Université de Strasbourg
Lie Fu, lie.fu@math.unistra.fr

M1-MF S1 2024-2025
feuille de TD

Algèbre I

Groupes

Exercice 1. Soit S un ensemble muni d'une loi de composition interne associative et admettant un élément neutre. Les éléments inversibles de S forment un groupe.

Exercice 2. Soit x, y, z des éléments d'un groupe tels que $xyz = 1$. A t-on $yzx = 1$? $yxz = 1$?

Exercice 3. Écrire toutes les manières possibles de former le produit de 4 éléments a, b, c, d dans cet ordre.

Exercice 4. Sur un ensemble (quelconque) S, la loi de composition interne $(a, b) \mapsto a$ est associative.

Exercice 5. Trouver un exemple de matrices de type 2×2 telles que $A^{-1}B \neq BA^{-1}$.

Exercice 6. Dans un groupe on a : $ab = b \Rightarrow a = 1$ et $ab = 1 \Rightarrow b = a^{-1}$.

Exercice 7. Soit a et b deux éléments d'un groupe. L'équation $ax = b$ a une unique solution.

Exercice 8. Soit G un groupe. Soit $(a, b) \mapsto a \circ b$ la loi de multiplication interne définie par $a \circ b = ba$ sur G. C'est une structure de groupe. (On l'appelle « groupe opposé » à G et on le note parfois G°).

Exercice 9. Déterminer tous les groupes de cardinal ≤ 6, leurs sous-groupes, leurs quotients et leurs automorphismes.

Exercice 10. Une partie H d'un groupe est dite *stable* si $gh \in H$ pour tous g et h dans H. Une partie stable *finie* est un sous-groupe.

Exercice 11. Un ensemble *fini* G (non vide) muni d'une loi de composition interne associative $(g, h) \mapsto g * h$ telle que $(\forall x, y, g \in G, gx = gy \Rightarrow x = y)$ et $(\forall x, y, g \in G, xg = yg \Rightarrow x = y)$ est un groupe. (L'**Exercice 4** montre qu'une seule de ces propriétés ne suffit pas pour avoir la conclusion.)

Exercice 12. Soit (G_α) une famille de sous-groupes distingués d'un groupe G. Si $\cap_\alpha G_\alpha = 1$, alors G est un sous-groupe de $\prod_\alpha G/G_\alpha$.

Exercice 13. Soit G le produit direct de deux sous-groupes A et B. Si H est un sous-groupe de G contenant A, alors H est le produit direct de A et de $H \cap B$.

Exercice 14. Soit H un sous-groupe distingué d'un groupe G, contenu dans le centre de G. Si G/H est monogène, alors G est abélien.

Exercice 15. Si tous les éléments d'un groupe G sont d'ordre ≤ 2, alors G est commutatif. Si G est fini, son ordre est une puissance de 2.

Exercice 16. Soit G un groupe et H un sous-groupe de G. On appelle système de représentants des classes à gauche mod H toute partie T de G qui rencontre toute classe à gauche mod H en un point et un seul ; cette condition équivaut à la suivante :
L'application $(x, y) \mapsto xy$ est une bijection de $T \times H$ sur G.

(1) Soit T un tel système de représentants. Pour tout g dans G et tout t dans T on note $x(g, t) \in T$ et $y(g, t) \in H$ les éléments tels que $gt = x(g, t)y(g, t)$. Soit S une partie engendrant G. Montrer que les éléments $y(g, t)$ pour $g \in S$ et $t \in T$ engendrent H. (Soit H' le sous-groupe que ces éléments engendrent, on montrera que TH' est stable par multiplication à gauche par les éléments de S puis par multiplication à gauche par tous les éléments de G ; d'où $TH' = G$ et $H' = H$).

(2) On suppose que l'indice $(G : H)$ est fini. Alors G peut être engendré par une partie finie si et seulement si c'est le cas pour H.

Exercice 17. Soit G un groupe produit direct de A et B et soit C_A le centre de A. Soit N un sous-groupe distingué de G tel que $N \cap A = \{1\}$, alors $N \subset C_A \times B$.
Soit $(S_i)_{i \in I}$ une famille finie de groupes simples non commutatifs. Les sous-groupes distingués de $\prod_{i \in I} S_i$ sont alors les produits partiels $\prod_{i \in J} S_i$ pour $J \subset I$.

Exercice 18. Dans un groupe fini G, le nombre des conjugués d'un élément $a \in G$ est égal à l'indice du normalisateur de a et est par suite un diviseur de l'ordre de G.

Exercice 19. Soit Γ le groupe des automorphismes d'un groupe G et Δ le groupe des automorphismes intérieurs. Alors Δ est un sous-groupe distingué de Γ.
Pour qu'un automorphisme σ de G soit permutable (ie commute) avec tous les automorphismes intérieurs de G, il faut et il suffit que, pour tout $x \in G$, $x^{-1}\sigma(x)$ appartienne au centre de G. En déduire que si le centre de G est réduit à l'élément neutre, il en est de même du centralisateur de Δ dans Γ.

Exercice 20. Soit G un groupe.
Si H est un sous-groupe d'indice n, alors l'indice de l'intersection N des conjugués de H est un diviseur de $n!$ (noter que G/N est isomorphe à un sous-groupe de $\mathfrak{S}_n$).
On dit que G est *résiduellement fini* si l'intersection de ces sous-groupes d'indice fini est $\{e\}$. Montrer que ceci équivaut à dire que G est isomorphe à un sous-groupe d'un produit de groupes finis.
On suppose que G peut être engendré par un ensemble fini. Pour tout entier n, l'ensemble P_n des sous-groupes d'indice n est alors fini.
Sous cette dernière hypothèse, on considère un endormorphisme f de G qui est surjectif. Pour tout n, l'application

$H \mapsto f^{-1}(H)$ est alors une bijection de P_n. En déduire que le noyau de f est contenu dans tout sous-groupe d'indice fini de G. En particulier, si G est résiduellement fini, f est bijectif.

Exercice 21. Soit p un nombre premier. Pour tout $n \in \mathbb{Z}$, on a alors $n^p = n \mod p$.
Soit x et y deux éléments d'un groupe G tels que $yxy^{-1} = x^n$ ($n \in \mathbb{Z}$) et $x^p = 1$. Alors $y^p x y^{-p} = x^n$ et y^{p-1} commute à x.
Si, dans un groupe G, tous les éléments $\neq 1$ sont d'ordre p et sont conjugués entre eux, alors G est d'ordre 1 ou 2. (Prouvez d'abord que G est commuatif en utilisant la question précédente).

Exercice 22. Les éléments (12)(34), (13)(24) et (14)(23) forment, avec l'élément neutre, un sous-groupe commutatif H de $\mathfrak{A}_4$. Ce groupe est distingué dans $\mathfrak{A}_4$ et dans $\mathfrak{S}_4$ et $\mathfrak{A}_4/H$ est cyclique d'ordre 3.
Le centralisateur de H dans $\mathfrak{S}_4$ est égal à H. L'application qui à $s \in \mathfrak{S}_4$ associe l'élément $x \mapsto sxs^{-1}$ de $\mathrm{Aut}(H)$ induit un isomorphisme de $\mathfrak{S}_4/H$ sur $\mathrm{Aut}(H)$ et ce dernier groupe est isomorphe à $\mathfrak{S}_3$.
Soit K un sous-groupe d'ordre 2 de H, alors K n'est pas distingué dans $\mathfrak{A}_4$.

Exercice 23. Soit G un groupe simple et H un sous-groupe d'indice fini $n > 1$. Alors G est fini d'ordre divisant $n!$ et G est commutatif si $n \leq 4$.

Exercice 24. Soit $p(n)$ le nombre de classes de conjugaison du groupe symétrique $\mathfrak{S}_n$. Ce nombre est égal au nombre des familles $(x_1, x_2, \ldots, x_n)$ d'entiers ≥ 0 telles que $\sum_{i=1}^{n} i x_i = n$. En déduire l'identité $\sum_{n=0}^{\infty} p(n) T^n = \prod_{m=0}^{\infty} \frac{1}{1-T^m}$.

Exercice 25. Dans un groupe cyclique d'ordre 20, trouver toutes les parties génératrices irréductibles (c'est-à-dire, toute sous-partie stricte engendre un sous-groupe strict) à 2 éléments.

Exercice 26. Soit x, u et v des éléments d'un groupe G tels que $x = uv = vu$, $u^p = 1$, $v^q = 1$ où p et q sont des entiers premiers entre eux. Il existe alors p' et q', premiers entre eux, tels que $u = x^{p'}$, $v = x^{q'}$.

Exercice 27. Soit x un élément d'ordre pq d'un groupe G où p et q sont premiers entre eux. Il existe alors u et v dans G tels que $x = uv$, $u^p = 1$, $v^q = 1$.

Exercice 28. Soit u_1, v_1, u_2, v_2 des éléments d'un groupe G tels que $u_1 v_1 = v_1 u_1 = u_2 v_2 = v_2 u_2$ et $u_1^p = u_2^p = v_1^q = v_2^q = 1$ où p et q sont premiers entre eux. On a alors $u_1 = u_2$ et $v_1 = v_2$

Exercice 29. Soit x un élément d'un groupe G dont l'ordre est $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$ où α_1, …, α_m sont des entiers ≥ 1 et p_1, …, p_m sont des nombres premiers deux à deux distincts. Il existe alors un unique m-uplets $(y_1, \ldots, y_m)$ d'éléments deux à deux permutables tel que $x = y_1 \cdots y_m$ et $y_1^{p^{\alpha_1}} = \cdots = y_m^{p^{\alpha_m}} = 1$.

Exercice 30. Trouver tous les groupes ayant exactement (1) un sous-groupe ; (2) deux sous-groupes ; (3) trois sous-groupes.

Exercice 31. Deux cycles de supports disjoints commutent.

Exercice 32. Quelles sont les décompositions en cycles disjoints des permutations suivantes

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 1 & 5 & 6 & 8 & 7 & 4 \end{pmatrix}$$

$$\beta = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 9 & 12 & 8 & 11 & 6 & 7 & 5 & 3 & 2 & 4 & 10 & 1 \end{smallmatrix}\right)$$

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

Exercice 33. Si une permutation est décomposée en cycles disjoints de longueurs m_1, m_2, …, m_k, alors sont ordre est le plus petit commun multiple des nombres m_1, …, m_k.

