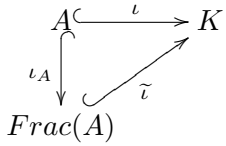
Examen 2020/2021 - Correction
4M002 - Algèbre et théorie de Galois
Anna Cadoret

Exercice 1.

(1) Soit $A \subset K$ un sous-anneau de valuation. Notons que comme K est un corps, A est intègre donc on peut effectivement parler de son corps des fractions (= localisé en l'idéal premier $\{0\}$). Comme $A \setminus \{0\} \subset K \setminus \{0\} = K^\times$ l'inclusion canonique $\iota : A \hookrightarrow K$ s'étend en un diagramme commutatif



Le morphisme $\widetilde{\iota} : Frac(A) \hookrightarrow K$ est injectif (puisque $Frac(A)$ est un corps). De plus, par construction, il vérifie $\widetilde{\iota}(a/b) = \widetilde{\iota}(a)\widetilde{\iota}(b)^{-1} = ab^{-1}$. Cela montre qu'il est aussi surjectif puisque pour tout $0 \neq x \in K$ soit $x \in A$ (donc $x = \widetilde{\iota}(a)$) soit $x^{-1} \in A$ donc $x = \widetilde{\iota}(a^{-1})$.

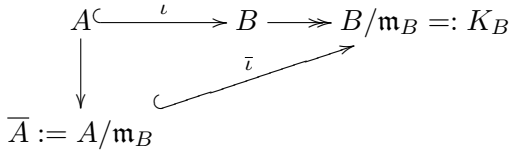
(2) Cela résulte immédiatement de la définition et du fait que $v_p : (K^\times, \cdot) \to (\mathbb{Z}, +)$ est un morphisme de groupes.

(3) (a) Soit $I, J \subset A$ deux idéaux et supposons $I \not\subset J$. Fixons $a \in I$ tel que $a \notin J$. Pour tout $b \in J$ on a $ba^{-1} \in A$ sinon, $ab^{-1} \in A$ donc $a = (ab^{-1})b \in J$: contradiction. Donc $b = (ba^{-1})a \in I$.

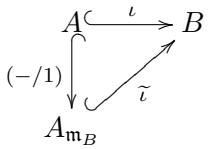
(b) Notons $\mathcal{I}_A$ l'ensemble des idéaux (stricts) $I \subsetneq A$. Comme $\mathcal{I}_A$ est un ensemble strictement ordonné pour l'inclusion $\subset$, on a encore $\mathfrak{m} = \cup_{I \in \mathcal{I}_A} I \in \mathcal{I}_A$. En effet, par définition pour tout $a \in \mathfrak{m}$ il existe $I_a \in \mathcal{I}_A$ tel que $a \in I_a$. En particulier, pour tout $a, b \in \mathfrak{m}$ on a $I_a \subset I_b$ ou $I_b \subset I_a$ Disons $I_a \subset I_b$. Alors pour tout $\alpha, \beta \in A$, $\alpha a + \beta b \in I_b \subset \mathfrak{m}$. Cela montre que $\mathfrak{m} \subset A$ est un idéal. Il est strict puisque $1 \notin I$, $I \in \mathcal{I}_A$.

(4) (a) Le fait que B est un sous-anneau de valuation résulte immédiatement de la définition puisque pour tout $0 \neq x \in K$ si $x \notin B$ *a fortiori* $x \notin A$ donc $x^{-1} \in A \subset B$. Pour montrer que $\mathfrak{m}_B \subset \mathfrak{m}_A$, il suffit de montrer que $\mathfrak{m}_B \subset \mathfrak{m}_A$ (puisque $\mathfrak{m}_B$ est un idéal de B et $A \subset B$. Soit donc $0 \neq b \in \mathfrak{m}_B$. Si $b \notin A$, $b^{-1} \in A \subset B$ donc $1 = b^{-1}b \in B\mathfrak{m}_B = \mathfrak{m}_B$: contradiction.
Par ailleurs $A \subset B$ implique $A^\times \subset B^\times$. Mais comme A, B sont locaux, $A^\times = A \setminus \mathfrak{m}_A$, $B^\times = B \setminus \mathfrak{m}_B$ donc $A^\times \subset B^\times$ équivaut à $\mathfrak{m}_B \subset \mathfrak{m}_A$. Supposons $\mathfrak{m}_B = \mathfrak{m}_A$ et fixons $b \in B$ si $b \notin A$, $b^{-1} \in A \subset B$ donc $b, b^{-1} \in B^\times = B \setminus \mathfrak{m}_B$. En particulier, $b^{-1} \in A \setminus \mathfrak{m}_A = A^\times$ donc $b \in A$: contradiction. Supposons de plus $\mathfrak{m}_B = \mathfrak{m}_A$ et montrons que cela implique $A = B$. En effet, soit $0 \neq b \in B$. Si $b \notin A$, $b^{-1} \in A \subset B$ *i.e.* $b \in B^\times$ donc $b^{-1} \notin \mathfrak{m}_B = \mathfrak{m}_A$ donc $b^{-1} \in A \setminus \mathfrak{m}_A = A^\times$, ou encore $b \in A^\times \subset A$: contradiction. La réciproque est immédiate.

