Contrôle final - Mercredi 9 janvier 2024

durée : 3 h

Le candidat attachera la plus grande importance à la clarté, à la précision et à la concision de la rédaction. Dans toutes les questions, il sera tenu le plus grand compte de la rigueur de la rédaction.

L'usage de tout document et de tout matériel électronique est interdit.

1 Anneaux et corps

Préambule : Par anneau on entend anneau unitaire. On notera (a) l'idéal engendré par un élément a d'un anneau commutatif. Étant donné une extension finie de corps E/F, le degré de E sur F (c.-à.-d. la dimension de E comme espace vectoriel sur F) sera noté par $[E : F]$.

Exercice 1. (Question de cours) Soit R un anneau intègre.

1. Rappeler la définition d'un idéal premier et d'un idéal maximal de R.
2. Rappeler la définition d'un anneau principal.
3. Montrer que si $R[x]$ est un anneau principal, alors R est un corps.
4. Soit A un anneau principal et $I \neq (0_A)$ un idéal premier de A. Montrer que I est un idéal maximal de A.

Exercice 2. Soit R un anneau commutatif. On suppose que toute suite strictement croissante d'idéaux de R est finie, c.à.d. si

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$$

est une suite infinie d'idéaux de R encastrés, alors il existe un entier $N \geq 1$ tel que $I_n = I_N$ pour tout $n \geq N$.

1. Soit $\varphi : R \to R$ un morphisme d'anneau de R vers R. Montrer que si φ est surjectif, alors φ est injectif. (Indication : On pourra considérer la suite d'idéaux $(I_n)_{n\geq 1}$ où $I_n = \mathrm{Ker}(\varphi^n)$.)
2. Donner un exemple d'un anneau commutatif unitaire A et un morphisme $f : A \to A$ qui est surjectif mais pas injectif.

Solution. 1. On pose $I_n = \mathrm{Ker}(\varphi^n)$. On a donc que $I_n \subseteq I_{n+1}$ pour tout $n \geq 1$. En fait, pour $x \in I_n$ on a que $\varphi^{n+1}(x) = \varphi(\varphi^n(x)) = \varphi(0_R) = 0_R$. Or par hypothèse, il existe $N \geq 1$ tel que $I_n = I_N$ pour tout $n \geq N$. Montrons que φ est injectif. Il suffit de montrer que $\mathrm{Ker}(\varphi) = \{0_R\}$. Soit $a \in \mathrm{Ker}(\varphi)$. Comme φ^N est surjectif, on a que $a = \varphi^N(x)$ pour un certain $x \in R$. On a donc que $0_R = \varphi(a) = \varphi^{N+1}(x)$ et donc $x \in I_{N+1}$. Il s'ensuit que $x \in I_N$, c'est à dire, $a = \varphi^N(x) = 0_R$. □

Solution. 2. Soit A l'ensemble des suites réelles $(a_n)_{n\geq 1}$. Alors A est un anneau unitaire commutatif pour l'addition et le produit de suites. On remarque que A n'est pas intègre (par exemple : $(1, 0, 1, 0, \ldots) \cdot (0, 1, 0, 1, \ldots) = (0, 0, 0, 0, \ldots)$). On considère l'application $\varphi : A \to A$ définie par $(a_1, a_2, a_3, \ldots) \mapsto (a_2, a_3, a_4, \ldots)$. On vérifie aisément que φ est bien un morphisme d'anneau surjectif mais pas injectif. □

Exercice 3. Soient $d_1, d_2 \in \mathbb{Q}$. On suppose que d_1, d_2 et $d_1 d_2$ ne sont pas des carrés, c'est à dire $d_1, d_2, d_1 d_2 \notin \{a^2 : a \in \mathbb{Q}\}$. On considère l'extension $\mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})/\mathbb{Q}$ engendrée par $\sqrt{d_1}$ et $\sqrt{d_2}$. On pose $\alpha = \sqrt{d_1} + \sqrt{d_2} \in \mathbb{C}$.

