Examen 2ème Session 2019/2020
MU4MA002 - Algèbre et théorie de Galois
Anna Cadoret

Avertissement.

Les réponses peuvent être rédigées en français ou en anglais.

Le sujet est long; le barême sera adapté en conséquence. Prenez donc le temps de *justifier soigneusement* vos réponses. Vous pouvez bien sûr admettre certaines questions.

Exercice 1. Dans tout cet exercice A désigne un anneau commutatif intègre. On note K son corps des fractions. On dit qu'un A-module N est injectif s'il vérifie la propriété suivante d'extension des morphismes. Pour tout morphisme injectif de A-modules $u : M' \to M$ et pour tout morphisme de A-modules $f : M' \to N$ il existe un morphisme de A-modules $f_u : M \to N$ tel que $f_u \circ u = f$. Les A-modules injectifs joue un rôle fondamental en cohomologie.

(1) L'objectif de cette question est de montrer que pour vérifier si N est un A-module injectif, on peut se contenter de vérifier la propriété (i) pour les morphismes injectifs de la forme $u : I \hookrightarrow A$, où I est un idéal de A. Autrement dit, on veut montrer que si pour tout idéal I de A et pour tout morphisme de A-modules $f : I \to N$ il existe un morphisme de A-modules $f_u : A \to N$ tel que $f_u \circ u = f$ alors N est injectif. On va vérifier la condition (i). Fixons donc un morphisme injectif de A-modules $u : M' \hookrightarrow M$ et un morphisme de A-modules $f : M' \to N$. On veut montrer qu'il existe un morphisme de A-modules $f_u : M \to N$ tel que $f_u \circ u = f$. Quitte à remplacer M' par $u(M')$, on peut supposer que $M' \subset M$.

   (a) Notons $\mathcal{E}$ l'ensemble des couples $(M^\#, f^\#)$ où $M' \subset M^\# \subset M$ est un sous-A-modules et $f^\# : M^\# \to N$ est un morphisme de A-modules tel que $f^\#|_{M'} = f : M' \to N$. On munit $\mathcal{E}$ de la relation d'ordre partiel $(M_1^\#, f_1^\#) \leq (M_2^\#, f_2^\#)$ si $M_1^\# \subset M_2^\#$ et $f_2^\#|_{M_1^\#} = f_1^\#$. Vérifier que $(\mathcal{E}, \leq)$ est un ensemble ordonné inductif non vide. En déduire qu'il existe $(M^\#, f^\#) \in \mathcal{E}$ tel que pour tout $(M^\flat, f^\flat) \in \mathcal{E}$, $(M^\#, f^\#) \leq (M^\flat, f^\flat)$ implique $(M^\#, f^\#) = (M^\flat, f^\flat)$. On veut montrer que $M^\# = M$. Fixons $m \in M$.

   (b) Soit $I := \{a \in A \mid am \in M^\#\}$. Montrer que I est un idéal de A et que l'application $g : I \to N$ définie par $g(a) = f^\#(am)$ est un morphisme de A-modules.

   (c) En utilisant la question précédente, montrer qu'il existe un morphisme de A-modules $g^\# : M^\# + Am \to N$ tel que $g^\#|_{M^\#} = f^\#$. Conclure.

(2) Montrer que K est un A-module injectif.

(3) On dit qu'un A-module N est divisible si pour tout $0 \neq a \in A$, le morphisme de A-modules $M \to M$, $m \to am$ de translation par a est surjectif. On suppose maintenant que A est un anneau principal et que ce n'est pas un corps.

   (a) Montrer que A n'est jamais un A-module injectif.

   (b) Montrer qu'un A-module N est injectif si et seulement si il est divisible.

   (c) En déduire qu'un A-module de type fini n'est jamais injectif.

   (d) Montrer que tout quotient d'un A-module injectif est injectif.

(4) L'objectif de cette question est de montrer que pour tout A-module M il existe un A-module injectif N et un morphisme innjectif de A-modules $u : M \hookrightarrow N$.