(b) Comme $\mathfrak{m}_B \subset \mathfrak{m}_A \subset A \subset B$, $\mathfrak{m}_B$ est un idéal de A. En notant $\iota : A \hookrightarrow B$ l'inclusion naturelle, le morphisme $A \overset{\iota}{\hookrightarrow} B \overset{p_{\mathfrak{m}_B}}{\to} B/\mathfrak{m}_B =: K_B$ a pour noyau $\mathfrak{m}_B$ donc se factorise en



avec $\overline{\iota} : \overline{A} \to K_B$ injectif. Comme K_B est un corps, cela montre que $A/\mathfrak{m}_B$ est intègre donc que $\mathfrak{m}_B$ est un idé l premier de A. Comme $A \setminus \mathfrak{m}_B \subset B \setminus \mathfrak{m}_B = B^\times$, par propriété universelle de la localisation l'inclusion naturelle s'étend en un digramme commutatif canonique



avec $\widetilde{\iota} : A_{\mathfrak{m}_B} \hookrightarrow B$ injectif. Et pour tout $b \in B$, si $b \in A$ on a $b = \widetilde{\iota}(b/1)$. Si $b \notin A$ on a $b^{-1} \in A \subset B$ donc $b, b^{-1} \in B^\times = B \setminus \mathfrak{m}_B$. En particulier, $b^{-1} \in A \setminus \mathfrak{m}_B$ donc $b^{-1} = \widetilde{\iota}(b^{-1}/1)$.

(c) Soit $b \in B$ tel que $\overline{b} := p_{\mathfrak{m}_B}(b) \notin \overline{A}$. En particulier $b \notin A$ donc $b^{-1} \in A$ donc $p_{\mathfrak{m}_B}(b^{-1}) = \overline{b}^{-1} \in \overline{A}$.

(d) Notons $\widetilde{R} := p_{\mathfrak{m}_B}^{-1}(R) \subset B$. Pour tout $0 \neq x \in K$, $x \in B$ ou $x^{-1} \in B$. Par symétrie il suffit de montrer que $x \in B$ implique $x \in \widetilde{R}$ ou $x^{-1} \in \widetilde{R}$. Puisque $\mathfrak{m}_B = \ker(p_{\mathfrak{m}_B}) \subset \widetilde{R}$, il suffit de traiter le cas où $x \in B \setminus \mathfrak{m}_B = B^\times$.Comme $p_{\mathfrak{m}_B} : B \to K_B$ est un morphisme d'anneaux, il induit un morphisme de groupes $p_{\mathfrak{m}_B} : B^\times \to K_B^\times = K_B \setminus \{0\}$; en particulier, $p_{\mathfrak{m}_B}(x^{-1}) = p_{\mathfrak{m}_B}(x)^{-1}$. Comme $R \subset K_B$ est un sous-anneau de valuation, on a $p_{\mathfrak{m}_B}(x) \in R$ ou $p_{\mathfrak{m}_B}(x^{-1}) = p_{\mathfrak{m}_B}(x)^{-1} \in R$ *i.e.* $x \in \widetilde{R}$ ou $x^{-1} \in \widetilde{R}$.

