Patrick Le Meur — Vincent Beck

Examen Mai 2007 - durée : 4h

La qualité de l'argumentation ainsi que sa clarté et sa concision seront prises en compte dans la notation.

Les résultats introduits dans une définition ou par les mentions "On remarquera que ...", "On admettra que ..." ou "Rappelons que ..." peuvent être utilisés librement et sans démonstration dans toutes les questions qui suivent leur introduction.

L'usage des notes/polycopiés de cours est interdit. L'usage d'appareils electroniques est interdit.

Exercice 1 — Questions diverses.

1. Soit A un anneau principal et soit M un sous A-module de type fini de $\mathrm{F}rac(\mathrm{A})$ (le corps des fractions de A). Que dire de M ?
2. Soit k un corps algébriquement clos. Soit M un $k[\mathrm{X}]$-module de type fini. Donner une condition nécessaire et suffisante simple sur M pour que M soit de torsion.
3. Soit k un corps, soit E un k-espace vectoriel de dimension finie et soit $f\colon \mathrm{E} \to \mathrm{E}$ une application linéaire. Supposons qu'il existe $x \in \mathrm{E}$ tel que E est engendré, comme k-espace vectoriel, par $\{f^i(x) \mid i \geqslant 0\}$. Décrire tous les sous-espaces vectoriels de E stables par f.
4. Quels sont les invariants de similitude d'une matrice de taille 2×2 ? de taille 3×3 ?
5. Soit $\mathrm{M} \in \mathrm{M}_n(k)$ où k est un corps. Supposons que M est trigonalisable. Décrire les invariants de similitude de M à partir de la réduction de Jordan de M.
6. Expliquer pourquoi le groupe de Galois d'un polynôme $\mathrm{P} \in \mathbb{Q}[\mathrm{X}]$ de degré 4 ne peut pas être isomorphe au groupe $\mathbb{H}_8$ des quaternions.

Exercice 2 — Caractère linéaire. Soit G un groupe. On dit que $\chi : \mathrm{G} \to \mathbb{C}^\times$ est un caractère linéaire de G si χ est un morphisme de groupes. On note $\widehat{\mathrm{G}}$ l'ensemble des caractères linéaires de G.

1. Montrer que $\widehat{\mathrm{G}}$ est un groupe.
2. Soit $n \in \mathbb{N}$. Déterminer $\widehat{\mathfrak{S}_n}$.
3. Soient $n \in \mathbb{N}$ et C_n un groupe cyclique d'ordre n. Montrer que $\widehat{\mathrm{C}_n} \overset{\text{gr.}}{\simeq} \mathrm{C}_n$.
4. Soient G et H deux groupes. Montrer que $\widehat{\mathrm{G} \times \mathrm{H}} \overset{\text{gr.}}{\simeq} \widehat{\mathrm{G}} \times \widehat{\mathrm{H}}$.
5. Soit G un groupe abélien fini. Montrer que $\widehat{\mathrm{G}} \overset{\text{gr.}}{\simeq} \mathrm{G}$.
6. Montrer que $\widehat{\mathrm{G}}$ est une partie libre de $\mathscr{F}(\mathrm{G}, \mathbb{C})$.

Définition 1 — Discriminant. Soient k un corps, $\mathrm{P} \in k[\mathrm{X}]$ un polynôme de degré n. On note $\alpha_1, \ldots, \alpha_n$ les racines (comptées avec multiplicité) de P dans $\overline{k}$ la cloture algébrique de k. On définit le discriminant de P comme

$$\mathrm{D}(\mathrm{P}) = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2 .$$

C'est un élément de k.

De plus, si P est séparable alors D(P) est un carré dans k si et seulement si $\mathrm{Gal}(\mathrm{P}) \subset \mathfrak{A}_n$.

Exercice 3 — Polynôme de degré 4. Soient k un corps et $\mathrm{P} = \mathrm{X}^4 + a\mathrm{X}^3 + b\mathrm{X}^2 + c\mathrm{X} + d \in k[\mathrm{X}]$ un polynôme irréductible de degré 4. On suppose $\operatorname{car} k \neq 2$ et $\operatorname{car} k \neq 3$ et on note L un corps de décomposition de P sur k.

