Université de Rennes

Agrégation

PROGRAMME DES TRAVAUX DIRIGÉS D'ALGÈBRE

SUGGESTIONS D'EXERCICES

CLASSIFICATION DES GROUPES ABÉLIENS DE TYPE FINI

Exercice 1. (*Caldero, Isomorphie ?*)

Les groupes $\mathbb{Z}/60\mathbb{Z} \times \mathbb{Z}/45\mathbb{Z} \times \mathbb{Z}/36\mathbb{Z}$ et $\mathbb{Z}/180\mathbb{Z} \times \mathbb{Z}/108\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ sont-ils isomorphes ?

ACTIONS DE GROUPES

Exercice 2. (*Des petites questions*)

On considère l'action d'un groupe G sur un ensemble E.

1. Montrer qu'un sous-ensemble de E est globalement stable par G si et seulement s'il est réunion d'orbites.
2. Montrer que deux orbites sont soit égales soit disjointes.
3. Montrer que deux éléments dans la même orbite ont des stabilisateurs conjugués.
4. On suppose que E est fini. Montrer que deux éléments conjugués dans le groupe G fixent le même nombre d'éléments.

Exercice 3. (*Action de groupe*)

On fixe une action d'un groupe G sur un ensemble fini E. On suppose que l'ordre de G est 15, que le cardinal de E est 17 et que E n'a pas de point fixé par tous les éléments du groupe G. Déterminer le nombre d'orbites et le cardinal de chacune d'elles.

SOUS-GROUPES DISTINGUÉS, CARACTÉRISTIQUES

Exercice 4. (*Exemples de sous-groupes caractéristiques*)

1. Montrer qu'un p-Sylow distingué est caractéristique.
2. Soit H un sous-groupe distingué d'un groupe fini G d'ordre est premier avec son indice. Montrer alors que H est le seul sous-groupe d'ordre $|H|$ et donc que H est caractéristique. *Indication : si J est un groupe d'ordre $|H|$, on pourra étudier le morphisme $J \subset G \to G/H$.*
3. Soit G un groupe fini d'ordre $p^\alpha q$ où p est premier et $q < p$. Montrer qu'il existe un unique p-Sylow.
4. Soit G un groupe fini et q le plus petit facteur premier de l'ordre de G. Soit H un sous-groupe d'indice q. Montrer que H est distingué. *On pourra montrer que l'action par translation à gauche de H sur G/H l'ensemble des classes gH à gauche est triviale*

Exercice 5. (*La réciproque du théorème de Lagrange*)

1. Le groupe symétrique $\mathfrak{S}_5$ a-t-il un élément d'ordre 6 ?
2. Chercher dans un groupe symétrique un contre-exemple à la réciproque du théorème de Lagrange sur l'ordre d'un élément dans un groupe.

Exercice 6. (*Groupe dérivé*)

Soit G un groupe. On appelle groupe des commutateurs de G et l'on note $D(G)$ le sous-groupe de G engendré par les éléments de la forme $xyx^{-1}y^{-1}$.

1. Montrer que $D(G)$ est distingué dans G et que le quotient $G/D(G)$ est abélien.
2. Montrer que $D(G)$ est le plus petit sous-groupe distingué de G tel que le quotient de G par ce sous-groupe soit abélien.

SUR LES p-GROUPES

Exercice 7. (*Le centre d'un p-groupe*)

1. Soit G un p-groupe agissant sur un ensemble fini E. Montrer que le cardinal de l'ensemble des points fixes de l'action est congru, modulo p, au cardinal de E.
2. En considérant une action de G sur lui-même, montrer que le théorème de Burnside : le centre d'un p-groupe non réduit à l'élément neutre n'est pas réduit à l'élément neutre.
3. Montrer que dans un p-groupe la réciproque du théorème de Lagrange est vraie : pour chaque diviseur de l'ordre de G, il y a un sous-groupe distingué de cet ordre.

Exercice 8. (*Groupe d'ordre p^2*)

1. Montrer que si le quotient d'un groupe par son centre est cyclique alors le groupe est abélien, donc égal à son centre.
2. Montrer qu'un groupe d'ordre p^2 est abélien, donc isomorphe soit à $\mathbb{Z}/p^2\mathbb{Z}$, soit à $(\mathbb{Z}/p\mathbb{Z})^2$.

Exercice 9. (*Groupe d'ordre p^3*)

Soit G un groupe non abélien d'ordre p^3 où p est un nombre premier.

1. Montrer que le centre $Z(G)$ de G est d'ordre p.
2. Montrer que $Z(G) = D(G)$.
3. En déduire que le nombre de classes de conjugaison est $p^2 + p - 1$. (On pourra étudier l'action de G sur lui-même par conjugaison : ses points fixes, l'orbite des éléments, le stabilisateur des éléments et appliquer la formule de Burnside...)
4. Montrer que $G/Z(G)$ est isomorphe à $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

SOUS-GROUPES DE SYLOW

Exercice 10. (*Un cas concret*)

Déterminer les sous-groupes de Sylow de $\mathbb{Z}/24\mathbb{Z}$.

Exercice 11. (*Étude de Σ_3*)

Donner les structures de cycles possibles dans Σ_3, le nombre d'éléments de Σ_3 ayant cette structure, et leur signature. Décrire les sous-groupes de Σ_3, et ceux qui sont distingués dans Σ_3.

Déterminer les sous-groupes de Sylow de Σ_3.

Exercice 12. (*Sylow des groupes diédraux*)

Soit $\mathcal{P}_n$ un polygone régulier à n côtés dans le plan euclidien orienté. On appelle groupe diédral D_n le groupe des isométries de $\mathcal{P}_n$.

1. Parmi les translations, les rotations, les symétries orthogonales, et les symétries glissées (composées d'une symétrie orthogonale et d'une translation dans l'axe de la symétrie), décrire des isométries du plan qui conservent le polygone régulier $\mathcal{P}_n$.
2. Déterminer, à l'aide de l'action naturelle de D_n sur l'ensemble des sommets de $\mathcal{P}_n$, le cardinal de D_n. En déduire la liste complète des éléments de D_n.
3. On suppose n impair. Déterminer les 2-Sylow de D_n et vérifier (sans référence au cours) qu'ils sont conjugués.
4. On suppose $n = 6$. Déterminer un 2-Sylow de D_6. Déterminer le nombre de 2-Sylow de D_6. Déterminer deux sous-groupes d'ordre 2 de D_6 non conjugués dans D_6. Donner un 3-Sylow de D_6. En dénombrant les éléments d'ordre 3, montrer qu'il n'y a qu'un seul 3-Sylow.

Exercice 13. (*Sylow dans les groupes linéaires finis*)

1. En comptant le nombre de bases de $\mathbb{F}_p^n$ déterminer le cardinal de $\mathrm{GL}(n, \mathbb{F}_p)$.
2. Montrer que l'ensemble des matrices triangulaires supérieures strictes est un p-sous-groupe de Sylow de $\mathrm{GL}(n, \mathbb{F}_p)$. Est-il distingué ?

Exercice 14. (*Sylow de $\mathrm{GL}(2)$*)

1. Vérifier que les p-Sylow de $\mathrm{GL}(2,\mathbb{F}_p)$ sont monogènes.
2. Soit A et B deux matrices de $\mathrm{GL}(2,\mathbb{F}_p)$ d'ordre p. Montrer que A est conjuguée à une puissance de B.