(5) Par transfert de factorialité, comme $\mathbb{Z}$ est factoriel, $\mathbb{Z}[X]$ est factoriel et si on note $\mathcal{P}$ l'ensemble des nombres premiers positifs, un système de représentants des irréductibles de $\mathbb{Z}[X]$ est $\mathcal{P} \cup \mathcal{P}_{\mathbb{Q}[X]}$ où $\mathcal{P}_{\mathbb{Q}[X]}$ est un système de représentants de contenu 1 par rapport à $\mathbb{Z}$ de l'ensemble des polynômes irréductibles de $\mathbb{Q}[X]$. Fixons un premier p de $\mathbb{Z}$. C'est aussi un premier de $\mathbb{Z}[X]$ donc il définit une valuation $v_p : \mathbb{Q}(X) \to \overline{\mathbb{Z}}$. Notons $B := \mathbb{Z}[X]_{v_p} := \{0\} \cup v_p^{-1}(\mathbb{Z}_{\geq 0})$. On a $\mathfrak{m}_B = pB$ et $K_B = \overline{\mathbb{F}}_p(X) = Frac(\mathbb{F}_p[X])$. Comme $\mathbb{F}_p[X]$ est factoriel, tout polynôme irréductible $\overline{P} \in \mathbb{F}_p[X]$ définit une valuation $v_{\overline{P}} : \mathbb{F}_p(x) \to \overline{\mathbb{Z}}$. Notons $R := \mathbb{F}_p[X]_{v_{\overline{P}}} = \{0\} \cup v_{\overline{P}}^{-1}(\mathbb{Z}_{\geq 0}) \subset \mathbb{F}_p(X)$. D'après (4) (d) $\widetilde{R} := p_{pB}^{-1}(R) \subsetneq B$ est un sous-anneau de valuation de $\mathbb{Q}(X)$. Il n'est pas de la forme $\mathbb{Z}[X]_v$ pour $v = v_q : \mathbb{Q}[X] \to \overline{\mathbb{Z}}$ une valuation associée à un irréductible $q \in \mathcal{P} \cup \mathcal{P}_{\mathbb{Q}[X]}$ car, de façon générale, avec les notations de (2), si $q \neq q' \in \mathcal{P}$, on a toujours $A_{v_q} \not\subset A_{v_{q'}}$ (puisque $q \notin A_{v_{q'}}$!). Or, ici, $\widetilde{R} \subset B$.

(6) Soit $R \subset K$ un sous-anneau local. 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) $R \in \mathcal{E}$ donc $\mathcal{E} \neq \emptyset$. Si $A_1 \subset A_2 \subset \cdots \subset A_n \subset A_{n+1} \subset \cdots K$ est une suite croissante pour $\subset$ d'éléments de $\mathcal{E}$, on note $A := \cup_{n \geq 1} A_n \subset K$. On vérifie immédiatement que c'est un sous-anneau de K. On a $R \subset A_1 \subset A$ et si $\mathfrak{m}_R A = A$ on aurait $1 = \sum_{i=1}^r \mu_i a$ avec $\mu_i \in \mathfrak{m}_R$ et $a_i \in A$ donc $a_i \in A_{n_i}$ pour un certain $n_i \geq 1$ $i = 1, \ldots, r$ mais cela contredirait $\mathfrak{m}_R A_n \subsetneq A_n$ pour $n \geq n_1, \ldots, n_r$. Par le lemme de Zorn, $\mathcal{E}$ contient donc un élément maximal, que l'on notera A, pour l'inclusion.

(b) Par définition $A \in \mathcal{E}$ donc $\mathfrak{m}_R A \subset A$ est un idéal strict de A. En invoquant encore le lemme de Zorn, il existe un idéal maximal $\mathfrak{m}$ de A tel que $\mathfrak{m}_R \subset \mathfrak{m}$. Comme A est intègre, le morphisme de localisation $A \to A_{\mathfrak{m}}$ est injectif. Par propriété universelle de $A \to A_{\mathfrak{m}}$ appliquée à l'inclusion naturelle $A \subset K$, on peut identifier $A_{\mathfrak{m}}$ au sous-anneau de K formé des éléments de la forme a/b, $a \in A$, $b \in A \setminus \mathfrak{m}$. Mais alors, $R \subset A \subset A_{\mathfrak{m}}$ et $\mathfrak{m}_R A_{\mathfrak{m}} \subsetneq A_{\mathfrak{m}}$ sinon on pourrait écrire $1 = \mu a/b$ avec $\mu \in \mathfrak{m}_R$, $a \in A$, $b \in A \setminus \mathfrak{m}$ donc $b = \mu a \in \mathfrak{m} \cap A \setminus \mathfrak{m}$: contradiction. Cela montre que $\mathfrak{m}_R A_{\mathfrak{m}} = A_{\mathfrak{m}}$ donc $A_{\mathfrak{m}} \in \mathcal{E}$ et, par maximalité de A, $A = A_{\mathfrak{m}}$. En particulier, 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) Si $\mathfrak{m}_R A[x] = A[x]$ on aurait $A[x] \in \mathcal{E}$ or $A \subset A[x]$ donc par maximalité de A, $A = A[x]$, ce qui contredirait $x \in K \setminus A$.

