Université de Strasbourg
M1 Algèbre S1 2024-2025
Lie Fu, `lie.fu@math.unistra.fr`

Algèbre I - Exercices Complémentaires

1 Groupes

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

Exercice 2. Dans un groupe, montrer que $ab = b \Rightarrow a = 1$ et $ab = 1 \Rightarrow b = a^{-1}$.

Exercice 3. Écrire toutes les manières possibles de former le produit de 4 éléments a, b, c, d dans cet ordre (c'est-à-dire toutes les façons de placer les parenthèses).

Exercice 4. Pour $n \geq 2$, montrer que $GL_n(\mathbb{Q})$ n'est pas commutatif. Et avec $\mathbb{Q}$ remplacé par un anneau A quelconque ?

Exercice 5. Soit G un groupe. Soit $(a, b) \mapsto a \circ b$ la nouvelle multiplication définie par $a \circ b = ba$ sur G. Montrer que c'est une structure de groupe. L'ensemble G muni de cette multiplication est souvent appelé le « groupe opposé » à G et on le note parfois G^{op}.

Montrer que G et G^{op} sont isomorphes.

Exercice 6. Une partie H d'un groupe est dite *stable* si $gh \in H$ pour tous g et h dans H. Montrer qu'une partie stable *finie* est un sous-groupe.

Exercice 7. Quels sont les sous-groupes de $\mathbb{Z}$? Justifiez. (Ici on vous demande de reconstituer un résultat que vous avez vu les années précédentes, de préférence sans aller relire votre cours.)

Exercice 8. Montrer que, si tous les éléments d'un groupe G sont d'ordre ≤ 2, alors G est commutatif. Si on suppose de plus que G est fini, pouvez-vous décrire ce groupe le plus précisément possible ? (Cette deuxième question est plus facile avec les concepts du chapitre suivant, nous y reviendrons.)

Exercice 9. Montrer qu'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. (Une seule de ces propriétés ne suffit pas pour avoir la conclusion.)

2 Anneaux

Exercice 10. Dans la définition d'un anneau, si l'on enlève la condition $0 \neq 1$, que se passe-t-il ?

Exercice 11. Montrer que, si A est un anneau, il existe un unique homomorphisme $\mathbb{Z} \longrightarrow A$.

Exercice 12. Lesquels sont des anneaux ?

- R_0 l'ensemble des polynomes $f \in \mathbb{R}[x]$ tel que $f(x) = f(-x)$ (opérations usuelles)
- R_1 l'ensemble des polynomes $f \in \mathbb{R}[x]$ tel que $f(x) = -f(-x)$ (opérations usuelles)
- 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 $\mathbb{R}^3$ 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 13. L'ensemble R des nombres rationnels de la forme a/b où b n'est *pas* un multiple de 6 est-il un sous-anneau de $\mathbb{Q}$?

Exercice 14. Soit M un groupe abélien, et soit $\mathrm{End}(M)$ l'ensemble des endomorphismes de M (c'est-à-dire les homomorphismes $M \longrightarrow M$). Sur $\mathrm{End}(M)$ on définit la loi $+$ par la formule, pour $f, g \in \mathrm{End}(M)$:

$$(f+g)(x) = f(x) + g(x)$$

pour tous les $x \in M$. Par ailleurs, on définit la multiplication $\circ$ par $(f \circ g)(x) = f(g(x))$. Montrer que $\mathrm{End}(M)$ est un anneau, dont on précisera les éléments neutres.

Exercice 15. Soit X un ensemble. Soit R l'ensemble des parties de X, on définit une addition et une multiplication comme suit :

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

On va montrer que R est un anneau. Pour commencer, on va noter S l'ensemble des homomorphismes de groupes abéliens $R \longrightarrow \mathbb{Z}/2\mathbb{Z}$; alors S est un anneau avec les opérations $(f+g)(r) = f(r) + g(r)$ et $(fg)(r) = f(r)g(r)$ pour $f, g \in S$ et $r \in R$ (on ne demande pas de vérifier ceci).

Pour A dans R on définit $\chi_A \in S$ 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.

3 Corps

Exercice 16. Soit p un entier. Montrer que $\mathbb{Z}/p\mathbb{Z}$ est un corps si et seulement si p est premier. (Ici encore, c'est censé être un rappel : vous avez déjà vu ça.)

Exercice 17. On note
$$\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}.$$
Montrer que $\mathbb{Q}[\sqrt{2}]$ est un corps (un sous-corps de $\mathbb{R}$, en fait).

Exercice 18. On note $\mathbb{H}$ l'ensemble des matrices réelles de la forme
$$\begin{pmatrix} x & -y & -z & -t \\ y & x & -t & z \\ z & t & x & -y \\ t & -z & y & x \end{pmatrix},$$
avec $x, y, z, t \in \mathbb{R}$. Les éléments de $\mathbb{H}$ sont appelés les *quaternions*. (La lettre $\mathbb{H}$, au fait, est une référence à Hamilton.) On note :

— i la matrice obtenue pour $x = 0, y = 1, z = 0, t = 0$,

— j la matrice obtenue pour $x = 0, y = 0, z = 1, t = 0$,

— k la matrice obtenue pour $x = 0, y = 0, z = 0, t = 1$.

Par ailleurs, on vous fait remarquer que pour $x = 1, y = 0, z = 0, t = 0$, on obtient la matrice identité, que l'on va noter simplement 1 dans la suite.

1. Montrer que $1, i, j, k$ est une base de $\mathbb{H}$, qui est un sous-espace vectoriel de $M_4(\mathbb{R})$.
2. Montrer que $i^2 = j^2 = k^2 = ijk = -1$.
3. En déduire que $\mathbb{H}$ est un sous-anneau de $M_4(\mathbb{R})$.
4. Pour $q = x1 + yi + zj + tk \in \mathbb{H}$ (avec $x, y, z, t \in \mathbb{R}$), on définit
$$\bar{q} = x1 - yi - zj - tk \in \mathbb{H}\,.$$
On appelle $\bar{q}$ le conjugué de q. Trouver une formule simple pour $q\bar{q}$.
5. Déduire de la question précédente que $\mathbb{H}$ est un corps. Est-il commutatif ?

