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

Exercice 1.

(1) Si M est de torsion, pour tout $m \in M$ soit $0 \neq a \in \mathbb{Z}$ tel que $am = 0$. On a alors $m \otimes 1 = m \otimes aa^{-1} = (am) \otimes a^{-1} = 0$. On conclut en utilisant que $M \otimes_{\mathbb{Z}} \mathbb{Q}$ est engendré comme $\mathbb{Z}$-module par les éléments de la forme $m \otimes x$, $m \in M$, $x \in \mathbb{Q}$. Inversement, rappelons que $\mathbb{Q}$ est le localisé de $\mathbb{Z}$ en $S := \mathbb{Z}\backslash\}0\}$ et donc qu'on a un isomorphisme canonique de $\mathbb{Q}$-modules $M \otimes_{\mathbb{Z}} \mathbb{Q} \tilde{\to} S^{-1}M$. Or si $S^{-1}M = 0$, on a en particulier pour tout $m \in M$, $m/1 = 0$ dans $S^{-1}M = 0$ *i.e.* il existe $a \in S$ tel que $am = 0$ dans M.

Mea culpa: j'ai réorganisé un peu les questions à la dernière minute, sans faire attention au fait que la démonstration de: $M \otimes /Z\mathbb{Q} = 0 \Rightarrow M$ de torsion se démontre utilise (2). (Evidemment, je n'ai pas sanctionné).

(2) Cours.

(3) Comme $v : M \to M''$ est surjective pour tout $m'' \in M''$ on peut écrire $m'' = v(m)$ donc $m'' \otimes 1 = v \otimes Id(m \otimes 1)$. On en déduit que $v \otimes Id : M \to M''$ est surjective puisque $M'' \otimes_{\mathbb{Z}} \mathbb{Q}$ est engendré comme $\mathbb{Q}$-module par les éléments de la forme $m'' \otimes 1$, $m'' \in M''$. L'inclusion $im(u \otimes Id) \subset \ker(v \otimes Id)$ est immédiate puisque $(v \otimes Id) \circ (u \otimes Id) = (v \circ u) \otimes Id = 0 \otimes Id = 0$. Inversement, comme dans la question (1), on a un diagramme commutatif dont les flèches verticales sont les isomorphismes canoniques

$$\begin{array}{ccccc} M' \otimes_{\mathbb{Z}} \mathbb{Q} & \xrightarrow{u \otimes Id} & M \otimes_{\mathbb{Z}} \mathbb{Q} & \xrightarrow{v \otimes Id} & M'' \otimes_{\mathbb{Z}} \mathbb{Q} \\ \downarrow \simeq & & \downarrow \simeq & & \downarrow \simeq \\ S^{-1}M' & \xrightarrow[S^{-1}u]{} & S^{-1}M & \xrightarrow[S^{-1}v]{} & S^{-1}M' \end{array}$$

or, l'inclusion $\ker(S^{-1}v) \subset im(S^{-1}u)$ se voit facilement: $m/s \in \ker(S^{-1}v)$ si et seulement si $v(m)/s = 0$ *i.e.* il existe $a \in S$ tel que $av(m) = v(am) = 0$ donc $am \in \ker(v) = im(u)$ ou, encore, il existe $m' \in M'$ tel que $am = u(m')$ *i.e.* $m = u(m')/a = S^{-1}u(m'/a) \in im(S^{-1}u)$. Enfin, il reste à voir que $\ker(S^{-1}u) = 0$ mais pour tout $m' \in M'$, $s \in S$, $S^{-1}u(m'/s) = u(m')/s = 0$ si et seulement si il existe $a \in S$ tel que $au(m') = u(am') = 0$ donc, comme $u : M' \to M$ est injective, cela implique $am' = 0$ donc $m'/1 = 0$.

(4) On rappelle que tout morphisme $f : E \to F$ de K-espaces vectoriels induit un isomorphisme $E/\ker(f) \tilde{\to} im(f)$, d'où on déduit que $dim(E) = dim(\ker(f)) + dim(im(f))$. En particulier, $dim(V) = dim(\ker(v)) + dim(im(v))$. Mais par définition d'une suite exacte courte, $im(v) = V''$ et $ker(v) = im(u) \tilde{\leftarrow} V'$ donc $dim(V) = dim(V') + dim(V'')$.

