, a^{-1}\} = \{a, a^3\} \\ gbg^{-1} &= a^n b^m b b^{-m} a^{-n} = a^n b a^{-n} = a^{2n} b \Rightarrow [b] = \{b, a^2 b\} \\ a^3 b &= ba = b(ab)b^{-1} \Rightarrow [ab] = \{ab, a^3 b\} \end{aligned}$$

(d) A més del trivial i el total, podem tenir subgrups de cardinal 4 i de cardinal 2. Tenim tants subgrups de cardinal 2 com elements d'ordre 2. És a dir, únicament $\langle a^2 \rangle$. Un subgrup de H_8 amb quatre elements necessàriament tindrà algun d'ordre 4 i, en conseqüència, serà cíclic. En tenim tres:

$$\begin{aligned} \langle a \rangle &= \{e, a, a^2, a^3\} \\ \langle b \rangle &= \{e, b, a^2, a^2 b\} \\ \langle ab \rangle &= \{e, ab, a^2, a^3 b\} \end{aligned}$$

L'estructura de reticle és



El subgrups d'ordre 4 tenen índex 2 i, per tant, són normals. Atès que $\langle a^2 \rangle$ és l'únic subgrup d'ordre 2, coincideix amb tots els seus conjugats i és, per tant, normal.
Tots els subgrups de H_8 són normals.

(e) El derivat H_8' és el més petit subgrup (normal) de H_8 amb quocient abelià. Atès que H_8 no és abelià, $H_8' \neq 1$. D'altra banda, $H_8/\langle a^2 \rangle$ té cardinal $4 = 2^2$. Per tant, és abelià. Així doncs,

$$H_8' = \langle a^2 \rangle = \{e, a^2\}$$

(f) Els elements del centre són els punts fixos de l'acció per conjugació. Així, segons hem vist al tercer apartat, $Z(H_8) = \{1, a^2\}$.
Tenim que $H_8/Z(H_8) = H_8/H_8'$ és abelià. Pot ser isomorf a $\mathbb{Z}/4\mathbb{Z}$ o bé a $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Alternativa 1: Sabem que $G/Z(G)$ cíclic $\Rightarrow$ G abelià. Per tant, $H_8/Z(H_8) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Té 5 subgrups: el trivial, el total i 3 subgrups d'ordre 2.

Alternativa 2: Els subgrups de $H_8/Z(H_8)$ estan en correspondència bijectiva amb els subgrups de H_8 que contenen $Z(H_8)$. Per tant, a més del trivial i el total, $H_8/Z(H_8)$ té 3 subgrups d'ordre 2. Això ens diu que no és cíclic i llavors $H_8/Z(H_8) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Alternativa 3: $g \in H_8 \Rightarrow g = a^n b^m \Rightarrow g^2 = a^n b^m a^n b^m = a^n a^{(-1)^m n} b^{2m} = a^n a^{(-1)^m n} a^{2m} \in \langle a^2 \rangle$. Per tant, al grup quocient $H_8/Z(H_8)$ tots els elements tenen ordre ≤ 2. Així doncs, $H_8/Z(H_8)$ és isomorf a $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Té 5 subgrups: el trivial, el total i 3 subgrups d'ordre 2.

(g) El grup H_8 és un 2−grup (té cardinal $8 = 2^3$) i, per tant, és resoluble.

Alternativa: $H_8 \supseteq \langle a^2 \rangle \supseteq 1$ és una torre normal abeliana.

(h) Les accions transitives *són* accions per translació sobre classes laterals. Si volem que $|H_8/H| = 4$, haurem d'agafar $H = \langle a^2 \rangle$. Però aquest subgrup és normal i, per tant, l'acció per translació no és fidel.

Enunciat 16 Demostra que si p i q són nombres primers, tot grup de cardinal p^2q és resoluble.