Vous pouvez aussi vous amuser à vérifier que $q_1\bar{q}_2 = \bar{q}_2\,\bar{q}_1$. Il est possible de limiter les calculs.

4 Généralités sur les modules

Exercice 19. 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. Montrer que $\varphi(V')$ est un sous-module de W et que $\varphi^{-1}(W')$ est un sous-module de V.

Exercice 20. Dans chacun des exemples ci-dessous, on considère un corps $\mathbb{K}$, on prend $V = \mathbb{K}^2$, et on met une structure de $\mathbb{K}[X]$-module sur V en utilisant l'endomorphisme $f\colon V \longrightarrow V$ dont la matrice F est précisée à chaque fois. On vous demande de faire la liste de tous les sous-$\mathbb{K}[X]$-modules de V puis de répondre aux questions suivantes : V est-il simple ? V est-il indécomposable ?

— $\mathbb{K} = \mathbb{R}$ et
$$F = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$
— $\mathbb{K} = \mathbb{C}$, même matrice F que dans la question précédente.
— $\mathbb{K} = \mathbb{Q}$ et
$$F = \begin{pmatrix} 2 & -1 \\ 0 & 3 \end{pmatrix}.$$
— Reprendre la question précédente en remplaçant le « 3 » par un « 2 ».

Exercice 21. Soit $A = \mathbb{C}[X]$ et V un A-module qui est de dimension finie sur $\mathbb{C}$. Montrer que V est simple si et seulement s'il est de dimension 1 sur $\mathbb{C}$. Que se passe-t-il si on remplace $\mathbb{C}$ par un autre corps ?

Exercice 22. Soit A un anneau. Déterminer tous les morphismes de A-modules de A^1 dans A^1. Puis, décrire l'anneau $\mathrm{End}_A(A^1)$ (*attention, il y a un petit piège sur cette deuxième partie*).

Exercice 23. Soit V un A-module simple, et soit $f\colon V \longrightarrow V$ un endomorphisme. Montrer que f est soit nul, soit un isomorphisme. Que dire de l'anneau $\mathrm{End}_A(V)$?

On appelle tout ceci le « lemme de Schur ».

Exercice 24. 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 25. Soit A un anneau commutatif 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 26. Un anneau R est dit *local* lorsque, pour tout $x \in R$, on a l'alternative suivante :

— ou bien x est inversible, c'est-à-dire qu'il existe $x^{-1} \in R$ tel que $xx^{-1} = x^{-1}x = 1$,

— ou bien x est nilpotent, c'est-à-dire qu'il existe un entier $n \geq 1$ tel que $x^n = 0$.

Montrer que, si M est un A-module tel que l'anneau $R = \mathrm{End}_A(M)$ est local, alors M est indécomposable (pensez à la contraposée).

Pour la réciproque, voir l'exercice suivant.

Exercice 27. *Extrait de l'examen de décembre 2021. Attention : cet exercice utilise des notions d'algèbre linéaire que nous n'avons pas encore revues (à savoir, le « théorème des noyaux »).*

Soit A une $\mathbb{C}$-algèbre et V un A-module. On suppose que V est de dimension finie comme espace vectoriel sur $\mathbb{C}$. Enfin, on suppose que V est indécomposable comme A-module.

Soit $f\colon V \longrightarrow V$ une application A-linéaire. En considérant les sous-espaces de V de la forme $\ker(f - \lambda I)^m$, avec $\lambda \in \mathbb{C}$, $m \in \mathbb{N}$ et en écrivant I pour l'identité de V, montrer que f ne possède qu'une seule valeur propre.

En déduire que f est soit nilpotente, soit inversible.

Autrement dit, l'anneau $\mathrm{End}_A(V)$ *est « local » au sens de l'exercice précédent.*

5 Idéaux

Exercice 28. Dans $\mathbb{Z}$, calculer la somme, le produit et l'intersection des idéaux $n\mathbb{Z}$ et $m\mathbb{Z}$.

Exercice 29. L'*annulateur* d'un A-module V est l'ensemble $I = \{a \in A \mid aV = 0\} = \{a \in A \mid \forall v \in V, av = 0\}$. Montrer que l'annulateur est 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 30.

1. Soit A un anneau commutatif, et soit I un idéal. On suppose que I est un module libre de rang n. Montrer que $n = 1$.
2. Soit A l'anneau $\mathbb{C}[X, Y] = \mathbb{C}[X][Y]$ et soit M l'idéal de A engendré par les deux éléments X et Y. M est-il un module libre ?

Exercice 31. Soient I et J des idéaux à gauche d'un anneau A avec $I + J = A$. Alors $I \cap J \subset IJ + JI$.

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

6 Quotients

Exercice 32. Soit A un anneau commutatif et I, J deux idéaux tels que $I + J = A$ (*on dit que* I *et* J *sont premiers entre eux*).

Montrer qu'il existe un isomorphisme d'anneaux

$$A/IJ \cong A/I \times A/J\,.$$

C'est le « lemme chinois ».

Exercice 33. Soit U un sous-module du A-module V. Montrer qu'il y a une bijection entre les sous-modules de V/U et les sous-modules W de V tels que $U \subset W \subset V$.

En déduire un critère pour que V/U soit un module simple.

Exercice 34. Soit A un anneau commutatif. Montrer que A est un corps si et seulement si les seuls idéaux de A sont $\{0\}$ et A.

Puis, si I est un idéal de A, utiliser ce qui précède pour donner un critère pour que A/I soit un corps.

Exercice 35. Soit V un A-module et I l'annulateur de V, et enfin soit J un idéal tel que $J \subset I$. Montrer que V a une structure de A/J-module.

