Examen (7 janvier 2026)

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

Toutes les réponses doivent être justifiées.

$\mathbf{F}_q$ 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.

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.)

3. (a) Le corps $\mathbf{F}_8$ admet-il un sous-corps isomorphe à $\mathbf{F}_4$?
   (b) Soit $F = \mathbf{Q}(\alpha_1, \dots, \alpha_n)$ où $\alpha_i \in \mathbf{C}, \alpha_i^2 \in \mathbf{Q}$ pour tout i. Montrer 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 $\mathbf{F}_{p^n} = \mathbf{F}_p(\alpha)$.
   (b) Montrer qu'il existe un polynôme irréductible dans $\mathbf{F}_p[x]$ de degré 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 $j \circ i = \mathrm{id}_F$.
   (b) Soit $F \le K \le \overline{F}$ 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 $K[x]$.

6. Soit ζ 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 $\alpha_1, \alpha_2, \dots, \alpha_m$ sont ses racines, alors $s_k(\alpha_1, \dots, \alpha_m) = (-1)^k a_{m-k}$, où s_k est le k-ième polynôme symétrique élémentaire. Commencer avec le cas où ζ est une racine primitive.)

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 $\phi(Z(G)) \subseteq \{\lambda I : \lambda \in \mathbf{C}\}$.
   (b) La représentation ϕ est dite *fidèle* si $\ker\phi = \{e\}$. Montrer que si G admet une représentation irréductible et fidèle, alors $Z(G)$ est cyclique.

8. Soit G un groupe fini et soit χ un caractère de G.

   (a) Montrer que si $g \in G$ avec $\operatorname{ord}(g) = n$, alors il existe des racines n-ièmes de 1 $\zeta_1, \dots, \zeta_d$ telles que
   $$\chi(g^k) = \sum_{j=1}^{d} \zeta_j^k \quad \text{pour tout } k.$$

   (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 $\operatorname{pgcd}(k, \operatorname{ord}(g)) = 1$, alors g et g^k sont conjugués.

   (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.)