(5) On note $T_M \subset M$ le sous-$\mathbb{Z}$-module de torsion. On sait alors, par le théorème de structure ($\mathbb{Z}$ est principal!) que M/T_M est un $\mathbb{Z}$-module libre de rang fini r. On a donc une suite exacte courte

$$0 \to T_M \to M \to \mathbb{Z}^{\oplus r} \to 0.$$

Par les questions (1) et (3), on en déduit un isomorphisme de $\mathbb{Q}$-espaces vectoriels

$$M \otimes_{\mathbb{Z}} \mathbb{Q} \tilde{\to} (\mathbb{Z}^{\oplus r}) \otimes_{\mathbb{Z}} \mathbb{Q}.$$

Mais par ailleurs, on a $(\mathbb{Z}^{\oplus r}) \otimes_{\mathbb{Z}} \mathbb{Q} \tilde{\to} (\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q})^{\oplus r} \tilde{\to} (S^{-1}\mathbb{Z})^{\oplus r} \tilde{\to} \mathbb{Q}^{\oplus r}$.

(6) D'après la question (3), on a une suite exacte courte de $\mathbb{Q}$-espaces vectoriels

$$0 \to M' \otimes_{\mathbb{Z}} \mathbb{Q} \to M \otimes_{\mathbb{Z}} \mathbb{Q} \to M'' \otimes_{\mathbb{Z}} \mathbb{Q} \to 0.$$

D'après la question (4)

$$dim(M \otimes_{\mathbb{Z}} \mathbb{Q}) = dim(M' \otimes_{\mathbb{Z}} \mathbb{Q}) + dim(M'' \otimes_{\mathbb{Z}} \mathbb{Q})$$

et on conclut par la question (5).

(7) Anneaux principaux.

(8) Comme $\mathbb{Z}$ est principal et $\mathbb{Z}^{\oplus 3}$ est un $\mathbb{Z}$-module libre de rang 3 on sait déjà que M est un $\mathbb{Z}$-module libre de rang ≤ 3. Par définition M est le noyau du morphisme de $\mathbb{Z}$-modules surjectif $\phi : \mathbb{Z}^{\oplus 3} \twoheadrightarrow \mathbb{Z}/2$, $(a,b,c) \to a+b+c \mathrm{mod} 2$; on a donc une suite exacte courte de $\mathbb{Z}$-modules

$$0 \to M \to \mathbb{Z}^{\oplus 3} \to \mathbb{Z}/2 \to 0.$$

Comme $\mathbb{Z}/2$ est de rang 0, on déduit de la question (6) que M est de rang 3. Notons e_1, e_2, e_3 les vecteurs de la base canonique de $\mathbb{Z}^{\oplus 3}$. Les vecteurs $m_1 = e_1 - e_2$, $m_2 = e_2 - e_3$ et $m_3 = 2e_3$ sont dans M et $\mathbb{Z}$-libres. De plus, tout $(a,b,c) \in M$ peut s'écrire sous la forme

$$(a,b,c) = \alpha m_1 + \beta m_2 + \gamma m_3$$

avec $\alpha = a$, $\beta = a+b$, $\gamma = \frac{a+b+c}{2}$.

Exercice 2.

(1) Clairement $T^p - T - a$ et $(T^p - T - a)' = -1$ sont premiers entre eux. Soit $\alpha \in \overline{K}$ une racine de $T^p - T - a$. On a alors $(\alpha+n)^p - (\alpha+n) - a = (\alpha^p + n^p) - (\alpha+n) - a = \alpha^p - \alpha - a + (n^p - n) = 0$ où on a utilisé qu'en caractéristique p, $(x+y)^p = x^p + y^p$ et que puisque $n \in \mathbb{F}_p$, $n^p = n$. Cela donne $p = deg(T^p - T - a)$ distinctes de $T^p - T - a$ donc on les a toutes.