En déduire que, si G est un groupe abélien fini tel que pour tout $g \in G$, on a $pg = 0$, où p est un nombre premier, alors $G \cong (\mathbb{Z}/p\mathbb{Z})^k$ pour un entier k. *(On en a parlé pour $p = 2$ dans un exercice précédent, et maintenant c'est beaucoup plus facile.)*

Exercice 36. Soit $\mathbb{K}$ est un corps commutatif, et soit

$$D = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in \mathbb{K}[X]$$

un polynôme. Dans cet exercice on va décrire un peu $V = \mathbb{K}[X]/(D)$ comme $\mathbb{K}[X]$-module. Comme d'habitude on va écrire x pour l'image de X dans le quotient $\mathbb{K}[X]/(D)$. L'endomorphisme $f\colon V \longrightarrow V$ qui donne la structure de $\mathbb{K}[X]$-module est la multiplication par x.

1. Écrire la matrice de f dans la base $1, x, x^2, \ldots, x^{n-1}$.
   On dit que c'est la matrice compagne du polynôme D.
2. Montrer que le polynôme charactéristique de f est D.
   Attention, ici le polynôme charactéristique est $\det(XI - f)$ *; on prend parfois la définition* $\det(f - XI)$*, ce qui ajoute simplement un signe, mais ici c'est important.*
   Indication : par récurrence sur n.
3. On rappelle que le *polynôme minimal* d'un endomorphisme f est le polynôme unitaire μ de degré minimal tel que $\mu(f) = 0$; en d'autres termes, l'idéal
   $$I = \{P \in \mathbb{K}[X] \mid P(f) = 0\}$$
   n'est autre que $I = (\mu)$. (Nous ferons des rappels si nécessaire.)
   Montrer que le polynôme minimal de f, dans la situation ci-dessus, est D.
   Puis, en déduire une autre réponse à la question précédente, sans calculs.

Exercice 37. *Extrait examen décembre 2021.* On se donne trois réels a, b, c avec $a \neq 0$. Montrer que :

— si $b^2 - 4ac < 0$, il existe un isomorphisme de $\mathbb{R}$-algèbres
$$\mathbb{R}[X]/(aX^2 + bX + c) \cong \mathbb{C}\,;$$

— si $b^2 - 4ac > 0$, il existe un isomorphisme de $\mathbb{R}$-algèbres
$$\mathbb{R}[X]/(aX^2 + bX + c) \cong \mathbb{R} \times \mathbb{R}\,;$$

— si $b^2 - 4ac = 0$, il existe un isomorphisme de $\mathbb{R}$-algèbres
$$\mathbb{R}[X]/(aX^2 + bX + c) \cong \mathbb{R}[X]/(X^2)\,.$$

Exercice 38.

1. Soit $\mathbb{K}$ un corps commutatif et $A = \mathbb{K}[X, Y] = \mathbb{K}[Y][X]$ (c'est une algèbre sur $\mathbb{K}$, commutative, ayant pour base comme $\mathbb{K}$-espace vectoriel les monômes X^nY^m avec $n, m \geq 0$).
   On pose $R = A/(XY - 1)$. Montrer qu'il existe un élément $x \in R$ tel que tout élément de R s'écrit
   $$\sum_m^n a_i x^i$$
   avec $a_i \in \mathbb{K}$, $m \leq n$ et (attention !) $n, m \in \mathbb{Z}$; montrer de plus que cet écriture est unique.
   On dit que R est l'anneau des polynômes de Laurent en x, et on note cet anneau en général $\mathbb{K}[x, x^{-1}]$.
2. On considère l'anneau $R = \mathbb{R}[X, Y]/(X^2 + Y^2 - 1)$. Trouver une base de R comme $\mathbb{R}$-espace vectoriel.
3. On considère $S = \mathbb{C}[X, Y]/(X^2 + Y^2 - 1)$. Montrer qu'il existe un isomorphisme de $\mathbb{C}$-algèbres $S \cong \mathbb{C}[t, t^{-1}]$.

7 Anneaux principaux et factoriels

Exercice 39. Construire, par un passage au quotient, un corps ayant (exactement) 4 éléments. Décrire le plus explicitement possible les opérations dans ce corps.

Exercice 40. Soit A un anneau principal. Soient $a, b \in A$. Montrer que les conditions suivantes sur un élément $d \in A$ sont équivalentes :

1. d est un pgcd de a et b, c'est-à-dire $(a, b) = (d)$.
2. d divise a ; d divise b ; si $x \in A$ divise a et b, alors x divise d.

Exercice 41. Soit A un anneau principal. Montrer le lemme de Gauss : si un élément premier $p \in A$ divise ab (avec $a, b \in A$), alors p divise a ou p divise b.

Indication : si p ne divise pas a, alors le pgcd de p et a est 1, et on a une relation de Bézout.

Exercice 42. Soit A un anneau euclidien, avec

$$\nu \colon A \smallsetminus \{0\} \longrightarrow \mathbb{N}$$

la fonction associée. Soit $x \in A$ tel que $x = ab$, où a et b ne sont pas inversibles. Montrer que $\nu(a) < \nu(x)$ et $\nu(b) < \nu(x)$.

Indication : écrire la division euclidienne de a par ab...

Exercice 43. Soit A un anneau euclidien.

1. Montrer que tout $x \in A$ non-inversible peut s'écrire

   $$x = p_1 p_2 \cdots p_k$$

   où chaque p_i est premier.
   Indication : procéder par récurrence sur $\nu(x)$ en utilisant l'exercice précédent. Il y a plusieurs façons de rédiger.
2. Utiliser le lemme de Gauss pour montrer que cette écriture est unique, dans le sens suivant : si

   $$p_1 \cdots p_k = q_1 \cdots q_\ell$$

   où les p_i et les q_i sont premiers, alors $k = \ell$, et après renumérotation si nécessaire, on a $(p_i) = (q_i)$.
   (On rappelle que la condition $(a) = (b)$ équivaut à dire qu'il existe u inversible tel que $b = ua$.)
3. Montrer que tout $x \in A$ peut s'écrire

   $$x = u p_1^{\alpha_1} \cdots p_k^{\alpha_k}$$

   où $u \in A^\times$, chaque p_i est premier, chaque α_i est un entier > 0, et pour $i \neq j$ on a $(p_i) \neq (p_j)$. Donner un énoncé d'unicité.
   Un anneau intègre dans lequel on peut montrer les résultats des questions (1) et (2) est appelé factoriel. *Nous venons donc de montrer qu'un anneau euclidien est factoriel.*

Exercice 44 (Entiers de Gauss)**.** On va étudier l'anneau

$$\mathbb{Z}[i] := \{a + bi \mid a, b \in \mathbb{Z}\}\,.$$

1. Montrer que, pour tout $z \in \mathbb{C}$, il existe $q \in \mathbb{Z}[i]$ tel que

   $$|z - q|^2 < 1\,.$$

2. Déduire de la question précédente que $\mathbb{Z}[i]$ est un anneau euclidien pour la fonction ν définie par $\nu(x) = |x|^2$.

