UNIVERSITÉ DE BORDEAUX
Théorie de Galois et représentations des groupes finis

Examen, le 19 décembre 2023

Durée 3h. Documents non autorisés

Exercice 1. Le théorème de d'Alembert-Gauss. Le but de cet exercice est de prouver que tout polynôme de degré $\geqslant 1$ à coefficients complexes possède une racine dans $\mathbf{C}$ (et, par conséquent, se décompose en produit de facteurs de degré 1 sur $\mathbf{C}$).

1a) Soit K une extension de degré 2 de $\mathbf{R}$. Prouver que -1 est un carré dans K et en déduire que K est isomorphe à $\mathbf{C}$.

Solution. Il existe $\alpha \in K$ tel que $K = \mathbf{R}[\alpha]$. Comme $[K : \mathbf{R}] = 2$, il existe un polynôme irréductible $f(X) = X^2 + ax + b \in \mathbf{R}[X]$ de degré 2 tel que $f(\alpha) = 0$. Donc

$$\alpha = \frac{-a + \delta}{2},$$

où $\delta^2 = a^2 - 4c$. Ici $a^2 - 4c < 0$, sinon $\delta \in \mathbf{R}$ et $\alpha \in \mathbf{R}$. En écrivant

$$-1 = \frac{\delta^2}{4c - a^2}, \qquad 4c - a^2 \geqslant 0,$$

on voit que $-1 = \beta^2$, $\beta = \delta/\sqrt{4c - a^2} \in K$. Donc, $K = \mathbf{R}[\beta]$, où $\beta^2 + 1 = 0$. On en déduit que

$$K \simeq \mathbf{R}[X]/(X^2 + 1) \simeq \mathbf{C}.$$

1b) Prouver que tout nombre complexe est un carré dans $\mathbf{C}$ et en déduire que $\mathbf{C}$ n'a pas d'extensions finies de degré 2.

Solution. Soit $z \in \mathbf{C}$. On écrit z sous une forme exponentielle $z = r\exp(i\theta)$, $r = |z|$. Alors $\sqrt{r}\exp(i\theta/2) \in \mathbf{C}$ est une racine carré de z. On en déduit que tout polyôme complexe de degré 2 admet une racine dans $\mathbf{C}$. Les mêmes arguments que ceux utilisés dans la question 1), montrent que $\mathbf{C}$ n'a pas d'extensions de degré 2.

Soit $f(X) \in \mathbf{R}[X]$ un polynôme irréductible sur $\mathbf{R}$ de degré $d \geqslant 2$. Soit $L/\mathbf{R}$ un corps de décomposition de $f(X)$. On note n le degré de

$L/\mathbf{R}$ et l'on pose $G = \mathrm{Gal}(L/\mathbf{R})$. Avertissement: on ne peut supposer ni que $d = 2$ ni que L est contenu dans $\mathbf{C}$ car ce sont des conséquences du théorème de d'Alembert-Gauss.

2) Montrer que d et n sont des nombres pairs.

Solution. On montre par l'absurde que d est pair. Supposons que d est impair et que $f(X)$ est unitaire. Alors $\lim_{x\to-\infty} f(X) = -\infty$ et $\lim_{x\to+\infty} f(X) = +\infty$. Par le théorème des valeurs intermédiaires, $f(X)$ admet une racine dans $\mathbf{R}$, ceux qui contredit son irréductibilité. Donc d est pair. Par le théorème de la base télescopique, d divise $n = [L : \mathbf{R}]$.

3) Posons $n = 2^m k$, où k est un nombre impair. En utilisant les théorèmes de Sylow prouver qu'il existe une sous-extension $\mathbf{R} \subset F \subset L$ telle que $[F : \mathbf{R}] = k$. Montrer ensuite que $k = 1$ et, par conséquent, $n = 2^m$.

Solution. Par le premier théorème de Sylow, $G = \mathrm{Gal}(L/\mathbf{R})$ admet un sous-groupe H d'ordre 2^m. Soit $F = L^H$. Par la correspondance de Galois, $[L : F] = 2^m$ et $[F : \mathbf{R}] = k$. Par le théorème de l'élément primitif, $F = \mathbf{R}[\alpha]$, où α est une racine d'un polynôme irréductible de degré k. Il découle maintenant de la question 2) que $k = 1$. Donc $n = 2^m$.

4) Montrer qu'un 2-groupe distinct de $\{e\}$ admet un sous-groupe **distingué** d'ordre 2.