1. Montrer que $k \subset \mathrm{L}$ est une extension galoisienne. Montrer que P a 4 racines distinctes dans L. On les note $\alpha_1, \alpha_2, \alpha_3, \alpha_4$.
2. On pose $\theta_1 = (\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4) \in \mathrm{L}$, $\theta_2 = (\alpha_1 + \alpha_3)(\alpha_2 + \alpha_4) \in \mathrm{L}$ et $\theta_3 = (\alpha_1 + \alpha_4)(\alpha_3 + \alpha_2) \in \mathrm{L}$ et $\mathrm{Q} = (\mathrm{X} - \theta_1)(\mathrm{X} - \theta_2)(\mathrm{X} - \theta_3) \in \mathrm{L}[\mathrm{X}]$. On dit que Q est la résolvante cubique de P. Montrer que $\mathrm{Q} \in k[\mathrm{X}]$.
3. Calculer les coefficients en X^2 et en X de Q.
4. Comparer les discriminants de P et Q.
5. Montrer que L contient un corps de décomposition de Q sur k. On l'appelle M.

6. Montrer que $\mathrm{M} \subset \mathrm{L}$ est galoisienne et que $k \subset \mathrm{M}$ l'est aussi.
7. Montrer que l'on a la suite exacte de groupe (où l'on explicitera les flèches).

$$1 \longrightarrow \mathrm{Gal}(\mathrm{L} \mid \mathrm{M}) \longrightarrow \mathrm{Gal}(\mathrm{L} \mid k) \longrightarrow \mathrm{Gal}(\mathrm{M} \mid k) \longrightarrow 1$$

8. Démontrer que $\mathrm{Gal}(\mathrm{L} \mid k)$ est divisible par 4. En déduire les cardinaux possibles pour $\mathrm{Gal}(\mathrm{L} \mid k)$.
9. Déterminer les classes de conjugaison de $\mathfrak{S}_4$.
10. Déterminer les sous-groupes de $\mathfrak{S}_4$ à conjugaison près. Lesquels sont transitifs ? Lesquels sont distingués ?
11. Déterminer le nombre de partition d'un ensemble à 4 éléments en parties à deux éléments. En déduire un morphisme surjectif de $\mathfrak{S}_4$ dans $\mathfrak{S}_3$ que l'on note ψ. Déterminer le noyau de ψ.
12. Montrer qu'on a le diagramme commutatif suivant où les lignes sont exactes.

$$\begin{tikzcd}
1 \arrow[r] & \mathrm{Gal}(\mathrm{L} \mid \mathrm{M}) \arrow[r] \arrow[d] & \mathrm{Gal}(\mathrm{L} \mid k) \arrow[r] \arrow[d] & \mathrm{Gal}(\mathrm{M} \mid k) \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & \mathrm{Ker}\,\psi \arrow[r] & \mathfrak{S}_4 \arrow[r, "\psi"] & \mathfrak{S}_3 \arrow[r] & 1
\end{tikzcd}$$

Expliciter les flèches.

13. On suppose que Q est irréductible dans $k[\mathrm{X}]$ et que le discriminant de Q est un carré dans k. Montrer que $\mathrm{Gal}(\mathrm{L} \mid k) = \mathfrak{A}_4$.
14. On suppose que Q est irréductible dans $k[\mathrm{X}]$ et que le discriminant de Q n'est pas un carré dans k. Montrer que $\mathrm{Gal}(\mathrm{L} \mid k) = \mathfrak{S}_4$.
15. On suppose que Q a une seule racine dans k et que P est irréductible dans $\mathrm{M}[\mathrm{X}]$. Montrer que $\mathrm{Gal}(\mathrm{L} \mid k)$ a 8 éléments.
16. On suppose que Q a une seule racine dans k et que P est réductible dans $\mathrm{M}[\mathrm{X}]$. Montrer que $\mathrm{Gal}(\mathrm{L} \mid k) = \mathbb{Z}/4\mathbb{Z}$.
17. On suppose que Q a trois racines dans k alors Montrer que $\mathrm{Gal}(\mathrm{L} \mid k) = (\mathbb{Z}/2\mathbb{Z})^2$.
18. Montrer que les réciproques des questions 13. à 17. sont vraies.
19. On suppose que Q a au moins une racine dans k. Montrer que le discriminant de Q est un carré dans k si et seulement si Q est scindé sur k.

Exercice 4 – Sous-corps de $\mathbb{Q}(\sqrt[15]{2}, j)$. Posons $x := \sqrt[15]{2}$ et $\mathrm{L} := \mathbb{Q}(x, j)$. Le but de cet exercice est de déterminer tous les sous-corps de L.

A) Préliminaires.