3. Montrer que $z \in \mathbb{Z}[i]$ est inversible si et seulement si $|z|^2 = 1$. En déduire la liste des éléments inversibles de $\mathbb{Z}[i]$ (il y en a 4).
   Cette question est utilisée dans la suite de nombreuses fois.
4. (Préliminaires arithmétiques.) Montrer que, si $p \in \mathbb{Z}$ est un nombre premier tel que $p = a^2 + b^2$ avec $a, b \in \mathbb{Z}$, alors ou bien $p = 2$, ou bien $p \equiv 1 \bmod 4$. La réciproque est vraie, mais nous ne la montrerons que plus tard ; pour l'instant, montrer que si p est un nombre premier impair (positif) tel que $p \equiv 1 \bmod 4$, alors il existe un entier x tel que $x^2 + 1$ est divisible par p.
   Cette deuxième partie nécessite qu'on se rappelle un résultat non trivial de l'an dernier en arithmétique.
5. Déduire de la question précédente que, si $p \in \mathbb{N}$ est un nombre premier tel que $p \equiv -1 \bmod 4$, alors p est également un élément premier de l'anneau $\mathbb{Z}[i]$.
6. Montrer que, si $z \in \mathbb{Z}[i]$ est tel que $p := |z|^2$ est un nombre premier de $\mathbb{Z}$, alors z est premier dans $\mathbb{Z}[i]$. De plus, montrer que $p \equiv 1 \bmod 4$ (ou $p = 2$).
7. Montrer que, si $z \in \mathbb{Z}[i]$ est premier, alors on est dans l'une ou l'autre des situations ci-dessus. En clair : ou bien $|z|^2$ est un nombre premier de $\mathbb{Z}$, ou bien il existe un inversible $u \in \mathbb{Z}[i]$ tel que $p := uz$ est un nombre premier de $\mathbb{Z}$ positif et $p \equiv -1 \bmod 4$.
   Indication : on suppose que $|z|^2$ n'est pas premier dans $\mathbb{Z}$, on note que $|z|^2 = z\bar{z}$ est un produit de deux éléments de $\mathbb{Z}[i]$, on utilise le lemme de Gauss...
8. Corollaire : montrer que si $p \in \mathbb{N}$ est un nombre premier avec $p \equiv 1 \bmod 4$, alors p est une somme de deux carrés (résultat dû à Fermat).
9. Factoriser entièrement (c'est-à-dire écrire comme produit de premiers) les nombres de 2 à 10 dans $\mathbb{Z}[i]$.

8 Groupes abéliens

Exercice 45. On considère le groupe abélien

$$V = \mathbb{Z}/36 \times \mathbb{Z}/30 \times \mathbb{Z}/2\,.$$

Écrire V comme un produit, comme dans les deux théorèmes de classification.

Exercice 46. On considère l'homomorphisme

$$f\colon \mathbb{Z}^n \longrightarrow \mathbb{Z}/2\mathbb{Z}$$

défini par

$$f(x_1, \ldots, x_n) = \sum_i x_i \bmod 2\,.$$

Soit $K = \ker(f)$. Trouver une base de $\mathbb{Z}^n$ « adaptée » à K, comme dans le théorème du même nom.

Exercice 47. Soit G un groupe fini. On appelle *exposant* de G le plus petit entier $e = e(G)$ tel que $g^e = 1$ pour tout $g \in G$; c'est le ppcm des ordres des éléments de G. En utilisant le théorème de classification, montrer que si G est abélien, alors il existe un $x \in G$ dont l'ordre est $e(G)$.

En prenant l'exemple du groupe symétrique S_3, vérifier qu'on ne peut pas généraliser ceci aux groupes non-abéliens.

Exercice 48. *Cet exercice présente une application classique, très importante, du précédent, mais il ne s'agit pas à proprement parler d'un exercice sur les groupes abéliens. On peut en dire autant de l'exercice qui suit.*

Soit $\mathbb{K}$ un corps commutatif.

1. Si $P \in \mathbb{K}[X]$ est de degré n, que peut-on dire du nombre de racines de P, et pourquoi ?

2. Soit G un sous-groupe fini de $\mathbb{K}^\times$. En utilisant la question précédente et l'exercice précédent, montrer que G est cyclique.

Exercice 49. Soit $\mathbb{K}$ un corps fini commutatif. (*On peut montrer en fait qu'un corps fini est toujours commutatif, c'est le théorème de Wedderburn, mais nous ne le ferons pas.*)

1. Rappeler ce qu'est la caractéristique p de $\mathbb{K}$.
2. Montrer que le cardinal de $\mathbb{K}$ est une puissance de p, disons $q = p^s$.
3. Écrivons $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Utiliser l'exercice précédent pour montrer qu'il existe un isomorphisme de $\mathbb{F}_p$-algèbres
$$\mathbb{K} \cong \mathbb{F}_p[X]/(D)$$
où (D) est un polynôme irréductible.
Indication : considérer l'homomorphisme $\mathbb{F}_p[X] \longrightarrow \mathbb{K}$ *défini par* $P \mapsto P(\alpha)$ *pour* α *bien choisi...*
Que nous dit la question précédente sur D ?

9 Réduction des endomorphismes

Exercice 50. Soit $\mathbb{K}$ un corps commutatif. On rappelle qu'un polynôme de $\mathbb{K}[X]$ de degré d est dit *scindé à racines simples sur* $\mathbb{K}$ s'il possède d racines distinctes dans $\mathbb{K}$.