Exercice 34. Soit α une permutation écrite comme un produit de cycles (pas nécessairement disjoints) et soit β une permutation. Alors $\beta\alpha\beta^{-1}$ est obtenue en remplaçant chaque nombre dans l'écriture en cycles par son image par β.

Exercice 35. Trouver dans le groupe $\mathfrak{S}_n$ tous les éléments permutables au cycle $(x_1, x_2, \ldots, x_n)$ où x_1, …, x_n est une permutation des nombres 1, 2, …, n.

Exercice 36. Les ensembles suivants engendrent le groupe $\mathfrak{S}_n$:

- l'ensemble de tous les cycles ;
- l'ensemble de toutes les transpositions ;
- l'ensemble des transpositions $(1\,2)$, $(2\,3)$, …, $(n-1\,n)$;
- l'ensemble des transpositions $(1\,2)$, $(1\,3)$, …, $(1\,n)$;
- l'ensemble constitué de $(x_1 x_2)$ et $(x_1 x_2 \ldots x_n)$ où x_1, …, x_n est une permutation des nombres 1, 2, …, n.

Exercice 37. Les ensembles suivants engendrent le groupe $\mathfrak{A}_n$:

- l'ensemble de tous les 3-cycles ;
- l'ensemble des cycles $(1\,2\,3)$, $(1\,2\,4)$, …, $(1\,2\,n)$.

Exercice 38. Soit N le normalisateur d'un élément a d'un groupe G. Alors le normalisateur de $x^{-1}ax$ est $x^{-1}Nx$. Même question avec le normalisateur et le centralisateur d'une partie.

Exercice 39. Soit G un groupe fini, $x \in G$, k le nombre des conjugués de x et k' le nombre des conjugués de x^n. Alors k' divise k.

Exercice 40. Soit, dans le groupe symétrique $\mathfrak{S}_n$, des permutations décomposées en produits de cycles disjoints : $x = (a_{11} \ldots a_{1k_1})(a_{21} \ldots a_{2k_2}) \cdots (a_{p1} \ldots a_{pk_p})$ $(1 < k_1 \leq k_2 \leq \cdots \leq k_p)$ et $y = (b_{11} \ldots b_{1\ell_1})(b_{21} \ldots b_{2\ell_2}) \cdots (b_{q1} \ldots b_{q\ell_q})$ $(1 < \ell_1 \leq \ell_2 \leq \cdots \leq \ell_q)$. Alors x et y sont conjugués dans $\mathfrak{S}_n$ si et seulement si $p = q$ et $k_1 = \ell_1$, $k_2 = \ell_2$, …, $k_p = \ell_p$.

Exercice 41. Partitionnez le groupe $\mathfrak{S}_4$ en classes de conjugaison.

Exercice 42. Partitionnez le groupe $\mathfrak{A}_4$ en classes de conjugaison. (Comparez le résultat à l'exercice précédent.)

Exercice 43. Soit p un nombre premier. Il existe, à isomorphisme près, un unique groupe non cyclique et d'ordre p^2. Ce groupe est commutatif.

Exercice 44. Montrer « explicitement » que $(123)(45)$ et $(35)(241)$ sont conjuquées.

Exercice 45. Notons $\alpha, \beta, \gamma, \delta, \tau$ les éléments suivant de $\mathfrak{S}_8$

$$\alpha = (123)(4568)$$
$$\beta = (34)(52618)$$
$$\gamma = (134)(2357)(1846)$$
$$\delta = (82143)(12)(15)$$
$$\tau = (874312)(56).$$

Calculer α^3, $\beta^2\alpha$, $\gamma\delta\tau$, $\gamma^4\delta^2$ et $\tau\delta\gamma$.

Exercice 46. Quels sont les ordres des deux éléments suivants de $\mathfrak{S}_{12}$:

$$\alpha = (1, 3, 2, 5, 4, 6, 7, 8, 12, 10, 9, 11)$$
$$\beta = (2, 1, 5, 8, 4).$$

Exercice 47. Soit la permutation

$$\alpha = (x_{11}x_{12}\dots x_{1k_1})(x_{21}x_{22}\dots x_{2k_2})\cdots(x_{i1}x_{i2}\dots x_{ik_i}).$$

Alors

$$\alpha^{-1} = (x_{ik_i}\dots x_{i2}x_{i1})\cdots(x_{2k_2}\dots x_{22}x_{21})(x_{1k_1}\dots x_{12}x_{11}).$$

Exercice 48. Trouver toutes les puissances du cycle $\alpha = (x_1 \dots x_n)$.

Exercice 49. Soient p et q deux permutations. Les décompositions en cycles disjoints de pq et qp sont les « mêmes ».

Exercice 50. Le groupe $\mathfrak{S}_7$ contient-il un élément d'ordre 5 ? d'ordre 10 ? d'ordre 15 ? Quel est le plus grand ordre possible d'un élément de $\mathfrak{S}_7$?

Exercice 51. Décomposer en cycles disjoints la permutation $i \mapsto n + 1 - i$.

Exercice 52. Combien de transpositions sont nécessaires pour écrire le cycle $(12 \dots n)$?

Exercice 53. Quel est le centralisateur de (12) dans $\mathfrak{S}_4$.

Exercice 54. Déterminer les sous-groupes d'ordre 4 de $\mathfrak{S}_4$. Lesquels sont distingués ?

Exercice 55. Avec les notations de l'**Exercice 45**, calculer $\alpha\delta\alpha^{-1}$, $\tau^{-2}\alpha\tau^2$, $\beta^{-5}\alpha\beta^5$. [utiliser l'exercice 34.]

Exercice 56. Soit $\alpha = (123)(456)(789)$, $\beta = (147)(258)(369)$, $\gamma = (456)(789)$. Alors α commuta avec β et γ et α est égal au produit d'une puissance de β et d'une puissance de γ.

Exercice 57. Trouver tous les éléments de $\mathfrak{S}_{10}$ permutables à $\alpha = (x_1x_2 \dots x_5)(x_6x_7 \dots x_{10})$, où $x_1, x_2, \dots, x_{10}$ sont des éléments de $\{1, 2, \dots, 10\}$ deux à deux distincts.

Exercice 58. Soient

$$\alpha = (123)(456789),$$
$$\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 5 & 9 & 4 & 7 & 6 & 8 & 2 & 3 \end{pmatrix}.$$

(1) α peut s'écrire comme le produit de 9, 11 et 15 transpositions différentes mais pas comme le produit de 5 transpositions.

(2) β est le produit de 4, 6, 8 et 10 transpositions différentes.

(3) α peut s'écrire comme le produit de n transpositions si et seulement si l'entier n est impair ≥ 7.

(4) β peut s'écrire comme le produit de n transpositions si et seulement si l'entier n est impair ≥ 4.

Exercice 59. Les ensembles suivants sont des parties génératrices irréductibles de $\mathfrak{S}_6$:

$$M_1 = \{(12), (34), (56), (23)(45)\}$$
$$M_2 = \{(12), (34), (123)(456)\}$$
$$M_3 = \{(12), (23), (24)(156)\}.$$

Exercice 60. Soit A une partie à deux éléments, génératrice de $\mathfrak{S}_4$. Montrer qu'aucun de ces éléments n'est une double transposition. [Se référer à l'exercice 22.]

Exercice 61. Calculer le nombre de permutations de $\mathfrak{S}_n$ n'ayant aucun point fixe.

Exercice 62. Décrire les 2-Sylow de $\mathfrak{S}_2$, $\mathfrak{S}_3$ et $\mathfrak{S}_4$.

Exercice 63. Décrire un p-Sylow de $\mathfrak{S}_p$ (p est premier). Décrire un p-Sylow de $\mathfrak{S}_{kp}$ pour $k < p$. Décrire un p-Sylow de $\mathfrak{S}_{p^2}$.

Exercice 64. Décrire un p-Sylow de $\mathfrak{S}_n$.

Exercice 65. Combien d'éléments d'ordre 5 peut contenir un groupe d'ordre 20 ?

Exercice 66. Un groupe d'ordre pq (p et q sont premiers) n'est pas simple.

Exercice 67. Un groupe d'ordre p^2q (p et q sont premiers) n'est pas simple.

Exercice 68. Trouver les 2-Sylow du groupe diédral D_{10}.

Exercice 69. Soit H un sous-groupe de G dont l'indice p est un nombre premier. Quel peut-être le nombre de conjugués de H ?
On suppose de plus que p est le plus petit diviseur premier de $|G|$, alors le groupe H est distingué.

Exercice 70. Soit G un groupe de cardinal p^rm (p premier et ne divise pas m). Alors G contient un groupe de cardinal p^e pour tout $e \leq r$.

Exercice 71. Soit G un groupe de cardinal pm (p premier et ne divise pas m). Soit S un p-Sylow de G et soit X l'ensemble des p-Sylow de G. Quel peut-etre le nombre d'orbites de S dans X ?

Exercice 72. Un groupe d'ordre 224 n'est jamais simple.

Exercice 73. Soit G un groupe fini et S, S' deux p-Sylow de G. Si S' normalise S alors $S' = S$. En déduire, en utilisant le lemme sur l'action des p-groupes et l'action de S sur les p-Sylow de G, que le nombre des p-Sylow de G est congru à 1 module p.

Exercice 74. Soit G un groupe fini et S un p-Sylow de G. L'indice dans G du normalisateur $N_G(S)$ est congru à 1 modulo p.

Exercice 75. Soit G un groupe fini, H un sous-groupe distingué de G. Soit $z : G \to G/H$ l'application de passage au quotient.

(1) Si S est un p-Sylow de G, alors $S \cap H$ est un p-Sylow de H.
(2) Tout p-Sylow de H est de la forme $S \cap H$ où S est un p-Sylow de G.
(3) Si S est un p-Sylow de G, alors $z(S)$ est un p-Sylow de G/H.
(4) Tout p-Sylow de G/H est de la forme $z(S)$ où S est un p-Sylow de G.

