Examen 2020/2021
4M002 - Algèbre et théorie de Galois
Anna Cadoret

Avertissement.

Sont autorisés: le polycopié du cours 2020/21, les notes manuscrites du cours 2020/21, les dictionnaires de langues papier. Sont interdits: les corrigés polycopiés et manuscrits des travaux dirigés, les polycopiés de cours des années antérieures etc.

Les réponses peuvent être rédigées en français ou en anglais. Elles doivent être *soigneusement justifiées.* Vous pouvez bien sûr admettre certaines questions. Le sujet est long; il ne sera pas nécessaire de le traiter intégralement pour avoir la note maximale.

Exercice 1. On rappelle qu'un anneau commutatif R est dit local s'il possède un unique idéal maximal, que l'on notera alors toujours $\mathfrak{m}_R$ dans la suite.

Soit K un corps commutatif. On dit qu'un sous-anneau $A \subset K$ est un sous-anneau de valuation si pour tout $0 \neq x \in K$, $x \in A$ ou $x^{-1} \in A$.

(1) Soit $A \subset K$ un sous-anneau de valuation. Montrer que K est le corps des fractions de A.
(2) Soit A un anneau factoriel de corps des fractions K et $\mathcal{P}$ un système de représentants modulo $A^\times$ des éléments irréductibles. Par définition, tout $0 \neq x \in K$ s'écrit alors de façon unique sous la forme $x = u\prod_{p\in\mathcal{P}} p^{v_p(x)}$ avec $u \in A^\times$ et $v_-(x) : \mathcal{P} \to \mathbb{Z}$ à support fini. Montrer que pour chaque $p \in \mathcal{P}$, $A_p := v_p^{-1}(\mathbb{Z}_{\geq 0}) \subset K$ est un sous-anneau de valuation.
(3) Soit $A \subset K$ un sous-anneau de valuation.
 (a) Montrer que l'ensemble des idéaux de A est totalement ordonnés pour l'inclusion *i.e.* que si $I, J \subset A$ sont deux idéaux alors $I \subset J$ ou $J \subset I$.
 (b) Déduire de ce qui précède (sans invoquer le lemme de Zorn!) que A est un anneau local *i.e.* qu'il possède un unique idéal maximal, que l'on notera $\mathfrak{m}_A$ dans la suite.
(4) $A \subset B \subset K$ des sous-anneaux. On suppose que $A \subset K$ est un sous-anneau de valuation.
 (a) Montrer que B est un sous-anneau de valuation et que $\mathfrak{m}_B \subset \mathfrak{m}_A$ avec $\mathfrak{m}_B = \mathfrak{m}_A$ si et seulement si $A = B$.
 (b) Montrer que $\mathfrak{m}_B$ est un idéal premier de A et que le morphisme canonique $A \to B$ s'étend en un isomorphisme $A_{\mathfrak{m}_B} \tilde{\to} B$.
 (c) Montrer que $\overline{A} := A/\mathfrak{m}_B \subset K_B := B/\mathfrak{m}_B$ est un sous-anneau de valuation.
 (d) Inversement, si $R \subset K_B$ est un anneau de valuation, montrer que l'image inverse de R par la projection canonique $B \to K_B = B/\mathfrak{m}_B$ est un sous-anneau de valuation de K.
(5) Rappeler pourquoi l'anneau des polynômes à une indéterminée $\mathbb{Z}[X]$ est un anneau factoriel. Exhiber un sous-anneau de valuation $A \subsetneq \mathbb{Q}(X)$ qui n'est pas de la forme de ceux de la question (2).
(6) Soit $R \subset K$ un sous-anneau local. L'objectif de cette question est de montrer qu'il existe un sous-anneau de valuation $A \subset K$ tel que $R \subset A$ et $\mathfrak{m}_R \subset \mathfrak{m}_A$. On note $\mathcal{E}$ l'ensemble des sous-anneaux $A \subset K$ tels que $R \subset A$ et $\mathfrak{m}_R A \subsetneq A$.
 (a) Montrer que $\mathcal{E} \neq \emptyset$ et que $\mathcal{E}$ muni de l'inclusion est un ensemble ordonné inductif. Par le lemme de Zorn, $\mathcal{E}$ contient donc un élément maximal, que l'on notera A, pour l'inclusion.
 (b) Montrer qu'il existe un idéal maximal $\mathfrak{m}$ de A tel que $\mathfrak{m}_R \subset \mathfrak{m}$ et que le morphisme de localisation $A \to A_\mathfrak{m}$ est un isomorphisme. En déduire que A est un anneau local, d'unique idéal maximal $\mathfrak{m}_A := \mathfrak{m}$.
 (c) Soit $x \in K \setminus A$. On note $A[x] \subset K$ le sous-anneau de K engendré par A et x.
  (i) Montrer que $\mathfrak{m}_R A[x] = A[x]$.
  (ii) En déduire qu'on peut écrire $1 = \alpha_0 + \alpha_1 x + \cdots + \alpha_m x^m$ avec $a_i \in \mathfrak{m}_R A$ puis $1 = a_1 x + \cdots + a_m x^m$ avec $a_i \in \mathfrak{m}_A$.