Soit V un espace vectoriel de dimension finie sur $\mathbb{K}$, et soit f un endomorphisme de V. Montrer l'équivalence des propositions ci-dessous :

1. f est diagonalisable,
2. il existe un polynôme P, scindé à racines simples sur $\mathbb{K}$, tel que $P(f) = 0$,
3. le polynôme minimal de f est scindé à racines simples.

Plus précisément, on vous demande de montrer (1) $\implies$ (2) $\implies$ (3) de manière élémentaire, et d'utiliser le théorème de classification pour (3) $\implies$ (1).

Exercice 51. Soit V un espace vectoriel de dimension finie sur le corps commutatif $\mathbb{K}$, et soit f un endomorphisme de V. Soit $U \subset V$ un sous-espace stable par f. On suppose que f est diagonalisable. En utilisant l'exercice précédent, montrer que la restriction de f à U est également diagonalisable. Puis (c'est un petit peu plus difficile), montrer que l'endomomorphisme de V/U induit par f est également diagonalisable.

10 Formes de Jordan

Exercice 52. Déterminer la forme de Jordan de la matrice $\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$.

Exercice 53. 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 54. 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 55. Trouver toutes les formes de Jordan possibles pour une matrice dont le polynome caractéristique est $(X + 2)^2(X - 5)^3$.

Exercice 56. 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 57. Déterminer tous les sous-espaces invariant d'un bloc de Jordan.

Exercice 58. Donner toutes les formes de Jordan possibles des matrices de type 8×8 dont le polynome minimal est $x^2(x-1)^3$.

Exercice 59. Démontrer ou réfuter : Une matrice complexe A est semblable à sa transposée.

Exercice 60. *Extrait examen décembre 2021.*

1. Soit $J = J_m(0)$ un bloc de Jordan de taille $m \times m$. Calculer $\dim\ker(J^k)$ pour tout $k \geq 1$. On pourra distinguer entre le cas $1 \leq k \leq m$ et le cas $k > m$.
2. Soit M une matrice $n \times n$ à coefficients dans $\mathbb{C}$, que l'on suppose nilpotente. Pour chaque $k \geq 1$, on note b_k le nombre de blocs de Jordan de taille k dans la forme de Jordan de M. Justifier les égalités suivantes, dans lesquelles on a écrit $d_k = \dim\ker(M^k)$:

$$\begin{cases} b_1 & +b_2 & +b_3 & +\cdots & +b_n & = & d_1 \\ b_1 & +2b_2 & +2b_3 & +\cdots & +2b_n & = & d_2 \\ b_1 & +2b_2 & +3b_3 & +\cdots & +3b_n & = & d_3 \\ \vdots & & & & & & \\ b_1 & +2b_2 & +3b_3 & +\cdots & +nb_n & = & d_n = n\,. \end{cases}$$

   En d'autres termes, pour chaque k avec $1 \leq k \leq n$ on vous demande de montrer

$$\dim\ker(M^k) = \sum_{m=1}^{k} mb_m + k \sum_{m=k+1}^{n} b_m\,.$$

3. Application. Soit M une matrice nilpotente complexe de taille 4×4. Décrire la forme de Jordan de M en fonction des nombres $d_1 = \dim\ker(M)$, $d_2 = \dim\ker(M^2)$ et $d_3 = \dim\ker(M^3)$.

11 Groupes

Exercice 61 (Le groupe diédral)**.** On définit deux matrices dans $GL_2(\mathbb{R})$:

$$R = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \text{ et } S = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

1. Si $v = \begin{pmatrix} x \\ y \end{pmatrix}$ est un vecteur, calculer Rv et Sv. Interpréter géométriquement les applications $v \mapsto Rv$ et $v \mapsto Sv$, et expliquer l'emploi des lettres R et S.
2. Montrer que R est d'ordre 4, et S est d'ordre 2. En déduire R^{-1} et S^{-1}.
3. Montrer que $SR = R^{-1}S$.
4. Montrer que
$$D_8 = \{R^iS^j \mid 0 \leq i < 4,\ 0 \leq j < 2\}$$
est un sous-groupe de $GL_2(\mathbb{R})$ d'ordre 8.
5. Sans écrire de matrice, calculer l'ordre de chaque élément de D_8.
6. Établir la liste de tous les sous-groupes de D_8 (il y en a 10, dont 7 sont cycliques).

7. Décrire les classes de conjugaison de tous les éléments (il y en a 5).

Exercice 62 (Le groupes des quaternions)**.** On note $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$, avec $i^2 = j^2 = k^2 = -1$.

1. Trouver les ordres de tous les éléments.
2. Établir la liste de tous les sous-groupes (il y en a 6), et montrer qu'ils sont tous distingués.
3. Décrire les classes de conjugaison de tous les éléments (il y en a 5).

Exercice 63. Décrire les classes de conjugaison dans le groupe symétrique S_n (*c'est censé être quelque chose que vous avez déjà vu, sinon on en discute*).

Exercice 64. Soit p un nombre premier impair, et soit $G = (\mathbb{Z}/p\mathbb{Z})^\times$.

1. Rappeler pouquoi G est cyclique.
2. Décrire l'unique sous-groupe d'indice 2.
3. Déduire de la question précédente que -1 est un carré modulo p si et seulement si $(-1)^{\frac{p-1}{2}} = 1 \bmod p$.
4. Traduire la question précédente en termes de la valeur de p mod 4. (*Ceci démontre un résultat annoncé quand nous nous parlions des entiers de Gauss.*)

Exercice 65. Soit G un groupe fini, soit H un sous-groupe, et on fait agir G sur G/H de la manière usuelle. Montrer que les stabilisateurs des différents éléments de G/H forment une classe de conjugaison.

