Correction de l'examen du 03/01/23
"Algèbre 1 - HAX708X"

Questions isolées *(6 points)*

a. Soit A un anneau commutatif. Démontrer que les A-modules simples sont les modules isomorphes à A/I, où I est un idéal maximal de A. (Montrer en particulier que ces A-modules sont deux à deux non isomorphes.)

Soit M un A-module simple : c'est le cas si pour tout $m \neq 0$ dans M, on a $M = Am$. Ainsi M est isomorphe à A/I_m où I_m est l'idéal annulateur d'un point $m \in M \setminus \{0\}$: $I_m = \{a \in A, am = 0\}$.

Maintenant un A-module de la forme A/I est simple si pour tout $x \in A/I$ non-nul, on a $Ax = A/I$: cette dernière relation est équivalente à demander que Ax contienne la classe de $1 \in A$, c'est à dire x est inversible. Conclusion : A/I est simple si et seulement si I est un idéal maximal de A.

Supposons que $A/I \sim A/J$ en tant que A-modules. Cela implique que $A/I \sim A/J$ en tant qu'anneau, et donc que $I = J$.

b. Soit I le noyau de l'homomorphisme d'anneaux de $\mathbb{C}[X,Y]$ dans $\mathbb{C}$ donné par $P(X,Y) \mapsto P(0,0)$. Montrer que I n'est pas un idéal principal.

On voit que $I = (X) + (Y)$. Supposons qu'il existe $P \in \mathbb{C}[X,Y]$ tel que $(X) + (Y) = (P)$. On remarque tout d'abord que $(X) + (Y) \neq \mathbb{C}[X,Y]$, donc le polynôme P n'est pas constant. De plus, l'inclusion $(X) \subset (P)$ signifie qu'il existe $A \in \mathbb{C}[X,Y]$ tel que $X = PA$. Sachant que P n'est pas constant, cela implique que A est un polynôme constant et donc que $(X) = (P)$. Si on travaille avec l'idéal (Y), on obtiendrait de manière similaire que $(Y) = (P)$. Cela est contradictoire avec le fait que $(X) \neq (Y)$.

c. Soit V un sous $\mathbb{Q}$-espace vectoriel de $\mathbb{Q}^n$ et soit $M := V \cap \mathbb{Z}^n$. Montrer que M est un $\mathbb{Z}$-module libre tel que $M \otimes_{\mathbb{Z}} \mathbb{Q}$ soit isomorphe à V.

M est un $\mathbb{Z}$-module libre comme sous-module du module libre $\mathbb{Z}^n$. On considère l'application canonique $\varphi : M \otimes_{\mathbb{Z}} \mathbb{Q} \to V$ qui envoie $m \otimes \alpha$ sur αm. Pour s'assurer que l'application linéaire φ est un isomorphisme, on peut utiliser le fait qu'il existe une base $(v_1, \ldots, v_n)$ de $\mathbb{Z}^n$ et des entiers naturels non-nuls $(k_1, \ldots, k_r)$ tels que $(k_1 v_1, \ldots, k_r v_r)$ est une base de M. Ici les k_i sont tous égaux à 1, car pour tout $v \in \mathbb{Q}^n$, on a $v \in V \iff \exists n \geq 1, nv \in M$. Finalement, $M = \mathbb{Z}v_1 \oplus \cdots \oplus \mathbb{Z}v_r$ tandis que $V = \mathbb{Q}v_1 \oplus \cdots \oplus \mathbb{Q}v_r$. On voit immédiatement que φ est un isomorphisme.

d. À isomorphisme près, combien y a-t-il de groupes abéliens de cardinal 100 ? En donner la liste.

On cherche les couples (d_1, d_2) d'entiers naturels vérifiant "d_1 divise d_2" et $d_1 d_2 = 100 = 2^2\,5^2$. Les solutions sont $(1, 2^2\,5^2)$, $(5, 2^2 \cdot 5)$, $(2, 2 \cdot 5^2)$ et $(2 \cdot 5, 2 \cdot 5)$.

Voici la liste des groupes abéliens correspondants :

$$\mathbb{Z}/100\mathbb{Z}, \quad \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/20\mathbb{Z}, \quad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/50\mathbb{Z}, \quad \mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$$

Exercice 1 *(6 points)*

L'anneau $\mathbb{C}[X_1,\dots,X_n]$, $n \geq 2$, est muni de l'action naturelle du groupe symétrique $\mathcal{S}_n$ par permutation des variables. On dit qu'un polynôme $P \in \mathbb{C}[X_1,\dots,X_n]$ est antisymétrique si pour tout $\sigma \in \mathcal{S}_n$, on a : $(\star)\quad \sigma \cdot P = \epsilon(\sigma)P$, où $\epsilon(\sigma)$ est la signature de σ. Soit $\Delta_n = \prod_{1\leq i<j\leq n}(X_i - X_j)$.

