# Correction de l'examen du 7 janvier 2026

Durée : 3h, les documents ne sont pas autorisés.

$\mathbf{F}_q$ dénote le corps fini à $q$ éléments. On rappelle et admet le fait que tout sous-groupe fini du groupe multiplicatif d'un corps est cyclique.

Toutes les représentations de groupes sont de dimension finie sur $\mathbf{C}$.

1. Lesquels des anneaux suivants sont principaux et lesquels sont factoriels :

$$\mathbf{Z}[x], \quad \mathbf{Z}[i], \quad \mathbf{R}[x], \quad \mathbf{C}[x,y], \quad \mathbf{Z}[\sqrt{-5}]\,?$$

Justifier brièvement (une ou deux phrases par anneau) vos réponses.

*Solution.* $\mathbf{Z}[i]$ et $\mathbf{R}[x]$ sont des domaines euclidiens et donc principaux et factoriels. $\mathbf{Z}$ est factoriel et donc $\mathbf{Z}[x]$ est factoriel aussi. $\mathbf{C}[x,y] = \mathbf{C}[x][y]$ est factoriel également.

$\mathbf{Z}[x]$ n'est pas principal parce que l'idéal $(2\ x)$ n'est pas principal (les seuls éléments de $\mathbf{Z}[x]$ qui divisent 2 et $x$ sont $\pm 1$). De manière similaire, l'idéal $(x\ y)$ n'est pas principal dans $\mathbf{C}[x,y]$.

$\mathbf{Z}[\sqrt{-5}]$ n'est pas factoriel (et donc pas principal non plus). En effet $6 = 2\cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$ et les éléments $2, 3, 1+\sqrt{-5}, 1-\sqrt{-5}$ sont irréductibles. □

2. Montrer que $\mathbf{Z}[i]/I$ est fini pour tout idéal non nul $I \trianglelefteq \mathbf{Z}[i]$. (*Indication :* Utiliser le fait que $I$ est principal et la division euclidienne.)

*Solution.* Comme $\mathbf{Z}[i]$ est un anneau principal, il existe $\alpha$ tel que $I = (\alpha)$. Soit $x + I$ un élément de $\mathbf{Z}[i]/I$. Alors il existe $q$ et $r$ tels que $x = q\alpha + r$ et $N(r) < N(\alpha)$. Donc $r + I = x + I$. Il reste à remarquer qu'il n'y a qu'un nombre fini d'éléments de $\mathbf{Z}[i]$ avec norme plus petite que $N(\alpha)$. □

3. (a) Le corps $\mathbf{F}_8$ admet-il un sous-corps isomorphe à $\mathbf{F}_4$ ?

*Solution.* Non. En effet, supposons que $K \leq \mathbf{F}_8$ et $[\mathbf{F}_8 : K] = d$. Alors $8 = |\mathbf{F}_8| = |K|^d$ ce qui n'est pas possible si $|K| = 4$. □

(b) Soit $F = \mathbf{Q}(\alpha_1, \ldots, \alpha_n)$ où $\alpha_i \in \mathbf{C}, \alpha_i^2 \in \mathbf{Q}$ pour tout $i$. Montrer que $\sqrt[3]{2} \notin F$.

*Solution.* Soit $F_k = \mathbf{Q}(\alpha_1, \ldots, \alpha_k)$. On montre par récurrence sur $k$ que $[F_k : \mathbf{Q}]$ est une puissance de 2. En effet, si $\alpha_{k+1} \in F_k$, alors $F_{k+1} = F_k$ et sinon, le polynôme minimal de $\alpha_{k+1}$ au dessus de $F_k$ est de degré 2 et donc $[F_{k+1} : F_k] = 2$. On conclut que $[F : \mathbf{Q}]$ est une puissance de 2. Or $[\mathbf{Q}(\sqrt[3]{2}) : \mathbf{Q}] = 3$ (le polynôme minimal de $\sqrt[3]{2}$ est $x^3 - 2$) et comme 3 ne peut pas diviser une puissance de 2, on voit que $\sqrt[3]{2} \notin F$. □

4. Soit $p$ un nombre premier et $n \in \mathbf{N} \smallsetminus \{0\}$.

(a) Montrer qu'il existe $\alpha \in \mathbf{F}_{p^n}$ tel que $\mathbf{F}_{p^n} = \mathbf{F}_p(\alpha)$.

*Solution.* Le groupe multiplicatif de $\mathbf{F}_{p^n}$ est cyclique ; soit $\alpha$ un générateur. Alors tout élément non nul de $\mathbf{F}_{p^n}$ est une puissance de $\alpha$ et, en particulier, $\mathbf{F}_{p^n} = \mathbf{F}_p(\alpha)$. □

(b) Montrer qu'il existe un polynôme irréductible dans $\mathbf{F}_p[x]$ de degré $n$.