Resolució 16 Si $p = q$, G és un p-grup i, per tant, és resoluble. Suposem doncs que $p \neq q$. Siguin n_p el nombre de $p-$subgrups de Sylow de G i n_q el nombre de q-subgrups de Sylow de G. Pels teoremes de Sylow sabem que

$$n_p \mid q \text{ i } n_p \equiv 1\,(mod\,p) \qquad \text{i} \qquad n_q \mid p^2 \text{ i } n_q \equiv 1\,(mod\,q).$$

Per provar la resolubilitat de G n'hi ha prou amb veure que $n_p = 1$ ó $n_q = 1$. En qualsevol d'aquests casos G tindrà un subgrup normal H (l'únic p-Sylow ó l'únic q-Sylow) resoluble (perquè és un p-grup ó un q-grup) de manera que el seu quocient G/H és també resoluble (perquè és un q-grup ó un p-grup). Per tant, G serà resoluble. Anem, doncs, a veure que $n_p = 1$ ó $n_q = 1$.

(a) Si $p > q$: Com $n_p \mid q$, aleshores $n_p = 1$ ó $n_p = q$. En aquest darrer cas, com $n_p = q \equiv 1 \pmod{p}$, aleshores $q > p$ que és una contradicció. Per tant $n_p = 1$ i acabem.

(b) Si $p < q$: Com $n_q \mid p^2$, aleshores $n_q = 1, n_q = p$ ó $n_q = p^2$.

i. Si $n_q = p$, raonant com al cas anterior, arribem a que $p > q$, que és contradicció.

ii. Si $n_q = p^2$, tenim dos casos. Si $n_p = 1$ acabem. Si $n_p = q$ arribem a contradicció comptant el nombre d'elements.

$$\sharp G \geq 1 + p^2(q-1) + (p^2-1) + 1 = qp^2 + 1 \quad \text{contradicció}$$

Els quatre sumands anteriors corresponen a:
(1): comptem l'element neutre
(2): són els elements diferents del neutre que aporten els $q-$Sylows, dels quals en tenim p^2 i dos a dos tenen intersecció trivial (són de cardinal primer)
(3): són els elements diferents del neutre aportats per un $p-$Sylow
(4): un $p-$Sylow diferent de l'anterior almenys aportarà un nou element

Enunciat 17 Sigui p un nombre primer. Una permutació a del conjunt finit $\{x_0, x_1, \ldots, x_{p-1}\}$ s'anomena *afinitat* si s'escriu

$$a(x_k) = x_{mk+n}\,,$$

per a certs $m \neq 0$ i n fixats. Considerem els subíndexs mòdul p. Denotem per $\mathbb{A}$ el conjunt d'aquestes afinitats. Notem que una afinitat no-trivial té com a molt un punt fix.

(a) Proveu que $\mathbb{A}$ és un grup resoluble. Pista: considereu l'afinitat $s(x_k) = x_{k+1}$ i justifiqueu que $\mathbb{A}/\langle s \rangle$ és abelià.

(b) Un subgrup es diu *característic* si és invariant per tots els automorfismes del grup. Observeu que el derivat d'un grup és un subgrup característic. Proveu que si K és un subgrup característic de N amb $N \lhd G$, aleshores $K \lhd G$.

(c) Proveu que si G és resoluble, aleshores tot subgrup normal no-trivial minimal de G és abelià.

Siguin k un cos perfecte i $f \in k[x]$ un polinomi irreductible de grau p. Denotem per $K = k(x_0, x_1, \ldots, x_{p-1})$ el seu cos de descomposició, i per $G = \mathrm{Gal}(f)$ el seu grup de Galois vist com a grup (transitiu) de permutacions sobre el conjunt d'arrels.

(d) Justifiqueu que podem suposar $s \in G$, i proveu que el normalitzador de $\langle s \rangle$ dins G està contingut en $\mathbb{A}$.

(e) Si N és un subgrup normal no-trivial minimal de G, proveu que N té ordre p. Deduïu que, reordenant les arrels si convé, es té $\langle s \rangle \lhd G$. Pista: considereu les accions de permutacions sobre les arrels per subgrups normals de G.