Exercice 15. (*Groupes de matrices sur $\mathbb{F}_2$*)

1. Déterminer l'ordre de $\mathrm{GL}(3,\mathbb{F}_2)$.
2. Décrire un 2-Sylow de $\mathrm{GL}(3,\mathbb{F}_2)$.
3. Soit $A = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$. Montrer que le polynôme minimal de A est irréductible de degré 3. En déduire que $\mathrm{GL}_3(\mathbb{F}_2) \cap \mathbb{F}_2[A]$ est un 7-Sylow de $\mathrm{GL}(3,\mathbb{F}_2)$.
4. Déterminer un 3-Sylow de $\mathrm{GL}(3,\mathbb{F}_2)$ à l'aide de la matrice $B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix}$.

PRODUIT SEMI-DIRECT

Exercice 16. (*Petites remarques utiles*)

1. Soit G un groupe fini et N et H deux sous-groupes de G. On suppose que $N \cap H = \{e_G\}$ et que $\mathrm{card}\, G = \mathrm{card}\, N \times \mathrm{card}\, H$. Montrer que $NH = G$.
2. Soit G un groupe et N et H deux sous-groupes de G. On suppose N distingué. Soit $p : G \to G/H$ la projection canonique. Montrer que
$$N \cap H = \{e_G\} \iff p_{|H} \text{ est injective.}$$
3. Soit G un groupe et N et H deux sous-groupes de G. On suppose que $N \cap H = \{e_G\}$ et que N et H sont distingués. Montrer que pour tout $(n,h) \in N \times H$,
$$hnh^{-1} = n.$$

Exercice 17. (*Produit semi-direct interne*)

Soit N un sous-groupe distingué d'un groupe G ($N \lhd G$) et H un sous groupe de G.

1. Montrer que NH est un sous-groupe de G.
2. On suppose désormais que $G = NH$ et que $H \cap N = \{e_G\}$. Montrer que $\varphi : N \times H \to G$, $(n,h) \mapsto nh$ est une bijection. Est-ce un isomorphisme de groupes ?
3. Montrer que si on munit $N \times H$ de la loi
$$(n,h) \star (n',h') = (n(hn'h^{-1}), hh'),$$
alors $N \times H$ est un groupe et $\varphi : (N \times H, \star) \to (G, \cdot)$ un isomorphisme de groupes. On notera $N \rtimes H := (N \times H, \star)$.
4. Déterminer $\varphi^{-1}(N)$ et $\varphi^{-1}(H)$.
5. Montrer que la loi $\star$ est la loi produit $(N \times H, \cdot \times \cdot)$ si et seulement si H est distingué dans G.

Exercice 18. (*Produits semi-directs externes*)

Soit $(N,\cdot)$ et $(H,)$ deux groupes et $c : (H,) \to (\mathrm{Aut}(N), \circ)$ un morphisme de groupes. On munit $N \times H$ de la loi
$$(n,h) \star_c (n',h') = (nc(h)(n'), hh')$$

1. Montrer que $N \rtimes_c H := (N \times H, \star_c)$ est un groupe dont $\overline{N} := N \times \{e_H\}$ est un sous groupe distingué et $\overline{H} := \{e_N\} \times H$ un sous-groupe
2. Vérifier que $N \rtimes_c H$ est isomorphe au produit semi-direct interne de $\overline{N}$ par $\overline{H}$.

Exercice 19. (*Caldero, Isomorphisme de produits semi-directs*)

Soit N et H deux groupes. Soit c et d deux morphismes que H vers $\mathrm{Aut}(N)$. Soit $\tau \in \mathrm{Aut}(H)$ et $\sigma \in \mathrm{Aut}(N)$ tels pour tout $h \in H$,
$$(d \circ \tau)(h)) = \sigma \circ c(h) \circ \sigma^{-1} \in \mathrm{Aut}(N).$$
Montrer que les produits semi-directs $N \rtimes_c H$ et $N \rtimes_d H$ sont isomorphes par l'isomorphisme $\iota : (n,h) \mapsto (\sigma(n), \tau(h))$. *Indication : on pourra traiter les cas $(\sigma,\tau) = (Id_N, \tau)$ puis $(\sigma,\tau) = (\sigma, Id_H)$*

Exercice 20. (*Groupes d'automorphismes*)

1. Montrer que les automorphismes du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ sont obtenus par multiplication par un inversible de $(\mathbb{Z}/n\mathbb{Z}, \times)$ et que l'application $(\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}), \circ) \to ((\mathbb{Z}/n\mathbb{Z})^\times, \times), f \mapsto f(1)$ est un isomorphisme de groupes.
2. Décrire un isomorphisme de $\mathbb{Z}/10\mathbb{Z}$ sur $(\mathbb{Z}/11\mathbb{Z})^\times$.
3. Montrer que si G et H sont deux groupes d'ordre premiers entre eux, alors
$$Aut(G \times H) = Aut(G) \times Aut(H).$$
4. En déduire le groupe des automorphismes de $\mathbb{Z}/133\mathbb{Z}$.
5. Soit p un nombre premier et n un entier naturel non nul. Montrer que
$$Aut((\mathbb{Z}/p\mathbb{Z})^n) = \mathrm{GL}(n, \mathbb{F}_p).$$
6. Montrer que $Aut(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \to Bij((1,0),(1,1),(0,1))$ est un isomorphisme.

Exercice 21. (*Exemple de produits semi-directs*)

1. Montrer que, après avoir fixé un générateur de $(\mathbb{Z}/11\mathbb{Z})^\star$, la donnée d'un morphisme de groupes de $\mathbb{Z}/5\mathbb{Z}$ dans $Aut(\mathbb{Z}/11\mathbb{Z})$ revient à la donnée d'un morphisme de groupes de $\mathbb{Z}/5\mathbb{Z}$ dans $\mathbb{Z}/10\mathbb{Z}$.
2. En déduire une structure de produit semi-direct sur $\mathbb{Z}/11\mathbb{Z} \rtimes \mathbb{Z}/5\mathbb{Z}$.
3. Montrer que toutes les structures de produit semi-direct non direct donnent des groupes isomorphes. *On pourra montrer que si* $\varphi, \psi \in \mathrm{Hom}(\mathbb{Z}/5\mathbb{Z}, \mathrm{Aut}(\mathbb{Z}/11\mathbb{Z})$ *alors il existe* $\gamma \in Aut(\mathbb{Z}/5\mathbb{Z})$ *tel que* $\psi = \varphi \circ \gamma$.
4. Soit p et q deux nombres premiers. Montrer que tous les morphismes de $\mathbb{Z}/p\mathbb{Z} \to Aut(\mathbb{Z}/q\mathbb{Z})$ sont de la forme $t \mapsto \{x \mapsto k^t x\}$ où k est un élément de $(\mathbb{Z}/q\mathbb{Z})^\star$ d'ordre 1 ou p.

GROUPES D'ORDRE INFÉRIEUR À 12

Exercice 22. (*Des petites questions*)

1. Soit p un nombre premier. Déterminer à isomorphisme près, tous les groupes d'ordre p.
2. Soit p un nombre premier. Déterminer à isomorphisme près, tous les groupes d'ordre p^2.
3. Donner des exemples de groupes d'ordre 6 non abéliens.
4. Déterminer l'ordre des groupes diédraux D_n.
5. Déterminer l'ordre des groupes alternés $\mathfrak{A}_n$.

Exercice 23. (*Groupes d'ordre 6*)

Soit G un groupe d'ordre 6.

1. Montrer que G admet un élément τ d'ordre 2 et un élément σ d'ordre 3.
2. Quelles sont les valeurs possibles de $\tau\sigma\tau$?
3. Déterminer, dans chacun des cas précédents, la structure de G à isomorphisme près.

Exercice 24. (*Étude de* Σ_4)

Donner les structures de cycles possibles dans Σ_4, le nombre d'éléments de Σ_4 ayant cette structure, et leur signature. Déterminer les sous-groupes distingués de Σ_4. En déduire que $\mathfrak{A}_4$ n'est pas un groupe simple, i.e. qu'il possède des sous-groupes distingués autres que $\{e\}$ et $\mathfrak{A}_4$.