(2) Si $T^p - T - a$ a une racine α dans K, la question (1) montre qu'il est totalement décomposé dans K. Par contre, si $T^p - T - a$ n'a pas de racine dans K et qu'on note $\alpha \in \overline{K}$ une racine dans $\overline{K}$, si $T^p - T - a$ n'était pas irréductible sur K il posséderait un diviseur dans $K[T]$ de la forme $\prod_{n \in S}(T - \alpha - n)$ avec $F \subset \mathbb{F}_p$ un sous-ensemble de cardinal $< p$. En considérant le terme de degré $|F| - 1$, on aurait alors $|F|\alpha \in K$: contradiction. Donc $T^p - T - a$ est irréductible sur K et est le polynôme minimal de α sur K. D'après la question (1), $K(\alpha) = K[T]/\langle T^p - T - a \rangle$ est alors le corps de décomposition de $T^p - T - a$ sur K donc (puisque $T^p - T - a$ est séparable de degré p)est galoisienne de degré p.
Variante: Notons $\mathcal{D}_F$ l'ensemble des diviseurs irréductibles de $F(T) := T^p - T - a$ dans $K[T]$. Si $P \in \mathcal{D}_F$, $P(T+1) \in \mathcal{D}_{F(T+1)}$ (observer que $F(T) \to F(T+1)$ est un automorphisme de la K-alg'ebre $K[T]$). Or on a vu en (1) (a) que $F(T+1) = F(T)$. Cela nous donne une action de $\mathbb{F}_p$ sur $\mathcal{D}_F$: $\mathbb{F}_p \times \mathcal{D}_F \to \mathcal{D}_F$, $(n,P) \to P(T+n)$. Mais comme p est premier, $|\mathbb{F}_p \cdot P| = 1, p$. Si $|\mathbb{F}_p \cdot P| = 1$, P a au moins p racines distinctes donc $P = F$ est irréductible. Si $|\mathbb{F}_p \cdot P| = p$, les $P(T+n)$, $n \in \mathbb{F}_p$ fournissent p diviseurs irréductibles distincts de F; ils sont donc nécessairement de degré 1 et F est totalement décomposé sur 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) $\ker(\epsilon) = L^{\langle\sigma\rangle} = L^{Gal(L/K)} = K$ par la correspondance de Galois.
   (b) On a $\epsilon^p = \sigma^p - Id^p = Id - Id = 0$, la première égalité venant du fait qu'on est en caractéristique p (plus précisément $\epsilon^p = \sigma^p + (-1)^p Id^p$ mais $(-1)^p = -1$ - même lorsque $p = 2$...) et la seconde du fait que σ est d'ordre p.
   (c) Si $\ker(\epsilon) = \ker(\epsilon^2)$ on aurait $K = \ker(\epsilon) = \ker(\epsilon^2) = \cdots = \ker(\epsilon^p) = L$: contradiction.
   (d) Soit $x \in \ker(\epsilon^2) \setminus \ker(\epsilon)$ et $\alpha := \frac{x}{\epsilon(x)}$. Puisque $\epsilon(x) \in \ker(\epsilon) = K$ et $x \notin \ker(\epsilon) = K$, on a $\alpha \notin K$. Par contre $\sigma(\alpha) - \alpha = \frac{\sigma(x) - x}{\epsilon(x)} = 1$ donc $\sigma(\alpha) = \alpha + 1$. On en déduit $\sigma(\alpha^p) = \sigma(\alpha)^p = \alpha^p + 1$ donc $\epsilon(\alpha^p - \alpha) = \sigma(\alpha)^p - \sigma(\alpha) = \alpha^p - \alpha$ *i.e.* $\alpha^p - \alpha \in \ker(\epsilon) = K$. D'après la question (1), $T^p - T - (\alpha^p - \alpha) \in K[T]$ est donc irréductible sur K.
   (e) Puisque $L \supset K(\alpha) \simeq K[T]/\langle T^p - T - (\alpha^p - \alpha) \rangle$ sont de même degré, on a en fait $L \simeq K(\alpha)$.