(a) Supposons d'abord que A est principal. Justifier que pour tout A-module M on a un morphisme surjectif $\oplus_{m\in M} A \twoheadrightarrow M$. En considérant l'inclusion canonique $\oplus_{m\in M} A \hookrightarrow \oplus_{m\in M} K$, montrer que M est un sous-A-module d'un quotient de $\oplus_{m\in M} K$. Conclure.

(b) On ne suppose plus A principal. Soit C un $\mathbb{Z}$-module. On note $Hom_{\mathbb{Z}}(A, C)$ l'ensemble des morphismes de $\mathbb{Z}$-modules $\varphi : (A, +) \to C$ que l'on munit de la structure de A-module définie par $a_0 \cdot \varphi : A \to C$, $a \to \varphi(a_0 a)$.

(i) Montrer que si C est un $\mathbb{Z}$-module injectif alors $Hom_{\mathbb{Z}}(A, C)$ est un A-module injectif.

(ii) Soit M un A-module. En appliquant (4) (a), montrer qu'il existe un $\mathbb{Z}$-module injectif C et un morphisme injectif de $\mathbb{Z}$-modules $u : M \hookrightarrow C$. (Indication: observer que pour tout A-module M on a un isomorphisme canonique de $\mathbb{Z}$-modules $Hom_A(M, Hom_{\mathbb{Z}}(A, C)) \tilde{\to} Hom_{\mathbb{Z}}(M, C)$).

(iii) En considérant l'application $M \to Hom_{\mathbb{Z}}(A, C)$, $m \mapsto (a \mapsto u(am))$ conclure.

Exercice 2. Si K/k et L/k sont deux extensions de corps on note $Hom_k(K, L)$ l'ensemble des k-plongements $K \hookrightarrow L$. Soit K/k et L/k deux extensions finies de corps et Ω/k une extension algébriquement close et telle que $Hom_k(K, \Omega) \neq \emptyset$, $Hom_k(L, \Omega) \neq \emptyset$. On se fixe des k-plongements $\iota_K : K \hookrightarrow \Omega$, $\iota_L : L \hookrightarrow \Omega$ et on identifie $K := \iota_K(K) \subset \Omega$, $L := \iota_L \subset \Omega$. On note $K \cdot L \subset \Omega$ le plus petit sous-corps de Ω contenant K, L.

(1) Montrer qu'on a un morphisme canonique surjectif de k-algèbres $c : K \otimes_k L \to K \cdot L$.

(2) On se place dans $\Omega = \mathbb{C}$.

(a) Montrer que pour tout entier $n \geq 1$ le polynôme $T^n - 2$ est irréductible sur $\mathbb{Q}$. On note $K_n := \mathbb{Q}[T]/(T^n - 2)$.

(b) Justifier que $T^n - 2$ a au moins une racine réelle et, si $n \geq 3$, deux racines complexes conjuguées. On note $\sqrt[n]{2}$ l'un des racines réelles de $T^n - 2$. Justifier que les autres racines de $T^n - 2$ sont les $\sqrt[n]{2}\zeta_n^k$, $k = 0, \ldots, n-1$, où ζ_n est une racine primitive $n$ième de l'unité dans $\mathbb{C}$.

(c) Calculer $[\mathbb{Q}(\sqrt[12]{2}) \cdot \mathbb{Q}(\sqrt[8]{2}) : \mathbb{Q}]$ et $[\mathbb{Q}(\sqrt[12]{2}) \cdot \mathbb{Q}(\sqrt[8]{2}\zeta_8) : \mathbb{Q}]$. En déduire que $K \cdot L$ dépend des k-plongements $K \hookrightarrow \Omega$, $L \hookrightarrow \Omega$.

(3) Montrer que les propriétés suivantes sont équivalentes:

(a) $K \otimes_k L$ est un corps;
(b) Le morphisme $c : K \otimes_k L \to K \cdot L$ est un isomorphisme;
(c) $[K \cdot L : k] = [K : k][L : k]$;
(d) $[K \cdot L : L] = [K : k]$,

auquel cas on dit que K/k et L/k sont linéairement disjointes sur k dans Ω. Montrer qu'alors $K \cdot L$ est indépendant des k-plongements $K \hookrightarrow \Omega$, $L \hookrightarrow \Omega$.