(f) Proveu que una equació irreductible de grau primer és resoluble per radicals si i només si totes les seves arrels són funció racional de dues d'elles. [La demostració presentada per Galois en una memòria l'any 1831 fou rebutjada per l'Acadèmia Francesa].

Resolució 17 (a) Es comprova fàcilment que la composició d'afinitats és afinitat, i que la inversa d'una afinitat també ho és. Per tant, $\mathbb{A}$ és un subgrup de permutacions de $\{x_0, \ldots, x_{p-1}\}$. Ara, l'afinitat s genera un grup cíclic d'ordre p: $s^r(x_k) = x_{k+r}$ i es comprova fàcilment que $[a, b] \in \langle s \rangle$, per a tot parell d'afinitats a, b. De manera que $\mathbb{A}/\langle s \rangle$ és abelià. De la successió exacta,

$$1 \to \langle s \rangle \to \mathbb{A} \to \mathbb{A}/\langle s \rangle \to 1$$

obtenim la resolubilitat de $\mathbb{A}$.

(b) Els automorfismes del grup preserven els commutadors i aquests generen el subgrup derivat. Els automorfismes interns de G restringeixen a automorfismes de N, per ser $N \lhd G$. Atès que K és un subgrup característic de N, aquells automorfismes deixen K invariant. Per tant, $K \lhd G$.

(c) Suposem que G és resoluble, i N és un subgrup normal no trivial minimal de G. Tenim $N' \subseteq N$, i el segon apartat porta a que $N' \lhd G$. La minimalitat de N proporciona que $N' = 1$ o bé $N' = N$. Ara bé, en ser G resoluble, N també ho és. Per tant, el cas $N' = N$ no es pot donar (algun derivada s'ha d'anul.lar). Per tant, N és abelià.

(d) En ser f irreductible de grau primer p, tenim que $G \subseteq \mathcal{S}_p$ té ordre múltiple de p i el teorema de Cauchy garanteix l'existència d'un element d'ordre p. Si reordenem les arrels convenientment, podem suposar que aquest element és la permutació $s(x_k) = x_{k+1}$. Sigui $a \in \mathrm{N}_G(\langle s \rangle)$. Aleshores, $asa^{-1} = s^m$ per algun $m \neq 0$. Considerem n donat per $x_n = a(x_0)$. Aleshores, tenim que a és l'afinitat

$$\begin{aligned} a(x_k) &= a(s^k(x_0)) = as^k a^{-1}(a(x_0)) = as^k a^{-1}(x_n) \\ &= s^{mk}(x_n) = x_{mk+n}\,. \end{aligned}$$

(e) Es veu fàcilment que tot subgrup normal no-trivial de G actua transitivament sobre el conjunt de les arrels $\{x_0, \ldots, x_{p-1}\}$ (fórmula de les òrbites i teorema fonamental de la teoria de Galois). Per (iii) sabem que N és abelià i aleshores els subgrups d'isotropia són tots trivials. Així doncs, la fórmula de les òrbites obliga que $|N| = p$.

(f) Suposem que G és resoluble. Pel cinquè apartat tenim que $\langle s \rangle$ és un subgrup normal de G, i pel quart sabem que G és un subgrup de les afinitats. Atès que una afinitat diferent de la identitat té com a molt un punt fix, tenim que

$$\mathrm{Gal}(K(x_0, \ldots, x_{p-1})/K(x_i, x_j)) = \{\mathrm{id}\}\,.$$

D'on obtenim $K(x_0, \ldots, x_{p-1}) = K(x_i, x_j)$, on x_i, x_j són dues arrels diferents qualssevol.
Recíprocament, si $K(x_0, \ldots, x_{p-1}) = K(x_i, x_j)$ aleshores G té com a molt grau $p(p-1)$. Pel teorema de Sylow, $\langle s \rangle$ és

l'únic p-subgrup de Sylow de G. Per tant, $\langle s \rangle$ és normal dins G. Ara, el quart apartat proporciona la inclusió $G \subseteq \mathbb{A}$ i juntament amb el resultat del primer apartat arribem a que G és resoluble, per ser subgrup d'un grup resoluble.