1. Calculer le polynôme minimal de x ainsi que celui de j sur $\mathbb{Q}$.
2. Calculer $[\mathrm{L} : \mathbb{Q}]$.
3. En déduire que $\mathbb{Q}(j)$ est l'unique sous-corps de L de degré 2 sur $\mathbb{Q}$.

B) Les automorphismes de L, le corps $\mathrm{L}^{\mathrm{A}ut(\mathrm{L})}$.

1. Justifier que $(\mathrm{L} : \mathrm{L}^{\mathrm{A}ut(\mathrm{L})})$ est une extension galoisienne. Quel est son degré ? Quel est son groupe de Galois ?
2. Soit ζ une racine primitive 5-ème de 1.
   (a) Montrer que $1 + \mathrm{X} + \mathrm{X}^2 + \mathrm{X}^3 + \mathrm{X}^4$ est le polynôme minimal de ζ sur $\mathbb{Q}$.
   (b) En déduire que $\zeta \notin \mathrm{L}$.
3. Soit $\sigma \in \mathrm{A}ut(\mathrm{L})$. Calculer $\sigma(\{j, j^2, x, jx, j^2x\})$.
4. En déduire que $|\mathrm{A}ut(\mathrm{L})| = 6$.
5. Décrire les éléments de $\mathrm{A}ut(\mathrm{L})$ comme des permutations de $\{j, j^2, x, jx, j^2x\}$. En déduire un isomorphisme de groupes $\mathrm{A}ut(\mathrm{L}) \xrightarrow{\sim} \mathcal{S}_3$.
6. Décrire les sous-groupes de $\mathrm{A}ut(\mathrm{L})$.
7. Montrer que $\mathrm{L}^{\mathrm{A}ut(\mathrm{L})} = \mathbb{Q}(x^3)$. **Nous noterons désormais** $k := \mathbb{Q}(x^3)$

8. Calculer le polynôme minimal de x^3 sur $\mathbb{Q}$. En déduire la valeur de $[\mathbb{Q}(x^3) : \mathbb{Q}]$.

C) Les sous-corps de L contenant k

1. Décrire tous les sous-corps de L contenant k. Pour chaque sous-corps, préciser le degré sur $\mathbb{Q}$.

D) Les sous-corps de L ne contenant pas k

Soit $\mathrm{E} \neq \mathbb{Q}$ un sous-corps de L ne contenant pas $k = \mathbb{Q}(x^3)$. Nous avons donc les extensions suivantes :

$$\begin{tikzcd}
 & \mathrm{E}(x^3) \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{Q}(x^3) \arrow[dr, dash] & & \mathrm{E} \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}$$

Nous allons déterminer E à partir de $\mathrm{E}(x^3)$ en distingant plusieurs cas en fonction des valeurs prises par $[\mathrm{E}(x^3) : \mathrm{E}]$ et $[\mathrm{E} : \mathbb{Q}]$.

1. Montrer que $\mathbb{Q}$ et $\mathbb{Q}(x^3)$ sont les seuls sous-corps de $\mathbb{Q}(x^3)$.
2. Calculons $[\mathrm{E}(x^3) : \mathrm{E}]$.
   (a) Montrer que $[\mathrm{E}(x^3) : \mathrm{E}] \in \{2, 3, 5\}$. Soit P le polynôme minimal de x^3 sur E.
   (b) Montrer que $deg(\mathrm{P}) = 5$ (on pourra, par exemple, raisonner par l'absurde).
   (c) En déduire que $[\mathrm{E}(x^3) : \mathrm{E}] = 5$. A quoi P est-il égal ?
3. Montrer que $[\mathrm{E} : \mathbb{Q}] \in \{2, 3, 6\}$.
4. Supposons que $[\mathrm{E} : \mathbb{Q}] = 6$.
   (a) Que vaut $\mathrm{E}(x^3)$?
   (b) Montrer que $x^5, j \in \mathrm{E}$. En déduire E.
   (c) Montrer que $(\mathrm{E} : \mathbb{Q})$ est galoisienne. Décrire son groupe de Galois ainsi que sa classe d'isomorphisme.
   (d) Décrire tous les sous-corps de E.
5. Supposons que $[\mathrm{E} : \mathbb{Q}] = 2$. Que vaut E ?
6. Supposons que $[\mathrm{E} : \mathbb{Q}] = 3$. En déduire que $\mathrm{E}(x^3) = \mathbb{Q}(tx)$ avec $t \in \{1, j, j^2\}$. Conclure que $\mathrm{E} = \mathbb{Q}(t^2x^5)$.
7. Conclure en dessinant le diagramme des sous-corps de $\mathbb{Q}(x, j)$: c'est le graphe dont les sommets sont les sous-corps de $\mathbb{Q}(x, j)$, tel qu'il y a une arête $\begin{array}{c}\mathrm{E}\\ \vert \\ \mathrm{F}\end{array}$ si et seulement si $\mathrm{F} \subseteq \mathrm{E}$ et tel que deux sous-corps de même degré sur $\mathbb{Q}$ se situent sur la même ligne horizontale.
8. Pour chaque corps E introduit dans la question précédente, trouver $\alpha \in \mathrm{E}$ tel que $\mathrm{E} = \mathbb{Q}(\alpha)$.
9. Considérons L comme un $\mathbb{Q}$-espace vectoriel. Calculer les invariants de similitude de l'application $\mathbb{Q}$-linéaire :
$$\begin{array}{rccc} \mu_x : & \mathrm{L} & \to & \mathrm{L} \\ & a & \mapsto & xa \end{array}$$