1. Montrer que $[\mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}) : \mathbb{Q}] = 4$.
2. Déterminer une base de $\mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$ en tant que $\mathbb{Q}$-espace vectoriel.
3. Montrer que $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$. En déduire que $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$.
4. Déterminer un polynôme $f(x) \in \mathbb{Q}[x]$ unitaire et de degré 4 tel que $f(\alpha) = 0$.
5. En déduire que $f(x)$ est le polynôme minimal de α.
6. Déterminer le polynôme minimal de $\sqrt{2} + \sqrt{3}$.

Solution. 1. On a que $\mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}) = \mathbb{Q}(\sqrt{d_1})(\sqrt{d_2})$. Or, $\sqrt{d_1}$ est racine du polynôme $p_1(x) = x^2 - d_1 \in \mathbb{Q}[x]$ et comme d_1 n'est pas un carré, il s'ensuit que $p_1(x)$ est irréductible dans $\mathbb{Q}[x]$ et donc $[\mathbb{Q}(\sqrt{d_1} : \mathbb{Q}] = 2$. On a aussi que $\{1, \sqrt{d_1}\}$ est une base de $\mathbb{Q}(\sqrt{d_1})$ sur $\mathbb{Q}$. On pose $p_2(x) = x^2 - d_2 \in \mathbb{Q}[x] \subseteq \mathbb{Q}(\sqrt{d_1})[x]$. Montrons que $p_2(x)$ est irréductible dans $\mathbb{Q}(\sqrt{d_1})[x]$. Il suffit de montrer que $\sqrt{d_2} \notin \mathbb{Q}(\sqrt{d_1})$. Supposons au contraire que $\sqrt{d_2} \in \mathbb{Q}(\sqrt{d_1})$. Alors $\sqrt{d_2} = a + b\sqrt{d_1}$ avec $a, b \in \mathbb{Q}$. Il s'ensuit que $d_2 = a^2 + b^2 d_1 + 2ab\sqrt{d_1}$ ou encore $a^2 + b^2 d_1 - d_2 + 2ab\sqrt{d_1} = 0$. On a donc que $a^2 + b^2 d_1 - d_2 = 2ab = 0$. Or, si $b = 0$ alors $d_2 = a^2$, une contradiction ; si $a = 0$, alors $d_2 = b^2 d_1$ qui implique $d_1 d_2 = b^2 d_1^2 = (bd_1)^2$, une contradiction. Ayant montré que $\sqrt{d_2} \notin \mathbb{Q}(\sqrt{d_1})$, il s'ensuit que $p_2(x)$ est irréductible dans $\mathbb{Q}(\sqrt{d_1})[x]$ et donc $[\mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}) : \mathbb{Q}(\sqrt{d_1})] = 2$. Finalement,

$$[\mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}) : \mathbb{Q}(\sqrt{d_1})][\mathbb{Q}(\sqrt{d_1} : \mathbb{Q}] = 2 \cdot 2 = 4.$$

□

Solution. 2. On a que $\{1, \sqrt{d_1}\}$ est une base de $\mathbb{Q}(\sqrt{d_1})$ sur $\mathbb{Q}$ et $\{1, \sqrt{d_2}\}$ est une base de $\mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$ sur $\mathbb{Q}(\sqrt{d_1})$. Il s'ensuit que $\{1, \sqrt{d_1}, \sqrt{d_2}, \sqrt{d_1 d_2}\}$ est une base de $\mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$ sur $\mathbb{Q}$. □

