Examen 2ème Session 2020/2021 - Correction
4M002 - Algèbre et théorie de Galois
Anna Cadoret

Exercice. Soit p un nombre premier. On note $\mathcal{S}_p$ le groupe des permutations de $\{1,\dots,p\}$.

(1) (a) Soit $c \in \mathcal{S}_p$ un p-cycle et $\tau \in \mathcal{S}_p$ une transposition. Notons $G \subset \mathcal{S}_p$ le sous-groupe engendré par c, τ. Quitte à renuméroter, on peut supposer $\tau = (1,2)$ et $c = (1, a_2, \dots, a_p)$ avec $a_k = 2$ pour un certain $2 \leq k \leq p$. Quitte à remplacer c par c^{k-1}, qui est encore un p-cycle puisque p est premier, on peut supposer que $c = (1,2,a_3,\dots,a_p)$. Enfin, quitte à renuméroter $\{a_3,\dots,a_p\} = \{3,\dots,p\}$, on peut supposer que $c = (1,2,\dots,p)$. On a alors $c^k \tau c^{-k} = (k+1, k+2) \in G$, $k = 1,\dots,p$ puis $(1,2)(2,3)(1,2) = (1,3) \in G$, $(1,3)(3,4)(1,3) = (1,4) \in G$ et par itération $(1,k) \in G$, $k = 1,\dots,p$ donc $(1,i)(1,j)(1,i) = (i,j) \in G$, $1 \leq i \neq j \leq p$.

(b) Soit $c \in \mathcal{S}_p$ d'ordre p. C'est un p-cycle ssi il agit transitivement sur $Z := \{1,\dots,p\}$. Or, comme p est premier, toute orbite non-triviale de c agissant sur Z est de longueur exactement p.

(2) Soit $P(T) \in \mathbb{Q}[T]$ irréductible de degré p ayant exactement deux racines non réelles. On note $K/\mathbb{Q}$ le corps de décomposition de P sur $\mathbb{Q}$.

(a) $K/\mathbb{Q}$ est normale puisque c'est le corps de décomposition d'un polynôme et séparable puisqu'on est en caractéristique 0. On note $G := Gal(K|\mathbb{Q})$ son groupe de Galois.

(b) Notons $Z := Z_K(P) = \{\alpha_1,\dots,\alpha_p\} \subset K$ les racines de $P(T)$ dans K. Puisque P est à coefficients dans $\mathbb{Q}$, l'action naturelle de G sur K stabilise Z et définit donc un morphisme de groupe $G \to \mathcal{S}_p = \mathcal{S}(Z)$. Ce morphisme est injectif car, par définition, $K = \mathbb{Q}(Z)$. On peut donc identifier G à un sous-groupe de $\mathcal{S}_p$. Ce sous-groupe est transitif sur Z. En effet, sinon, il existe une orbite $\mathcal{O} \in Z/G$ de cardinal $1 \leq |\mathcal{O}| < p$. Posons $P_{\mathcal{O}}(T) := \prod_{\alpha\in\mathcal{O}}(T-\alpha) = \sum_{0\leq i\leq|\mathcal{O}|} a_i T^i \in K[T]$. Comme $\mathcal{O}$ est G-stable et que G agit par automorphisme de K-algèbre sur $K[T]$, on a pour tout $\sigma \in G$,

$$\begin{array}{ll} \sigma \cdot P_{\mathcal{O}}(T) & = \prod_{\alpha\in\mathcal{O}}(T-\sigma(\alpha)) = \prod_{\alpha\in\mathcal{O}}(T-\alpha) = P_{\mathcal{O}}(T) \\ & \sum_{0\leq i\leq|\mathcal{O}|} \sigma(a_i) T^i \end{array}$$

Donc $a_i \in K^G$, $i = 0,\dots|\mathcal{O}|$. Comme $K/\mathbb{Q}$ est galoisienne de groupe G, $K^G = \mathbb{Q}$. Mais cela contredit l'irréductibilité de $P(T)$ sur $\mathbb{Q}$.

(c) D'après (2) (b), G contient un sous-groupe d'indice p. En particulier, $p||G|$. Par le lemme de Cauchy, G contient un élément d'ordre p, qui est un p-cycle d'après (1) (b).

(d) On peut supposer que K est plongé dans $\mathbb{C}$. Puisque $P(T)$ est à coefficient dans $\mathbb{Q}$, la conjugaison complexe $\iota : \mathbb{C} \tilde{\to} \mathbb{C}$ stabilise Z donc $K = \mathbb{Q}(Z)$. Par hypothèse P possède exactement deux racines non-réelles, qui sont donc échangées par ι alors que les $p-2$ racines réelles, elles, sont invariantes par ι. Autrement dit, la restriction $\iota|_K^K$ de ι à K induit une transposition de Z. Puisque d'après (2) (c), G contient aussi un p-cycle, on conclut par (1).