Exercice 76. Soit G un groupe fini, S un p-Sylow de G et H un sous-groupe de G contenant $N_G(S)$. Alors $N_G(H) = H$

Exercice 77. (Critère pour qu'un groupe soit un produit direct, bon à savoir) Soit G un groupe et H, K des sous-groupes de G.

— Si H (ou K) est distingué, alors le sous-groupe engendré par H et K est égal à HK.
— Si H et K sont distingués et si $H \cap K = \{1\}$, alors le sous-groupe HK est isomorphe au produit direct $H \times K$. En particulier si $HK = G$ alors G est isomorphe à $H \times K$.

Exercice 78. Il y a exactement (à isomorphisme près) deux groupes d'ordre 6.

Exercice 79. Tout groupe d'ordre 15 est cyclique. Il y a (à isomorphisme près) exactement deux groupes d'ordre 21.

Exercice 80. Un groupe d'ordre $2p$ (p premier) est cyclique ou diédral.

Exercice 81. Soit G un groupe d'ordre 30 et K un 5-Sylow, H un 3-Sylow. Alors H ou K est distingué et HK est cyclique. Trouver tous les groupes d'ordre 30.

Exercice 82. Soit G un groupe d'ordre 55. Il existe alors x d'ordre 11 dans G et y d'ordre 5. Il existe r tel que $yxy^{-1} = x^r$. Les restes possibles de r modulo 11 sont 1, 3, 4, 5, 9. Toutes ses valeurs sont possibles et il y a deux groupes d'ordre 55.

Exercice 83. Tout groupe abélien est résoluble.

Exercice 84. Le groupe des quaternions est résoluble.

Exercice 85. Si p et q sont premiers, tout groupe d'ordre pq est résoluble.

Exercice 86. Un groupe G est résoluble si et seulement si il existe une suite finie décroissante de sous-groupes $H_0 = G \supset H_1 \supset \cdots \supset H_m = \{1\}$ telle que H_k contient les commutateurs de H_{k-1}.

Exercice 87. Un sous-groupe d'un groupe résoluble est résoluble. Un quotient d'un groupe résoluble est résoluble. Soit N un sous-groupe distingué de G. Alors G est résoluble si et seulement si N et G/N le sont.

Quleques exercices sur les produits semi-directs.

Exercice 88. [à faire au moins une fois dans sa vie] Soit G un groupe, H un sous-groupe distingué et K un sous-groupe. Alors l'action de K par conjugaison sur G induit un homomorphisme $\phi : K \to \mathrm{Aut}(H)$. Alors L'application $H \times K \to G \mid (h, k) \to hk$ est une bijection si et seulement si $H \cap K = \{1\}$ et le groupe engendré par H et K est égal à G. En supposant que cette application est bijective, l'ensemble $H \times K$ est ainsi muni d'une loi de groupe ; écrire cette loi en termes des lois de groupes sur H et K et de ϕ.
Inversement, avec la formule trouvée, étant donné deux groupes H et K et un homomorphisme $\phi : K \to \mathrm{Aut}(H)$, construire une loi de composition interne sur $H \times K$ et montrer que c'est une loi de groupe.

Exercice 89. Décrire tous les sous-groupes du groupe H des quaternions. Ils sont tous distingués et H n'est jamais produit semidirect de deux de ses sous-groupes propres.

Exercice 90. Décrire les sous-groupes du groupe diédral D_8. Lesquels sont distingués ? D_8 est-il produit semi-direct de sous-groupes propres ?

Exercice 91. Si pour tous a et b dans un groupe G on a $(ab)^2 = a^2b^2$, alors G est commutatif.
Construire, comme produit semi-direct, un groupe d'ordre 27, non commutatif, où tout élément est d'ordre 3 (et en particulier où la relation $(ab)^3 = a^3b^3$ est vérifiée)

Exercice 92. Soient H et K deux sous-groupes finis distingués d'un groupe G dont les ordres sont premiers entre eux. Alors $xy = yx$ pour tout $x \in H$ et tout $y \in K$ et $H \times K \simeq HK$. Si $H_1, \ldots, H_r$ sont des sous-groupes distingués dont les ordres sont premiers entre eux deux à deux, alors $H_1 \times \cdots \times H_r \simeq H_1 \cdots H_r$.

Exercice 93. Soit G un groupe fini, N un sous-groupe distingué tel que les ordres de N et de G/N sont premiers entre eux. Si H est un groupe dont l'ordre est celui de G/N alors G est le produit semi-direct de N par H. Si g est un automorphisme de G, alors $g(N) = N$.

Exercice 94. Soient G un groupe et H un sous-groupe distingué de G tel que G/H soit cyclique d'ordre fini n. Soit x un élément de G dont l'image $\bar{x}$ dans G/H engendre G/H. Soit ϕ l'automorphisme $h \mapsto xhx^{-1}$ de H et soit $y = x^n$. Montre que $\phi(y) = y$ et que ϕ^n est l'automorphisme intérieur de H défini par y.
Soit τ le morphisme de $\mathbb{Z}$ dans $\mathrm{Aut}(H)$ donné par $\tau(m) = \phi^m$ et soit $E = H \rtimes_\tau \mathbb{Z}$ le produit semi-direct correspondant. Montrer que l'élément (y^{-1}, n) de E engendre un sous-groupe central C_y de E et que le quotient E/C_y est isomorphe à G.

Anneaux

Exercice 95. L'ensemble $\{0\}$ est un anneau unitaire.

Exercice 96. Soit A un anneau unitaire. Alors $1_A = 0_A$ si et seulement si $A = \{0_A\}$.

Exercice 97. Dans un anneau unitaire A, on a $-x = (-1_A) \cdot x = x \cdot (-1_A)$ $(\forall x \in A)$.

Exercice 98. Le produit de convolution fait de $\mathrm{L}^1(\mathbb{R};\mathbb{C})$ un anneau commutatif.

Exercice 99. Si A est un anneau, il y a un unique homomorphisme $\mathbb{Z} \to A$.

Exercice 100. Soit V un k-espace vectoriel, en particulier V est un groupe abélien. On note $\mathrm{End}_+(V)$ l'anneau des homomorphismes de groupes de V dans V et on note $\mathrm{End}_k(V)$ l'anneau des applications k-linéaires de V dans V. Alors $\mathrm{End}_k(V)$ est un sous-anneau de $\mathrm{End}_+(V)$. Est-ce un idéal ? Et si k est $\mathbb{Q}$? un corps fini ? un corps $\mathbb{F}_p$ (p premier) ?

Exercice 101. [exercice fleuve] Calculer l'anneau $\mathrm{End}_+(\mathbb{Z})$. Et l'anneau $\mathrm{End}_+(\mathbb{Z}/n\mathbb{Z})$. Puis l'anneau $\mathrm{End}_+(\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})$ (n premier puis n puissance d'un nombre premier). Calculer $\mathrm{End}_+(\mathbb{Z} \times \mathbb{Z})$. Si p est premier, calculer $\mathrm{End}_+(\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/p\mathbb{Z})$, $\mathrm{End}_+(\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/p^2\mathbb{Z})$, $\mathrm{End}_+(\mathbb{Z}/p^k\mathbb{Z} \times \mathbb{Z}/p^\ell\mathbb{Z})$. Si n et m sont permiers entre eux, alors $\mathrm{End}_+(\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z})$ est « naturellement » isomorphe à $\mathrm{End}_+(\mathbb{Z}/n\mathbb{Z}) \times \mathrm{End}_+(\mathbb{Z}/m\mathbb{Z})$. Étudier encore l'anneau $\mathrm{End}_+(\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z})$ lorsque n divise m. Continuer autant que vous le pouvez afin de pouvoir répondre à la question suivante : pour G un groupe abélien de type fini, quand est-ce que $\mathrm{End}_+(G)$ est commutatif ?

Exercice 102. Décrire, « le plus possible », les anneaux $\mathbb{C}[\mathbb{Z}/2\mathbb{Z}]$, $\mathbb{C}[\mathbb{Z}/n\mathbb{Z}]$, $\mathbb{C}[\mathfrak{S}_3]$, etc.

Exercice 103. Lesquels sont des anneaux ?

- R_0 l'ensemble des polynomes $f \in \mathbb{R}[x]$ tel que $f(x) = f(-x)$.
- R_1 l'ensemble des polynomes $f \in \mathbb{R}[x]$ tel que $f(x) = -f(-x)$.
- R_2 les matrices réelles de type 2×2 avec la multiplication matricielle habituelle.
- R_3 l'ensemble des matrices réelles de type 2×2 avec la multiplication $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} aa' & bb' \\ cc' & dd' \end{pmatrix}$.
- R_4 l'ensemble R_4 muni du produit croisé $\begin{pmatrix} a \\ b \\ c \end{pmatrix} \times \begin{pmatrix} a' \\ b' \\ c' \end{pmatrix} = \begin{pmatrix} bc' - cb' \\ ca' - ac' \\ ab' - ba' \end{pmatrix}$

Exercice 104. L'ensemble R des nombres rationels de la forme a/b où b n'est *pas* un multiple de 6 est-il un sous-anneau de $\mathbb{Q}$?

Exercice 105. Soit X un ensemble. Soit R l'ensemble des parties de X, on définit une addition et une multiplication comme suit :

$$A + B = (A \cup B) \smallsetminus (A \cap B)$$
$$AB = A \cap B.$$

Pour A dans R on pose $\chi_A : R \to \mathbb{F}_2$ par $\chi_A(x) = 1$ si $x \in A$ et $\chi_A(x) = 0$ si $x \notin A$.

(1) Vérifier que $A + \emptyset = A$ et $A + A = \emptyset$.
(2) Montrer que $\chi_{A+B} = \chi_A + \chi_B$ et que $\chi_{AB} = \chi_A\chi_B$.
(3) Montrer que $A = B \Leftrightarrow \chi_A = \chi_B$.
(4) Montrer que R est un anneau commutatif.

Exercice 106. Soit I un idéal à gauche d'un anneau A et $k \in \mathbb{N}$. Alors $(I + IR)^k \subset I^k + I^kR$.