Exercice 66. Soit G un p-groupe, qui agit sur un ensemble fini X. On note

$$\mathrm{Fix}(X) = \{x \in X \mid g \cdot x = x \text{ pour tout } g \in G\}\,.$$

Montrer que

$$|X| \equiv |\,\mathrm{Fix}(X)| \bmod p\,.$$

Application. Le *centre* d'un groupe G est par définition

$$\mathcal{Z}(G) = \{x \in G \mid gx = xg \text{ pour tout } g \in G\}\,.$$

(C'est un sous-groupe de G.) Montrer que, si G est un p-groupe, alors $\mathcal{Z}(G)$ est un sous-groupe non-trivial.

Exercice 67 (deuxième théorème de Sylow)**.** Soit G un groupe fini et p un nombre premier. On suppose qu'il existe deux sous-groupes H et K de G tels que K est un p-groupe, et $|G/H|$ est premier à p. Montrer qu'il existe $g \in G$ tel que $K \subset gHg^{-1}$.

Indication : on fait agir K sur G/H et on fait appel aux deux exercices précédents.

Exercice 68. Soit p un nombre premier. Calculer l'ordre du groupe $GL_n(\mathbb{Z}/p\mathbb{Z})$. Puis, montrer que le sous-groupe U formé des matrices unipotentes, c'est-à-dire triangulaires supérieures avec des 1 sur la diagonale, est un sous-groupe de Sylow.

Exercice 69. Soit G un groupe fini.

1. (Théorème de Cayley.) Montrer qu'il existe un entier n et un homomorphisme injectif $G \longrightarrow S_n$.
   Indication : on fait agir G sur lui-même par multiplication à gauche, et on montre que l'application correspondante $\phi\colon G \longrightarrow S(G)$ est injective.
2. Déduire de la question précédente qu'il existe un entier n tel que, pour tout premier p, il existe un homomorphisme injectif $G \longrightarrow GL_n(\mathbb{Z}/p\mathbb{Z})$.

Exercice 70. Soit G un groupe fini et K, H deux sous-groupes.

1. Montrer que, dans l'action de K sur G/H, les stabilisateurs sont de la forme $K \cap gHg^{-1}$.

2. En déduire que si H est un p-Sylow de G, alors il existe $g \in G$ tel que $K \cap gHg^{-1}$ est un p-Sylow de K.
3. Déduire de ce qui précède une autre démonstration du premier théorème de Sylow.
   Indication : utiliser les deux exercices précédents.

Exercice 71. 1. Soit G un groupe fini et K, H deux sous-groupes. On pose

$$KH = \{kh \mid k \in K, h \in H\}\,.$$

   Montrer que, si K est distingué, l'ensemble KH est un sous-groupe de G.
2. Soit G un groupe d'ordre pq, où p et q sont premiers et $p > q$.
   (a) Montrer que G possède un unique p-Sylow K, et que celui-ci est distingué.
   (b) Soit H un q-Sylow. Montrer que $G = KH$, et que $K \cap H = \{1\}$.
3. Montrer qu'il n'y a que deux groupes d'ordre 6, à isomorphisme près.

Exercice 72. Soit p un nombre premier et $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

1. Préliminaire : combien y-a-t-il de polynômes irréductibles et unitaires de degré 2 dans $\mathbb{F}_p[X]$?
   Conseil : il est bien plus facile de compter tous les polynômes unitaires de degré 2, de compter tous ceux qui ne sont pas irréductibles, puis de faire une soustraction...
2. Montrer que le groupe $GL_2(\mathbb{F}_p)$ possède $p^2 - 1$ classes de conjugaison.

Exercice 73. Lister tous les groupes d'ordre 8, à isomorphisme près. Il y en a 5.

Compléter l'esquisse suivante. On connait tous les groupes abéliens par le théorème de classification. Si G est d'ordre 8 et non abélien, son exposant doit être 4 (pourquoi ?) Soit H un sous-groupe cyclique d'ordre 4 de G. S'il existe $g \in G - H$ d'ordre 2, alors $G \cong D_8$; sinon $G \cong Q_8$.

Pour information, il existe 14 groupes d'ordre 16, ainsi que 51 groupes d'ordre 32, puis 257 d'ordre 64... et 49 487 365 422 groupes d'ordre 1024. Il y a environ 50 milliards de groupes d'ordre ≤ 2000, et 99% de ceux-ci sont d'ordre 1024.

Exercice 74. Soit p un nombre premier et k un entier.

1. Montrer que pour $1 \leq \ell \leq p^k - 1$ on a

$$\binom{p^k - 1}{\ell} \equiv \pm 1 \bmod p\,.$$

   Indication : développer le polynôme $(X-1)^{p^k-1}$ dans $\mathbb{Z}/p\mathbb{Z}[X]$ de deux façons différentes.
2. En déduire que $\binom{p^k}{p^{k-1}}$ est divisible par p mais pas par p^2.
3. Soit G un groupe d'ordre p^k, et soit X l'ensemble des parties de G de cardinal p^{k-1}. On fait agir G sur X de la façon naturelle. Montrer qu'il existe $A \in X$ tel que $|\mathrm{orb}A|$ n'est pas divisible par p^2 ; en déduire que le stabilisateur de A est d'ordre p^{k-1}.
4. Nous avons donc démontré que tout groupe d'ordre p^k contient un sous-groupe d'ordre p^{k-1}. Dans cette question, on vous demande de prouver la même chose, mais par récurrence sur l'ordre du groupe, en utilisant le quotient $G/\mathcal{Z}(G)$, en faisant appel à un exercice ci-dessus.

12 Représentations

Exercice 75. On note $\mathbb{H}$ l'algèbre des quaternions (cf exercice 18).

1. Montrer que l'on peut voir $\mathbb{H}$ comme un espace vectoriel sur $\mathbb{C}$ avec pour base $1, j$.
2. Pour $x \in Q_8$ et $h \in \mathbb{H}$, on pose $\rho_x(h) = hx^{-1}$. Montrer que ceci définit une représentation ρ de Q_8 dans l'espace vectoriel (complexe) $\mathbb{H}$. Aurait-on pu prendre $\rho_x(h) = xh$?
3. Écrire les 8 matrices correspondant aux 8 éléments de Q_8.

Exercice 76. 1. Soit $\omega = \exp(2i\pi/3)$. On considère le groupe $G = \{1, \omega, \omega^2\} \cong \mathbb{Z}/3\mathbb{Z}$. Écrire les matrices de la représentation régulière.