Déterminer les sous-groupes de Sylow de Σ_4.

Exercice 25. (*Groupes d'ordre* pq)

Soit G un groupe d'ordre pq, où p et q sont deux nombres premiers distincts. On suppose que $p < q$.

1. Montrer qu'il n'y a qu'un q-Sylow Q et qu'il est distingué.
2. Montrer que G est produit semi-direct $Q \rtimes P$ où P est un p-Sylow de G.
3. Si p ne divise pas $q-1$, déterminer la structure de G.
4. Si $p = 2$, déterminer le morphisme structurel $\varphi : \mathbb{Z}/p\mathbb{Z} \to Aut(\mathbb{Z}/q\mathbb{Z}) \equiv \mathbb{Z}/(q-1)\mathbb{Z}$. Déterminer alors la structure de G.
5. Si p divise $q-1$, montrer qu'il n'y a qu'un seul produit semi-direct non abélien, à isomorphisme près.

Exercice 26. (*Groupe non abélien d'ordre* 8)

Soit G un groupe d'ordre 8.

1. Enumérer quatre groupes d'ordre 8, deux à deux non isomorphes, et même 5 si possible.
2. On suppose que tous les éléments de G sont d'ordre 2. Montrer que G est abélien. Soit a et b deux éléments non neutres distincts de G. Montrer que $\{e, a, b, ab\}$ est un sous-groupe d'ordre 4 de G. Déterminer un isomorphisme de G avec un groupe connu.
3. On suppose que G admet un élément a d'ordre 4. Soit b un élément hors du sous-groupe engendré par a. Montrer que $< a >$ est distingué et que b^2 appartient à $< a >$.
   i) Quel est l'ordre de b si $b^2 = a$ ou si $b^2 = a^3$? Conclure dans ce cas.
   ii) Si $b^2 = e$, montrer que G est un produit semi-direct et en déduire un isomorphisme avec un groupe connu.
   iii) Si tous les éléments hors de $< a >$ ont un carré égal à a^2, établir la liste des éléments et la table de multiplication de G à l'aide seulement de a et b.

Exercice 27. (*Groupe non abélien d'ordre* 8)

Soit G un groupe non abélien d'ordre 8.

1. Montrer que G contient un élément d'ordre 4. Soit H le sous-groupe qu'il engendre.
2. Montrer que si $G - H$ contient un élément d'ordre 2, G est un produit semi-direct. Après avoir vérifié que $Aut(\mathbb{Z}/4\mathbb{Z}) = \mathbb{Z}/2\mathbb{Z}$, montrer qu'il existe une unique structure de tel produit semi-direct non abélien.
3. Montrer que si $G - H$ n'a pas d'élement d'ordre 2, on retrouve la table de $\mathbb{H}_8$ en choisissant i l'élément d'ordre 4 qui engendre H et j un élément d'ordre 4 dans $G - H$. *On pourra montrer que i^2 est le seul élément d'ordre 2 est qu'il est donc central. On le notera -1.*

Exercice 28. (*Les groupes d'ordre 10*)

Soit G un groupe d'ordre 10.

1. Montrer que G est un produit semi-direct.
2. Déterminer les automorphismes d'ordre 2 de $\mathbb{Z}/5\mathbb{Z}$.
3. En déduire les deux possibilités pour les classes d'isomorphismes de G.

Exercice 29. (*Les groupes d'ordre 33*)

Déterminer à isomorphisme près tous les groupes d'ordre 33.(On pourra déterminer le nombre de sous-groupe d'ordre 11 et le nombre de sous-groupe d'ordre 3.)

Exercice 30. (*Groupe d'ordre 63*)

Montrer qu'un groupe d'ordre 63 n'est pas simple.

Exercice 31. (*Forme de Jordan*)

Dans tout cet exercice, on notera $J = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$ et $L = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ de $M_3(\mathbb{R})$.

Soit u un endomorphisme nilpotent de $\mathbb{R}^3$.

1. Quelles sont les valeurs possibles du rang de u ?
2. Supposons u de rang 1. Donner la forme de Jordan de u. En déduire que $\mathrm{im}(u) \subset \ker u$.
3. Supposons u de rang 2. Donner la forme de Jordan de u. En déduire que $\mathrm{im}(u) \subset \ker u^2$.

Exercice 32. (*Matrice à paramètres*)

1. Soit $M = \begin{pmatrix} 1 & a & 1 \\ 0 & 1 & b \\ 0 & 0 & c \end{pmatrix}$ de $\mathrm{M}_3(\mathbb{R})$. Si $c \neq 1$, calculer $(M - \mathrm{id}_3)(M - c\,\mathrm{id}_3)$. En déduire le polynôme minimal de M en fonction de a, b et c. Pour quelles valeurs de $a, b, c \in \mathbb{R}$ la matrice M est-elle diagonalisable ?
2. Pour quelles valeurs de $a \in \mathbb{C}$ la matrice symétrique $\begin{pmatrix} -1 & a \\ a & 1 \end{pmatrix}$ de $\mathrm{M}_2(\mathbb{C})$ est-elle diagonalisable ?

Exercice 33. (*Densité des matrices diagonales*)

Les deux questions suivantes sont indépendantes.

1. Soit $\mathbb{K}$ un corps commutatif et soit $n \in \mathbb{N}^\star$. Montrer que $\mathrm{GL}_n(\mathbb{K})$ est dense dans $\mathrm{M}_n(\mathbb{K})$ i.e. que toute matrice de $\mathrm{M}_n(\mathbb{K})$ est limite d'une suite de matrices de $\mathrm{GL}_n(\mathbb{K})$ (au sens de la norme sur $\mathrm{M}_n(\mathbb{K})$ définie dans le cours). On pourra par exemple commencer par montrer que, pour $k \in \mathbb{N}$ suffisamment grand, la matrice $A_k := A - \frac{1}{k} I_n$ est inversible.
2. Soit $n \in \mathbb{N}^\star$. Montrer que l'ensemble des matrices diagonalisables de $\mathrm{M}_n(\mathbb{C})$ est dense dans $\mathrm{M}_n(\mathbb{C})$ i.e. que toute matrice de $\mathrm{M}_n(\mathbb{C})$ est limite d'une suite de matrices diagonalisables de $\mathrm{M}_n(\mathbb{C})$ (au sens de la norme sur $\mathrm{M}_n(\mathbb{C})$ définie dans le cours). On pourra par exemple commencer par montrer que toute matrice triangulaire supérieure est limite d'une suite de matrices ayant chacune ses valeurs propres deux à deux distinctes.

CLASSIFICATION DES CONIQUES EUCLIDIENNES AFFINES

Coste (*Coniques, quadriques projectives*),
http://agreg-maths.univ-rennes1.fr/documentation/docs/coquproj.pdf

Exercice 34. (*Droites et quadriques*)

Une quadrique d'un espace projectif $P(V)$ est le lieu des zéros d'une forme quadratique f sur V.

1. Montrer que toute quadrique qui contient trois points distincts d'une droite d contient toute la droite d.
2. Déterminer la dimension de l'espace des quadriques de $P^3(K)$.
3. Soit d_1, d_2, d_3 trois droites de $P^3(K)$. Montrer qu'il existe une quadrique qui les contient.

Exercice 35. ()

On considère le plan euclidien muni d'un un repère orthonormé $(O, \overrightarrow{i}, \overrightarrow{j})$ et la courbe (C) d'équation

$$4x^2 - 4xy + y^2 - 3x - y - 1 = 0$$

1. Montrer que (C) est une parabole.
2. Trouver un repère orthonormé $(S, \overrightarrow{u_1}, \overrightarrow{u_2})$ tel que (C) ait une équation de la forme $x^2 = 2py$ dans ce repère.