Exercice 107. Soient I et J des idéaux à gauche d'un anneau unitaire A avec $I + J = A$. Alors $I \cap J \subset IJ + JI$.

Exercice 108. Soient I et J des idéaux d'un anneau unitaire commutatif A avec $I + J = A$. Alors $I \cap J = IJ$.

Exercice 109. Soient A un anneau unitaire et I un idéal à gauche et S un sous-ensemble de A. Alors l'ensemble, noté IS, égal au sous-groupe additif engendré par $\{xs\}_{x\in I, s\in S}$, est un idéal à gauche. Si S est un idéal à droite, alors IS est un idéal bilatère.

Exercice 110. Dans $\mathbb{Z}$, calculer la somme, le produit et l'intersection des idéaux $n\mathbb{Z}$ et $m\mathbb{Z}$.

Exercice 111. Soit A un anneau non nul (commutatif et unitaire). Soit $S \subset A$ un sous-ensemble stable par multiplication et ne contenant pas 0. Il existe alors $\mathfrak{p}$ un idéal maximal parmi les idéaux ayant une intersection vide avec S. Tout tel idéal est premier.

Exercice 112. Soit A un anneau intègre (commutatif et unitaire) et soit S un sous-ensemble de $A \smallsetminus \{0_A\}$ stable par multiplication. Alors l'ensemble $S^{-1}A$ des éléments du corps des fractions de A qui s'écrivent a/s avec $a \in A$ et $s \in S$ est un anneau.

Exercice 113. Soit A un anneau principal (intègre, commutatif est unitaire) et soit $S \subset A \smallsetminus \{0_A\}$ un sous-ensemble stable par multiplication. Alors l'anneau $S^{-1}A$ est principal.

Exercice 114. Soit A un anneau factoriel (intègre, commutatif est unitaire) et soit $S \subset A \smallsetminus \{0_A\}$ un sous-ensemble stable par multiplication. Alors l'anneau $S^{-1}A$ est factoriel ; ses éléments irréductibles sont les $p \in A$ tel que $(p) \cap S = \emptyset$.

Exercice 115. Soit A un anneau factoriel (…) et $p \in A$ irréductible. Alors $S = A \smallsetminus (p)$ est stable par multiplication et l'anneau $S^{-1}A$ est principal.

Exercice 116. Dans un anneau principal (…) A, soient a_1, …, a_n des éléments de A et soit d tel que $(d) = (a_1, \ldots, a_n)$ alors d est le plus grand diviseur commun à a_1, …, a_n.

Exercice 117. Le groupe des inversibles de l'anneau $\mathbb{Z}/p^r\mathbb{Z}$ est cyclique si $p \geq 3$ est premier et est $\simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{r-2}\mathbb{Z}$ si $p = 2$. (Si $p \geq 3$, alors ce groupe est engendré par $1 + p$ et un groupe cyclique d'ordre $p - 1$; si $p = 2$ alors il est le produit du groupe engendré par 5 et du groupe engendré par -1.)

Exercice 118. L'anneau $\mathbb{Z}[i]$ est principal. Quelles sont ses unités ?

Exercice 119. Soit D un entier ≥ 1 et notons $\mathbb{Z}[\sqrt{-D}]$ l'ensemble des nombres complexes de la forme $a + ib\sqrt{D}$, $a, b \in \mathbb{Z}$. C'est un anneau. La conjugaison complexe induit un automorphisme de R. Si $D \geq 2$, les unités de $\mathbb{Z}[\sqrt{-D}]$ sont ± 1. Dans $\mathbb{Z}[\sqrt{-5}]$ les éléments 3, $2 \pm \sqrt{-5}$ sont irréductibles, 3 et $2 + i\sqrt{5}$ n'ont pas de ppcm et 9 et $3(2 + i\sqrt{5})$ n'ont pas de pgcd.

Exercice 120. Soit K un anneau commutatif (unitaire) et soit R l'ensemble des fonctions de $\mathbb{N}^*$ dans K (pas nécessairement à support fini). On munit R de l'addition usuelle des fonctions et du produit de convolution : si $f, g \in R$ et si $m \in \mathbb{N}^*$

$$f * g(m) = \sum_{xy=m} f(x)g(y).$$

Alors R est un anneau commutatif dont l'unité est la fonction $\delta : \mathbb{N}^* \to K$ telle que $\delta(1) = 1_K$ et $\delta(m) = 0_K$ pour tout $m \geq 2$. Si K est intègre alors R l'est aussi.
Une fonction $f : \mathbb{N}^* \to K$ est dite *multiplicative* si $f(mn) = f(m)f(n)$ pour tous $m, n \in \mathbb{N}^*$ *premiers entre eux*. Si f et g sont multiplicatives, alors $f * g$ est multiplicative. Deux fonctions multiplicatives sont égales si et seulement si elles coïncident sur les puissances des nombres premiers.
La *fonction de Möbius* est la fonction $\mu : \mathbb{N}^* \to K$ tel que $\mu(1) = 1_K$, $\mu(n) = (-1_K)^r$ si n est le produit de r nombres premiers deux à deux distincts et $\mu(n) = 0$ sinon (c'est-à-dire s'il existe p premier tel que p^2 divise n). Alors μ est multiplicative. Soit $\phi \in R$ la fonction constante égale à 1_K. Alors $\mu * \phi = \delta$ (le vérifier d'abord sur les puissances des nombres premiers). Expliciter l'égalité $\mu * (\phi * f) = f$ (« formule d'inversion de Möbius »).

Exercice 121. Si $A[X]$ est factoriel, alors A est factoriel. (Les éléments irréductibles de degré 0 de $A[X]$ sont les irréductibles de A).

Exercice 122. Que peut-on dire de l'image réciproque d'un idéal maximal ? et si f est surjectif ?

Exercice 123. Soit $\mathfrak{P}$ un idéal premier d'un anneau unitaire commutatif A et soient I_1, …, I_n des idéaux. Si $\mathfrak{P}$ contient le produit $I_1 I_2 \cdots I_n$, alors il contient l'un des I_k.

Exercice 124. Si I est un idéal non premier, il existe des idéaux I_1, I_2 distincts de I et tels que $I \subset I_1$, $I \subset I_2$ et $I_1 I_2 \subset I$.

Exercice 125. Soit A un anneau, un élément $a \in A$ est dit *nilpotent* s'il existe $n \in \mathbb{N}$ tel que $a^n = 0$.

- L'ensemble $\mathrm{Nil}(A)$ des éléments nilpotents est un idéal.
- Si $\mathfrak{P}$ est un idéal premier alors $\mathrm{Nil}(A) \subset \mathfrak{P}$.
- Soit $s \notin \mathrm{Nil}(A)$. Il existe alors un idéal premier $\mathfrak{P}$ ne contenant pas s (appliquer **Exercice 111** à $S = \{1, s, s^2, \ldots, s^n, \ldots\}$). En conclure que $\mathrm{Nil}(A)$ est l'intersection des idéaux permiers.

Exercice 126. Lorsque A est un anneau commutatif unitaire (pas nécessairement intègre), calculer $A[X]^*$.

Exercice 127. Soit B un anneau et A un sous-anneau de B. On dit qu'un élément $b \in B$ est *entier sur* A s'il existe $n \in \mathbb{N}^*$ et $a_0, \ldots, a_{n-1}$ dans A tels que

$$b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0.$$

Un anneau intègre A (commutatif et unitaire) est dit *intégralement clos* si tout élément de $K = \mathrm{Frac}(A)$ qui est entier sur A appartient à A.

- Un anneau factoriel est intégralement clos.
- Soit $d \in \mathbb{Z} \setminus \{0\}$ est un entier sans facteur carré, on pose $\mathbb{Z}[\sqrt{d}] = \{x \in \mathbb{C} \mid \exists a, b \in \mathbb{Z}, x = a + b\sqrt{d}\}$. Si $d = 1 \mod 4$, alors $\mathbb{Z}[\sqrt{d}]$ n'est pas intégralement clos.

Exercice 128. Dans un anneau factoriel A, on a, pour tous a, $b \in A$, $ab = \mathrm{pgcd}(a, b)\,\mathrm{ppcm}(a, b)$.

Exercice 129. Soit A un anneau euclidien relativement à v. Soit $K = \mathrm{Frac}(A)$ et soit $s \in A \setminus \{0\}$. Alors $A_s = \{x \in K \mid \exists a \in A, n \in \mathbb{N}, x = \frac{a}{s^n}\}$ est un anneau euclidien.

Exercice 130. Soit k un corps. Étudier l'irréducibilité des polynomes suivant dans $k[X, Y]$: $Y - X^2$, $X^2 + Y^2 + 1$, $X^2 + Y^2 - 1$, $X^2 - Y^2 - 1$, $Y^2 - X^3$, $X^3 - Y^2 - X$, $XY^3 - X^2Y - Y^2 + X$.

Exercice 131. Soit A l'anneau $\mathbb{C}[X, Y]/(Y^2 - X^3)$, notons x et y les images de X et Y dans A.

- Montrer qu'on définit un morphisme de A dans $\mathbb{C}[T]$ en posant $\phi(x) = T^2$ et $\phi(y) = T^3$. Montrer que ϕ est injectif. Quel est son image ?
- Montrer que $\mathrm{Frac}(A)$ est isomorphe à $\mathbb{C}(T)$. En déduire que A n'est pas intégralement clos (utiliser **Exercice 127** et considérer l'élément T de $\mathrm{Frac}(A)$).

Exercice 132. L'anneau $\mathbb{C}[X, Y]/(X^3 - Y^2 - X)$ n'est pas factoriel (si x, y sont les images de X et Y, montrer que y est irréductible mais que (y) n'est pas premier car $y^2 = x(x - 1)(x + 1)$).

Exercice 133. Les anneaux $\mathbb{C}[X, Y]/(Y - X^2)$ et $\mathbb{C}[X, Y]/(XY - 1)$ sont factoriels et même principaux (trouver des anneaux plus simples auquels ils sont isomorphes).

Exercice 134. Soient P et Q dans $\mathbb{C}[X, Y]$ sans facteur commun.