Solution. 3. On a que $\alpha = \sqrt{d_1} + \sqrt{d_2} \in \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$ et donc $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$. Pour montrer l'inclusion inverse il suffit de montrer que $\sqrt{d_1} \in \mathbb{Q}(\alpha)$. Or, $(\alpha - \sqrt{d_1})^2 = d_2$, et donc

$$\alpha^2 - 2\alpha\sqrt{d_1} + d_1 = d_2$$

ou encore

$$\sqrt{d_1} = \frac{\alpha^2 + d_1 - d_2}{2\alpha} \in \mathbb{Q}(\alpha).$$

□

Solution. 4. On a montré que $\alpha^2 + d_1 - d_2 = 2\alpha\sqrt{d_1}$. En prenant le carré on a

$$\alpha^4 + 2(d_1 - d_2)\alpha^2 + (d_1 - d_2)^2 = 4\alpha^2 d_1$$

ou encore

$$\alpha^4 - 2(d_1 + d_2)\alpha^2 + (d_1 - d_2)^2 = 0$$

qui montre que α est racine du polynôme $f(x) = x^4 - 2(d_1 + d_2)x^2 + (d_1 - d_2)^2 \in \mathbb{Q}[x]$. □

Solution. 5. On pose $m_\alpha(x) \in \mathbb{Q}[x]$ le polynôme minimal de α dans $\mathbb{Q}[x]$. On a que $m_\alpha(x)$ est un polynôme unitaire et $m_\alpha(\alpha) = 0$. De plus, le degré de $m_\alpha(x)$ est égal à $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$. Il s'ensuit que $m_\alpha(x) = f(x)$.

□

Solution. 6. Par application des question précédentes avec $d_1 = 2$ et $d_2 = 3$ on trouve que le polynôme minimal de $\sqrt{2}+\sqrt{3}$ est $x^4 - 2(2+3)x^2 + (2-3)^2 = x^4 - 10x^2 + 1$. □

Exercice 4. Soit $F = \mathbb{F}_q$ un corps fini de cardinalité $q \geq 2$. On note $0 = 0_F$ et $1 = 1_F$. Soit E une extension de F de degré p avec p premier. Le but de cet exercice sera de déterminer le nombre de polynômes irréductibles unitaires de degré p dans $F[x]$. On pose $g(x) = x^{q^p} - x \in F[x]$.

1. Déterminer la cardinalité du corps E.
2. En déduire que $g(a) = 0$ pour tout $a \in E$.
3. En déduire que E est un corps de décomposition de $g(x)$ et que le polynôme $g(x)$ admet q^p racines distinctes.
4. Montrer que $g(x)$ peut s'écrire comme un produit
$$g(x) = f_1(x)f_2(x)\cdots f_r(x) \qquad (*)$$
avec $f_i(x) \in F[x]$ irréductible et unitaire pour chaque $1 \leq i \leq r$.
5. En déduire que $f_i(x) \neq f_j(x)$ pour $1 \leq i < j \leq r$ et que le degree de $f_i(x)$ est 1 ou p pour tout $1 \leq i \leq r$.
6. Montrer que $x - a \in F[x]$ divise $g(x)$ pour tout $a \in F$.
7. Soit $f(x) \in F[x]$ un polynôme irréductible unitaire de degré p. Montrer que $f(x)$ divise $g(x)$.
8. En utilisant que la somme des degrés des $f_i(x)$ dans (*) est égal à le degré de $g(x)$, déduire que le nombre de polynômes irréductibles unitaires de degré p dans $F[x]$ est $\frac{q^p-q}{p}$.

Solution. 1. Comme l'extension E/F est de degré p, il s'ensuit qu'il existe une base $\{e_1, e_2, \ldots, e_p\}$ de E sur F de cardinalité p. Or, tout élément $x \in E$ peut s'écrire de manière unique sous la forme $x = a_1e_1 + a_2e_2 + \cdots + a_pe_p$ avec les $a_i \in F$. Ainsi le cardinal de E est q^p. □

Solution. 2. Par application du théorème de Lagrange au group multiplicatif $E^* = E\setminus\{0\}$ qui est d'ordre $q^p - 1$, il s'ensuit que $a^{q^p-1} = 1$ pour tout $a \in E^*$ et donc $a^{q^p} = a$ pour tout $a \in E^*$. D'autre part on a aussi que $a^{q^p} = a$ pour $a = 0$ et donc $a^{q^p} = a$ pour tout $a \in E$ qui montre que tout élément de E est racine du polynôme $g(x)$. □

