Université Pierre et Marie Curie - Paris VI — Faculté de Mathématiques
Master Mathématiques et applications — 2015–2016

Algèbre et théorie de Galois

Examen du 15 décembre 2015. Durée 3h00.
Seuls documents autorisés : poly et notes de cours. Smartphones éteints.

Exercice 1. Soit A un anneau commutatif *noethérien* et B une A-algèbre. Pour un élément $b \in B$, on note $A[b]$ la A-sous-algèbre de B engendrée par b. On dit que b est *entier sur* A s'il existe un polynôme *unitaire* $f \in A[X]$ tel que $f(b) = 0$.

i. Montrer que (b est entier sur A) $\Leftrightarrow$ ($A[b]$ est de type fini en tant que A-module).

ii. Si b, b' sont entiers sur A, montrer que $A[b, b']$ est de type fini en tant que A-module.

iii. Montrer que l'ensemble des éléments $b \in B$ entiers sur A est un sous-anneau de B. On l'appelle *clôture intégrale de A dans B.*

Exercice 2. Posons $\delta := \det((X_i^{j-1})_{1\leqslant i,j\leqslant n}) \in \mathbb{Z}[X_1, \cdots, X_n]$.

i. Écrivons $\delta = \sum_{\nu\in\mathbb{N}^n} a_\nu X^\nu$. Montrer que $a_\nu \neq 0 \Rightarrow \sum_{i=1}^n \nu_i = n(n-1)/2$.

ii. Montrer que $X_i - X_j$ divise δ pour tout $i \neq j$.

iii. Montrer que $\delta = \pm \prod_{1\leqslant i<j\leqslant n}(X_i - X_j)$. Déterminer le signe.

Exercice 3. Soit $K \supset \mathbb{Q}$ une extension finie. On note $\mathcal{O}_K$ la clôture intégrale de $\mathbb{Z}$ dans K au sens de l'exercice 1. On l'appelle l'*anneau des entiers de K.*

i. Pour $\alpha \in K$ de polynôme minimal $f_\alpha \in \mathbb{Q}[X]$, montrer que $\alpha \in \mathcal{O}_K \Leftrightarrow f_\alpha \in \mathbb{Z}[X]$. En déduire que $\mathcal{O}_\mathbb{Q} = \mathbb{Z}$ et $\mathcal{O}_K \cap K' = \mathcal{O}_{K'}$ si $K' \subset K$.

ii. Supposons $K = \mathbb{Q}(\sqrt{d})$ avec $d \in \mathbb{Z}$ sans facteur carré. Montrer que si $\alpha = a + b\sqrt{d}$ avec $b \neq 0$, alors $f_\alpha = X^2 - 2aX + (a^2 - db^2)$. En déduire que

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{si } d \equiv 2, 3 \pmod 4 \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & \text{si } d \equiv 1 \pmod 4 \end{cases}$$

iii. Revenons au cas général. Montrer que $\forall \alpha \in K$, $\exists n \in \mathbb{N}^*$ tel que $n\alpha \in \mathcal{O}_K$. En déduire qu'on peut trouver $\alpha \in \mathcal{O}_K$ tel que $K = \mathbb{Q}(\alpha)$.

TSVP

iv. Supposons $K \supset \mathbb{Q}$ galoisienne de groupe G et posons $n := [K : \mathbb{Q}]$.

(a) Montrer que $\mathcal{O}_K$ est stable sous G et $(\mathcal{O}_K)^G = \mathbb{Z}$. En déduire que $\forall \alpha \in \mathcal{O}_K$, on a $\mathrm{tr}(\alpha) := \sum_{\sigma \in G} \sigma(\alpha) \in \mathbb{Z}$.

(b) Soit α tel que $K = \mathbb{Q}(\alpha)$ et $\sigma_1, \cdots, \sigma_n$ une numérotation de G. Utiliser l'exercice 2 pour montrer que la matrice $(\sigma_j(\alpha^{i-1}))_{1 \leqslant i,j \leqslant n}$ est inversible. En déduire que G est un ensemble linéairement indépendant du K-ev $\mathrm{Hom}_{\mathbb{Q}-\mathrm{ev}}(K, K)$.

(c) Soit $\alpha \in \mathcal{O}_K$ tel que $K = \mathbb{Q}(\alpha)$. Considérons l'application $\mathbb{Q}$-linéaire

$$T : \ K \longrightarrow \mathbb{Q}^n, \ \ x \mapsto (\mathrm{tr}(x), \mathrm{tr}(\alpha x), \cdots \mathrm{tr}(\alpha^{n-1} x)).$$

Montrer que T est injective. En déduire que $\mathcal{O}_K$ est un $\mathbb{Z}$-module de type fini, puis qu'il est libre de rang n sur $\mathbb{Z}$.

v. Montrer en général que $\mathcal{O}_K$ est un $\mathbb{Z}$-module libre de rang $[K : \mathbb{Q}]$.

Rappel. Dans les deux exercices suivants, on pourra utiliser le résultat suivant vu en TD : si $f \in \mathbb{Z}[X]$ est unitaire séparable de réduction $\overline{f} \in \mathbb{F}_p[X]$ séparable, alors il existe un élément $\sigma_p \in G_f$ et une bijection

$$R := \{\text{racines de } f \text{ dans } \overline{\mathbb{Q}}\} \xrightarrow{\sim} \overline{R} := \{\text{racines de } \overline{f} \text{ dans } \overline{\mathbb{F}}_p\}$$

telle que la permutation $\alpha \mapsto \sigma_p(\alpha)$ de R corresponde à la permutation $\overline{\alpha} \mapsto \overline{\alpha}^p$ de $\overline{R}$.

Exercice 4. Soit $n \geqslant 2$ un entier et p, q deux premiers distincts.

i. Montrer qu'il existe un polynôme unitaire $f \in \mathbb{Z}[X]$ de degré n tel que $(f \bmod p)$ soit irréductible dans $\mathbb{F}_p[X]$ et $(f \bmod q)$ soit séparable et égal au produit d'un polynôme irréductible de degré 2 et d'un polynôme scindé dans $\mathbb{F}_q[X]$.

ii. Pour un tel f, montrer que $G_f = \mathfrak{S}_n$.

Exercice 5. Soit $f = X^5 + 20X - 16 \in \mathbb{Q}[X]$.

i. Montrer que f est irréductible et que G_f contient un 5-cycle.

ii. En réduisant modulo 7, montrer que G_f contient un 3-cycle.

iii. Montrer que la conjugaison complexe induit un élément non-trivial de G_f. En conclure que $|G_f|$ est divisible par 30.

iv. Montrer que G_f est contenu dans $\mathfrak{A}_5$.

v. Après avoir montré que tout sous-groupe d'indice 2 d'un groupe fini est distingué, en conclure que $G_f = \mathfrak{A}_5$.