- Il existe A, B dans $\mathbb{C}[X, Y]$ et D dans $\mathbb{C}[X]$ avec $D \neq 0$ et $D = AP + BQ$ (travailler dans l'anneau $\mathbb{C}(X)[Y]$).
- En déduire que $V = \{(x, y) \in \mathbb{C}^2 \mid P(x, y) = Q(x, y) = 0\}$ est fini.

Exercice 135. (Comment reconnaître qu'un anneau n'est pas euclidien) Soit A un anneau euclidien relativement à $v : A \to \mathbb{N}$. Montrer qu'il existe $x \notin A^*$ tel que la restriction à $A^* \cup \{0\}$ de la projection canonique de A sur $A/(x)$ soit surjective :

- si A est un corps, prendre $x = 0$.
- sinon prendre x dans $A \setminus (A^* \cup \{0\})$ avec $v(x)$ minimal.

Exercice 136. Soit $A = \mathbb{R}[X, Y]/(X^2+Y^2+1)$ et soient ξ, η les images dans A de X et Y.

- Montrer que tout élément de A s'écrit de manière unique $u = a(\xi)\eta + b(\xi)$ où $a, b \in \mathbb{R}[X]$ (utiliser la division euclidienne par $X^2 + Y^2 + 1$).
- Montrer que la donnée d'un homomorphisme de $\mathbb{R}$-algèbres de A dans $\mathbb{C}$ équivaut à la donnée d'un couple $(x, y) \in \mathbb{C}^2$ avec $x^2 + y^2 + 1 = 0$.
- Déduire des deux premières questions que l'on a $A^* = \mathbb{R}^*$ (montrer qu'un élément $u \in A \setminus \mathbb{R}^*$ peut être envoyé sur 0 par un homomorphisme $A \to \mathbb{C}$ en trouvant une solution, dans $\mathbb{C}^2$, au système d'équations $a(x)y + b(x) = 0$, $x^2 + y^2 + 1 = 0$).
- Montrer que A n'est pas euclidien (montrer que les conclusions de **Exercice 135** ne peuvent être vérifiées).

Exercice 137. Montrer que $\mathbb{C}[X, Y]/(X^2 + Y^2 + \varepsilon)$ est principal pour $\varepsilon = \pm 1$ (par un changement de variables se ramener à $XY - 1$, voir **Exercice 133**)

Exercice 138. Montrer que $\mathbb{R}[X, Y]/(X^2+Y^2-1)$ n'est pas factoriel.

Exercice 139. Soit K un anneau unitaire (pas nécessairement commutatif). Pour x et y dans le centre de K et non nuls, on désigne par $K[I, J]$ (ou $K_{x,y}[I, J]$) la K-algèbre obtenue de la manière suivante :

- les éléments de $K[I, J]$ sont des combinaisons linéaires $a + bI + cJ + dIJ$ avec $a, b, c, d \in K$.
- L'addition se fait terme à terme.
- La multiplication est entièrement déterminée par (un peu d'associativité) et $I^2 = x$, $J^2 = y$, $IJ = -JI$ et, pour tout c dans K, $cI = Ic$, $cJ = Jc$.

(1) Écrire le produit de $a + bI + cJ + dIJ$ et de $a' + b'I + c'J + d'IJ$

(2) Montrer que $K[I, J]$ est bien une K-algèbre. (On parle d'algèbre de quaternions généralisée).

(3) Si (x, y) est changé en (y, x), $(x, -xy)$, $(\lambda^2 x, y)$, on obtient des algèbres isomorphes.

(4) le sous anneau $K[I] = \{a+bI, a, b \in K\}$ a un automorphisme d'ordre 2 :$r = a + bI \mapsto \bar{r} = a - bI$.

(5) Ce morphisme s'étend en un automorphisme (intérieur) de $K[I, J]$: $q \mapsto \bar{q} = J^{-1}qJ = \frac{1}{y}JqJ$. Si $q = a + bJ$ (avec $a, b \in K[I]$) alors $\bar{q} = \bar{a} + \bar{b}J$.

(6) Par $a + bJ \mapsto \begin{pmatrix} a & by \\ \bar{b} & \bar{a} \end{pmatrix}$, l'algèbre $K[I, J]$ est isomorphe à un sous-anneau de $M_2(K[I])$.

(7) Soit F un corps commutatif. Alors $F[I, J]$ est un corps si et seulement si on a : $\forall a, b, c, d \in F$, $(a^2 - b^2x - c^2y + d^2xy = 0 \Leftrightarrow a = b = c = d = 0)$.

(8) Si $F = \mathbb{R}$ alors $\mathbb{R}[I, J]$ est un corps si et seulement si $x < 0$ et $y < 0$.

(9) $\mathbb{C}[I, J]$ n'est jamais un corps.

Corps

Exercice 140. Soit α la classe de X dans $\mathbb{F}_4 = \mathbb{F}_2[X]/(X^2+X+1)$. Alors $(1,\alpha)$ est une base du $\mathbb{F}_2$-espace vectoriel $\mathbb{F}_4$. Les éléments de $\mathbb{F}_4$ sont $\{0,1,\alpha,1+\alpha\}$. Donner leurs polynômes minimaux.

Exercice 141. Identifier le sous-groupe additif sous-jacent au corps $\mathbb{F}_4$.

Exercice 142. Écrire les tables d'addition et de multiplication de $\mathbb{F}_4$ et de $\mathbb{Z}/(4)$; les comparer.

Exercice 143. Trouver une racine treizième de 3 dans le corps $\mathbb{F}_{13}$.

Exercice 144.

(1) Vérifier que le polynôme $P = X^3 + X + 1$ est irréductible dans $\mathbb{F}_2[X]$.

(2) Soit β la classe de X dans le corps $\mathbb{F}_8 = \mathbb{F}_2[X]/(P)$; alors $(1,\beta,\beta^2)$ est une base du $\mathbb{F}_2$-espace vectoriel $\mathbb{F}_8$.

(3) Les éléments de $\mathbb{F}_8$ sont alors

$$\{0,1,\beta,1+\beta,\beta^2,1+\beta^2,\beta+\beta^2,1+\beta+\beta^2\}.$$

(4) Donner le polynôme minimal de chacun de ces éléments.

Exercice 145. Déterminer le nombre de polynômes irréductibles (et unitaires) de degré 3 dans le corps $\mathbb{F}_3$.

Exercice 146.

(1) La décomposition $X^4-X = X(X-1)(X^2+X+1)$ est un produit de facteurs irréductibles dans $\mathbb{F}_2[X]$ et dans $\mathbb{Z}[X]$;

(2) La décomposition $X^8-X = X(X-1)(X^6+X^5+X^4+X^3+X^2+X+1)$ est un produit de facteurs irréductibles dans $\mathbb{Z}[X]$, mais pas dans $\mathbb{F}_2[X]$;

(3) On a, dans $\mathbb{F}_2[X]$, $X^8-X = X(X+1)(X^3+X+1)(X^3+X^2+1)$ et ces facteurs sont irréductibles ;

(4) Vérifier la décomposition $X^{16} - X = X(X-1)(X^2+X+1)(X^4+X^3+X^2+X+1)(X^8-X^7+X^5-X^4+X^3-X+1)$ dans $\mathbb{Z}[X]$ et est un produit de facteurs irréductibles ;

(5) On a, dans $\mathbb{F}_2[X]$, $X^{16}-X = X(X-1)(X^2+X+1)(X^4+X^3+X^2+X+1)(X^4+X^3+1)(X^4+X+1)$ et ces facteurs sont irréductibles.

Exercice 147. Trouver des factorisations de $X^9 - X$ et de $X^{27} - X$ dans $\mathbb{F}_3$. Montrer que les facteurs de vos factorisations sont irréductibles.

Exercice 148. Factoriser $X^{16} - X$ dans $\mathbb{F}_4$ puis dans $\mathbb{F}_8$.

Exercice 149. Déterminer tous les polynômes f tel que $f(\alpha) = 0$ pour tout α dans $\mathbb{F}_q$.

Exercice 150. Soit K un corps fini. Le produit des éléments non nuls de K est égal à -1.

Exercice 151. Tout élément de $\mathbb{F}_p$ a exactement une racine p-ième.

Exercice 152. Soit p un nombre premier. Quels sont les nombres entiers n pour lesquels il existe un corps K d'ordre n et un élément de K^* d'ordre p.

Exercice 153. Faire ces questions *sans* utiliser les résultats sur les corps finis.

(1) Soit $F = \mathbb{F}_p$, quel est le nombre de polynômes irréductibles et unitaires de degré 2 à coefficients dans F ?

(2) Soit $f(X)$ l'un de ces polynômes (le nombre trouvé à la question précédente est strictement positif !). Montrer que $K = F[X]/(f)$ est un corps à p^2 éléments et que tous ses éléments s'écrivent d'une seule manière sous la forme $a+b\alpha$ où a, b sont dans F et α est la classe de X dans K. Montrer que tout élément de la forme $a+b\alpha$ avec $b \neq 0$ est la racine d'un polynôme irréductible de degré 2 dans $F[X]$.

(3) Montrer que tout polynôme de degré 2 dans $F[X]$ a une racine dans $\mathbb{K}$.

(4) Montrer que tous les corps K obtenus par la construction des questions précédentes sont isomorphes.

Modules

Exercice 154. Soit A un anneau (commutatif et unitaire). Déterminer tous les morphismes de A-modules de A dans A.

Exercice 155. Soit W un sous-module d'un A-module V. Pour tout w dans W, montrer que $-w$ appartient à W.

Exercice 156. Soit $\varphi : V \to W$ un morphisme de A-modules et soient V' un sous-module de V et W' un sous-module de W. Alors $\varphi(V')$ est un sous-module de W et $\varphi^{-1}(W')$ est un sous-module de V.

Exercice 157. Soit V un groupe abélien. Alors V a au plus une structure de $\mathbb{Q}$-module dont la loi de composition interne est l'addition du groupe V. Un groupe abélien fini non nul n'a aucune structure de $\mathbb{Q}$-module.

Exercice 158. Soit α un entier algébrique et $A = \mathbb{Z}[\alpha]$. Alors, pour tout entier m, A/mA est fini. Quel est son ordre ?