(4) On note $F : K \to K$, $x \to x^p$ le Frobenius.
   (a) Il faut montrer que tout polynôme irréductible P de $K[T]$ est séparable *i.e.* est premier avec sa dérivée ou, encore, est de dérivée non nulle. Or $P'(T) = 0$ si et seulement si $P = Q(T^p) = \sum_{0 \leq n \leq d} a_n T^{pn} = \sum_{0 \leq n \leq d} b_n^p T^{pn} = (\sum_{0 \leq n \leq d} b_n T^n)^p$: contradiction.
   (b) Supposons $F(K) \subsetneq K$, et soit $a \in K \setminus F(K)$ et $\alpha \in \overline{K}$ une racine de $T^p - a \in K[T]$. On a alors $T^p - a = T^p - \alpha^p = (T - \alpha)^p$. Donc si $T^p - a$ n'était pas irréductible sur K, il aurait un facteur de la forme $(T - \alpha)^n$ avec $1 \leq n < p$. En considérant le terme de degré $n - 1$, a-on aurait alors $n \in \alpha \in K$ donc $\alpha \in K$: contradiction puisque $a \notin F(K)$.
   (c) Si on trouve un corps K comme dans la question (4) (b) on aura gagné puisque l'extension $K(\alpha) = K[T]/\langle T^p - a \rangle$ est normale de degré p mais pas séparable. Prenons par exemple $K = \mathbb{F}_p(T)$ et $a = T$.

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

(1) $P_a(T) := (T-a)(T-b) = T^2-10T+4 \in \mathbb{Q}[T]$ est de degré 2 sans racine dans $\mathbb{Q}$ donc est irréductible sur $\mathbb{Q}$. C'est donc le polynôme minimal de a sur $\mathbb{Q}$. De plus, $ab = 4 \in \mathbb{Q}$ donc $b = 4a^{-1} \in \mathbb{Q}(a)$. Cela montre que P_a est totalement décomposé sur $\mathbb{Q}$. Autrement dit, $\mathbb{Q}(a)$ est le corps de décomposition du polynôme (évidemment séparable puisqu'on est en caractéristique 0) P_a. C'est donc une extension galoisienne de $\mathbb{Q}$, de degré $[\mathbb{Q}(a) : \mathbb{Q}] = deg(P_a) = 2$. Comme il n'y a qu'un seul groupe d'ordre 2 - $\mathbb{Z}/2$ - on a forcément $Gal(\mathbb{Q}(a)/\mathbb{Q}) \simeq \mathbb{Z}/2$ (explicitement, le générateur de $Gal(\mathbb{Q}(a)/\mathbb{Q})$ est le $\mathbb{Q}$-automorphisme de $\mathbb{Q}(a)$ qui échange a et b.

(2) $Q_\alpha(T) = (T-\alpha)(T+\alpha) = T^2 - a \in \mathbb{Q}(a)[T]$ est annulateur de α. Pour montrer qu'il est irréductible sur $\mathbb{Q}(a)$, il faut montrer que $\alpha \notin \mathbb{Q}(a)$. Sinon, on pourrait écrire $\alpha = u + v\sqrt{21}$ avec $u, v \in \mathbb{Q}$ donc $a = 5 + \sqrt{21} = u^2 + 21v^2 + 2uv\sqrt{21}$. D'où $2uv = 1$ et $5 = u^2 + 21v^2 = u^2 + \frac{21}{4u^2}$ ou encore $0 = 4u^4 - 20u^2 + 21$. Mais le polynôme $4T^4 - 20T^2 + 21$ n'a pas de racines dans $\mathbb{Q}$ (ses racines sont $\pm\sqrt{\frac{7}{2}}, \pm\sqrt{\frac{3}{2}}$ comme on le voit en résolvant d'abord $0 = 4\Theta^2 - 20\Theta + 21$). De la même façon, on montre que $Q_\beta(T) = (T-\beta)(T+\beta) = T^2 - b \in \mathbb{Q}(b)[T]$ est le polynôme minimal de β sur $\mathbb{Q}(a)$.

(3) On a $[\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}(a)][\mathbb{Q}(a) : \mathbb{Q}] = 2 \cdot 2 = 4$ d'après les questions (1) et (2). En particulier, le polynôme minimal de α sur $\mathbb{Q}$ est de degré 4. Si on trouve un polynôme de $\mathbb{Q}[T]$ de degré 4 qui annule α, on aura gagné. Or $P_\alpha = (T^2-5)^2 - 21 = T^4 - 10T^2 + 4 \in \mathbb{Q}[T]$ convient.

(4) On a $ab = 4$ donc $\alpha\beta = 2$ donc $\beta = 2\alpha^{-1} \in \mathbb{Q}(\alpha)$.