2. Même question avec $G = S_3$.
   Cette fois-ci il y a 6 matrices 6×6*...*
3. On prend $G = D_8$. Écrire les matrices de R et S dans la représentation régulière.

Exercice 77. Finir la démonstration du lemme du cours qui affirme l'existence d'un produit hermitien G-invariant pour toute représentation du groupe fini G.

Exercice 78. À toute permutation $\sigma \in S_n$, on fait correspondre l'endomorphisme ρ_σ de $\mathbb{C}^n$ qui agit sur la base canonique $e_1, \ldots, e_n$ par la formule

$$\rho_\sigma(e_i) = e_{\sigma(i)}\,.$$

1. Montrer que
$$\rho_\sigma(x_1, \ldots, x_n) = (x_{\sigma^{-1}(1)}, \ldots, x_{\sigma^{-1}(n)})\,.$$
2. Montrer que $\sigma \mapsto \rho_\sigma$ est une représentation de S_n dans $\mathbb{C}^n$.
   On l'appelle souvent « la représentation naturelle de S_n *dans* $\mathbb{C}^n$*. » Dans la suite, nous écrirons* V *pour l'espace vectoriel* $\mathbb{C}^n$ *muni de cette représentation.*
3. Soit
$$U = \{(x, x, \ldots, x) \mid x \in \mathbb{C}\} \subset V\,.$$
   Montrer que U est un sous-$\mathbb{C}[S_n]$-module de V, et trouver un autre sous-module W tel que $V = U \oplus W$.
4. On souhaite montrer que W est irréductible. Soit M un sous-module non-nul de W ; on va donc montrer que $M = W$.
   (a) Montrer qu'il suffit d'établir que $(1, -1, 0, \ldots, 0) \in M$.
   (b) Montrer que M contient un vecteur dont la dernière coordonnée est nulle, puis conclure par récurrence sur n.

Exercice 79. Soit S un $\mathbb{C}[G]$-module irréductible, où G est fini, soit k un entier, et soit

$$S^k = S \times S \times \cdots \times S$$

(k facteurs). En utilisant le lemme de Schur, montrer que $\mathrm{End}_{\mathbb{C}[G]}(S)$ est isomorphe à $M_k(\mathbb{C})$, l'algèbre des matrices complexes de taille $k \times k$.

Indication : il existe des inclusions évidentes $\iota_j \colon S \longrightarrow S^k$ *et des projections* $p_j \colon S^k \longrightarrow S$*. Si* $\phi \colon S^k \longrightarrow S^k$ *est* G*-linéaire, alors la considération de* $p_j \circ \phi \circ \iota_i$ *vous donne un scalaire* a_{ij} *à mettre dans une matrice.*
Puis, en utilisant l'exercice 22, montrer que $\mathbb{C}[G]$ est isomorphe à un produit d'algèbres de matrices.

Exercice 80. Soit V un $\mathbb{C}[G]$-module, où G est fini. Montrer que V est irréductible $\iff (V, V) = 1$.

Exercice 81. Soit V un $\mathbb{C}[G]$-module irréductible, où G est fini.

1. Montrer qu'il existe un homomorphisme de modules $\mathbb{C}[G] \longrightarrow V$ qui est surjectif.
2. Déduire de la question précédente que V est isomorphe à un sous-module de $\mathbb{C}[G]$.

Exercice 82. Soit G un groupe fini. Montrer qu'il y a équivalence entre :

1. G est abélien,
2. toutes les représentations irréductibles de G sont de dimension 1.

Pour (1) $\implies$ (2), on utilisera le lemme de Schur (il y aura une autre démonstration, très différente, dans le cours). Pour (2) $\implies$ (1), on montrera d'abord que toute représentation $\rho\colon G \longrightarrow GL(V)$ vérifie que $\rho(G)$ est abélien.

Exercice 83. Dans chacun des exemples suivants, on donne un groupe fini G et une représentation, et on vous demande d'écrire les valeurs du caractère correspondant. On pourra déterminer les classes de conjugaison de G, puisqu'un caractère est toujours constant sur ces classes.

1. $G = Q_8$, pour la représentation de l'exercice 75.
2. $G = D_8$, avec la représentation obtenue en considérant l'inclusion $D_8 \subset \mathbb{C}^2$.
3. $G = S_3$ et la représentation régulière.
4. $G = S_3$ et la représentation W de l'exercice 78.

Exercice 84. Soit G un groupe fini.

1. Soit V un $\mathbb{C}[G]$-module. On note $V^* = \hom(V, \mathbb{C})$, que l'on voit comme un $\mathbb{C}[G]$-module (ici $\mathbb{C}$ désigne la représentation triviale de G). On dit que V^* est la *représentation duale* de V. Quel est le caractère de V^* ?
2. Soient V et W deux représentations de G. On pose $V \otimes W = \hom(V^*, W)$ (prononcé « V tenseur W »). Quel est le caractère de $V \otimes W$? En déduire que, si on a une troisième représentation U, alors $(U \otimes V) \otimes W \cong U \otimes (V \otimes W)$.
3. Soit V une représentation de dimension 1. Montrer que $V \otimes V^*$ est isomorphe à la représentation triviale.
4. Montrer que, si V est de dimension 1, et si W est irréductible, alors $V \otimes W$ est également irréductible.

Exercice 85. Soient x et y deux éléments d'un groupe fini G. Montrer l'équivalence de :

1. x et y sont conjugués dans G,
2. $\chi(x) = \chi(y)$ pour chaque caractère χ de G.

Exercice 86. On considère le groupe diédral D_8.

1. Montrer que D_8 possède 4 caractères de degré 1 et un caractère irréductible de degré 2 (et aucun autre caractère irréductible).
2. Montrer qu'il existe $x, y \in D_8$ tels que $xyx^{-1}y^{-1} = R^2$. En déduire que, si χ est un caractère de degré 1, alors $\chi(R^2) = 1$; puis déterminer complètement quels sont les caractères de degré 1.
3. Écrire la table des caractères de D_8 à l'aide des questions précédentes. Puis, comparer avec les calculs de l'exercice 83.
4. Reprendre les questions précédentes en remplaçant D_8 par Q_8, et R^2 par -1. Que constate-t-on ?