(4) Montrer que si $[K : k]$ et $[L : k]$ sont premiers entre eux alors K/k, L/k sont linéairement indépendantes sur k.

(5) Montrer que si K/k, L/k sont linéairement indépendantes sur k alors $K \cap L = k$. Montrer que si K/k est galoisienne, la réciproque est vraie.

(6) Montrer que si K/k, L/k sont linéairement indépendantes sur k et que K/k est galoisienne alors $K \cdot L/L$ est galoisienne et déterminer son groupe de Galois.

(7) Montrer que si K/k, L/k sont galoisiennes et linéairement indépendantes sur k alors $K \cdot L/k$ est galoisienne et déterminer son groupe de Galois.

Exercice 3. On note $\overline{\mathbb{Q}} \subset \mathbb{C}$ la clôture algébrique de $\mathbb{Q}$ dans $\mathbb{C}$ et $\iota : \overline{\mathbb{Q}} \tilde{\to} \overline{\mathbb{Q}}$ la restriction de la conjugaison complexe à $\overline{\mathbb{Q}}$. Soit k une extension finie de $\mathbb{Q}$. Le groupe $Aut(\overline{\mathbb{Q}})$ des automorphismes de corps de $\overline{\mathbb{Q}}$ agit naturellement sur l'ensemble $Hom(k, \overline{\mathbb{Q}})$ des morphismes de corps $k \hookrightarrow \overline{\mathbb{Q}}$ par $\sigma \cdot \rho = \sigma \circ \rho$, $\sigma \in Aut(\overline{\mathbb{Q}}$, $\rho \in Hom(k, \overline{\mathbb{Q}})$. Si ι agit trivialement sur $Hom(k, \overline{\mathbb{Q}})$, on dit que k est totalement réelle et si ι agit sans point fixe sur $Hom(k, \overline{\mathbb{Q}})$, on dit que k est totalement imaginaire.

(1) Montrer que si k est une extension galoisienne de $\mathbb{Q}$ alors k est soit totalement réelle, soit totalement imaginaire.

(2) Montrer que si k est totalement imaginaire alors $[k : \mathbb{Q}]$ est paire.

(3) Donner un exemple d'extension finie k de $\mathbb{Q}$ qui n'est ni totalement réelle, ni totalement imaginaire.

(4) Soit k_1, k_2 deux extensions finies de $\mathbb{Q}$ contenues dans une même extension k de $\mathbb{Q}$. Notons $k_1 \cdot k_2 \subset k$ le plus petit sous-corps de k contenant k_1 et k_2. Montrer que si k_1, k_2 sont totalement réelles (respectivement totalement imaginaires) alors $k_1 \cdot k_2$ est encore totalement réelle (resp. totalement imaginaire). En déduire qu'une extension finie k de $\mathbb{Q}$ contient une plus grande sous-extension $k^+ \subset k$ (respectivement $k^- \subset k$) qui est totalement réelle (respectivement totalement imaginaire).

(5) Soit k une extension finie de $\mathbb{Q}$. Montrer que les conditions suivantes sont équivalentes:
   (a) $k^- = k$ et $[k : k^+] = 2$;
   (b) Il existe $\iota_k \in Aut(k|\mathbb{Q})$ d'ordre 2 tel que pour tout $\rho \in Hom(k, \overline{\mathbb{Q}})$, $\iota \circ \rho = \rho \circ \iota_k$.
   On dit qu'une extension finie k de $\mathbb{Q}$ qui vérifie les propriétés (a), (b) ci-dessus est un corps CM.