Exercice 1. Les cardinaux $60 \times 45 \times 36 = (2^2 \times 3 \times 5) \times (3^2 \times 5) \times (2^2 \times 3^2) = 2^4 \times 3^5 \times 5^2$ et $(2^2 \times 3^2 \times 5) \times (2^2 \times 3^3) \times 5 = 2^4 \times 3^5 \times 5^2$ sont égaux. On cherche à écrire la forme canonique de chaque groupe

$$\begin{aligned}\mathbb{Z}/60\mathbb{Z} \times \mathbb{Z}/45\mathbb{Z} \times \mathbb{Z}/36\mathbb{Z} &\equiv (\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}) \times (\mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}) \\ &\equiv \mathbb{Z}/3\mathbb{Z} \times (\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}) \\ &\equiv \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/(4 \times 9 \times 5)\mathbb{Z} \times \mathbb{Z}/(4 \times 9 \times 5)\mathbb{Z}\end{aligned}$$

$$\begin{aligned}\mathbb{Z}/180\mathbb{Z} \times \mathbb{Z}/108\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} &\equiv (\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/27\mathbb{Z}) \times \mathbb{Z}/5\mathbb{Z} \\ &\equiv (\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/27\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}) \\ &\equiv \mathbb{Z}/(4 \times 9 \times 5)\mathbb{Z} \times \mathbb{Z}/(4 \times 27 \times 5)\mathbb{Z}\end{aligned}$$

Par unicité de la forme canonique, les deux groupes ne sont pas isomorphes.

Exercice 3. Par la seconde formule des classes, le cardinal des orbites est un diviseur de l'ordre de G, soit ici 1, 3, 5 ou 15. Comme aucun élément de E n'est fixé par tous les éléments de G, il n'y a pas d'orbite à 1 élément. On note n_i le nombre d'orbites à i éléments. La première formule des classes donne

$$3n_3 + 5n_5 + 15n_{15} = 17.$$

On vérifie que la seule valeur possible pour n_{15} est 0, puis que $n_5 = 1$ et $n_3 = 4$.

Exercice 4.

1. Comme tous les p-Sylow d'un groupe fini sont conjugués, si l'un est distingué, il est unique. Son image par un automorphisme est aussi de même cardinal, donc un p-Sylow. Il est donc caractéristique.
2. Soit H un sous-groupe distingué d'un groupe fini G tel que son ordre est premier avec son indice. Soit J un sous-groupe de G de même ordre que H. Le morphisme $J \subset G \to G/H$ est un morphisme de groupes. L'ordre de son image est un diviseur de l'ordre de J donc de H, mais aussi un diviseur de l'ordre de G/H, c'est à dire l'indice de H. C'est donc 1. Le sous-groupe J est donc dans le noyau de $G \mapsto G/H$ et par égalité des cardinaux, $J = H$.
3. Par le théorème de Sylow, le nombre de p-Sylow vaut 1 modulo p et divise q : c'est donc 1.
4. On considère l'action par translation à gauche de H sur G/H. L'orbite de eH n'a qu'un élément. Le cardinal d'une autre orbite est plus petit que $\operatorname{card} G/H - 1$, c'est à dire $q - 1$ et est un divise l'ordre de H, donc de l'ordre de G : c'est donc 1. Toutes les orbites sont donc réduites à un élément. Pour tout $g \in G$ et $h \in H$, $hg^{-1}H = g^{-1}H$, donc $gHg^{-1} = H$ et H est distingué.

Exercice 5.

1. L'élément de $\mathfrak{S}_5$ sont $(1,2)(3,4,5)$ est d'ordre $\operatorname{ppcm}(2,3) = 6$.
2. Les profils possibles d'éléments de $_4$ soit $(.), (..), (..)(..), (...), (....)$. Il n'y a donc pas d'élément d'ordre 4 alors que 4 divise l'ordre $4! = 24$ de $\mathfrak{S}_4$.

Exercice 6.

1. Comme pour tout automorphisme $\varphi : G \to G$, $\varphi(xyx^{-1}y^{-1}) = \varphi(x)\varphi(y)\varphi(x)^{-1}\varphi(y)^{-1}$ est un commutateur, $D(G)$ est stable par tout automorphisme, et en particulier distingué. On note $\pi : G \to G/D(G)$ l'application quotient naturelle. Soit c et c' deux éléments de $G/D(G)$. Il existe g et g' dans G tels que $c = \pi(g)$ et $c' = \pi(g')$. Comme $cc'c^{-1}c'^{-1} = \pi(g)\pi(g')\pi(g)^{-1}\pi(g')^{-1}) = \pi(gg'g^{-1}g'^{-1}) = 1_{G/D(G)}$, le groupe $G/D(G)$ est abélien.
2. Soit H un sous-groupe distingué de G tel que G/H soit abélien. Soit x et y dans G. On note $p : G \to G/H$ l'application quotient naturelle. Alors, $p(xyx^{-1}y^{-1}) = p(x)p(y)p(x)^{-1}p(y)^{-1} = 1_{G/H}$ car G/H est supposé abélien. Ainsi, le commutateur $xyx^{-1}y^{-1}$ est dans H. Comme $D(G)$ est engendré par les commutateurs, il est inclus dans H.

Exercice 7.

1. Le cardinal d'une orbite est un diviseur de l'ordre du groupe, donc soit 1 soit un multiple de p. Par la première formule de classes, on en déduit que le nombre d'orbites à un élément, c'est à dire le nombre de points fixes de l'action est un multiple de p.
2. On considère l'action d'un p-groupe G par conjugaison sur lui-même. Le centre est l'ensemble des points fixes de cette action. Par la question précédente, le cardinal du centre est un multiple de p. Le centre n'est donc pas réduit à l'élément neutre.
3. Soit p un nombre premier. Supposons la réciproque du théorème de Lagrange vraie dans tout groupe d'ordre p^n. Soit G un groupe d'ordre p^{n+1} et $d = p^\beta$ un diviseur de l'ordre p^{n+1} différent de 1. Notons p^z l'ordre de $Z(G)$. Si $z \geq \beta$, on trouve dans $Z(G)$ un sous-groupe d'ordre p^β, qui sera automatiquement distingué dans G. Sinon, comme $G/Z(G)$ est un p-groupe d'ordre p^{n+1-z}, on peut lui appliquer l'hypothèse de

récurrence et trouver un sous-groupe distingué d'ordre $p^{\beta-z}$. Sa préimage dans G sera un sous-groupe distingué de G.

Exercice 8. 1. Soit G un groupe tel que $G/Z(G)$ soit cyclique engendré par $[g] \in G/Z(G)$. Soit a et a' deux éléments de G. Il existe deux puissances n et n', deux éléments c et c' dans le centre de G tels que $a = cg^n$ et $a' = c'g^{n'}$. Alors $aa' = cg^n c'g^{n'} = cc'g^{nn'} = c'g^{n'}cg^n = a'a$, car c et c' commutent avec tous les éléments de G.

2. Soit G un groupe d'ordre p^2. Comme G est un p groupe, son centre n'est pas réduit à l'élément neutre. Par conséquent, $G/Z(G)$ est un groupe d'ordre $p^2/p = p$ ou $p^2/p^2 = 1$. Dans le premier cas, G est abélien par la question précédente et dans le second G est abélien car égal à son centre.

Exercice 9. 1. Soit p un nombre premier et G un groupe non abélien d'ordre p^3. Le centre de G est d'ordre 1, p ou p^2. Comme G est un p-groupe, son centre n'est pas réduit à l'élément neutre. Si $Z(G)$ est d'ordre p^2, alors $G/Z(G)$ d'ordre p est cyclique, ce qui impliquerait que G serait abélien. La seule possibilité est que $Z(G)$ soit d'ordre p.