(ii) Donc $1 \in \mathfrak{m}_R A[x]$ *i.e.* on peut écrire $1 = \alpha_0 + \alpha_1 x + \cdots + \alpha_m x^m$ avec $a_i \in \mathfrak{m}_R A \subset \mathfrak{m}$. En particulier $(1 - \alpha_0) \in RA \setminus \mathfrak{m} = A^\times$ donc $1 = (1-\alpha_0)^{-1}(\alpha_1 x + \cdots + \alpha_m x^m) = a_1 x + \cdots + a_m x^m$ 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 $b_i \in \mathfrak{m}_A$ et $n(\geq 1)$ minimal. En particulier, $x^{n+1} = b_1 x^{n-1} + \cdots + b_n \in \sum_{1 \leq i \leq n} A x^i$ et par récurrence immédiate $x^{n+N} \in \sum_{1 \leq i \leq n} A x^i$, $N \geq 1$. Cela impose $m \leq n$. Par symmétrie on doit avoir $m = n$. Mais alors on aurait $1 - a_n b_n = (a_1 + a_n b_{n-1})x + \cdots + (a_{n-1} + a_n b_1)x^{n-1} + x^{n-1}$ où encore, puisque $A - a_n b_n \in 1 + \mathfrak{m}_A \subset A^\times$, $1 = (1 - a_n b_n)^{-1}((a_1 + a_n b_{n-1})x + \cdots + (a_{n-1} + a_n b_1)x^{n-1} + x^{n-1})$, ce qui contredit la minimalité de $m = n$.
Par conséquent on ne peut avoir à la fois $x, x^{-1} \in A$. Autrement dit, $A \subset K$ est un sous-anneau de valuation de K.

(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 $\mathfrak{m}_{R_1} \subset \mathfrak{m}_{R_2}$. D'après la question (3), $\mathcal{E}$ contient les sous-anneaux de valuation de K. D'après la question (6) les éléments maximaux de $(\mathcal{E}, \leq)$ sont des sous-anneaux de valuation de K. D'après la question (4) si $A_1, A_2 \subset K$ sont deux sous-anneaux de K tels que $A_1 \subsetneq A_2$ alors $\mathfrak{m}_{A_2} \subsetneq \mathfrak{m}_{A_1}$ donc $A_1 \not\leq A_2$ et $A_2 \not\leq A_1$.

Exercice 2.

(1) (a) $\Rightarrow$ (b): On applique la définition de projectif avec $\phi = f : M \twoheadrightarrow P$ et $f = Id : P \to P$.
(b) $\Rightarrow$ (c): On consière l'unique morphisme de A-modules (propriété universelle de la somme directe) $f : A^{(P)} = \oplus_{p\in P} Ae_p \twoheadrightarrow P$qui envoie l'élément de base e_p sur p. En notant $Q := \ker(f)$ on a une suite exacte courte de A-modules

$$0 \to Q \to A^{(P)} \xrightarrow{f} P \to 0.$$

D'après (b), cette suite exacte courte se scinde, ce qui équivaut à $A^{(P)} \simeq Q \oplus P$.
(c) $\Rightarrow$ (a): Par propriété universelle de la somme directe il existe un unique morphisme $g : P \oplus Q \to M''$ tel que $g \circ \iota_P = f$, $g \circ \iota_Q = 0$. Ecrivons $P \oplus Q \simeq A^{(I)} = \oplus_{i\in I} Ae_i$ et pour chaque $i \in I$ choisissons $m_i \in \phi^{-1}(g(e_i))$ (on utilise ici la surjectivité de ϕ). Toujours par propriété universelle de la somme directe il existe un unique morphisme $\widetilde{g} : A^{(I)} \to M$ tel que $g(e_i) = m_i$. Par construction $\phi \circ \widetilde{g} = g$ donc $\phi \circ \widetilde{g} \circ \iota_P = g \circ \iota_P = f$. On peut donc prendre $\widetilde{f} = \widetilde{g} \circ \iota_P$.