Exercice 159. Un A-module V est dit *simple*, s'il est non nul et si ses seuls sous-modules sont $\{0\}$ et V. Tout module simple est alors de la forme A/M où M est un idéal maximal. Tout morphisme entre deux modules simples est ou bien nul, ou bien un isomorphisme.

Exercice 160. L'*annulateur* d'un A-module V est l'ensemble $I = \{a \in A \mid aV = 0\} = \{a \in A \mid \forall v \in V, av = 0\}$/ L'annulateur est alors un idéal de A. Quel est l'annulateur du $\mathbb{Z}$-module $\mathbb{Z}/(2) \times \mathbb{Z}/(3) \times \mathbb{Z}/(4)$? du $\mathbb{Z}$-module $\mathbb{Z}$?

Exercice 161. Soit V un A-module. On note $\mathrm{End}_A(V)$ l'ensemble des morphismes de A-modules de V dans V. Muni de l'addition et de la composition des applications, $\mathrm{End}_A(V)$ est alors un anneau non-commutatif. On l'appelle l'*anneau des endomorphismes* de V.

Exercice 162. Si V est un A-module simple, alors $\mathrm{End}_A(V)$ est un corps.

Exercice 163. Déterminer $\mathrm{End}_A(V)$ pour $V = A$, $V = A/I$ si I est un idéal.

Exercice 164. Soient $W \subset V \subset U$ des A-modules. Décrire des homomorphismes naturels entre les modules quotients U/W, U/V et V/W. Montrer que $(U/W)/(V/W) \simeq U/V$.

Exercice 165. Soient V et W des sous-modules d'un A-module U. Alors $V \cap W$ et $V + W$ sont des sous-nodules et $(V + W)/W$ est isomorphe à $V/(V \cap W)$.

Exercice 166. Soit A l'anneau $\mathbb{C}[X, Y]$ et soit M l'idéal de A engendré par les deux éléments X et Y. M est-il un module libre ? (justifier).

Exercice 167. Soit M une matrice de type $n \times n$ à coefficients dans un anneau A et soit $f : A^n \to A^n$ la multiplication (à gauche) par M et posons $d = \det(M)$. Est-il vrai que l'image de φ est dA^n ? (justifier)

Exercice 168. Soit I un idéal d'un anneau A. Est-il vrai que si A/I est un A-module libre alors $I = 0$? (justifier)

Exercice 169. Soit A un anneau (commutatif et unitaire) et soit V un A-module libre de rang fini. Est-il vrai que toute partie génératrice contient une base ? et que toute partie libre est contenue dans une base ? (justifier)

Exercice 170. Soit I un idéal d'un anneau $(\ldots)$ A. Alors I est un A-module libre si et seulement si I est l'idéal principal engendré par un élément α qui n'est pas un diviseur de 0.

Exercice 171. Soit M la matrice d'un homomorphisme $\varphi : \mathbb{Z}^n \to \mathbb{Z}^m$. Alors φ est injectif si et seulement si le rang de M est n. Et φ est surjectif si et seulement si le pgcd des mineurs de taille $m \times m$ de M est égal à 1.

Exercice 172. En appliquant les opérations élémentaires sur les lignes et les colonnes, réduire les matrices suivantes sous forme diagonale : $\begin{pmatrix} 3 & 1 \\ -1 & 2 \end{pmatrix}$, $\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}$, $\begin{pmatrix} 3 & 1 & -4 \\ 2 & -3 & 1 \\ -4 & 6 & -2 \end{pmatrix}$. Pour la première, dessiner le sous-module Λ de $\mathbb{Z}^2$ correspondant et les bases commensurables de $\mathbb{Z}^2$ et Λ.

Exercice 173. Soit A une matrice à coefficients dans $k[t]$ (k est un corps commutatif). Et soit A' obtenue à partir de A à l'aide d'opérations élémentaires. Décrire la relation entre $\det A$ et $\det A'$.

Exercice 174. Soit $A = \begin{pmatrix} 4 & 7 & 2 \\ 2 & 4 & 6 \end{pmatrix}$. Déterminer des matrices à coefficients entiers P^{-1} et Q telles que $P^{-1}AQ$ est diagonale à coefficients se divisant successivement.

Exercice 175. Soit A une matrice à coefficients entiers et soit $(d_1, d_2, \ldots, d_r)$ tel que $d_i > 0$, d_i divise d_{i+1} et A se ramène par opérations élémentaires à la matrice diagonale dont les coefficients sont $d_1, \ldots, d_r, 0, \cdots, 0$. Montrer que d_1 est le pgcd des coefficients de A. Montrer que $d_1 d_2$ est le pgcd des déterminants des mineurs de type 2×2 de A. Généraliser.

Exercice 176. Déterminer les solutions de $AX = 0$ où $A = \begin{pmatrix} 4 & 7 & 2 \\ 2 & 4 & 6 \end{pmatrix}$.

Exercice 177. Trouver des bases des sous-modules suivant de $\mathbb{Z}^3$: le sous-module engendré par $(1, 0, -1)$, $(2, -3, 1)$, $(0, 3, 1)$, $(3, 1, 5)$; l'ensemble des solutions du système $x + 2y + 3z = 0$ et $x + 4y + 9z = 0$.

Exercice 178. Les matrices $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ engendrent le groupe $\mathrm{SL}_2(\mathbb{Z})$.

Exercice 179. Le groupe $\mathrm{SL}_n(\mathbb{Z})$ est engendré par les matrices $\mathrm{I}_n + e_{i,j}$ ($i \neq j$) où $e_{i,j}$ est la matrice dont le seul coefficient non nul est égal à 1 et est un position (i, j).

Exercice 180. Soit $\varphi : \mathbb{Z}^k \to \mathbb{Z}^k$ l'homomorphisme (de $\mathbb{Z}$-modules) donné par la multiplication à gauche par une matrice à coefficients entiers A. Montrer que l'image de φ est d'indice fini si et seulement si la matrice A est inversible et que, dans ce cas, l'indice est égal à $|\det A|$.

Exercice 181. Soit $A = (a_1, \ldots, a_n)^t$ un vecteur colonne à coefficients entiers. En utilisant les opérations sur les lignes, montrer qu'il existe une matrice P de $\mathrm{GL}_n(\mathbb{Z})$ telle que $PA = (d, 0, \ldots, 0)^t$ où d est le plus grand diviseur commun de $a_1, \ldots, a_n$. Si $d = 1$ montrer que A est la première colonne d'une matrice $M \in \mathrm{SL}_n(\mathbb{Z})$.

Exercice 182. Déterminer les groupes abéliens dont des matrices de présentations sont $\begin{pmatrix} 2 \\ 0 \end{pmatrix}$, $\begin{pmatrix} 0 \\ 5 \end{pmatrix}$, $\begin{pmatrix} 2 & 0 & 0 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{pmatrix}$, $\begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix}$, $\begin{pmatrix} 2 & 4 \\ 1 & 4 \end{pmatrix}$, $\begin{pmatrix} 4 & 6 \\ 2 & 3 \end{pmatrix}$.

Exercice 183. Donner un anneau A et u idéal I de A qui ne soit pas de type fini.

Exercice 184. Écrire comme une somme directe de groupes cycliques le groupe abélien présenté par la matrice $\begin{pmatrix} 2 & 2 & 2 \\ 2 & 2 & 0 \\ 2 & 0 & 2 \end{pmatrix}$.

Exercice 185. Écrire le groupe engendré par x et y avec la relation $3x + 4y = 0$ comme un produit de groupes cycliques.

Exercice 186. Écrire comme produit direct de groupes cylciques les groupes engendrés par x, y et z et les relations suivantes :

(1) $3x + 2y + 8z = 0$, $2x + 4z = 0$.
(2) $x + y = 0$, $2x = 0$, $4x + 2z = 0$, $4x + 2y + 2z = 0$.
(3) $2x + y = 0$, $x - y + 3z = 0$.
(4) $2x - 4y = 0$, $2x + 2y + z = 0$.
(5) $7x + 5y + 2z = 0$, $3x + 3y = 0$, $13x + 11y + 2z = 0$.

Modules sur anneaux principaux

Exercice 187. Soit S un sous-anneau de $R = \mathbb{C}[t]$ contenant $\mathbb{C}$ mais différent de $\mathbb{C}$. Montrer que R est un S-*module* de type fini. (Indication : prenons $p \in S$ de degré > 0, pour tout $f \in R$ utiliser la division euclidienne de f par p puis la division euclidienne du quotient obtenue dans la première division par p et ainsi de suite.)

Exercice 188. Soit S l'idéal $(2, 1+\delta)$ de $\mathbb{Z}[\delta]$ où $\delta = \sqrt{5}$. Donner une matrice de présentation de S.

Exercice 189.

(1) Le nombre d'éléments de $\mathbb{Z}/(p^e)$ dont l'ordre divise p^ν est égal à p^ν si $\nu \leq e$ et à p^e si $\nu \geq e$.

(2) Soient $W_1, \ldots, W_k$ des groupes abéliens finis et $q \in \mathbb{N}^*$; notons u_j le nombre d'éléments de W_j dont l'ordre divise q. Le nombre d'éléments de $V = W_1 \times W_2 \times \cdots \times W_k$ dont l'ordre divise q est $u_1 u_2 \cdots u_k$.

(3) Si, de plus, W_j est d'ordre $d_j = p^{e_j} > 1$, posons r_1 le nombre d'indices j tels que d_j est égal à p, r_2 le nombre de j tels que d_j est égal à p^2 et ainsi de suite. Le nombre d'éléments de V dont l'ordre divise p^ν est p^{s_ν} où $s_1 = r_1 + r_2 + \cdots + r_n + \ldots$ (la somme est finie) et $s_2 = r_1 + 2r_2 + 2r_3 + \cdots$, $s_3 = r_1 + 2r_2 + 3r_3 + 3r_4 + \cdots$, etc.

(4) Relier la question précédente à un théorème du cours.

Exercice 190. Soit f l'application linéaire dont la matrice est $\begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}$. Le $\mathbb{C}[X]$-module correspondant est-il cyclique ?

Exercice 191. Déterminer la forme de Jordan de la matrice $\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$.