2. Le centre de G est un sous-groupe distingué d'ordre p tel que le quotient $G/Z(G)$ soit d'ordre p^2, donc abélien. Par conséquent, $D(G) \subset Z(G)$. Comme G n'est pas abélien, $D(G)$ n'est pas d'ordre p : il est donc d'ordre p égal à $Z(G)$.

3. On étudie l'action de G sur lui-même par conjugaison. Les orbites sont les classes de conjugaison. Les points fixes sont exactement les éléments du centre : il y en a p. Le stabilisateur d'un élément y hors du centre contient le centre et y : c'est donc un sous-groupe d'ordre p^2. Il n'y a donc pas d'orbites de cardinal $p^3/p = p^2$. Le nombre N d'orbites est donc $p + \frac{p^3-p}{p} = p^2 + p - 1$. Le lemme de Burnside permet aussi de conclure :

$$N = \frac{1}{\operatorname{card} G} \sum_{x \in G} \operatorname{card} stab(x) = \frac{1}{p^3}(p \times p^3 + (p^3 - p) \times p^2) = p^2 + p - 1.$$

4. Comme $G/Z(G)$ est un groupe abélien d'ordre p^2, mais non cyclique (car G n'est pas abélien), il est isomorphe à $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Exercice 10. Dans un groupe abélien, les p-Sylow sont uniques. On décompose $24 = 2^3 \times 3$. Le 3-Sylow est engendré par un élément d'ordre 3, donc 8 ou -8. Le 2-Sylow est engendré par un élément d'ordre 8 par exemple 3.

Exercice 12. 1. Le centre de gravité de $\mathcal{P}_n$, noté O est conservé par les isométries (qui sont affines) : aucune translation ou symétrie glissée différente de l'identité n'est donc dans D_n. Les n rotations r^k de centre O est d'angle $k \times 2\pi/n$ ($0 \leq k \leq n-1$) conservent $\mathcal{P}_n$. Si n est impair, les n symétries axiales d'axe passant par O et un des n sommets, et si n est pair les $n/2$ symétries axiales d'axe passant par deux sommets opposés et les $n/2$ symétries axiales d'axe passant par les milieux de deux côtés opposés sont des éléments de D_n.

2. À l'aide des n rotations, on constate que tous les sommets sont dans la même orbite. Le stabilisateur d'un sommet S est composé de l'identité et de la symétrie axiale d'axe (OS). Par conséquent $\operatorname{card} D_n = \operatorname{card} \mathcal{O}(S) \operatorname{card} stab(S) = 2n$. La liste précédente est donc complète.

3. Si n est impair, les 2-Sylow sont d'ordre 2, engendré par une involution. Comme le demi-tour n'est pas dans D_n, les générateurs sont les n symétries axiales. En conjuguant par l'une des rotations, comme les rotations sont transitives sur les sommets, on retrouve que tous les Sylow sont conjugués.

4. Si $n = 6$, $2n = 2^2 \times 3$, les deux Sylow sont d'ordre 4. Le sous-groupe engendré par deux symétries axiales s_1 et s_2 d'axe orthogonaux contient $\{Id, s_1, s_2, r_\pi\}$ stable par produit. Donc, $< s_1, s_2 >= \{Id, s_1, s_2, r_\pi\}$ est un 2-Sylow. Le nombre de 2-Sylow est congru à 1 modulo 2 et divise 3 : c'est donc 1 ou 3. Mais, pour chaque paire de sommets opposés, on peut construire un 2-Sylow : il y en a donc 3 et ils sont tous conjugés par une rotation. Comme une symétrie axiale et un demi-tour n'ont pas le même déterminant, ils ne sont pas conjugués. Ils engendrent donc deux sous-groupes d'ordre 2 non conjugués dans D_6. Le sous-groupe engendré par la rotation d'angle $2\pi/3$ est d'ordre 3 : c'est donc un 3-Sylow. Le nombre de 3-Sylow est 1 ou 4. Les 3-Sylow sont des groupes cycliques d'ordre 3, d'intersections deux à deux triviales et contenant chacun deux éléments d'ordre 3. Il y aurait alors huit éléments d'ordre 3. Mais il y a six symétries axiales d'ordre 2. Il n'y a donc qu'un seul 3-Sylow.

Exercice 13. 1. Comme un endomorphisme est caractérisé par l'image d'une base, et comme un endomorphisme est un isomorphisme si et seulement si il transforme une base en une base, il suffit de dénombrer le nombre de bases pour en déduire le cardinal du groupe linéaire $\mathrm{GL}(n, \mathbb{F}_p)$. Il y a $p^n - 1$ choix pour le

premier vecteur, qui doit être non nul. Il y en a $p^n - p$ pour le second qui ne doit pas être colinéaire au premier. On obtient ainsi

$$\operatorname{card} \mathrm{GL}(n, \mathbb{F}_p) = (p^n - 1)(p^n - p) \cdots (p^n - p^{n-1}) = p^{\frac{n(n-1)}{2}} (p^n - 1)(p^{n-1} - 1) \cdots (p - 1).$$

2. Comme p est premier avec $p^i - 1$, les p-Sylow de $\mathrm{GL}(n, \mathbb{F}_p)$ sont d'ordre $p^{\frac{n(n-1)}{2}}$. L'ensemble S des matrices triangulaires supérieures strictes (avec des 1 sur la diagonale) est un sous-groupe d'ordre $p^{\frac{n(n-1)}{2}}$: c'est donc un p-Sylow. La conjugaison par la matrice anti-diagonale $\begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & \cdots & 1 & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ 1 & 0 & \cdots & 0 & 0 \end{pmatrix}$ donne le sous-groupe des matrices triangulaires inférieures strictes. Le sous-groupe S n'est donc pas distingué.

Exercice 14.

1. Par l'exercice précédent, les p-Sylow de $\mathrm{GL}(2, \mathbb{F}_p)$ sont d'ordre p premier donc monogènes.
2. Soit A et B deux matrices de $\mathrm{GL}(2, \mathbb{F}_p)$ d'ordre p. Le sous-groupe engendré par B est un p-Sylow : il est donc conjugué au p-Sylow des puissances de A. Il existe donc $P \in \mathrm{GL}(2, \mathbb{F}_p)$ et $k \in \mathbb{N}$ tel que $B = PA^kP^{-1}$.

Exercice 15.

1. Le groupe $\mathrm{GL}(3, \mathbb{F}_2)$ est d'ordre $(2^3 - 1)(2^3 - 2)(2^3 - 2^2) = 2^3 \times 7 \times 3$.
2. L'ensemble des matrices triangulaires supérieures strictes est un 2-Sylow d'ordre 2^3.
3. Le polynôme minimal de A est $P(X) = X^3 + X^2 + 1$ de degré 3 sans racine dans $\mathbb{F}_2$ donc irréductible. En particulier $A(A^2 + A) = I$ et donc $A^{-1} = A^2 + A$ est un polynôme en A. On montre de même que toute matrice B inversible de $\mathbb{F}_2[A]$ (i.e. polynôme en A) admet pour inverse un polynôme en B donc en A. Par conséquent $\mathrm{GL}(3, \mathbb{F}_2) \cap \mathbb{F}_2[A]$ est un sous-groupe de $\mathrm{GL}(3, \mathbb{F}_2)$. Comme P est irréductible, l'algèbre $\mathbb{F}_2[A]$ isomorphe au corps $\mathbb{F}_2[X]/(P)$ est d'ordre $2^3 = 8$. Le groupe de ses inversibles est donc d'ordre 7. C'est un 7-Sylow.
4. Le polynôme minimal de B est $(X-1)(X^2+X+1)$. L'algèbre $\mathbb{F}_2[B]$ est donc isomorphe à $\mathbb{F}_2[X]/(X - 1) \times \mathbb{F}_2[X]/(X^2 + X + 1)$. Le groupe de ses inversibles est donc d'ordre $(2 - 1) \times (2^2 - 1) = 3$: c'est un 3-Sylow.