*Solution.* Soit $\alpha$ comme dans (a) et soit $f$ le polynôme minimal de $\alpha$ sur $\mathbf{F}_p$. Alors $f$ est irréductible et $\deg f = [\mathbf{F}_p(\alpha) : \mathbf{F}_p] = [\mathbf{F}_{p^n} : \mathbf{F}_p] = n$. □

5. Soit $F$ un corps et soit $\overline{F}$ sa clôture algébrique.

   (a) Soit $i\colon F \to K$ un plongement de corps tel que $K$ est algébrique au dessus de $i(F)$. Montrer qu'il existe un plongement $j\colon K \to \overline{F}$ tel que $j \circ i = \mathrm{id}_F$.

   *Solution.* Soit $\overline{K}$ la clôture algébrique de $K$. Comme $K$ est algébrique au dessus de $F$, $\overline{K}$ est également une clôture algébrique de $F$. Par l'unicité de la clôture algébrique, $\overline{K}$ et $\overline{F}$ sont isomorphes au dessus de $F$ et on peut prendre pour $j$ la restriction à $K$ d'un tel isomorphisme. □

   (b) Soit $F \leq K \leq \overline{F}$ avec $[K : F] < \infty$. Montrer que les énoncés suivants sont équivalents :

   (i) $K$ est le corps de décomposition d'un polynôme $f \in F[x]$.

   (ii) Pour tout plongement $j\colon K \to \overline{F}$ qui fixe $F$, $j(K) = K$.

   (iii) Tout polynôme irréductible de $F[x]$ qui a une racine dans $K$ se décompose dans $K[x]$.

   *Solution.* (i) ⇒ (ii). Soit $A \subseteq K$ l'ensemble des racines de $f$ et soit $j$ un plongement comme dans (ii). Alors $K = F(A)$ et $j(A) = A$ car $j$ fixe les coefficients de $f$. Il s'en suit que $j(K) = K$.
   (ii) ⇒ (iii). Soit $g \in F[x]$ un polynôme irréductible et $\alpha \in K$ une racine de $g$. Soit $\beta \in \overline{F}$ une autre racine de $g$. Alors $F(\alpha) \cong F[x]/(g) \cong F(\beta)$. Soit $i\colon F(\beta) \to F(\alpha) \subseteq K$ l'isomorphisme qui envoie $\beta$ sur $\alpha$ et fixe $F$. Par (a), il existe $j\colon K \to \overline{F}$ tel que $j \circ i = \mathrm{id}_{F(\beta)}$. Maintenant par (ii), $\beta = j(i(\beta)) = j(\alpha) \in K$.
   (iii) ⇒ (i). Soit $K = F(\alpha_1, \ldots, \alpha_n)$ et soit $g_i$ le polynôme minimal de $\alpha_i$. Alors par (iii) tout $g_i$ se décompose dans $K[x]$ et $K$ est le corps de décomposition de $f = \prod_i g_i$. □

6. Soit $\zeta$ une racine $n$-ième de 1. Montrer que

$$\sum_{\{d<n : \mathrm{pgcd}(d,n)=1\}} \zeta^d \in \mathbf{Z}.$$

(*Indication :* On pourrait utiliser les formules de Viète : si $f(x) = x^m + \sum_{i<m} a_i x^i$ est un polynôme unitaire et $\alpha_1, \alpha_2, \ldots, \alpha_m$ sont ses racines, alors $s_k(\alpha_1, \ldots, \alpha_m) = (-1)^k a_{m-k}$, où $s_k$ est le $k$-ième polynôme symétrique élémentaire. Commencer avec le cas où $\zeta$ est une racine primitive.)

*Solution.* Si $\zeta$ est primitive, alors $\Xi := \{\zeta^d : d < n, \mathrm{pgcd}(d,n) = 1\}$ est l'ensemble des racines du polynôme cyclotomique $\Phi_n$. Comme $\Phi_n$ est unitaire à coefficients entiers, par les formules de Viète, la somme de ses racines est un entier aussi.