Exercice 5 – Bases de réseaux d'un espace vectoriel euclidien.

Soit k un corps de caractéristique nulle. Soit V un k-espace vectoriel de dimension finie n.

Définition 2 Pour $n \in \mathbb{N}\backslash\{0\}$, posons $\mathrm{GL}_n(\mathbb{Z}) := \{\mathrm{X} \in \mathrm{M}_n(\mathbb{Z}) \mid (\exists \mathrm{Y} \in \mathrm{M}_n(\mathbb{Z}))\ \mathrm{XY} = \mathrm{YX} = \mathrm{I}_n\}$, où $\mathrm{I}_n \in \mathrm{M}_n(k)$ est la matrice identité. On remarquera que $\mathrm{GL}_n(\mathbb{Z})$ est un sous-groupe de $\mathrm{GL}_n(k)$.

Définition 3 Un **sous-réseau** de V est un sous-groupe Γ du groupe additif $(\mathrm{V}, +)$ tel que Γ est un groupe abélien libre admettant une base $(e_1, \ldots, e_t)$ telle que $e_1, \ldots, e_t$ soient linéairement indépendants (sur k). Un tel t-uplet $(e_1, \ldots, e_t)$ est alors appelé une **$\mathbb{Z}$-base de** Γ.

Dans la situation de la définition précédente, on remarquera que $rg(\Gamma) = t \leqslant dim_k(\mathrm{V})$.

Définition 4 Un **réseau** de V est un sous-réseau Γ de V tel que $rg(\Gamma) = dim_k(\mathrm{V})$. Ainsi, Γ admet, en tant que groupe abélien libre, une base qui est une base du k-espace vectoriel V.

Par exemple, $\mathbb{Z}^2$ est un réseau de $\mathbb{R}^2$. Le sous-groupe $\mathbb{Z} + \mathbb{Z}\sqrt{2} < \mathbb{R}$ est libre de rang 2 et n'est pas un sous-réseau de $\mathbb{R}$.

On remarquera qu'un sous-groupe Γ de $(\mathrm{V}, +)$ est un sous-réseau si et seulement si Γ est réseau du k-espace vectoriel engendré par Γ.

Définition 5 Supposons que $k = \mathbb{R}$, que V est un $\mathbb{R}$-espace vectoriel normé non réduit à 0 et que Γ est un réseau de V. Le réel :

$$\mathrm{M}in_{ar}(\Gamma) := inf\{|x| \mid x \in \Gamma \backslash \{0\}\}$$

est appelé le **minimum arithmétique de** Γ.

Nous admettrons que $\mathrm{M}in_{ar}(\Gamma) > 0$ **et que la borne inférieure de la définition précédente est atteinte.**

A) Préliminaires

1. Soit Γ un sous-groupe de V. Montrer que si Γ est de type fini, alors Γ est un groupe abélien libre.
2. Soit $\mathrm{X} \in \mathrm{M}_n(\mathbb{Z})$, montrer que $\mathrm{X} \in \mathrm{GL}_n(\mathbb{Z})$ si et seulement si $det(\mathrm{X}) = \pm 1$.
3. Soit Γ un sous-réseau de V. Montrer que toute base du groupe abélien libre Γ est une $\mathbb{Z}$-base de Γ (on pourra introduire le sous-espace vectoriel engendré par Γ et utiliser la question précédente).