Solution. Soit $\mathcal{G}$ un 2-groupe distinct de $\{e\}$. Alors le centre Z de $\mathcal{G}$ est un sous-groupe non-trivial de $\mathcal{G}$. Soit $z \in Z$ un élément d'ordre 2^a, $a \geqslant 1$. Alors $g = z^{a-1}$ est un élément d'ordre 2 qui commute avec tous les éléments de $\mathcal{G}$. Donc $\langle g\rangle = \{e, g\}$ est un sous-groupe distingué d'ordre 2.

5) Prouver qu'il existe une chaîne d'extensions

$$\mathbf{R} = L_0 \subset L_1 \subset L_2 \subset \cdots \subset L_m = L$$

telle que $[L_{i+1} : L_i] = 2$ pour tout $i = 0, 1, \ldots, m-1$.

Solution. On sait déjà que $|G| = 2^m$. Par la question précédente, G admet un sous groupe distingué H d'ordre 2. Soit $L_{m-1} = L^H$. Alors $[L : L_{m-1}] = 2$ et $L_{m-1}/\mathbf{R}$ est une extension galoisienne de degré 2^{m-1}.

Donc $\mathrm{Gal}(L_{m-1}/\mathbf{R})$ est d'ordre 2^{m-1} et en appliquant le même argument, on montre par récurrence qu'il existe une chaîne d'extensions

$$\mathbf{R} = L_0 \subset L_1 \subset L_2 \subset \cdots \subset L_m = L$$

telle que $[L_{i+1} : L_i] = 2$ pour tout $i = 0, 1, \ldots, m-1$.

6) En déduire que $m = 1$, puis prouver le théorème de d'Alembert-Gauss.

Solution. Par la question 1a), $[L_1 : \mathbf{R}] = 2$ et $L_1 \simeq \mathbf{C}$. Par la question 1b), L_1 n'a pas d'extensions de degré 2, d'où $m = 1$. On a montré que $L = \mathbf{C}$.

Soit M une extension finie de $\mathbf{C}$. Comme $[\mathbf{C} : \mathbf{R}] = 2$, l'extension $M/\mathbf{R}$ est finie. Par le théorème de l'élément primitif, $M = \mathbf{R}[\alpha]$, où α est une racine d'un polynôme irréductible $f(X)$ sur $\mathbf{R}$. Par l'étude précédente, le corps de décomposition L de $f(X)$ coïncide avec $\mathbf{C}$. Donc $M = \mathbf{C}$. On en déduit que chaque polynôme irréductible à coefficients dans $\mathbf{R}$ admet une racine dans $\mathbf{C}$.

Exercice 2. Représentations des groupes d'ordre p^3.

Première partie. Soit p un nombre premier et soit G un groupe *non-abélien* d'ordre p^3.

1) Montrer que le centre $Z(G)$ est un sous-groupe d'ordre p et que le quotient $G/Z(G)$ est abélien.

Solution. Comme G est un p-groupe, $Z(G)$ est un sous-groupe non-trivial de G. On remarque que $|Z(G)| = p^3$ implique $Z(G) = G$ ce qui est impossible car G est non-abélien. Supposons que $|Z(G)| = p^2$. Soit $g \in G \setminus Z(G)$. Alors le sous-groupe $\langle g, Z(G)\rangle$ engendré par $Z(G)$ et g est strictement plus grand que $Z(G)$, d'où on tire que $\langle g, Z(G)\rangle = G$. Comme g commute avec les éléments de $Z(G)$, on en déduit que G est abélien et $Z(G) = G$. Cette contradiction montre que $|Z(G)| \neq p^2$. Donc $|Z(G)| = p$. Le quotient $G/Z(G)$ est un groupe d'ordre p^2. Il est bien connu que tout groupe d'ordre p^2 (p premier) est abélien.

2) Montrer que $[x, y] \in Z(G)$ pour tous $x, y \in G$. En déduire que $[G, G] = Z(G)$.

Solution. On sait que si un groupe quotient G/H est abélien, alors

$[G,G] \subset H$. Par la question 1), $G/Z(G)$ est abélien, d'où $[G,G] \subset Z(G)$. D'autre part, $[G,G] \neq \{e\}$. Comme $|Z(G)| = p$ (p premier), on en déduit que $[G,G] = Z(G)$.

3) Montrer que G a exactement p^2 représentations complexes de degré 1 (à isomorphisme près).