(6) Soit k un corps CM. Par définition k est totalement imaginaire donc ι agit sans point fixe sur $Hom(k, \overline{\mathbb{Q}})$. Comme ι est d'ordre 2, cela signifie que toutes les orbites de ι sur $Hom(k, \overline{\mathbb{Q}})$ sont de cardinal 2. Un type sur k est la donnée d'un sous-ensemble $\Phi \subset Hom(k, \overline{\mathbb{Q}})$ contenant exactement un représentant de chaque orbite de ι. Concrètement cela signifie que $Hom(k, \overline{\mathbb{Q}})$ s'écrit comme réunion disjointe $Hom(k, \overline{\mathbb{Q}}) = \Phi \sqcup \iota\Phi$.

   (a) Soit Φ un type sur k. Montrer que pour tout $\sigma \in Aut(\overline{\mathbb{Q}})$, $\sigma\Phi := \{\sigma \circ \rho \mid \rho \in \Phi\}$ est encore un type sur k.

   (b) Soit $\rho \in Hom(k, \overline{\mathbb{Q}})$ et $\widehat{k^\rho}$ la clôture galoisienne de $\rho(k)$ dans $\overline{\mathbb{Q}}$. Rappeler pourquoi $\widehat{k} := \widehat{k^\rho}$ ne dépend pas de ρ, l'inclusion canonique $Hom(k, \widehat{k}) \hookrightarrow Hom(k, \overline{\mathbb{Q}})$ est une bijection et l'action de $Aut(\overline{\mathbb{Q}})$ sur $Hom(k, \widehat{k}) \tilde{\to} Hom(k, \overline{\mathbb{Q}})$ se factorise *via* $Aut(\overline{\mathbb{Q}}) \twoheadrightarrow Gal(\widehat{k}|\mathbb{Q})$.

   (c) On note $T(k)$ l'ensemble des types sur k. D'après (2) (a), (b) $G := Gal(\widehat{k}|\mathbb{Q})$ agit sur $T(k)$ par $\sigma \cdot \Phi = \sigma\Phi$, $\sigma \in G$, $\Phi \in T(k)$. Soit $\Phi \in T(k)$. On note $S_\Phi := \{\sigma \in G \mid \sigma \cdot \Phi = \Phi\} \subset G$ le stabilisateur de Φ dans G et $k_\Phi := \widehat{k}^{S_\Phi} \subset \widehat{k}$ la $\mathbb{Q}$-sous-extension de $\widehat{k}$ lui correspondant par la correspondance de Galois.

      (i) Tout morphisme de corps $\rho : k \hookrightarrow \widehat{k}$ est en particulier un morphisme de groupes abéliens $(k, +) \to (\widehat{k}, +)$. On peut donc voir $Hom(k, \widehat{k})$ comme un sous-ensemble du groupe $Hom_{\mathbb{Z}}(k, \widehat{k})$ des morphismes de groupes $(k, +) \to (\widehat{k}, +)$. L'action naturelle de $\widehat{k}$ sur $Hom_{\mathbb{Z}}(k, \widehat{k})$ fait de $Hom_{\mathbb{Z}}(k, \widehat{k})$ un $\widehat{k}$-espace vectoriel (si $x_1, x_2 \in k$ et $\upsilon_1, \upsilon_2 \in Hom_{\mathbb{Z}}(k, \widehat{k})$, $x_1\upsilon_1 + x_2\upsilon_2$ est le morphisme de groupes abéliens $\hat{y} \to x_1\upsilon_1(\hat{y}) + x_2\upsilon_2(\hat{y})$). Soit $\rho_1, \ldots, \rho_r \in Hom(k, \widehat{k})$ deux à deux distincts. Montrer que $\rho_1, \ldots, \rho_r$, vus comme éléments de $Hom_{\mathbb{Z}}(k, \widehat{k})$, sont linéairement indépendants sur $\widehat{k}$.

      (ii) On note $k'_\Phi \subset \widehat{k}$ la $\mathbb{Q}$-sous-extension de corps de $\widehat{k}$ engendrée par les éléments de la forme $x_\Phi := \sum_{\rho \in \Phi} \rho(x)$, $x \in k$. Montrer que $k'_\Phi \subset k_\Phi$ puis que $k'_\Phi = k_\Phi$.

(iii) Montrer que k_Φ est un corps CM.

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