Considérons maintenant le cas général. Soit $\xi$ une racine $n$-ième primitive et soit $\zeta = \xi^a$ avec $0 \leq a < n$. Alors

$$\sum_{\{d<n : \mathrm{pgcd}(d,n)=1\}} \zeta^d = \sum_{\{d<n : \mathrm{pgcd}(d,n)=1\}} \xi^{da} = \sum_{\eta \in \Xi} \eta^a.$$

C'est un polynôme symétrique en les racines de $\Phi_n$ ; comme $\Phi_n \in \mathbf{Z}[x]$ est unitaire, par les formules de Viète et le théorème fondamental des polynômes symétriques, on obtient que la somme s'exprime comme un polynôme à coefficients entiers en les coefficients de $\Phi_n$ et c'est donc un entier. □

7. Soit $G$ un groupe fini et $\phi\colon G \to \mathrm{GL}(V)$ une représentation irréductible. Soit $Z(G)$ le *centre* de $G$, i.e., le sous-groupe défini par

$$Z(G) = \{z \in G : zg = gz \text{ pour tout } g \in G\}.$$

(a) Montrer que $\phi(Z(G)) \subseteq \{\lambda I : \lambda \in \mathbf{C}\}$.

*Solution.* Soit $z \in Z(G)$. Alors $\phi(z)$ commute avec $\phi(g)$ pour tout $g \in G$ et par le lemme de Schur, $\phi(z) = \lambda I$ pour un $\lambda \in \mathbf{C}$. □

(b) La représentation $\phi$ est dite *fidèle* si $\ker\phi = \{e\}$. Montrer que si $G$ admet une représentation irréductible et fidèle, alors $Z(G)$ est cyclique.

*Solution.* Si $\phi$ est fidèle, le groupe $\phi(Z(G)) \leq \mathrm{GL}(V)$ est isomorphe à $Z(G)$ et par (a), il est isomorphe à un sous-groupe fini de $\mathbf{C}^\times$ et donc cyclique. □

8. Soit $G$ un groupe fini et soit $\chi$ un caractère de $G$.

(a) Montrer que si $g \in G$ avec $\mathrm{ord}(g) = n$, alors il existe des racines $n$-ièmes de 1 $\zeta_1, \ldots, \zeta_d$ telles que

$$\chi(g^k) = \sum_{j=1}^{d} \zeta_j^k \quad \text{pour tout } k.$$

*Solution.* On rappelle que toute matrice d'ordre $n$ est diagonalisable et ses valeurs propres sont des racines $n$-ièmes de 1. Soit $\phi$ la représentation de $\chi$. Alors $\phi(g)$ est conjuguée à $\mathrm{diag}(\zeta_1, \ldots, \zeta_d)$ et $\phi(g^k)$ est conjuguée à $\mathrm{diag}(\zeta_1^k, \ldots, \zeta_d^k)$. Comme la trace est invariante par conjugaison, on a $\chi(g^k) = \mathrm{Tr}(\phi(g^k)) = \sum_{j=1}^{d} \zeta_j^k$. □

(b) À partir de maintenant on suppose que $G = S_m$, le groupe symétrique. Montrer que si $g \in G$ et $k$ est un entier avec $\mathrm{pgcd}(k, \mathrm{ord}(g)) = 1$, alors $g$ et $g^k$ sont conjugués.

*Solution.* Soit $g = \tau_1 \cdots \tau_s$ la décomposition en cycles disjoints de $g$. On note par $|\tau_i|$ la longueur du cycle $\tau_i$. Alors $\mathrm{ord}(g) = \mathrm{ppcm}(|\tau_1|, \ldots, |\tau_s|)$ et donc $\mathrm{pgcd}(k, |\tau_i|) = 1$ pour tout $i$. Il s'en suit que $\tau_i^k$ est un cycle de la même longueur que $\tau_i$ et $g^k = \tau_1^k \cdots \tau_s^k$ est conjugué à $g$. □

(c) Montrer que pour tout $g \in S_m$, $\chi(g) \in \mathbf{Z}$. (*Indication :* On pourrait utiliser les deux parties précédentes, le fait que $\chi(g)$ est un entier algébrique et l'exercice 6.)

*Solution.* Soit $n = \mathrm{ord}(g)$. On choisit $\zeta_1, \ldots, \zeta_d$ comme dans (a) et on dénote $\Phi = \{k < n : \mathrm{pgcd}(k, n) = 1\}$. Comme $\chi$ est constant sur les classes de conjugaison de $G$, par (b) on a que $\chi(g^k) = \chi(g)$ pour tout $k \in \Phi$. On obtient :

$$|\Phi|\chi(g) = \sum_{k\in\Phi} \chi(g^k) = \sum_{k\in\Phi} \sum_{j=1}^{d} \zeta_j^k = \sum_{j} \sum_{k\in\Phi} \zeta_j^k.$$

Par l'exercice 6, $\sum_{k\in\Phi} \zeta_j^k \in \mathbf{Z}$ pour tout $j$. On conclut que $\chi(g) \in \mathbf{Q}$ et comme c'est un entier algébrique, c'est un entier. □