(1) Montrer qu'un polynôme $P(X_1,\dots,X_n)$ est antisymétrique si et seulement si pour tout $1 \leq i < j \leq n$, on a : $(\star\star)\quad P(\dots,X_i,\dots,X_j,\dots) = -P(\dots,X_j,\dots,X_i,\dots)$.

Cela est dû au fait que les transpositions engendrent le groupe symétrique $\mathcal{S}_n$. On remarque que $(\star\star)$ correspond à $(\star)$ lorsque σ est égal à la transposition (i,j). Ensuite, si les conditions $(\star\star)$ sont satisfaites, on obtient $(\star)$ pour une permutation σ en la décomposant en produit $\tau_1\cdots\tau_k$ de transpositions : on utilise alors que $\epsilon(\sigma) = (-1)^k$.

(2) Montrer que Δ_n est antisymétrique. *On pourra procéder par récurrence sur n.*

Pour $n = 2$, le polynôme $\Delta_2 = X_1 - X_2$ est antisymétrique (par rapport à l'action de $\mathcal{S}_2$).

Supposons maintenant que Δ_n est antisymétrique (par rapport à l'action de $\mathcal{S}_n$) et considérons le polynôme

$$\Delta_{n+1} = \Delta_n \prod_{1\leq k\leq n}(X_k - X_{n+1}).$$

Considérons une transposition (i,j) avec $1 \leq i < j \leq n+1$.

Premier cas : $j \leq n$. Alors $(i,j) \in \mathcal{S}_n$ et d'après l'hypothèse de récurrence on a $(i,j)\cdot\Delta_n = -\Delta_n$ et $(i,j)\cdot\prod_{1\leq k\leq n}(X_k - X_{n+1}) = \prod_{1\leq k\leq n}(X_k - X_{n+1})$, donc $(i,j)\cdot\Delta_{n+1} = -\Delta_{n+1}$

Second cas : $j = n+1$. Dans ce cas on pose

$$\Delta_n = \Delta \prod_{k<i}(X_k - X_i)\prod_{i<k}(X_i - X_k) = (-1)^{n-i}\Delta\prod_{k\neq i}(X_k - X_i)$$

avec Δ un polynôme sans les variables X_i et X_{n+1}. Cela permet d'écrire

$$\Delta_{n+1} = (-1)^{n-i}\underbrace{\prod_{k\neq i}(X_k - X_i)(X_k - X_{n+1})}_{T}\times\Delta\times(X_i - X_{n+1})$$

On peut conclure que $(i,n+1)\cdot\Delta_{n+1} = -\Delta_{n+1}$ car $(i,n+1)\cdot(X_i - X_{n+1}) = -(X_i - X_{n+1})$, $(i,n+1)\cdot\Delta = \Delta$ et $(i,n+1)\cdot T = T$.

(3) Pour $P \in \mathbb{C}[X_1,\dots,X_n]$, montrer qu'il existe $Q \in \mathbb{C}[X_1,\dots,X_n]$ et $R \in \mathbb{C}[X_2,\dots,X_n]$ uniques, tels que $P = Q\cdot(X_1 - X_2) + R$.

On travaille avec l'anneau intègre $A = \mathbb{C}[X_2,\dots,X_n]$, et on considère les polynômes $P, X_1 - X_2$ comme éléments de $A[X_1]$. Sachant que $X_1 - X_2$ est un polynôme unitaire de $A[X]$, on peut faire la division euclidienne de P par $X_1 - X_2$ dans $A[X_1]$: il existe un unique couple $(Q,R) \in A[X_1]^2$ tel que $P = Q\cdot(X_1 - X_2) + R$ avec $\text{degré}_{A[X_1]}(R) < \text{degré}_{A[X_1]}(X_1 - X_2) = 1$. Cette dernière condition signifie que $R \in A = \mathbb{C}[X_2,\dots,X_n]$

(4) Supposons que $P \in \mathbb{C}[X_1,\dots,X_n]$ soit antisymétrique.

— Montrer que le polynôme R ci-dessus est égal à 0.