(2) Evident par la caractérisation (c).

(3) Si $\phi : M' \to M$ est un morphisme de A-modules, modulo les isomorphismes canoniques $M' \otimes_A A^{(I)} \tilde{\to} M'^{\,I}$, $M \otimes_A A^{(I)} \tilde{\to} M^{(I)}$ le morphisme $\phi \otimes Id : M' \otimes_A A^{(I)} \to M \otimes_A A^{(I)}$ s'identifie au morphisme $\oplus_{i\in I} m'_i \mapsto \oplus_{i\in I} \phi(m'_i)$. En particulier, $\phi : M' \to M$ est injectif (si et) seulement si $\phi \otimes Id : M' \otimes_A A^{(I)} \to M' \otimes_A A^{(I)}$ est injectif. Si P est un A-module projectif, d'après la caractérisation (c), il existe un A-module Q tel que $P \oplus Q$ est libre. Là encore, modulo les isomorphismes canoniques $M' \otimes_A P \oplus Q) \tilde{\to} (M' \otimes_A P) \oplus (M' \otimes_A Q)$, $M \otimes_A P \oplus Q) \tilde{\to} (M \otimes_A P) \oplus (M \otimes_A Q)$ le morphisme $\phi \otimes Id : M' \otimes_A (P \oplus Q) \to M \otimes_A (P \oplus Q)$ s'identifie au morphisme $(\phi \otimes Id_P) \oplus (\phi \otimes Id_Q) : (M' \otimes_A P) \oplus (M' \otimes_A Q) \to (M \otimes_A P) \oplus (M \otimes_A Q)$. Or $(\phi \otimes Id_P) \oplus (\phi \otimes Id_Q) : (M' \otimes_A P) \oplus (M' \otimes_A Q) \to (M \otimes_A P) \oplus (M \otimes_A Q)$ est injectif (si et) seulement si $\phi \otimes Id_P : M' \otimes_A P \to M \otimes_A P$ et $\phi \otimes Id_Q : M' \otimes_A Q \to M \otimes_A Q$ sont injectifs. Et comme $P \oplus Q$ est libre donc plat, $(\phi \otimes Id_P) \oplus (\phi \otimes Id_Q) : (M' \otimes_A P) \oplus (M' \otimes_A Q) \to (M \otimes_A P) \oplus (M \otimes_A Q)$ est injectif.

(4) Cf cours.

(5) L'exactitude de la première ligne est la question (4), celle de la seconde est par défintion et celle de la troisième est une partie (facile) du lemme du serpent. L'exactitude des deux premières colonnes est par définition. Pour la troisième colonne, ce qui n'est pas tout à fait évident est l'injectivité de $I \otimes_A P \to P$, $a \otimes p \mapsto ap$. Cela vient de la suite exacte de A-modules

$$0 \to I \to A \to A/I \to 0$$

et du fait que P est plat car projectif d'après la question (3) donc que la suite

$$0 \to I \otimes_A P \to A \otimes_A P \to (A/I) \otimes_A P \simeq P/IP \to 0$$

est encore exacte. Par le lemme du serpent, la troisième ligne est donc en fait une suite exacte courte.

(6) (a) C'est un cas particulier du lemme de Nakayama. On rappelle l'argument. Soit $m_1, \ldots, m_r$ un système de générateurs de M comme A-module de longueur minimale. L'égalité $\mathfrak{m}M = M$ implique que $m_j = \sum_{1\le i\le r} \mu_{i,j} m_i$, $\mu_{i,j} \in \mathfrak{m}$, $i = 1, \ldots, r$. Donc, si $r \ge 1$, en utilisant que $1 - \mu_{j,j} \in 1 + \mathfrak{m} \subset A^\times$ on a $m_j = (1 - \mu_{j,j})^{-1} \sum_{1\le i\ne j\le r} \mu_{i,j} m_i$, ce qui contredit la minimalité de r. Donc $M = 0$.

