Examen 2018/2019
4M002 - Algèbre et théorie de Galois
Anna Cadoret

Avertissement.

Sont autorisés: le polycopié du cours, les notes manuscrites du cours et des travaux dirigés , les dictionnaires de langues papier.

Les réponses peuvent être rédigées en français ou en anglais. Elles doivent être *soigneusement justifiées*. Vous pouvez bien sûr admettre certaines questions.

Exercice 1.

(1) On rappelle qu'une $\mathbb{Z}$-module M est dit de torsion si pour tout $m \in M$ il existe $0 \neq a \in \mathbb{Z}$ tel que $am = 0$. Montrer q'un $\mathbb{Z}$-module M est de torsion si et seulement si $M \otimes_{\mathbb{Z}} \mathbb{Q} = 0$.

(2) On note $S := \mathbb{Z} \setminus \{0\}$ et on rappelle que le corps des fractions $\mathbb{Q}$ de $\mathbb{Z}$ est par définition le localisé $S^{-1}\mathbb{Z}$ de $\mathbb{Z}$ en S. Soit M un $\mathbb{Z}$-module. Montrer qu'on a un isomorphisme canonique de $\mathbb{Q}$-modules

$$M \otimes_{\mathbb{Z}} \mathbb{Q} \tilde{\to} S^{-1}M.$$

(3) Montrer que si

$$0 \to M' \stackrel{u}{\to} M \stackrel{v}{\to} M'' \to 0$$

est une suite exacte de $\mathbb{Z}$-modules la suite

$$0 \to M' \otimes_{\mathbb{Z}} \mathbb{Q} \stackrel{u\otimes Id}{\to} M \otimes_{\mathbb{Z}} \mathbb{Q} \stackrel{v\otimes Id}{\to} M'' \otimes_{\mathbb{Z}} \mathbb{Q} \to 0$$

est une suite exacte de $\mathbb{Q}$-espaces vectoriels. On pourra montrer dans l'ordre que:
- $v \otimes Id : M \otimes_{\mathbb{Z}} \mathbb{Q} \to M'' \otimes_{\mathbb{Z}} \mathbb{Q}$ est surjective;
- $im(u \otimes Id) \subset \ker(v \otimes Id)$;
- $\ker(v \otimes Id) \subset im(u \otimes Id)$;
- $u \otimes Id : M' \otimes_{\mathbb{Z}} \mathbb{Q} \to M \otimes_{\mathbb{Z}} \mathbb{Q}$ est injective.

(4) Soit V un $\mathbb{Q}$-espace vectoriel de dimension finie et

$$0 \to V' \stackrel{u}{\to} V \stackrel{v}{\to} V'' \to 0$$

une suite exacte courte de K-espaces vectoriels. Montrer que $dim(V) = dim(V') + dim(V'')$. Cela vous rappelle-t-il un résultat classique d'algèbre linéaire?

(5) Soit M un $\mathbb{Z}$-module de type fini. Montrer que le rang de M est égal à la $\mathbb{Q}$-dimension de $M \otimes_{\mathbb{Z}} \mathbb{Q}$.

(6) Déduire des questions précédentes que si

$$0 \to M' \to M \to M'' \to 0$$

est une suite exacte de $\mathbb{Z}$-modules $rang(M) = rang(M') + rang(M'')$.

(7) Les résultats des questions précédentes se généralisent-ils à des anneaux plus généraux que $\mathbb{Z}$? Si oui, lesquels?

(8) Soit $M := \{(a, b, c) \in \mathbb{Z}^3 \mid 2|a + b + c\} \subset \mathbb{Z}^3$. Montrer que M est un sous-$\mathbb{Z}$-module libre de rang ≤ 3 et que $\mathbb{Z}^3/M \simeq \mathbb{Z}/2$. En déduire que M est de rang 3 et donner une $\mathbb{Z}$-base de M.

Exercice 2. Soit K un corps de caractéristique $p > 0$. L'objectif des questions (1) à (3) est de montrer que toute extension galoisienne L/K de degré p est de la forme $L = K[T]/\langle T^p - T - a\rangle$ avec $T^p - T - a \in K[T]$ irréductible. La question (4) est indépendante.

(1) Soit $\overline{K}$ une clôture algébrique de K et soit $a \in K$. Montrer que le polynôme $T^p - T - a \in K[T]$ est séparable et que si $\alpha \in \overline{K}$ est une racine de $T^p - T - a$, les racines des $T^p - T - a$ sont les $\alpha + n$, $n \in \mathbb{F}_p$.

(2) En déduire que:
- soit $T^p - T - a$ a une racine dans K, auquel cas il est totalement décomposé sur K;
- soit $T^p - T - a$ est irréductible sur K, auquel cas $L = K[T]/\langle T^p - T - a\rangle$ est une extension galoisienne cyclique de degré p (donc cyclique) de K.

(3) Inversement, soit L/K une extension galoisienne de degré p donc cyclique. Soit $\sigma \in Gal(L/K)$ un générateur. On introduit l'endormorphisme K-linéaire $\epsilon := Id - \sigma : L \to L$.

(a) Déterminer le noyau de ϵ.
(b) Calculer ϵ^p.
(c) En déduire que $\ker(\epsilon) \subsetneq \ker(\epsilon^2)$.
(d) Soit $x \in \ker(\epsilon^2) \setminus \ker(\epsilon)$ et $\alpha := \frac{x}{\epsilon(x)}$. Montrer que $\alpha \notin K$ mais que $\alpha^p - \alpha \in K$. Déterminer le polynôme minimal de α sur K.
(e) En déduire que $L = K(\alpha)$.

(4) On note $F : K \to K$, $x \to x^p$ le Frobenius.

(a) Montrer que si $F : K \to K$ est surjectif toute extension algébrique de K est automatiquement séparable.
(b) Si $F(K) \subsetneq K$, montrer que pour tout $a \in K \setminus F(K)$ le polynôme $T^p - a \in K[T]$ est irréductible sur K.
(c) Donner un exemple de corps K possedant une extension non galoisienne de degré p.

Exercice 3. On note $a = 5 + \sqrt{21}$, $\alpha = \sqrt{a}$, $b = 5 - \sqrt{21}$, $\beta = \sqrt{b}$.

(1) Déterminer le polynôme minimal de a sur $\mathbb{Q}$. Montrer que $\mathbb{Q}(a)/\mathbb{Q}$ est une extension galoisienne et déterminer son groupe de Galois.

(2) Déterminer les polynômes minimaux de α et β sur $\mathbb{Q}(a)$.

(3) Calculer $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ et déterminer le polynôme minimal de α sur $\mathbb{Q}$.

(4) Montrer que $\beta \in \mathbb{Q}(\alpha)$.

(5) Montrer que $\mathbb{Q}(\alpha)/\mathbb{Q}$ est galoisienne.

(6) Montrer qu'on a un morphisme de groupes surjectif $Gal(\mathbb{Q}(\alpha)/\mathbb{Q}) \to Gal(\mathbb{Q}(a)/\mathbb{Q})$. Déterminer son noyau.

(7) Exhiber deux éléments distincts d'ordre 2 de $Gal(\mathbb{Q}(\alpha)/\mathbb{Q})$.

(8) Déterminer $Gal(\mathbb{Q}(\alpha)/\mathbb{Q})$.

(9) Déterminer tous les sous-corps de $\mathbb{Q}(\alpha)$ (on pourra calculer $(\alpha + \beta)^2$ et $(\alpha - \beta)^2$).

anna.cadoret@imj-prg.fr
IMJ-PRG- Sorbonne Université.