Solution. Les représentations complexes de degré 1 (à isomorphisme près) sont en bijection avec le groupe $\mathrm{Hom}(G/[G,G], \mathbf{C}^*)$ d'ordre

$$|G/[G,G]| = |G/Z(G)| = p^2.$$

4) Montrer que G a exactement $p-1$ représentations complexes irréductibles de degré > 1 (à isomorphisme près) et que ces représentations sont toutes de degré p. Indication : vous pouvez utiliser le fait (démontré en TD) que le degré d'une représentation irréductible divise l'ordre du groupe.

Solution. D'après un théorème de cours,

$$\sum_{\chi \in \mathrm{Irr}(G} n_\chi^2 = p^3,$$

où n_χ est le degré des représentations irréductibles associées à un caractère χ. Comme n_χ divise p^3, on voit que $n_\chi \neq p^2, p^3$. Donc

$$\begin{aligned}&(\text{nombre de représentations de degré } 1)+\\ &\qquad p^2(\text{nombre de représentations de degré } p) = p^3.\end{aligned}$$

Comme G a exactement p^2 représentations de degré 1, on en déduit que

$$p^2(\text{nombre de représentations de degré } p) = p^3 - p^2,$$

d'où l'assertion voulue.

Deuxième partie. On pose $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$ et on considère le groupe multiplicatif matriciel

$$H = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \middle| \, a, b, c \in \mathbf{F}_p \right\}.$$

On note V l'espace vectoriel $C(\mathbf{F}_p, \mathbf{C})$ des fonctions $f : \mathbf{F_p} \to \mathbf{C}$. Rappelons que cet espace est muni de la base canonique $\{f_m\}_{m\in\mathbf{F}_p}$:

$$f_m(x) = \begin{cases} 1, & \text{si } x = m, \\ 0, & \text{sinon.} \end{cases}$$

Soit $\zeta \neq 1$ une racine complexe de l'unité d'ordre p. On considère l'application

$$\rho^{(\zeta)} : H \to \mathrm{GL}(V),$$

$$\rho^{(\zeta)}_\sigma(f)(x) := \zeta^{cx-b} f(x-a), \qquad \sigma = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}.$$

5) Montrer que $\rho^{(\zeta)}$ est un morphisme de groupes.

Solution. Soient

$$\sigma_1 = \begin{pmatrix} 1 & a_1 & b_1 \\ 0 & 1 & c_1 \\ 0 & 0 & 1 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 1 & a_2 & b_2 \\ 0 & 1 & c_2 \\ 0 & 0 & 1 \end{pmatrix}.$$

Alors

$$\sigma_1\sigma_2 = \begin{pmatrix} 1 & a_1+a_2 & b_1+b_2+a_1c_2 \\ 0 & 1 & c_1+c_2 \\ 0 & 0 & 1 \end{pmatrix},$$

et

$$\rho^{(\zeta)}_{\sigma_1\sigma_2}(f)(x) = \zeta^{(c_1+c_2)x-(b_1+b_2+a_1c_2)} f(x-(a_1+a_2)).$$

D'autre part,

$$\rho^{(\zeta)}_{\sigma_1} \circ \rho^{(\zeta)}_{\sigma_2}(f)(x) = \rho^{(\zeta)}_{\sigma_1}(\zeta^{c_2x-b_2} f(x-a_2)) =$$
$$= \zeta^{c_1x-b_1}\zeta^{c_2(x-a_1)-b_2} f(x-a_1-a_2) = \zeta^{(c_1+c_2)x-(b_1+b_2+a_1c_2)} f(x-(a_1+a_2)).$$

Donc $\rho^{(\zeta)}_{\sigma_1\sigma_2}(f) = \rho^{(\zeta)}_{\sigma_1} \circ \rho^{(\zeta)}_{\sigma_2}(f)$.

6) Expliciter l'action de $\rho^{(\zeta)}_\sigma$ sur la base $\{f_m\}_{m\in\mathbf{F}_p}$.

Solution. On a

$$\rho^{(\zeta)}_\sigma(f_m)(x) = \zeta^{cx-b} f_m(x-a) = \begin{cases} \zeta^{c(a+m)-b}, & \text{si } x = a+m, \\ 0, & \text{sinon.} \end{cases}$$

Donc $\rho^{(\zeta)}_\sigma(f_m) = \zeta^{c(a+m)-b} f_{a+m}$.