Solution. 3. On vient de montrer que $g(x)$ admet q^p racines (distinctes) dans le corps E. Or, comme $g(x)$ est de degré q^p, il s'ensuit que E contient toutes les racines de $g(x)$ et donc $g(x)$ est scindé sur E. De plus E est une extension minimale de F contenant toutes les racines de $g(x)$. Il s'ensuit que E est un corps de décomposition de $g(x)$. □

Solution. 4. Comme $F[x]$ est un anneau factoriel, on a que $g(x) \in F[x]$ peut s'écrire comme un produit $g(x) = g_1(x)g_2(x)\cdots g_r(x)$ avec les $g_i(x)$ irréductibles. Or, pour tout $1 \leq i \leq r$, on peut écrire $g_i(x) = a_i f_i(x)$ avec $a_i \in F$ et $f_i(x)$ unitaire et irréductible (car $g_i(x)$ est irréductible). On a donc $g(x) = af_1(x)f_2(x)\cdots f_r(x)$ avec $a = a_1a_2\cdots a_r$. Comme les polynômes $g(x)$ et $f_1(x)f_2(x)\cdots f_r(x)$ sont unitaires, il s'ensuit que $a = 1$. □

Solution. 5. Par application de la question 3., toute racine de $g(x)$ est de multiplicité 1 et donc $f_i(x) \neq f_j(x)$ pour $i \neq j$. Pour $1 \leq i \leq r$, on a que le polynôme $f_i(x)$ admet une racine $\alpha_i \in E$. En fait, comme $f_i(x) \in F[x] \subseteq E[x]$, il existe une extension E'/E contenant une racine α_i de $f_i(x)$ (il suffit de prendre E' un corps de rupture de $f_i(x) \in E[x]$). Mais dans $E[x]$ on a que $g(x) = \prod_{e\in E}(x - e)$ et donc dans E' on a que $0 = g(\alpha_i) = \prod_{e\in E}(\alpha_i - e)$. Il s'ensuit que $\alpha_i - e = 0$ pour un certain $e \in E$, qui montre que $\alpha_i \in E$. De plus, comme $f_i(x)$ est unitaire et irréductible, il s'ensuit que $f_i(x)$ est le polynôme minimal de $\alpha_i \in E$ et donc $[F(\alpha_i) : F] = \deg f_i(x)$. D'autre part, $[F(\alpha_i) : F]$ divise $[E : F] = p$ et donc $\deg f_i(x) = 1$ ou p. □

Solution. 6. Par application de la question 2 on a que $g(a) = 0$ pour tout $a \in E$ et donc en particulier pour tout $a \in F$. Il s'ensuit que $x - a$ divise $g(x)$. En fait, comme $F[x]$ est un anneau euclidien (résultat de cours), on peut écrire $g(x) = q(x)(x - a) + r$ pour un certain $q(x) \in F[x]$ et $r \in F$. On posant $x = a$ on trouve que $r = 0$. □

Solution. 7. Soit $f(x) \in F[x]$ un polynôme unitaire irréductible de degré p. Soit E'/F un corps de rupture de $f(x)$ contenant une racine α de $f(x)$. Alors on a que $[E' : F] = \deg f(x) = p$. Par application de la question 2. on a que tout $a \in E'$ est racine de $g(x)$. En particulier $g(\alpha) = 0$. Comme $F[x]$ est un anneau factoriel on peut écrire $g(x) = q(x)f(x) + r(x)$ avec $q(x), r(x) \in F[x]$ et $\deg r(x) < p$. En posant $x = \alpha$ on trouve que $r(\alpha) = 0$. Mais comme $f(x)$ est le polynôme minimal de α dans $F[x]$, il s'ensuit que $r(x) = 0$ et donc $f(x)$ divise $g(x)$. □