(5) Comme on est en caractéristique 0, il suffit de montrer que $\mathbb{Q}(\alpha)$ est le corps de décomposition de P_α. Or les racines de P_α sont $\pm\alpha$, $\pm\beta$. Donc la conclusion résulte de la question (4).

(6) D'après la question (1), $\mathbb{Q}(a)/\mathbb{Q}$ est une sous-extension galoisienne de $\mathbb{Q}(\alpha)/\mathbb{Q}$. Il résulte donc de la correspondance de Galois que le morphisme de restriction $\sigma \to \sigma|_{\mathbb{Q}(a)}$ induit une suite exacte courte de groupes

$$1 \to Gal(\mathbb{Q}(\alpha)/\mathbb{Q}(a)) \to Gal(\mathbb{Q}(\alpha)/\mathbb{Q}) \to Gal(\mathbb{Q}(a)/\mathbb{Q}) \to 1$$

(7) Comme $Gal(\mathbb{Q}(\alpha)/\mathbb{Q}(a))$ est d'ordre 2, on dispose déjà du générateur σ de $Gal(\mathbb{Q}(\alpha)/\mathbb{Q}(a))$ (explicitement, c'est le $\mathbb{Q}$-automorphisme de $\mathbb{Q}(\alpha)$ qui fixe a, b et échange α, $-\alpha$ d'une part et β, $-\beta$ d'autre part). Il suffit d'exhiber un autre élément d'ordre 2 qui n'est pas dans le noyau. Pour cela, considérons le générateur τ de $Gal(\mathbb{Q}(a)/\mathbb{Q})$. Il envoie Q_α sur Q_β donc ses antécédents par la projection $Gal(\mathbb{Q}(\alpha)/\mathbb{Q}) \twoheadrightarrow Gal(\mathbb{Q}(a)/\mathbb{Q})$ sont les $\mathbb{Q}$-automorphismes $\tau^\pm$ de $\mathbb{Q}(\alpha)$ définis respectivement par $\tau^+(\alpha, -\alpha) = (\beta, -\beta)$ et $\tau^-(\alpha, -\alpha) = (-\beta, \beta)$. Ils sont tous deux d'ordre 2.
Variante: On peut aussi utiliser que le morphisme d'évaluation $Gal(\mathbb{Q}(\alpha)/\mathbb{Q}) \to Z_{\mathbb{Q}(\alpha)}(P_\alpha)$ est bijectif et donc calculer explicitement $Gal(\mathbb{Q}(\alpha)/\mathbb{Q})$: $\sigma^\pm(\alpha) = \pm\alpha$, $\tau^\pm(\alpha) = \pm\beta$. On a alors $\sigma^+ = Id$ et σ^-, τ^+, τ^- d'ordre 2.

(8) Comme $Gal(\mathbb{Q}(\alpha)/\mathbb{Q})$ est d'ordre 4, il n'y a que deux possibilités: $Z/4$ ou $\mathbb{Z}/2 \times \mathbb{Z}/2$. Mais $\mathbb{Z}/4$ n'a qu'un élément d'ordre 4 donc c'est nécessairement $\mathbb{Z}/2 \times \mathbb{Z}/2$.

(9) Avec les notations de la question (8), on a 3 sous-extensions non triviales de degé 2 de $\mathbb{Q}(\alpha)/\mathbb{Q}$ correspondant aux trois sous-groupes $\langle\sigma\rangle$, $\langle\tau^+\rangle$, $\langle\tau^-\rangle$ de $Gal(\mathbb{Q}(\alpha)/\mathbb{Q})$. Explicitement, il s'agit de

$$\mathbb{Q}(a) = \mathbb{Q}(\alpha)^{\langle\sigma\rangle},\ \mathbb{Q}(\alpha+\beta) = \mathbb{Q}(\alpha)^{\langle\tau^+\rangle},\ \mathbb{Q}(\alpha-\beta) = \mathbb{Q}(\alpha)^{\langle\tau^-\rangle}$$

En effet, les inclusions $\subset$ sont claires et puisque $(\alpha+\beta)^2 = 14$ donc $\alpha+\beta = \sqrt{14} \notin \mathbb{Q}$ et $(\alpha-\beta)^2 = 6$ donc $\alpha-\beta = \sqrt{6} \notin \mathbb{Q}$, ce sont des égalités.

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