(b) Notons $I := im(p) \subset P$. On a par définition une suite exacte courte $0 \to I \to P \to P/I \to 0$ donc d'après la question (4), une suite exacte $I \otimes_A A/\mathfrak{m} \to P \otimes_A A/\mathfrak{m} \to (P/I) \otimes_A A/\mathfrak{m} \to 0$. Mais comme les $\overline{p}_1, \ldots, \overline{p}_r$ forment une $A/\mathfrak{m}$-base de $P \otimes_A A/\mathfrak{m} \simeq P/\mathfrak{m}P$, le morphisme $I \otimes_A A/\mathfrak{m} \to P \otimes_A A/\mathfrak{m}$ est surjectif. Donc $(P/I)/\mathfrak{m}(P/I) \simeq (P/I) \otimes_A A/\mathfrak{m} = 0$. D'après la question (6) (a) on a donc $P/I = 0$.

(c) Comme P est un A-module plat, d'après la question (5) appliquée avec $I = \mathfrak{m}$) et la suite exacte courte $0 \to \ker(p) \to \oplus_{1\le i\le r} Ap_i \xrightarrow{p} P \to 0$, on obtient une suite exacte courte

$$0 \to \ker(p)/\mathfrak{m}\ker(p) \to \oplus_{1\le i\le r} A/\mathfrak{m}\overline{p}_i \xrightarrow{\overline{p}} P/\mathfrak{m}P \to 0.$$

Mais puisque les $\overline{p}_1, \ldots, \overline{p}_r$ forment un $A/\mathfrak{m}$-base de $P/\mathfrak{m}P$ le morphisme $\overline{p} : \oplus_{1\le i\le r} A/\mathfrak{m}\overline{p}_i \to P/\mathfrak{m}P$ est un isomorphisme; en particulier $\ker(p) = \mathfrak{m}\ker(p)$ donc, en appliquant de nouveau la question (6) (a), $\ker(p) = 0$.

Exercice 3.

(1) Notons $P_x(T) = T^n + \sum_{1\le i\le n} a_i T^{n-i} \in K[T]$ le polynôme minimal de x sur K. La famille $1, x, \ldots, x^{n-1}$ est une K-base de $K(x)$. SI on calcule la matrice de L_x dans cette K-base on obtient la matrice compagnon $C(P)$ de P puisque $L_x(x^i) = x^{i+1}$, $i = 0, \ldots, n-2$ et $L_x(x^{n-1}) = x^n = -\sum_{1\le i\le n-1} a_i x^{n-i}$.

La première partie de la question résulte donc du fait que le polynôme minimal de $C(P)$ est P. Pour la seconde, la trace de $C(P)$ est $-a_1 = \sum_{1\leq i\leq n} x_i$.

(2) Si on choisit une $K(x)$-base $\underline{e} := e_1, \dots, e_m$ de L et la K-base $1, x, \dots, x^{n-1}$ de $K(x)$ on obtient la K-base $e_i x^j$, $1 \leq i \leq m$, $0 \leq j \leq n-1$ et la matrice de L_x dans $e_i x^j$, $1 \leq i \leq m$, $0 \leq j \leq n-1$ ordonnée lexicographiquement est une matrice diagonale par blocs formée de m blocs $C(P)$. En particulier, $tr_{L|K}(x) = [L : K(x)]tr_{K(x)|K}(x)$.

(3) Par définition $x_1, \dots, x_n$ son les racines de $P_x = P_{k(x)|k}(x, T)$ donc les valeurs propres de L_x. Fixons une clôture algébrique $K \subset \overline{K}$. La théorie de la réduction sur un corps algébriquement clos nous donne une $\overline{K}$-base de $K(x) \otimes_K \overline{K}$ dans laquelle la matrice de $L_x : K(x) \otimes_K \overline{K} \to K(x) \otimes_K \overline{K}$ est triangulaire supérieure avec pour diagonale $x_1, \dots, x_n$. Dans cette même base la matrice de $L_{x^k} = {L_x}^k$ est donc encore triangulaire supérieure avec pour diagonale $x_1^k, \dots, x_n^k$. D'où la conclusion.