Exercice 16.

1. L'application $N \times H \to G, (n, h) \mapsto nh$ est injective (car $nh = n'h'$ implique que l'élément ${n'}^{-1}n = h'h^{-1}$ de $N \cap H$ est e_G et donc $n = n'$ et $h = h'$) entre ensembles de même cardinal. C'est donc une bijection.
2. Puisque $p_{|H}$ est un morphisme de groupes, $p_{|H}$ est injective ssi $p_{|H}^{-1}e = e_G$, ssi $N \cap H = \{e_G\}$.
3. Soit $(n, h) \in N \times H$. Alors $hnh^{-1}n^{-1} = (hnh^{-1})n^{-1} = h(nh^{-1}n^{-1})$ est dans $N \cap H$ donc égal à e_G.

Exercice 17.

1. Soit nh et $n'h'$ deux éléments de l'ensemble NH. Les éléments

$$nhn'h' = \big(n(hn'h^{-1})\big)\, hh' \text{ et } (nh)^{-1} = h^{-1}n^{-1} = (h^{-1}n^{-1}h)h^{-1}$$

sont dans NH, qui est donc un sous-groupe de G.

2. Soit (n, h) et (n', h') deux éléments de l'ensemble $N \times H$. Si $nh = n'h'$, alors $(n')^{-1}n = h'h^{-1}$ est à la fois dans N et dans H donc égal à l'élément neutre. On en déduit que $n = n'$ et $h = h'$. L'application φ est donc injective. Par égalité $G = NH$, c'est une surjection et donc une bijection. Dans le groupe Σ_3 d'ordre 6, on considère $N =< (1, 2, 3) >$ distingué d'ordre 3 et $H :=< (1, 2) >$ d'ordre 2.

$$((1, 2, 3), (1, 2)) \times ((1, 2, 3), (1, 2) = ((1, 3, 2), Id)$$
$$\text{et } (1, 2, 3)(1, 2)(1, 2, 3)(1, 2) = (1, 2, 3)(2, 1, 3) = Id$$

L'application φ n'est donc pas un morphisme de groupe en général.

3. Soit (n, h) et (n', h') deux éléments de l'ensemble $N \times H$. Alors

$$\varphi(n, h) \cdot \varphi(n', h') = nhn'h'$$
$$\text{et } \varphi((n, h) \star (n', h')) = \varphi(n(hn'h^{-1}), hh') = nhn'h'$$

La loi $\star$ sur $N \times H$ est donc induite par la loi de groupe $\cdot$ sur G par la bijection φ : par conséquent, $(N \times H, \star)$ est un groupe (e.g. l'inverse de (n, h) est $\varphi^{-1}(\varphi(n, h)^{-1})$, l'image par φ^{-1} de l'inverse de $\varphi(n, h)$ dans $(G, \cdot)$ soit $(h^{-1}n^{-1}h, h^{-1})$) et φ est un isomorphisme de groupes.

4. Comme $\varphi(N \times \{e_G\}) = N$ et φ est une bijection, on obtient $\varphi^{-1}(N) = N \times \{e_G\}$ et de même $\varphi^{-1}(H) = \{e_G\} \times H$.

5. Notons d'abord que, comme φ est un isomorphisme, $\{e_G\} \times H$ est distingué dans $N \rtimes H$ si et seulement si H est distingué dans G. Si pour tout ($n \in N$ et tout $h \in H$, $(n,e)\star(e,h)\star(n,e)^{-1} = (n,h)\star(n^{-1},e) = (nhn^{-1}h^{-1},h)$ est dans $\{e_G\} \times H$, alors pour tout n et tout h on a $hnh^{-1} = n$ et $\star = \cdot \times \cdot$. La réciproque est simple.

Exercice 18. 1. On calcule

$$((n,h) \star_c (n',h')) \star_c (n'',h'') = (n \cdot c(h)(n'), hh') \star_c (n'',h'') = (n \cdot c(h)(n') \cdot c(hh')(n''), hh'h'')$$
$$(n,h) \star_c ((n',h') \star_c (n'',h'')) = (n,h) \star_c (n' \cdot c(h')(n''), h'h'') = (n \cdot c(h)(n' \cdot c(h')(n'')), hh'h'')$$

Or puisque c est un morphisme de groupes,

$$c(h)(n') \cdot c(hh')(n'') = c(h)(n') \cdot c(h)(c(h')(n'')) = c(h)(n' \cdot c(h')(n''))$$

et $\star$ est donc associative. On vérifie que (e_N, e_H) est un élément neutre et que l'inverse de (n,h) est (n^{-1},h^{-1}).

$$(n,h) \star_c (n',h') \star_c (n,h)^{-1} = (n \cdot c(h)(n'), hh') \star_c (n^{-1},h^{-1}) = (n \cdot c(h)(n') \cdot c(hh')(n^{-1}), hh'h^{-1})$$

Ainsi, avec $h' = e_H$, on vérifie que $\overline{N} := N \times \{e_H\}$ est distingué dans $N \rtimes_c H$.

2. L'application $\Phi : (\overline{N} \rtimes \overline{H}, \star) \to (N \rtimes_c H, \star_c)((n,e),(e,h)) \mapsto (n,h)$ est une bijection et, puisque

$$\begin{aligned}((n,e),(e,h)) \star ((n',e),(e,h')) &= ((n,e) \star_c (e,h) \star_c (n',e) \star_c (e,h)^{-1}, (e,h) \star_c (e,h') \\ &= ((n,h) \star_c (n',h^{-1}), (e,hh')) = ((nc(h)(n'),e),(e,hh')) \\ (n,h) \star_c (n',h) &= (nc(h)(n'), hh')\end{aligned}$$

c'est un isomorphisme de groupes.

Exercice 19. Dans le cas $(\sigma,\tau) = (Id_N,\tau)$, on a par hypothèse $d \circ \tau = c$.

$$\begin{aligned}\iota(n,h) \star_d \iota(n',h) &= (n,\tau(h)) \star_d (n',\tau(h')) = (nd(\tau(h))(n'), \tau(h)\tau(h')) \\ \iota((n,h) \star_c (n',h)) &= (nc(h)(n'), \tau(hh')).\end{aligned}$$

Dans le cas $(\sigma,\tau) = (\sigma, Id_H)$, on a par hypothèse $d(h) = \sigma \circ c(h) \circ \sigma^{-1}$, soit $d(h) \circ \sigma = \sigma \circ c(h)$.

$$\begin{aligned}\iota(n,h) \star_d \iota(n',h) &= (\sigma(n),h) \star_d (\sigma(n'),h') = (\sigma(n)d(h)(\sigma(n')), hh') \\ \iota((n,h) \star_c (n',h)) &= (\sigma(nc(h)(n')), hh') = (\sigma(n)(\sigma \circ c)(h)(n'), hh')\end{aligned}$$

Dans les deux cas, la bijection ι est un isomorphisme de groupes. Le cas général est simplement la composition de ces deux cas particuliers.