7) On note χ_ζ le caractère de la représentation $\rho^{(\zeta)}$. Montrer que

$$\chi_\zeta(\sigma) = \begin{cases} p\zeta^{-b}, & \text{si } a = c = 0, \\ 0, & \text{sinon.} \end{cases}$$

Indication : calculer d'abord $\sum_{x \in \mathbf{F}_p} \zeta^x$.

Solution. On a

$$\sum_{x \in \mathbf{F}_p} \zeta^x = \sum_{n=0}^{p-1} \zeta^n = \frac{\zeta^p - 1}{\zeta - 1} = 0.$$

Si $a = c = 0$, on a $\rho_\sigma^{(\zeta)}(f_m) = \zeta^{-b} f_m$. Donc la matrice de $\rho_\sigma^{(\zeta)}$ dans la base $\{f_m\}_{m \in \mathbf{F}_p}$ est $\zeta^{-b} I_p$, où I_p désigne la matrice identité. Donc $\chi_\zeta(\sigma) = p\zeta^{-b}$. Si $a \neq 0$, la diagonale de la matrice de $\rho_\sigma^{(\zeta)}$ dans la base $\{f_m\}_{m \in \mathbf{F}_p}$ est nulle et $\chi_\zeta(\sigma) = 0$. Si $a = 0$ et $c \neq 0$, alors $\rho_\sigma^{(\zeta)}(f_m) = \zeta^{cm-b} f_m$ et

$$\chi_\zeta(\sigma) = \sum_{m \in \mathbf{F}_p} \zeta^{cm-b} = \zeta^{-b} \sum_{m \in \mathbf{F}_p} \zeta^{cm} = \zeta^{-b} \sum_{m \in \mathbf{F}_p} \zeta^m = 0$$

(la multiplication par $c \neq 0$ est une bijection de $\mathbf{F}_p$ sur $\mathbf{F}_p$).

8) Montrer que $\rho^{(\zeta)}$ est irréductible.

Solution. On a

$$\langle \chi_\zeta, \chi_\zeta \rangle = \frac{1}{|H|} \sum_{\sigma \in H} \chi_\zeta(\sigma) \overline{\chi_\zeta(\sigma)} = \frac{1}{p^3} \sum_{b \in \mathbf{F}_p} p\zeta^{-b} \overline{p\zeta^{-b}} = \frac{1}{p^3} \sum_{b \in \mathbf{F}_p} p^2 = 1.$$

Donc $\rho^{(\zeta)}$ est irréductible.

9) Donner la liste des représentations irréductibles de degré > 1 de H à isomorphisme près.

Solution. Les formules de la question 7) montrent que les caractères χ_ζ où $\zeta \neq 1$ parcourt $p-1$ racines primitives de l'unité d'ordre p, sont deux à deux distincts. Donc les représentations $\rho^{(\zeta)}$ sont deux à deux non isomorphes. Comme le nombre de représentations irréductibles de H de degré p est égal à $p-1$ (cf. question 4), on en déduit que $\rho^{(\zeta)}$ donnent toutes les représentations irréductibles de H de degré > 1.

10) Question bonus. Décrire la structure du groupe $H/[H,H]$ et donner la liste des représentations de degré 1 de H (à isomorphisme près).

Solution. Un calcul direct montre que

$$[\sigma_1, \sigma_2] := \sigma_1\sigma_2\sigma_1^{-1}\sigma_2^{-1} = \begin{pmatrix} 1 & 0 & a_1c_2 - a_2c_1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

On en déduit que

$$[H, H] = \left\{ \begin{pmatrix} 1 & 0 & x \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \middle| \, x \in \mathbf{F}_p \right\}.$$

Pour toute matrice $\sigma \in H$, la matrice σ^p est de la forme

$$\sigma^p = \begin{pmatrix} 1 & 0 & \star \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \in [H, H].$$

Comme le groupe $H/[H, H]$ est abélien d'ordre p^2 on en déduit que $H/[H, H] \simeq \mathbf{Z}/p\mathbf{Z} \oplus \mathbf{Z}/p\mathbf{Z}$ et les classes

$$A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot [H, H], \qquad B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \cdot [H, H]$$

sont des générateurs de $H/[H, H]$. Les représentations de degré 1 de $H/[H, H]$ sont les caractères de $H/[H, H]$. Chaque caractère $\psi : H/[H, H] \to \mathbf{C}^*$ est complètement défini par les valeurs $\psi(A)$ et $\psi(B)$ qui parcourent les racines complexes de l'unité d'ordre p.

FIN