(4) (a) On a $-\frac{1}{a}(\sum_{n\geq 0}(\frac{T}{a})^n)(T-a) = (\sum_{n\geq 0}(\frac{T}{a})^n)(1-\frac{T}{a}) = 1$ donc, dans $K[[T]]$, $T-a$ est inversible d'inverse $-\frac{1}{a}(\sum_{n\geq 0}(\frac{T}{a})^n)$.

(b) Si K est algébriquement clos, on peut écrire $P(T) \in K[T]$ sous la forme $P(T) = (T-a_1)\cdots(T-a_n)$, qui est donc inversible d'après la question (4) (a).

(5) On a

$$\frac{P'_x}{P_x} = \sum_{1\leq i\leq n} \frac{1}{T-x_i} = \frac{1}{T}\sum_{1\leq i\leq n} \frac{1}{1-\frac{x_i}{T}} = \frac{1}{T}\sum_{1\leq i\leq n}\sum_{n\geq 0} \frac{x_i^n}{T^n} = \frac{1}{T}\sum_{n\geq 0} \frac{tr_{k(x)|k}(x^n)}{T^n},$$

où la dernière égalité est la question (3).

(6) $\mathbb{F}_p(X)[Y]/\langle Y^p - X\rangle$ n'est pas une extension séparable de $\mathbb{F}_p(X)$ car le polynôme minimal de Y est $T^p - X$.

(7) Rappelons que $P_x(T) \in K[T]$ est irréductible sur K. En particulier, comme $deg(P'_x) \leq deg(P_x) - 1$, on a seulement deux possibilités: P_x et P'_x sont premiers entre eux ou $P'_x = 0$ (ce deuxième cas ne pouvant se produire que si K est de caractéristique $p > 0$). Ce qui montre déjà (b) $\Leftrightarrow$ (c). L'équivalence (c) $\Leftrightarrow$ (d) est la question (5). Montrons (a) $\Rightarrow$ (b) par contraposée. On se place sur une clôture algébrique $\overline{K}$ de K et soit x une racine commune de P_x et P'_x dans $\overline{K}$. Ecrivons $P_x(T) = (T-x)Q_0(T)$, $P'_x(T) = (T-x)Q_1(T) = Q_0(T) + (T-x)Q'_0(T)$. On a donc $(T-x)|Q_0(T)$ donc $(T-x)^2|P_x(T)$. L'implication (b) $\Rightarrow$ (a) se montre également par contraposée: si P_x a une racine α d'ordre ≥ 2 dans $\overline{L}$, on a $(T-\alpha)^2|P_x$ donc $T-\alpha|P'_x$.

(8) L'implication (c) $\Rightarrow$ (b) est tautologique. Pour (b) $\Rightarrow$ (c), s'il existe $z \in L$ tel que $tr_{L|K}(z) \neq 0$ alors pour tout $0 \neq x \in L$ si $tr_{L|K}(xy) = 0$, $y \in L$ on a forcément $x = 0$ sinon, on obtiendrait une contradiction en prenant $y := x^{-1}z$. Si L/K est séparable, comme elle est aussi finie elle admet un élément primitif $x \in L$ séparable sur k *i.e.* $L = K(x)$ et l'implication (a) $\Rightarrow$ (b) résulte alors de la caractérisation (d) de la séparabilité de x sur K dans la question (7) (et de (2)). Il reste à voir (b) $\Rightarrow$ (a). Si K est de caractéristique 0, l'implication est triviale. Supposons donc K de caractéristique $p > 0$. Soit $x \in L$ tel que $tr_{L|K}(x) \neq 0$. Par la question (2), $tr_{L|K}(x) = [L : K(x)]tr_{K(x)|K}(x)$. Donc $tr_{L|K}(x) \neq 0$ ssi $p \not| [L : K(x)]$ et $tr_{K(x)|K}(x) \neq 0$. Mais $p \not| [L : K(x)]$ implique $L/K(x)$ séparable (dans la question (7) on a vu que si $x \in L$ n'est pas séparable sur K alors $p|[K(x) : K]|[L : K]$) et, d'après la caractérisation (d) de la séparabilité $tr_{K(x)|K}(x) \neq 0$ implique $K(x)/K$ séparable. On conclut en invoquant la transitivité de la séparabilité: si $L/K(x)$ et $K(x)/K$ sont séparables alors L/K est séparable.

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