(iii) Soit $m(\geq 1)$ minimal tel que $1 = a_1 x + \cdots + a_m x^m$ avec $a_i \in \mathfrak{m}_A$. Si on suppose que $x^{-1} \notin A$, en appliquant le même argument à x^{-1}, on peut donc aussi écrire $1 = b_1 x^{-1} + \cdots + b_n x^{-n}$ avec $a_i \in \mathfrak{m}_A$ et $n(\geq 1)$ minimal. Montrer qu'alors $m = n$ et en déduire une contradiction. Conclure.

(7) On note $\mathcal{E}$ l'ensemble des sous-anneaux locaux $R \subset K$ muni de la relation d'ordre $\leq$ definie par $R_1 \leq R_2$ si $R_1 \subset R_2$ et $\mathfrak{m}_{R_1} \subset \mathfrak{m}_{R_2}$. Déduire des questions (3), (4), (6) que les sous-anneaux de valuations de K sont exactement les éléments maximaux de $(\mathcal{E}, \leq)$.

Exercice 2. Soit A un anneau commutatif. On dit qu'un A-module P est

- *projectif* si pour tout morphisme surjectif de A-modules $\phi : M \to M''$ et pour tout morphisme de A-modules $f : P \to M''$ il existe un morphisme de A-modules $\widetilde{f} : P \to M$ tel que $\phi\widetilde{f} = f$. Visuellement:

$$\begin{tikzcd} & P \arrow[dl, dotted, "\exists\widetilde{f}"'] \arrow[d, "f"] & \\ M \arrow[r, "\phi"] & M'' \arrow[r] & 0 \end{tikzcd}$$

- *plat* si pour tout morphisme injectif de A-modules $\phi : M' \to M$, le morphisme $\phi \otimes Id : M' \otimes_A P \to M \otimes_A P$ est encore injectif.

(1) Soit P un A-module. Montrer que les propriétés suivantes sont équivalentes:
  (a) P est projectif;
  (b) Pour tout morphisme surjectif de A-modules $f : M \to P$ admet une section *i.e.* un morphisme de A-modules $s : P \to M$ tel que $f \circ s = Id$;
  (c) Il existe un A-module Q tel que $P \oplus Q$ est un A-module libre.

(2) Montrer qu'un A-module libre est projectif.

(3) Montrer qu'un A-module libre est plat. En déduire qu'un A-module projectif est plat.

(4) Soit $0 \to M' \overset{\iota}{\to} M \overset{p}{\to} M'' \to 0$ une suite exacte courte de A-modules et P un A-module. Montrer que la suite de A-modules

$$M' \otimes_A P \overset{\iota\otimes Id}{\to} M \otimes_A P \overset{p\otimes Id}{\to} M'' \otimes_A P \to 0$$

est encore exacte.

(5) Soit $0 \to M' \overset{\iota}{\to} M \overset{p}{\to} P \to 0$ une suite exacte courte de A-modules avec P plat et soit $I \subset A$ un idéal. Justifier qu'on a un diagramme commutatif à lignes et colonnes exactes

$$\begin{tikzcd} & & & 0 \arrow[d] & \\ & I \otimes_A M' \arrow[r, "Id\otimes\iota"] \arrow[d] & I \otimes_A M \arrow[r, "Id\otimes p"] \arrow[d] & I \otimes_A P \arrow[r] \arrow[d] & 0 \\ 0 \arrow[r] & M' \arrow[r, "\iota"] \arrow[d] & M \arrow[r, "p"] \arrow[d] & P \arrow[r] \arrow[d] & 0 \\ & M'/IM' \arrow[r, "\overline{\iota}"] \arrow[d] & M/IM \arrow[r, "\overline{p}"] \arrow[d] & P/IP \arrow[r] \arrow[d] & 0 \\ & 0 & 0 & 0 & \end{tikzcd}$$

et en déduire que la suite $0 \to M'/IM' \overset{\overline{\iota}}{\to} M/IM \overset{\overline{p}}{\to} P/IP \to 0$ est encore exacte.