B) Facteurs directs d'un réseau

Rappelons qu'un sous-groupe Λ d'un groupe abélien Γ est dit **facteur direct de** Γ si et seulement si il existe Λ' un sous-groupe de Γ tel que $\Gamma = \Lambda \oplus \Lambda'$. Rappelons que Λ est facteur direct de G si et seulement si la suite exacte $0 \to \Lambda \to \Gamma \to \Gamma/\Lambda \to 0$ est scindée.

1. Soit Γ un groupe libre de rang fini n, soit $\Lambda < \Gamma$ un sous-groupe, et soient $(a_1, \ldots, a_s)$ les facteurs invariants de Λ par rapport à Γ. Montrer que les conditions suivantes sont équivalentes :
   - (i) Λ est un facteur direct de Γ.
   - (ii) Γ/Λ est libre.
   - (iii) Γ/Λ est sans torsion.
   - (iv) $a_1 = a_2 = \ldots = a_s = 1$.
2. Supposons en outre (dans cette question) que Γ est un réseau d'un k-espace vectoriel V. Montrer que les conditions suivantes sont équivalentes :
   - (i) Λ est un facteur direct de Γ.
   - (ii) $\Lambda = \Gamma \cap \mathrm{V}ect_{\mathbb{Q}}(\Lambda)$.
   - (iii) $\Lambda = \Gamma \cap \mathrm{V}ect_k(\Lambda)$.

C) Image d'un réseau par une application linéaire surjective

Soit $p\colon \mathrm{V} \to \mathrm{W}$ une application linéaire surjective. Notons $\mathrm{F} = \mathrm{K}er(p)$. Soit Γ un réseau de V. Le but de ce paragraphe est de caractériser le fait que $p(\Gamma)$ est un réseau de W.

1. Justifier que $\Gamma \cap \mathrm{F}$ et $p(\Gamma)$ sont des groupes abéliens libres.
2. Montrer qu'il existe une $\mathbb{Z}$-base $(e_1, \ldots, e_n)$ de Γ ainsi qu'un entier $s \in \{0, \ldots, n\}$ tels que $(e_1, \ldots, e_s)$ est une base de $\Gamma \cap \mathrm{F}$ et tels que $(p(e_{s+1}), \ldots, p(e_n))$ est une base de $p(\Gamma)$.
3. Montrer que les conditions suivantes sont équivalentes :
   - (i) $p(\Gamma)$ est un réseau de W.
   - (ii) $\Gamma \cap \mathrm{F}$ est un réseau de F.

(*iii*) $rg(p(\Gamma)) \leqslant \dim_k(\mathrm{W})$.

(*iv*) $rg(\Gamma \cap \mathrm{F}) \geqslant \dim_k(\mathrm{F})$.

(*v*) $rg(p(\Gamma)) = \dim_k(\mathrm{W})$.

(*vi*) $rg(\Gamma \cap \mathrm{F}) = \dim_k(\mathrm{F})$.

D) Algorithme de construction d'une base d'un réseau

Supposons désormais que V est un $\mathbb{R}$-espace vectoriel euclidien non réduit à $\{0\}$, nous noterons $|\,.\,|$ la norme associée. Soit Γ un réseau de V et soit $\Lambda < \Gamma$ un facteur direct de Γ avec $\Lambda \neq \Gamma$. Posons $\mathrm{F} := \mathrm{V}ect_{\mathbb{R}}(\Lambda)$ et $\mathrm{W} := \mathrm{F}^{\perp}$. Soit $p\colon \mathrm{V} \to \mathrm{W}$ la projection orthogonale parallèlement à F.

1. Montrer qu'il existe $v \in \Gamma \backslash \Lambda$ tel que $|p(v)| = \mathrm{M}in_{ar}(p(\Gamma))$.
2. Montrer que $p(\Gamma)$ est un réseau de W.
3. Montrer que $\Lambda + \mathbb{Z}v$ est un groupe abélien libre de rang $rg(\Lambda) + 1$.
4. Montrer que $\Lambda + \mathbb{Z}v$ est un facteur direct de Γ (on pourra auparavant montrer que $\Gamma/(\Lambda + \mathbb{Z}v)$ est sans torsion).

Déduire des questions précédentes un algorithme permettant le calcul d'une base d'un réseau Γ de $\mathrm{V} = \mathbb{R}^n$ (en utilisant le minimum arithmétique).