Exercice 192. Montrer que $\begin{pmatrix} 1 & 1 & 1 \\ -1 & -1 & -1 \\ 1 & 1 & 1 \end{pmatrix}$ est une matrice idempotente (ie. satisfait la relation $X^2 = X$). Trouver sa forme de Jordan.

Exercice 193. Soit V un espace vectoriel complexe de dimension 5 et f un endomorphisme de V dont le polynome caractéristique est $(X - \alpha)^5$. Sous l'hypothèse que le rang de $f - \alpha\mathrm{Id}$ est 2, quelles sont les formes de Jordan possibles pour f ?

Exercice 194. Trouver toutes les formes de Jordan possibles pour une matrice dont le polynome caractéristique est $(X + 2)^2(X - 5)^3$.

Exercice 195. Quelle est la forme de Jordan d'une matrice dont le polynome caractéristique est $(X - 2)^2(X - 5)^3$ et telle que l'espace propre associé à la valeur propre 2 est de dimension 1, tandis que l'espace propre associé à la valeur propre 5 est de dimension 2 ?

Exercice 196.

(1) Montrer que, pour un bloc de Jordan, l'ensemble des vecteurs propres est un espace vectoriel de dimension 1.

(2) Réciproquement, sous l'hypothèse que tous les vecteurs propres d'une matrice A, à coefficients complexes, sont les multiples d'un seul vecteur, montrer que la forme de Jordan de A a au plus un bloc.

Exercice 197. Déterminer tous les sous-espaces invariant d'un bloc de Jordan.

Exercice 198. Résoudre l'équation différentielle, $\frac{dX}{dt} = AX$ lorsque A est le bloc de Jordan (a) $\begin{pmatrix} 2 & 0 \\ 1 & 2 \end{pmatrix}$, (b) $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$, (c) $\begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$.

Exercice 199. Résoudre l'équation différentielle, $\frac{dX}{dt} = AX$ lorsque A est (a) la matrice $\begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix}$, (b) la matrice de **Exercice 191**, (c) la matrice de **Exercice 192**.

Exercice 200. Démontrer ou réfuter : des matrices complexes de type $n \times n$ sont semblables si et seulement si elles ont la même forme de Jordan.

Exercice 201. Soit $R = F[X]$ l'algèbre des polynomes en une variable sur un corps (commutatif) F et soit V le R-module engendré par un élément v vérifiant la relation $(X^3 + 3X + 2)v = 0$. Dans une base de V que vous choisirez, quelle est la matrice de l'application linéaire de multiplication par X ?

Exercice 202. Soit V un $F[X]$-module et $(v_1, \ldots, v_n)$ une base du F-espace vectoriel V. Soit B la matrice dans cette base de l'application F-linéaire f donnée par la multiplication par X. Montrer que $A = X\mathrm{Id} - B$ est une matrice de présentation pour le $F[X]$-module V.

Exercice 203. Soit $p(X)$ un polynome à coefficients dans un corps F. Montrer qu'il existe un entier n et une matrice de type $n \times n$ dont le polynome caractéristique est $p(X)$.

Exercice 204. Démontrer ou réfuter : une matrice complexe A telle que $A^2 = A$ est diagonalisable.

Exercice 205. Soit A une matrice à coefficents complexes de type $n \times n$ et telle que $A^k = \mathrm{Id}$. Montrer que la forme de Jordan de A est diagonale.

Exercice 206. Démontrer le théorème de Cayley–Hamilton.

Exercice 207. Soit f un endomorphisme d'un $\mathbb{C}$-espace vectoriel de dimension finie.

(1) Montrer que le polynome minimal $m(X)$ de f divise le polynome caractéristique $p(X)$ de f.

(2) Montrer que toute racine de $p(X)$ est aussi une racine de $m(X)$.

(3) Montrer que f est diagonalisable si et seulement si $m(X)$ n'a pas de racine multiple.

Exercice 208. Donner toutes les formes de Jordan possibles des matrices de type 8×8 dont le polynome minimal est $x^2(x-1)^3$.

Exercice 209. Démontrer ou réfuter : Une matrice complexe A est semblable à sa transposée.

Exercice 210. Montrer que les rangs des opérateurs $(A-\alpha\mathrm{Id})^\nu$ (α variant dans $\mathbb{C}$, ν variant dans $\mathbb{N}$) permettent de distinguer entre elles les formes de Jordan, et en conclure que la forme de Jordan ne dépend que de l'endomorphisme A et pas de la base choisie.

Exercice 211. Montrer que les concepts suivants sont équivalents :

- Les R-modules pour $R=\mathbb{Z}[i]$;
- Les groupes abéliens V munis d'un homomorphisme $\phi : V \to V$ tel que $\phi\circ\phi = -\mathrm{Id}$.

Exercice 212. Quand est-ce que $\mathbb{F}_p$ a une structure de $\mathbb{Z}[i]$-module ? Et pour $\mathbb{F}_p \times \mathbb{F}_p$?

Exercice 213. Classifier les modules de type fini sur l'anneau $\mathbb{C}[\epsilon]$, où $\epsilon^2 = 0$.

Exercice 214. Le groupe $\mathbb{Q}/\mathbb{Z}$ n'est pas somme directe (infinie) de groupes cycliques.

Exercice 215. Le groupe abélien $(\mathbb{Q},+)$ n'est pas la somme directe de deux sous-groupes propres.

Exercice 216. Le groupe multiplicatif $\mathbb{Q}^*$ est le produit direct d'un groupe cyclique d'ordre 2 est d'un groupe abélien libre de base dénombrable.

Exercice 217. Soit $\varphi\colon A \to \mathbb{C}^*$ un homomorphisme non trivial défini sur un groupe abélien fini A. Alors $\sum_{a\in A}\varphi(a) = 0$.

Représentations des groupes

Exercice 218. (Matrices de permutation) Soient S_n le groupe des permutations de $\{1,\dots,n\}$, K un corps, et ρ l'application de S_n dans $\mathrm{GL}(n,K)$ qui à une permutation σ associe la matrice $(\rho(\sigma)_{i,j})_{i,j\in\{1,\dots,n\}}$ telle que, pour tout (i,j), $\rho(\sigma)_{i,j}=0$ si $i\neq\sigma(j)$ et $\rho(\sigma)_{i,j}=1$ si $i=\sigma(j)$.

- ρ est une représentation ;
- Si $(e_i)_{i=1,\dots,n}$ désigne la base canonique de K^n, $\rho(\sigma)$ est caractérisé par la propriété $\rho(\sigma)\cdot e_j = e_{\sigma(j)}$ pour tout $j=1,\dots,n$;
- Pour tout σ, $\chi_\rho(\sigma)(=\mathrm{tr}(\rho(\sigma)))$ est égal au nombre de points fixes par σ dans $\{1,\dots,n\}$.

Exercice 219. (Représentation régulière gauche) Soient G un groupe et $V=K^{(G)}$ l'espace vectoriel de base $(\delta_g)_{g\in G}$. Pour tout g dans G, la règle $\delta_h\mapsto\delta_{gh}$ définit un élément $\rho(g)$ de $\mathrm{End}(V)$ (autrement dit, pour tout $v=\sum_{h\in G}\lambda_h\delta_h$, $\rho(g)v=\sum_{h\in G}\lambda_h\delta_{gh}$). Pour tous g,h dans G, $\rho(gh)=\rho(g)\rho(h)$. En déduire que, pour tout g, $\rho(g)$ appartient à $\mathrm{GL}(V)$ et que ρ est une représentation.

Exercice 220. Définir la représentation régulière droite. Observer que cela donne aussi une représentation de $G\times G$.

Exercice 221. Soient G un groupe, X un ensemble, $G\times X\to X \mid (g,x)\mapsto g\cdot x$ une opération de G sur X, $V(=K^{(X)})$ l'espace vectoriel de base $(\delta_x)_{x\in X}$ et $\rho: G\to\mathrm{End}(V)$ l'application qui à g associe l'endomorphisme défini par $\delta_x\mapsto\delta_{g\cdot x}$ pour tout x dans X. Alors ρ est une représentation.
Retrouver les représentations des trois exercices précédents en appliquant cette construction à des couples (G,X) adéquats.

Exercice 222. Décrire toutes les représentations de $G=\{\pm1\}$ sur un corps K de caractéristique différente de 2.
Décrire toutes les représentations de G sur un corps K de caractéristique 2 (pour démarrer, remarquer que $x^2-1=(x-1)^2$).

Exercice 223. (Décomposition de Dunford) Soient g un élément de $\mathrm{GL}(n,\mathbf{C})$ et d un élément diagonalisable de $\mathrm{GL}(n,\mathbf{C})$, u un élément unipotent de $\mathrm{GL}(n,\mathbf{C})$ (i.e. $u-\mathrm{Id}$ est nilpotent) tels que $g=du=ud$. Si $u\neq\mathrm{Id}$, alors g est d'ordre infini.

Exercice 224. Quel est la forme "normale" (ou de Jordan, ou etc.) d'un élément de $\mathrm{GL}(n,\mathbf{R})$ d'ordre fini ?

Exercice 225. Soit V un G-module. Il existe une unique structure de G-module sur V^* telle que

$$\langle g\cdot f, g\cdot v\rangle = \langle f,v\rangle \quad \forall f\in V^*, v\in V, g\in G.$$

Si $\rho: G\to\mathrm{GL(V)}$ est le morphisme définissant la représentation, alors le morphisme correspondant à V^* est $G\to\mathrm{GL}(V^*)\mid g\mapsto {}^t\rho(g)^{-1}$. Autrement dit, pour tout $g\in G$, tout $f\in V^*$, $g\cdot f$ est la forme linéaire $f\circ\rho(g^{-1})$.

Exercice 226. La structure de G-module sur $\mathrm{Hom}(V,W)$ définie (ou non) en cours est l'unique structure de G-module $(g,\phi)\mapsto g\cdot\phi$ telle que

$$(g\cdot\phi)(g\cdot v)=g\cdot(\phi(v)) \quad \forall g\in G,\phi\in\mathrm{Hom}(V,W),v\in V.$$

Exercice 227. Si V et W sont deux G-représentations de $G=\{\pm1\}$ décrites par les paires d'entiers (n,m) et (n',m') respectivement (voir le cours), quelles sont les paires d'entiers qui décrivent la représentation V^* et la représentation $\mathrm{Hom}(V,W)$. Exprimer les caractères (que l'on peut noter χ_{V^*} et $\chi_{\mathrm{Hom}(V,W)}$) de ces dernières en fonction des caractères de V et de W.