Exercice 20. 1. Soit f un automorphisme de $(\mathbb{Z}/n\mathbb{Z},+)$. Pour tout $a \in \mathbb{Z}/n\mathbb{Z}$, $f(a) = f(1+1+\cdots+1) = af(1)$. Par ailleurs, il existe $b \in \mathbb{Z}/n\mathbb{Z}$ tel que $f(b) = 1$ et donc $bf(1) = 1$. Le facteur $f(1)$ est donc un inversible de $(\mathbb{Z}/n\mathbb{Z},\times)$. Réciproquement, si λ est un inversible de $(\mathbb{Z}/n\mathbb{Z},\times)$, alors $a \mapsto \lambda a$ est un automorphisme de $(\mathbb{Z}/n\mathbb{Z},+)$. L'application $\Phi : (\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}),\circ) \to ((\mathbb{Z}/n\mathbb{Z})^\times,\times), f \mapsto f(1)$ est une bijection. On vérifie simplement que $f \circ g$ est la multiplication par $f(1)g(1)$. L'application Φ est donc un isomorphisme de groupes.

2. Le groupe $(\mathbb{Z}/11\mathbb{Z})^\times$ des inversibles du corps fini $\mathbb{Z}/11\mathbb{Z}$ est cyclique d'ordre 10. Comme $2^5 \equiv -1 \not\equiv 1[11]$ et $2^2 \equiv 4 \not\equiv 1[11]$, l'ordre de 2 dans le groupe $(\mathbb{Z}/11\mathbb{Z})^\times$ d'ordre 2×5 est $10 : 2$ est donc un générateur. Par conséquent, le morphisme $(\mathbb{Z}/10\mathbb{Z},+) \to ((\mathbb{Z}/11\mathbb{Z})^\times,\times)$ qui envoie le générateur 1 sur 2 est un isomorphisme de groupes.

3. Soit $f \in \mathrm{Aut}(G \times H)$. Soit $g \in G$. L'application $\alpha : H \to G \times H, h \mapsto f(g,h)$ est un morphisme de groupe, car la loi sur $G \times H$ est choisie comme la loi produit. De même, l'application $\beta : G \times H \to G, (g,h) \mapsto g$ est un morphisme de groupe. L'image de la composée $\beta \circ \alpha : H \to G$ est d'ordre un diviseur commune de l'ordre de H et de G, donc 1 par hypothèse. Il existe donc $a(g) \in G$ tel que pour tout $(g,h) \in G \times H, f(g,h) = (a(g), b(g,h))$. En échangeant les rôles de G et H, on trouve en fait $f(g,h) = (a(g), b(h))$. Comme la restriction de f au sous-groupe $G \times \{e_H\}$ est un automorphisme de groupes, a est dans $\mathrm{Aut}(G)$. On vérifie alors que l'application $(\mathrm{Aut}(G \times H),\circ) \to (\mathrm{Aut}(G) \times \mathrm{Aut}(H),\circ \times \circ), f = (a,b) \mapsto (a,b)$ est un isomorphisme de groupes.

4. Comme 11 et 13 sont premiers entre eux,

$$\mathrm{Aut}(\mathbb{Z}/133\mathbb{Z}) \equiv \mathrm{Aut}(\mathbb{Z}/11\mathbb{Z} \times \mathbb{Z}/13\mathbb{Z}) \equiv \mathrm{Aut}(\mathbb{Z}/11\mathbb{Z}) \times \mathrm{Aut}(\mathbb{Z}/13\mathbb{Z}) \equiv \mathbb{Z}/10\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}.$$

5. Il suffit de remarquer que les automorphismes du groupe abélien $((\mathbb{Z}/p\mathbb{Z})^n,+)$ sont des isomorphismes linéaires du $\mathbb{F}_p$-espace vectoriel $((\mathbb{Z}/p\mathbb{Z})^n,+,\cdot)$ car le produit par un scalaire se déduit de l'addition.

6. Comme tout automorphisme de $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ fixe $(0,0)$, l'application $\Phi : Aut(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \to Bij((1,0),(1,1),(0,1)), f \mapsto f$ est bien définie, morphisme de groupes et injective. Par ailleurs,

$$\operatorname{card} \operatorname{Aut}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) = \operatorname{card} \operatorname{GL}(n\mathbb{F}_2) = (2^2-1)(2^2-2) = 6 = 3!.$$

L'application Φ est donc un isomorphisme de groupes.

Exercice 21.

1. Ayant fixé le générateur 2 de $(\mathbb{Z}/11\mathbb{Z})^\times$, on a montré que $\operatorname{Aut}(\mathbb{Z}/11\mathbb{Z}) \to (\mathbb{Z}/11\mathbb{Z})^\times, f \mapsto f(1)$ et $\mathbb{Z}/10\mathbb{Z} \mapsto (\mathbb{Z}/11\mathbb{Z})^\times, n \mapsto 2^n$ sont des isomorphismes de groupes. On en déduit un isomorphisme $\operatorname{Aut}(\mathbb{Z}/11\mathbb{Z}) \to \mathbb{Z}/10\mathbb{Z}$. Ainsi, la donnée d'un morphisme de groupes de $\mathbb{Z}/5\mathbb{Z} \to \operatorname{Aut}(\mathbb{Z}/11\mathbb{Z})$ revient à la donnée d'un morphisme de groupes de $\mathbb{Z}/5\mathbb{Z} \to \mathbb{Z}/10\mathbb{Z}$.
2. En utilisant le morphisme $(\mathbb{Z}/5\mathbb{Z},+) \to (\mathbb{Z}/10\mathbb{Z},+), n \mapsto 2n$, on obtient une structure de produit semi-direct $\mathbb{Z}/5\mathbb{Z} \rtimes \mathbb{Z}/11\mathbb{Z}$.
3. Soit $\varphi, \psi \in \operatorname{Hom}(\mathbb{Z}/5\mathbb{Z}, \operatorname{Aut}(\mathbb{Z}/11\mathbb{Z}))$. Les automorphismes $\varphi(1)$ et $\psi(1)$ de $\mathbb{Z}/11\mathbb{Z}$ sont deux éléments du groupe cyclique $\operatorname{Aut}(\mathbb{Z}/11\mathbb{Z})$: ils sont d'ordre 1 ou 5. Pour l'ordre 1, on trouve le produit direct. S'ils sont d'ordre 5, ils sont générateurs du seul sous-groupe d'ordre 5 du groupe cyclique $\operatorname{Aut}(\mathbb{Z}/11\mathbb{Z})$. Il existe donc k inversible de $\mathbb{Z}/5\mathbb{Z}$ tel que $\psi(1) = \varphi(1)^{\circ k} = \varphi(k)$. On a donc $\psi = \varphi \circ \gamma$ où $\gamma : \mathbb{Z}/5\mathbb{Z} \to \mathbb{Z}/5\mathbb{Z}, n \mapsto kn$ est un automorphisme. Les deux produits semi-directs associés à φ et à ψ sont donc isomorphes.
4. Soit φ un morphisme de $\mathbb{Z}/p\mathbb{Z}$ dans $\operatorname{Aut}(\mathbb{Z}/q\mathbb{Z})$. Les automorphismes de $\mathbb{Z}/q\mathbb{Z}$ sont obtenus comme multiplication par un inversible de $\mathbb{Z}/q\mathbb{Z}$. Ceux qui sont dans l'image d'un morphisme depuis $\mathbb{Z}/p\mathbb{Z}$ sont d'ordre 1 (donc identité) ou p. L'application $\mathbb{Z}/p\mathbb{Z} \to \operatorname{Aut}(\mathbb{Z}/q\mathbb{Z}) \to (\mathbb{Z}/q\mathbb{Z})^\times, t \mapsto \varphi(t)(1)$ est composée de morphismes de groupes : elle est donc caractérisée par l'image de 1 et de la forme $t \mapsto k^t$ où $k := \varphi(1)(1)$. Par conséquent, φ est de la forme $t \mapsto (x \mapsto k^t x)$ où k est d'ordre 1 ou p.

Exercice 25.