Solution. 8. Par application des question précédentes on a que i)

$$g(x) = f_1(x)f_2(x)\cdots f_r(x) \qquad (*)$$

avec les $f_i(x) \in F[x]$ irréductibles et unitaires ; ii) $f_i(x) \neq f_j(x)$ pour $1 \leq i < j \leq r$; iii) $\deg f_i(x) = 1$ ou p ; iv) tout polynôme irréductible unitaire de degré 1 ou p apparaît dans la factorisation (*) de $g(x)$. Comme $q^p = \deg g(x) = \sum_{i=1}^{r} \deg f_i(x)$ on a que $q^p = q + pN_p$ où N_p est le nombre de polynômes irréductibles unitaires de degré p dans $F[x]$. Ainsi $N_p = \frac{q^p - q}{p}$. □

2 Représentations de groupes

Préambule : Par *représentation* d'un groupe fini G on entendra un morphism $\rho_V : G \to GL(V)$ où V est un $\mathbb{C}$-espace vectoriel non-nul de dimension finie. La dimension de V est appelée le *degré* de la représentation ρ_V. On note $\mathrm{irrep}(G)$ le nombre de représentations irréductibles de G, à isomorphisme près, et $\mathrm{Conj}(G)$ l'ensemble des classes de conjugaison de G.

Exercice 5. Soit $\rho_V : G \to GL(V)$ une représentation d'un groupe fini G. On note χ_V le caractère de la représentation ρ_V.

1. Soit $g \in G$ un élément d'ordre 4 qui est conjugué à son inverse. Montrer que $\chi_V(g) \in \mathbb{Z}$.
2. Soit $g \in G$ un élément d'ordre 3 qui est conjugué à son inverse. Montrer que $\chi_V(g) \in \mathbb{Z}$ et que $\chi_V(g) \equiv \chi_V(e) \pmod 3$.
3. On considère l'application
$$\det_V : G \to \mathbb{C}^*.$$
définie par $g \mapsto \det \rho_V(g)$. Montrer que $\det_V$ est une représentation de G de degré 1.
4. On suppose que G est un groupe non-abélien. Montrer que si G est *simple* (c'est à dire, les seuls sous-groupes distingués (normaux) de G sont $\{e\}$ et G) alors $\det_V$ est la représentation triviale, c.à.d. $\det_V(g) = 1$ pour tout $g \in G$.

Solution. 1. Pour chaque $x \in G$, l'endomorphisme $\rho_V(x)$ est diagonalisable. Il existe donc une base $\mathcal{B}_V$ de V telle que la matrice de $\rho_V(g)$ relative à la base $\mathcal{B}_V$ est diagonale
$$\begin{pmatrix} \lambda_1 & 0 & \dots & 0 \\ 0 & \lambda_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \lambda_n \end{pmatrix}$$
avec $n = \dim V$. Comme g est un élément d'ordre 4, on a que $\lambda_k^4 = 1$ et donc $\lambda_k \in \{\pm 1, \pm i\}$ pour tout $1 \leq k \leq n$. Or, comme g et g^{-1} sont conjugués, on a que $\chi_V(g) = \chi_V(g^{-1}1)$ et donc
$$\sum_{k=1}^{n} \lambda_k = \chi_V(g) = \chi_V(g^{-1}) = \sum_{k=1}^{n} \lambda_k^{-1} = \sum_{k=1}^{n} \overline{\lambda_k} = \overline{\chi_V(g)}$$
qui montre que $\chi_V(g) \in \mathbb{R}$. Ainsi $\mathrm{Card}\{k : \lambda_k = i\} = \mathrm{Card}\{k : \lambda_k = -i\}$, c'est à dire il y a le même nombre d'occurrences de i et $-i$ sur la diagonale de la matrice $\rho_V(g)$. Il s'ensuit que $\chi_V(g)$ est une somme de ± 1 et donc un nombre entier. □