Exercice 228. Si V est un G-module et W est un H-module, alors $\mathrm{Hom}(V,W)$ est un $(G\times H)$-module.

Exercice 229. D'après l'exercice précédent, $Z=\mathrm{Hom}(V^*,W)$ est un $(\mathrm{GL}(V)\times\mathrm{GL}(W))$-module, i.e. on dispose d'un morphisme ψ de $\mathrm{GL}(V)\times\mathrm{GL}(W)$ dans $\mathrm{GL}(Z)$. (Ça parait un peu artificiel de mettre V^* mais ça simplifie en fait les formules plus bas.)

- Si (V,ρ) et (W,ρ') sont deux G-modules, alors la représentation $\mathrm{Hom}(V^*,W)$ est donnée par la composition de ψ avec le morphisme $G\to\mathrm{GL}(V)\times\mathrm{GL}(W)\mid g\mapsto(\rho(g),\rho'(g))$.
- En utilisant une base $(e_i)_{i=1,\dots,n}$ de V, une base $(f_j)_{j=1,\dots,m}$ de W et une base $(E_{i,j})_{(i,j)\in\{1,\dots,n\}\times\{1,\dots,m\}}$ de Z (à construire avec les deux bases précédentes), on obtient un morphisme $\mathrm{GL}(n,K)\times\mathrm{GL}(m,K)\to\mathrm{GL}(nm,K)$ (souvent noté $(A,B)\mapsto A\otimes B$ et appelé "produit de Kronecker"). Décrire les coefficients de la matrice $A\otimes B$ en fonction de ceux de A et de B.

Exercice 230. Soit G un groupe et soient V, W des représentations de G (sur un corps K). Alors les deux ensembles $\mathrm{Hom}_G(V,W)$ et $\mathrm{Hom}(V,W)^G$ sont égaux.

Exercice 231. Soient G un groupe fini, K un corps dont la caractéristique ne divise pas l'ordre $|G|$ de G et V une représentation de G sur le corps K. Alors $p: V\to V\mid v\mapsto\frac{1}{|G|}\sum_{g\in G}g\cdot v$ est un G-morphisme. De plus p est un projecteur d'image V^G, les invariants de G dans V.

Exercice 232. Soit (V,ρ) une représentation sur $\mathbf{C}$ de dimension finie (notée n) d'un groupe fini G, et soit χ son caractère. Alors, pour tout $g\in G$:

- $\chi(g)$ est la somme de n nombres complexes de module 1.
- $|\chi(g)|=\chi(e_G)$ si et seulement si $\rho(g)$ est un multiple de l'identité.
- $\chi(g)=\chi(e_G)$ si et seulement si $\rho(g)$ est l'identité.

Exercice 233. Décrire toutes les représentations irréductibles d'un groupe fini cyclique puis toutes les représentations irréductibles d'un groupe fini abélien.

Exercice 234. On note D_{2n} le groupe diédral d'ordre $2n$, c'est-à-dire le groupe des symétries du polygone régulier à n sommets. Trouver le plus de représentations irréductibles de D_{2n}. Pouvez-vous affirmer les avoir trouver toutes ?

Exercice 235. Soit X un ensemble fini muni d'une action (à gauche) d'un groupe fini G. La représentation de permutations associée à (G, X) est notée V.

(1) La dimension des invariants V^G est égale au nombre d'orbites de G dans X.

(2) Lorsque cette dimension est égale à 1 (i.e. lorsque l'action de G sur X est transitive), décrire le G-supplémentaire U de V^G.

(3) Si l'action de G sur X est doublement transitive (i.e. pour tous $x_1 \neq y_1$ et $x_2 \neq y_2$ dans X, il existe $g \in G$ tel que $g \cdot x_1 = x_2$ et $g \cdot y_1 = y_2$) alors U est un G-module irréductible.

Exercice 236. Trouver un sous-groupe abélien d'indice 3 du groupe alterné A_4. En déduire que toutes ses représentations irréductibles sont de degré ≤ 3.

Exercice 237. Calculer le groupe dérivé $[D_{2n}, D_{2n}]$ du groupe diédral D_{2n}. En déduire le nombre de caractères de degré 1. Expliquer pourquoi les autres représentations irréductibles sont toutes de degré 2. Déterminer leur nombre.

Exercice 238. Soit $\rho : G \to \mathrm{GL}(V)$ une représentation d'un groupe fini. Si l'espace vectoriel engendré par $\rho(G)$ est égal à $\mathrm{End}(V)$, alors V est de degré fini et est irréductible.

Exercice 239. Donner la table des caractères d'un groupe cyclique (fini). Vérifier les relations d'orthogonalité.

Exercice 240. (Retour sur les actions par permutations) Soit X un G-ensemble fini pour un groupe G fini (c'est-à-dire G agit à gauche sur X). Soit $V = \mathcal{F}_{\mathbb{C}}(X)$ la représentation associée. "Calculer" le caractère de V.
La représentation V^* est G-isomorphe à V. La représentation $\mathrm{End}(V)$ est la représentation associée à l'action ("diagonale") de G sur $X \times X$. En déduire que la dimension de $\mathrm{End}_G(V)$ est au moins égale à 2 et est égale à 2 si et seulement si l'action de G sur X est doublement transitive.
Soit $W \subset V$ le sous espace constitué des fonctions constantes $X \to \mathbb{C}$ et $U \subset V$ celui des fonctions de somme nulle, de sorte que W et U sont des sous-modules en somme directe. On a alors l'inégalité $\langle \chi_U, \chi_U \rangle + 1 \leq \dim \mathrm{End}_G(V)$. En déduire que U est irréductible si et seulement si l'action de G sur X est doublement transitive.

Exercice 241. Déterminer les caractères des représentations régulières gauche et droite. Que pouvez-vous en déduire ?

Exercice 242. Les classes de conjugaison de $G \times G$ sont les sous-ensembles de la forme $\mathcal{O} \times \mathcal{O}'$ où $\mathcal{O}$, $\mathcal{O}'$ sont les classes de conjugaison de G.
Déterminer χ_b le caractère de la représentation birégulière. Il vaut mieux chercher seul.e mais je donne tout de même la réponse pour pouvoir continuer l'exercice : si $\mathcal{O} \neq \mathcal{O}'$ alors $\chi_b(\mathcal{O} \times \mathcal{O}') = 0$ et $\chi_b(\mathcal{O} \times \mathcal{O}) = \sharp G / \sharp \mathcal{O}$.
Dans la suite de cet exercice, $\langle \cdot, \cdot \rangle_G$ désignera le produit scalaire hermitien sur les fonctions $G \to \mathbb{C}$ (mais, comme souvent, seules les fonctions centrales interviendront) et $\langle \cdot, \cdot \rangle_{G \times G}$ celui sur les fonctions $G \times G \to \mathbb{C}$. Soient V_1 et V_2 deux représentations de G de sorte que $\mathrm{Hom}(V_1, V_2)$ est une représentation de $G \times G$. On a la relation

$$\langle \chi_b, \chi_{\mathrm{Hom}(V_1,V_2)} \rangle_{G \times G} = \langle \chi_{V_1}, \chi_{V_2} \rangle_G.$$

En utilisant les relations d'orthogonalité, trouver que, pour tous π et π' dans $\widehat{G}$, $\langle \chi_b, \chi_{\mathrm{Hom}(\pi,\pi')} \rangle_{G \times G}$ vaut 0 si $\pi' \neq \pi$ et 1 si $\pi' = \pi$. Retrouver alors la décomposition de la représentation birégulière en irréductibles.
Réciproquement, dériver les relations d'orthogonalité de la décomposition de la représentation birégulière.

Exercice 243. Un groupe est abélien si et seulement si toutes ses représentations irréductibles sont de degré 1.

Exercice 244. Le caractère χ_V d'une représentation d'un groupe fini G est multiplicatif (c'est-à-dire, $\forall g, h \in G$ $\chi_V(gh) = \chi_V(g)\chi_V(h)$) si et seulement si V est de degré 1.

Exercice 245. Soient V un espace vectoriel de dimension 2 et (v_1, v_2) une base de V. L'application linéaire définie sur la base par $v_1 \mapsto v_2$, $v_2 \mapsto -v_1 - v_2$ induit une représentation du groupe cyclique d'ordre 3. Décomposer cette représentation en irréductibles. Déterminer son caractère.

Exercice 246. Déterminer les classes de conjugaison dans A_4 et leurs cardinaux (le sous-groupe (distingué) de l'**Exercice 236** peut-être utile). Trouver 3 caractères de A_4 de degré 1 (le même sous-groupe peut-être utile). Compléter ensuite la table des caractères de A_4. Décrire "explicitement" la dernière représentation irréductible.

Exercice 247. Soit D_8 le groupe diédral d'ordre 8. Décrire le sous-groupe $[D_8, D_8]$ et les classes de conjugaison de D_8. Trouver 4 caractères de degré 1 de D_8. Calculer le caractère de la dernière représentation irréductible pour compléter la table des caractères. Pouvez-vous construire cette représentation ?

Exercice 248. Soit Q_8 l'ensemble à 8 éléments $\{\pm 1, \pm i, \pm j, \pm k\}$ muni de la loi de composition interne (associative) déterminée par $i^2 = j^2 = k^2 = -1$, $ij = k$ et les multiplications "évidentes" par 1 et -1. C'est un groupe (en fait c'est mieux de montrer que c'est un sous-groupe de $\mathrm{GL}_2(\mathbb{C})$). Déterminer $[Q_8, Q_8]$, les classes de conjugaison, 4 caractères de degré 1 puis compléter la table des caractères. Constater que c'est (éventuellement à permutation des colonnes près) la même table que celle de D_8. Pouvez-vous construire la dernière représentation irréductible ?