(6) On suppose que A est un anneau local *i.e.* qu'il possède un unique idéal maximal, que l'on note $\mathfrak{m}$. L'objectif de cette question est de montrer qu'un A-module plat de type fini est libre.
  (a) Soit M un A-module de type fini. Montrer que $\mathfrak{m}M = M$ si et seulement si $M = 0$.
  (b) Soit P un A-module plat et de type fini et $p_1, \ldots, p_r \in P$ un système de représentants d'une $A/\mathfrak{m}$-base de $P/\mathfrak{m}P$. Montrer que le morphisme de A-modules

$$p : \bigoplus_{1\leq i\leq r} Ap_i \to P,\ a_1p_1 \oplus \cdot \oplus a_rp_r \mapsto \sum_{1\leq i\leq r} a_ip_i$$

est surjectif.

(c) Montrer que $p : \bigoplus_{1\leq i\leq r} Ap_i \to P$ est un isomorphisme.

Exercice 3. Soit L/K une extension finie de corps. Pour tout $x \in L$ l'application de multiplication à gauche $L_x : L \to L$, $y \to xy$ est un endomorphisme du K-espace vectoriel L; on note $P_{L|K}(x,T) \in K[T]$ son polynôme minimal unitaire et $tr_{L|K}(x) \in K$ sa trace.

(1) Montrer que $P_{K(x)|K}(x,T) =: P_x(T)$ est le polynôme minimal de x sur K. On note $x_1,\dots,x_n$ les racines de $P_x(T)$ (comptées avec multiplicité) dans une clôture algébrique fixée $\overline{L}$ de L. Montrer que $tr_{K(x)|K}(x) = \sum_{1\leq i\leq n} x_i = -a_1$, où $P_x(T) = T^n + \sum_{1\leq i\leq n} a_i T^{n-i}$.

(2) Montrer que $tr_{L|K}(x) = [L : K(x)]tr_{K(x)|K}(x)$.

(3) Montrer que pour tout entier $k \geq 1$, $tr_{K(x)|K}(x^k) = \sum_{1\leq i\leq n} x_i^k$.

(4) On note $K[[T]]$ l'anneau des séries formelles à coefficients dans K *i.e.*, comme K-espace vectoriel $K[[T]]$ est l'ensemble $K^{\mathbb{N}}$ des suites à coefficients dans K. On note $\underline{a} = \sum_{n\in\mathbb{Z}} a_n T^n$. Soit $\sum_{n\in\mathbb{Z}} a_n T^n, \sum_{n\in\mathbb{Z}} b_n T^n \in K[[T]]$. Comme pour tout $n \geq 0$, $\sum_{p+q=n} a_p b_q$ est une somme finie, on peut définir

$$\sum_{n\geq 0} a_n T^n \cdot \sum_{n\geq 0} b_n T^n = \sum_{n\geq 0} (\sum_{p+q=n} a_p b_q) T^n$$

et on vérifie que $K[[T]]$ muni de ce produit est une K-algèbre commutative d'unité $1 = (\delta_{0,n})_{n\in\mathbb{Z}}$. Par définition, $K[T] \subset K[[T]]$.

(a) Montrer que pour tout $a \in K$, $T - a$ admet un inverse dans $K[[T]]$;

(b) Supposons K algébriquement clos. Montrer que tout $0 \neq P \in K[T]$ admet un inverse dans $K[[T]]$.

(5) Montrer que $\frac{P_x'(T)}{P_x(T)} = \frac{1}{T}\sum_{k\geq 0} tr_{K(x)|K}(x^k)\frac{1}{T^k}$ dans $\overline{L}[[\frac{1}{T}]]$.

(6) On rappelle que $x \in L$ est séparable sur K si les racines de P_x dans $\overline{L}$ sont deux à deux distinctes et que l'extension L/K est séparable si tout $x \in L$ est séparable sur K. Donner une exemple d'extension L/K finie qui n'est pas séparable.

(7) Soit $x \in L$. Montrer que les propriétés suivantes sont équivalentes.

(a) x est séparable sur L;

(b) $P_x(T)$ et $P_x'(T)$ sont premiers entre eux;

(c) $P_x'(T) \neq 0$;

(d) Il existe $k \geq 1$ tel que $tr_{K(x)|K}(x^k) \neq 0$.

(8) Montrer que les propriétés suivantes sont équivalentes.

(a) L/K est séparable;

(b) $tr_{L|K} : L \to K$ n'est pas l'application nulle;

(c) La forme K-bilinéaire $L \times L \to K$, $(x,y) \mapsto tr_{L|K}(xy)$ n'est pas dégénérée.

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