1. Les q-Sylow sont d'indice p, le plus petit diviseur premier de l'ordre de G : ils sont donc distingués. On peut aussi dire par le théorème de Sylow que le nombre de q-Sylow vaut 1 modulo q et divise $p < q$: c'est donc 1. Comme tous les q-Sylow sont conjugués, le q-Sylow est distingué.
2. Soit P un p-Sylow de G. Comme l'ordre du sous-groupe $P \cap Q$ divise à la fois p et q, c'est 1. Par ailleurs, $\operatorname{card} P \operatorname{card} Q = \operatorname{card} G$. Donc $G = Q \rtimes P$.
3. La structure de groupe semi-directe de G est décrite par un morphisme $P \to \operatorname{Aut}(Q)$, soit $\mathbb{Z}/p\mathbb{Z} \to (\mathbb{Z}/q\mathbb{Z})^\times \equiv \mathbb{Z}/(q-1)\mathbb{Z}$. Si p ne divise pas $q-1$, aucun élément de $\operatorname{Aut}(Q)$ n'est d'ordre p. Le morphisme de structure est donc trivial et le produit est direct.
4. Si $p = 2$, le seul élément d'ordre 2 du groupe cyclique $\mathbb{Z}/(q-1)\mathbb{Z}$ est $(q-1)/2$. Il n'y a donc qu'une structure de produit semi-direct non direct : on retrouve le groupe diédral D_q.
5. Si p divise $q-1$, il y a des éléments d'ordre p dans le groupe cyclique $\operatorname{Aut}(Q)$, donc des structures de produits semi-direct non direct sur $Q \times P$. Les éléments d'ordre p sont puissances $\sigma^{\circ k} (1 \le k \le p-1)$ d'un élément σ d'ordre p. Le morphisme $\varphi_k : n \mapsto \left(\sigma^{\circ k}\right)^{\circ n} = \sigma^{\circ kn}$ s'écrit comme $\varphi_1 \circ m_k$ où $m_k : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ est l'automorphisme de multiplication par l'inversible k. Par les critères d'isomorphie des structures de produit semi-direct, les structures non directes sont toutes isomorphes ici.

Exercice 30. soit G un groupe d'ordre 63. L'ordre 63 se décompose en $3^2 \times 7$. Le nombre de 7-Sylow est 1 modulo 7 et divise 3^2 : c'est donc 1. Le 7-Sylow est donc un sous-groupe distingué et G n'est donc pas simple.

Exercice 31.

1. Comme u est nilpotent, il n'est pas inversible. Son rang peut donc être 0 (avec comme exemple la matrice nul), 1 avec comme exemple $\begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ et 2 avec comme exemple $\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$
2. Supposons u de rang 1. Son noyau est donc par la formule du rang, de dimension 2. Sa forme de Jordan a donc deux blocs, nécessairement un de taille 2 et un de taille 1 : c'est donc la matrice L. Dans une base (v_1, v_2, v_3) où l'endomorphisme u a L pour matrice, $\operatorname{im} u = \operatorname{Vect}(v_1)$ et $\ker u = \operatorname{Vect}(v_1, v_3)$. On peut donc affirmer $\operatorname{im} u \subset \ker u$.
3. Supposons u de rang 2. Son noyau est donc par la formule du rang, de dimension 1. Sa forme de Jordan a donc un seul bloc : c'est donc la matrice J. Dans une base (v_1, v_2, v_3) où l'endomorphisme u a J pour matrice, $\operatorname{im} u = \operatorname{Vect}(v_1, v_2)$ et $\ker u^2 = \operatorname{Vect}(v_1, v_2)$. On peut donc affirmer $\operatorname{im} u \subset \ker u^2$.

Exercice 32.

1.

$$(M - \mathrm{id}_3)(M - c\,\mathrm{id}_3) = \begin{pmatrix} 0 & a & 1 \\ 0 & 0 & b \\ 0 & 0 & c-1 \end{pmatrix} \begin{pmatrix} 1-c & a & 1 \\ 0 & 1-c & b \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & a(1-c) & ab \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

Notons que le polynôme minimal a les même facteurs irréductibles que le polynôme caractéristique. Si $c = 1$, comme $M - \mathrm{id}$ n'est pas nulle, M n'est pas diagonalisable. On suppose désormais que $c \neq 1$. Si $a = 0$, le polynôme minimal est $(X-1)(X-c)$. Si $a \neq 0$, le polynôme minimal est le polynôme caractéristique donc $(X-1)^2(X-c)$. La matrice M n'est donc diagonalisable que si $c \neq 1$ et $a = 0$.

2. Le polynôme caractéristique de la matrice est $X^2 - 1 - a^2$. Son discriminant est $\Delta = 4(1+a^2)$. Si $a \neq \pm i$, Δ est non nul. La matrice qui a alors deux valeurs propres distinctes, est diagonalisable. Si $a = \pm i$, la matrice a pour polynôme caractéristique X^2, mais elle n'est pas nulle : elle n'est donc pas diagonalisable.

Exercice 33.

1. On suppose que $\mathbb{K}$ contient le corps des nombres rationels $\mathbb{Q}$. Soit A une matrice de $\mathrm{M}_n(\mathbb{K})$. On note $sp(A)$ l'ensemble fini des valeurs propres de A. L'ensemble des entiers naturels k non nuls tels que $1/k$ soit dans $sp(A)$ est un ensemble fini. Ainsi, il existe $N \in \mathbb{N}^\star$ tel que pour $k \geq N$, $1/k$ n'est pas dans $sp(A)$ et $A_k := A - 1/kI_n$ est donc inversible. Par ailleurs,
$$\|A - A_k\| = \|\frac{1}{k} I_n\| \leq \frac{1}{k}\|I_n\| = \frac{1}{k}\sqrt{\mathrm{tr}({}^t\overline{I_n} I_n)} \leq \frac{1}{k}\sqrt{n}$$
qui tend vers 0 quand k tend vers $+\infty$. La suite de matrices inversibles $(A_k)_{k\geq N}$ tend donc vers A. On en déduit que l'ensemble $\mathrm{GL}_n(\mathbb{K})$ est dense dans $\mathrm{M}_n(\mathbb{K})$.

2. Soit A une matrice de $\mathrm{M}_n(\mathbb{C})$ et $\lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_{n-1} \leq \lambda_n$ ses n valeurs propres comptées avec multiplicités et ordonnées. Il existe une matrice de passage P et une matrice de Jordan J triangulaire supérieure à diagonale $\mathrm{diag}(\lambda_1, \lambda_2, \cdots, \lambda_{n-1}, \lambda_n)$ telles que $A = PJP^{-1}$. Pour tout entier $k \in \mathbb{N}^\star$, on note
$$A_k := P\left(J + \mathrm{diag}(\frac{1}{k^n}, \frac{1}{k^{n-1}}, \cdots, \frac{1}{k^2}, \frac{1}{k})\right)P^{-1}.$$
Puisque ses valeurs propres
$$\lambda_1 + \frac{1}{k^n} < \lambda_2 + \frac{1}{k^{n-1}} < \cdots < \lambda_{n-1} + \frac{1}{k^2} < \lambda_n + \frac{1}{k}$$
sont toutes deux à deux distinctes, la matrice A_k est diagonalisable. Par ailleurs,
$$\|A - A_k\| \leq \|P\|\,\mathrm{diag}(\frac{1}{k^n}, \frac{1}{k^{n-1}}, \cdots, +\frac{1}{k^2}, \frac{1}{k})\|\|P^{-1}\| \leq \|P\|\|P^{-1}\|\sqrt{n(\frac{1}{k})^2} \leq \frac{\|P\|\|P^{-1}\|\sqrt{n}}{k}$$
qui tend vers 0 quand k tend vers $+\infty$. La suite de matrices diagonalisables $(A_k)_{k\geq N}$ tend donc vers A.