Posons $\tilde{Q} = (1,2)\cdot Q$ et $\tilde{R} = (1,2)\cdot R$. La relation $P = Q\cdot(X_1 - X_2) + R$ implique que $P = \tilde{Q}\cdot(X_1 - X_2) - \tilde{R}$. L'unicité de la division euclidienne permet de voir que $R = -\tilde{R}$. Comme $R = R(X_2,X_3,\dots,X_n)$, on a $\tilde{R} = R(X_1,X_3,\dots,X_n)$. La relation $R(X_2,X_3,\dots,X_n) = -R(X_1,X_3,\dots,X_n)$ implique que

$$R(0,X_3,\dots,X_n) = R(X_2,X_3,\dots,X_n) = -R(X_1,X_3,\dots,X_n) = -R(0,X_3,\dots,X_n)$$

et donc $R = 0$.

— En déduire que $P = \Delta_n \cdot S$ où S est un polynôme symétrique de $\mathbb{C}[X_1, \dots, X_n]$.
$X_1 - X_2$ divise P donc $X_{\sigma(1)} - X_{\sigma(2)} = \sigma \cdot (X_1 - X_2)$ divise $\sigma \cdot P = \pm P$ pour tout $\sigma \in \mathcal{S}_n$. Ainsi, les polynômes $X_i - X_j, i < j$ forment une famille de diviseurs irréductibles, distincts deux à deux, du polynôme antisymétrique P. Sachant que $\mathbb{C}[X_1, \dots, X_n]$ est une anneau factoriel, on peut conclure que leur produit Δ_n divise P : il existe un unique $S \in \mathbb{C}[X_1, \dots, X_n]$ tel que $P = \Delta_n S$. Sachant que $\sigma \cdot P = \epsilon(\sigma) P$ et $\sigma \cdot \Delta_n = \epsilon(\sigma)\Delta_n$, on en déduit que $\sigma \cdot S = S$ pour tout $\sigma \in \mathcal{S}_n$. Le polynôme S est symétrique.

Exercice 2 *(4 points)*

Soit A l'ensemble des nombres rationnels qui s'écrivent comme une fraction $\frac{a}{b}$ avec b impair.

(1) Montrer que A est un sous-anneau de $\mathbb{Q}$.
Immédiat.

(2) Déterminer ses éléments inversibles ainsi que ses éléments irréductibles.
$\frac{a}{b} \in A$ est inversible s'il existe $\frac{a'}{b'} \in A$ tel que $\frac{a}{b}\frac{a'}{b'} = 1$, c'est à dire $aa' = bb'$. Comme b et b' sont impairs, a et a' sont aussi impairs. Ainsi, $A^\times = \{\frac{a}{b};\ a, b \text{ impairs}\}$.

Tout élément non-nul $x \in A$ s'exprime sous la forme $x = 2^k \frac{a}{b}$ avec $a, b \in \mathbb{Z}$ impairs et $k \in \mathbb{N}$. Il est irréductible si et seulement si $k = 1$.

(3) Montrer que pour tout $x \in \mathbb{Q}$, il existe un entier $n \in \mathbb{N}$ tel que $2^n x \in A$.
Immédiat.

(4) Montrer que A est un anneau principal.
Soit I un idéal (non-nul) de A. Remarquons que pour $x \in A \setminus \{0\}$, la décomposition $x = 2^k \frac{a}{b}$ avec $a, b \in \mathbb{Z}$ impairs, montre que $2^k \in I$. On pose $n(I) = \inf\{n \in \mathbb{N}, 2^n \in I\}$. On montre alors assez facilement que $I = (2^{n(I)})$.

Exercice 3 *(4 points)*

Soit G un groupe fini et $\mathbb{C}[G]$ son algèbre de groupe.

(1) Expliquer le fait d'une représentation linéaire complexe de G est exactement un $\mathbb{C}[G]$-module.
Une représentation linéaire complexe de G est un espace vectoriel complexe V de dimension finie équipée d'un morphisme de groupes $\rho : G \to \mathrm{GL}(V)$.

On peut alors définir un morphisme d'anneaux $\tilde{\rho} : \mathbb{C}[G] \to \mathrm{End}(V)$, en posant

$$\tilde{\rho}\left(\sum_{g \in G} \lambda_g \delta_g\right) = \sum_{g \in G} \lambda_g \rho(g).$$

Le morphisme $\tilde{\rho}$ munit V d'une structure de $\mathbb{C}[G]$-module.