Exercice 87. Soit G un groupe fini.

1. Pour chaque classe de conjugaison K dans G, on choisit $x_K \in K$. Montrer que, si χ_1 et χ_2 sont des caractères irréductibles de G, on a

$$(\chi_1, \chi_2) = \sum_K \frac{1}{|\mathrm{stab}_G(x_K)|} \bar{\chi_1}(x)\chi_2(x)\,.$$

   Ici $\mathrm{stab}_G(x_K)$ désigne le stabilisateur de x_K dans l'action de conjugaison (qu'on appelle aussi le centralisateur de x_K).

2. Soit A la table des caractères de G, pour une numérotation $\chi_1, \dots, \chi_s$ des caractères et une numérotation K_1 des classes de conjugaison. Montrer que

$$A^{-1} = D \cdot {}^t\bar{A}\,,$$

où

$$D = \begin{pmatrix} \frac{1}{|\mathrm{stab}_G(x_{K_1})|} & & \\ & \ddots & \\ & & \frac{1}{|\mathrm{stab}_G(x_{K_s})|} \end{pmatrix}.$$

3. Utiliser la question (2) pour montrer la « deuxième relation d'orthogonalité », qui affirme que pour $x, y \in G$ on a

$$\sum_{\chi} \chi(x)\bar{\chi(y)} = \begin{cases} |\mathrm{stab}_G(x)| & \text{si } x \text{ et } y \text{ sont} \\ & \text{conjugués}\,, \\ 0 & \text{sinon}\,. \end{cases}$$

Ici la somme porte sur les caractères irréductibles de G.

4. *Exemple.* On suppose que la table des caractères de G est

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & \bar{\zeta_3} & \zeta_3 \\ 1 & 1 & \zeta_3 & \bar{\zeta_3} \\ 3 & -1 & 0 & 0 \end{pmatrix}$$

où $\zeta_3 = \exp(2i\pi/3)$. Calculer l'ordre du groupe, puis la taille des classes de conjugaison. Puis, montrer que G possède un unique 2-Sylow, qui est le noyau d'une représentation. Quel est le groupe, selon vous ?

Exercice 88. *Extrait examen décembre 2021.*

On note A_4 pour le groupe alterné de rang 4, c'est-à-dire le sous-groupe de S_4 formé des permutations de signature $+1$.

1. Écrire la liste des éléments de A_4 (il y en a 8 d'ordre 3, et 3 d'ordre 2, ainsi que l'élément neutre).
2. Montrer que (123) et (132) ne sont pas conjugués dans A_4.
3. On rappelle que la table des caractères de S_4 est

	I	(12)	(12)(34)	(123)	(1234)
χ_1	1	1	1	1	1
χ_2	1	−1	1	1	−1
χ_3	2	0	2	−1	0
χ_4	3	1	−1	0	−1
χ_5	3	−1	−1	0	1

Soit V_i un $\mathbb{C}[S_4]$-module de caractère χ_i, pour $1 \leq i \leq 5$. Montrer que la restriction de V_4 au sous-groupe A_4 est encore irréductible. Montrer également qu'il existe un isomorphisme de $\mathbb{C}[A_4]$-modules entre V_4 et V_5.

4. Montrer que A_4 possède 3 caractères irréductibles de degré 1, et un unique caractère irréductible de degré 3. Puis, montrer plus précisément que la table des caractères de A_4 est de la forme

	I	(12)(34)	(123)	(132)
ξ_1	1	1	1	1
ξ_2	1	?	?	?
ξ_3	1	?	?	?
ξ_4	3	−1	0	0

5. Soit $x = (12)(34)$. Montrer que $\xi_2(x) = \pm 1$ et $\xi_3(x) = \pm 1$. Puis, montrer que

$$1 + \xi_2(x) + \xi_3(x) - 3 = 0\,.$$

   En déduire les valeurs de $\xi_2(x)$ et $\xi_3(x)$.

6. Finir d'écrire la table des caractères de A_4.

Exercice 89. *Extrait examen juin 2022.*

Soit G un groupe fini, et ρ une représentation de G dans l'espace vectoriel V (de dimension finie sur $\mathbb{C}$ comme d'habitude). Soit $\chi = \chi_S$ le caractère d'une représentation irréductible quelconque S de G.

On définit $\pi\colon V \longrightarrow V$ par

$$\pi = \frac{\dim(S)}{|G|} \sum_{x \in G} \bar{\chi(x)}\, \rho_x\,.$$

1. Montrer que π est G-linéaire.
2. Soit $U \subset V$ un sous-espace stable par ρ (= un sous-$\mathbb{C}[G]$-module). On suppose que U est irréductible. Montrer que la restriction π' de π à U est de la forme $\pi' = \lambda I$ pour $\lambda \in \mathbb{C}$ (avec I l'identité de U). Puis, montrer plus précisément que $\lambda = 1$ si $U \cong S$, et $\lambda = 0$ sinon.
3. Déduire de la question précedente que $\pi \circ \pi = \pi$, et décrire l'image de π.
4. On suppose que

$$V = V_1 \oplus V_2 \oplus \cdots \oplus V_k$$

   avec V_i irréductible. De plus, on fait l'hypothèse que V_i n'est pas isomorphe à V_j si $i \neq j$. Montrer à l'aide de la question précédente que la décomposition ci-dessus est unique au sens suivant : si

$$V = V_1' \oplus V_2' \oplus \cdots \oplus V_\ell'$$

   avec chaque V_i' irréductible, alors $k = \ell$ et, après renumérotation si nécessaire, on a $V_i = V_i'$ pour tout i.

   Remarques. Attention, ce n'est pas seulement $V_i \cong V_i'$, mais bien une égalité. On fait remarquer également que, si votre réponse à la question (3) est suffisamment détaillée (et la description de l'image de π suffisamment précise), la question (4) est normalement facile.