Solution. 2. De même il existe une base $\mathcal{B}_V$ de V telle que la matrice de $\rho_V(g)$ relative à la base $\mathcal{B}_V$ est diagonale
$$\begin{pmatrix} \lambda_1 & 0 & \dots & 0 \\ 0 & \lambda_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \lambda_n \end{pmatrix}$$

avec $n = \dim V$. Comme g est un élément d'ordre 3, on a que $\lambda_k^3 = 1$ et donc $\lambda_k \in \{1, j, j^2\}$ où $j = \exp \frac{2\pi i}{3}$. Finalement comme g et g^{-1} sont conjugués, on a que $\chi_V(g) = \chi_V(g^{-1})$ et donc comme dans la question précédente, $\chi_V(g) \in \mathbb{R}$. Ainsi, si on pose $r = \text{Card}\{k : \lambda_k = j\}$, alors $r = \text{Card}\{k : \lambda_k = j^2\}$, et donc $\chi_V(g) = rj + rj^2 + (n-2r)1$. Or, comme $1 + j + j^2 = 0$, il s'ensuit que $\chi_V(g) = -r + n - 2r = n - 3r \in \mathbb{Z}$. De plus, $\chi_V(g) = n - 3r = \chi_V(e) - 3r \equiv \chi_V(e) \pmod 3$. □

Solution. 3. Comme l'endomorphisme $\rho_V(g)$ est inversible pour tout $g \in G$, on a que $\det \rho_V(g) \neq 0$ et donc $\det_V(g) \in \mathbb{C}^*$. Montrons que $\det_V$ est un morphisme de groupes : Pour tout $g_1, g_2 \in G$ on a que

$$\det_V(g_1 g_2) = \det(\rho_V(g_1 g_2)) = \det(\rho_V(g_1)\rho_V(g_2)) = \det(\rho_V(g_1))\det(\rho_V(g_2)) = \det_V(g_1)\det_V(g_2).$$

. □

Solution. 4. Comme $\text{Ker}(\det_V) = \{g \in G : \det_V(g) = 1\}$ est un sous-groupe distingué de G et G est supposé être un groupe simple, il s'ensuit que $\text{Ker}(\det_V) = \{e\}$ ou G. Or si $\text{Ker}(\det_V) = \{e\}$ on aurait que $\det_V$ est injectif et donc G serait isomorphe à $\text{Im}(\det_V)$ qui est un sous-groupe de $\mathbb{C}^*$. Mais comme $\mathbb{C}^*$ est abélien, on aurait que G est abélien, une contradiction. On a donc que $\text{Ker}(\det_V) = G$, c'est à dire $\det_V(g) = 1$ pour tout $g \in G$. □

Exercice 6. Soit $\rho_V : G \to GL(V)$ une représentation d'un groupe fini G.

1. Rappeler la définition d'une *sous-représentation* ρ_W de ρ_V.
2. On pose
$$V^G = \{v \in V \,|\, \rho_V(g)(v) = v \text{ pour tout } g \in G\}.$$
Montrer que V^G est une sous-représentation de ρ_V.
3. On considère l'application
$$\pi_V : V \to V.$$
définie par
$$\pi_V(v) = \sum_{g \in G} \rho_V(g)(v).$$
Montrer que l'application π_V est une projection G-linéaire de V vers V^G.
4. On pose $G = C_4 =< g : g^4 = e >$ le groupe cyclique d'ordre 4 et on considère la représentation ρ_V de G définie par
$$\rho_V(g) = \begin{pmatrix} i & 0 & 0 \\ i-1 & 1 & 0 \\ i-1 & 0 & 1 \end{pmatrix}$$
Il sera admit que ρ_V est bien une représentation de G de degré 3. Déterminer V^G.
5. Écrire ρ_V comme une somme de représentations irréductibles de G.