(2) Montrer que le centre de $\mathbb{C}[G]$ est l'espace vectoriel engendré par les $\phi_C := \sum_{x \in C} \delta_x$, où C est une classe de conjugaison de G.
$\phi = \sum_{g \in G} \lambda_g \delta_g$ appartient au centre de $\mathbb{C}[G]$ si et seulement si $\phi \delta_h = \delta_h \phi$ pour tout $h \in G$, c'est à dire $\phi = \delta_h \phi \delta_{h^{-1}}, \forall h \in G$. Cette dernière relation siginifie que

$$\sum_{g \in G} \lambda_g \delta_g = \sum_{g \in G} \lambda_g \delta_{hgh^{-1}} = \sum_{g \in G} \lambda_{h^{-1}gh} \delta_g$$

La fonction $\lambda : G \to \mathbb{C}$ est donc invariante par conjugaison. Notons $\lambda(C)$ la valeur que prend λ sur une classe de conjugaison $C \subset G$. On a ainsi montré que $\phi = \sum_C \lambda(C) \phi_C$.

(3) Montrer que si $\rho : G \to \mathrm{GL}(V)$ est une représentation irréductible, alors $\rho(\phi_C) := \sum_{x \in C} \rho(x)$ est une homothétie.
L'application linéaire $\rho(\phi_C) : V \to V$ commute avec l'action de G, car ϕ_C appartient au centre de $\mathbb{C}[G]$: on a $\rho(\phi_C) \circ \rho(g) = \rho(g) \circ \rho(\phi_C), \forall g \in G$.

Sachant que V est une représantation irréductible de G, on peut conclure grace au Lemme de Schur que $\rho(\phi_C) := \sum_{x \in C} \rho(x)$ est une homothétie.

Exercice 4 *(4 points)*

On considère une base de $\mathbb{C}^6$ notée $(e_\sigma)_{\sigma\in\mathcal{S}_3}$. On considère la représentation $\rho : \mathcal{S}_3 \to GL_6(\mathbb{C})$ du groupe symétrique $\mathcal{S}_3$ définie par

$$\forall \tau \in \mathcal{S}_3, \quad \forall \sigma \in \mathcal{S}_3, \qquad \rho(\sigma)(e_\tau) = e_{\sigma\tau\sigma^{-1}}.$$

(1) Décrire les classes de conjugaison de $\mathcal{S}_3$.

Il y a trois classes de conjugaison : C_1 est le singleton réduit à l'identité, C_2 contient les trois transpositions, et C_3 contient les deux 3-cycles.

(2) Déterminer la table des caractères irréductibles du groupe $\mathcal{S}_3$.

$\mathcal{S}_3$ admet trois représentations irréductibles :

(a) $V_1 = \mathbb{C}$ est la représentation triviale.

(b) V_2 est la représentation de dimension 1 définie par la signature.

(c) $V_3 = \{(x,y,z) \in \mathbb{C}^3,\ x+y+z=0\}$ est munie de l'action canonique de $\mathcal{S}_3$ sur $\mathbb{C}^3$.

On note $\chi_k : \mathcal{S}_3 \to \mathbb{C}$ le caractère de la représentation V_k. Voici la table des caractères irréductibles du groupe $\mathcal{S}_3$

	C_1	C_2	C_3
χ_1	1	1	1
χ_2	1	-1	1
χ_3	2	0	-1

(3) Décomposer ρ en somme directe de représentations irréductibles.

Chaque $\rho(\sigma)$ permute les éléments de la base $(e_\tau)_{\tau\in\mathcal{S}_3}$. Ainsi la trace de $\rho(\sigma)$ est égal au nombre de $\tau \in \mathcal{S}_3$ tels que $\rho(\sigma)(e_\tau) = e_\tau$, c'est à dire $\tau = \sigma\tau\sigma^{-1}$. Notons χ_ρ le caractère de ρ. On a donc

— $\chi_\rho(Id) = 6$,
— $\chi_\rho(\tau) = 2$ si τ est une transposition,
— $\chi_\rho(\tau) = 3$ si τ est un 3-cycle.

On sait que la représentation $V = (\mathbb{C}^6, \rho)$ admet une décomposition $V \simeq n_1V_1 \oplus n_2V_2 \oplus n_3V_3$. Alors $\chi_\rho = n_1\chi_1 + n_2\chi_2 + n_3\chi_3$, et ainsi

$$n_k = \langle \chi_\rho, \chi_k \rangle$$

pour tout $k \in \{1,2,3\}$. Ici $\langle -,- \rangle$ désigne le produit hermitien sur $\mathbb{C}[G]$ défini par la relation $\langle \phi, \psi \rangle = \frac{1}{6}\sum_{\tau\in\mathcal{S}_3} \phi(\tau)\overline{\psi(\tau)}$.

Finalement, on obtient $n_1 = 3$ et $n_2 = n_3 = 1$. On a donc montré que V est isomorphe à la représentation $V_1 \oplus V_1 \oplus V_1 \oplus V_2 \oplus V_3$.