(3) Montrons que $P(T) = T^5 - 6T + 3 \in \mathbb{Q}[T]$ est irréductible et admet exactement deux racines non réelles. Pour l'irréductibilité, on peut appliquer Eisenstein pour le premier 3. Pour voir que $P(T)$ admet exactement deux racines non réelles, on étudie les variations de la fonction $P : t \to P(t)$ sur $\mathbb{R}$ et on observe qu'elle admet exactement trois zéros sur $\mathbb{R}$, dans les intervalles $]-\infty, -(\frac{6}{5})^{1/4}[$, $]-(\frac{6}{5})^{1/4}, (\frac{6}{5})^{1/4}[$ et $](\frac{6}{5})^{1/4}, +\infty[$.

Problème. Soit $\phi : A \to B$ un morphisme d'anneaux (qui munit donc B d'une structure de A-algèbre donc de R-module) et M un B-module.

(1) On fait agir B sur $Der_A(B,M)$ par l'action induite de celle de B sur $M^B(\supset Der_A(B,M))$ *i.e.* $\beta \cdot d : B \to M$ est défini par $(\beta \cdot d)(b) = \beta d(b)$.

(2) On note $F := \oplus_{b\in B} Bdb$ le B-module libre de base indexée par les éléments de B et $R \subset F$ le sous-B-module engendré par les éléments de la forme $d(bb') - bdb' - b'db$, $d(b+b') - db - db'$, $b, b' \in B$ et da, $a \in A$. Soit $d_{B|A} : B \to F/R =: \Omega^1_{B|A}$ la composée de l'application $B \hookrightarrow F$, $b \mapsto db$ et de la projection canonique $F \twoheadrightarrow \Omega^1_{B|A}$.

(a) Le fait que $d_{B|A} : B \to F/R =: \Omega^1_{B|A}$ est une A-dérivation résulte tautologiquement de la construction.

(b) Soit M un B-module et $d : B \to M$ une A-dérivation. S'il existe un morphisme de B-modules $\phi : \Omega^1_{B|A} \to M$ tel que $\phi \circ d_{B|A} = \delta$, on a nécessairement $\phi(d_{B|A}b) = \delta b$, $b \in B$. Comme, par construction, $\Omega^1_{B|A}$ est engendré comme B-module par les $d_{B|A}b$, $b \in B$, cela montre déjà l'unicité de ϕ sous réserve de son existence. Montrons l'existence. Pour cela, utilise la propriété universelle du B-module libre F, qui nous assure qu'il existe un unique morphisme de B-module $\widetilde{\phi} : F \to M$ tel que $\widetilde{\phi}(db) = \delta b$, $b \in B$. Comme $\delta : B \to M$ est une A-dérivation, on a $R \subset \ker(\widetilde{\phi})$ donc le morphisme de B-module $\widetilde{\phi} : F \to M$ passe au quotient en un morphisme de B-module $\phi : F/R \to M$ tel que $\phi \circ d_{B|A} = \delta$.

Rem. On notera que $\Omega^1_{B|A}$ est engendré, comme B-module, par les db, $b \in B$.

(3) On suppose que $B = A[\underline{T}] := A[T_1, \ldots, T_r]$ est la A-algèbre des polynômes à r indéterminées sur A et soit $\delta : A[\underline{T}] \to M$ une A-dérivation. On a par induction sur a que $\delta T^a = aT^{a-1}\delta T$ puis par induction sur r que $\delta(\underline{T}^{\underline{a}}) = \sum_{1\le i\le r} a_i T_1^{a_1} \cdots T_i^{a_i - 1} \cdots T_r^{a_r} \delta T_i$ et on conclut par A-linéarité. Autrement dit, $\delta : A[\underline{T}] \to M$ est uniquement déterminée par ses valeurs en $T_1, \ldots, T_r$. Inversement, on vérifie que l'application $d : A[\underline{T}] \to \oplus_{1\le i\le r} A[\underline{T}]dT_i$ définie par $dP = \sum_{1\le i\le r} \frac{\partial P}{\partial T_i} dT_i$ est bien une A-dérivation et qu'elle vérifie la propri'eté universelle de $d_{A[\underline{T}]|A} : A[\underline{T}] \to \Omega^1_{A[\underline{T}]|A}$. En effet, par propriété universelle de la somme directe $\oplus_{1\le i\le r} A[\underline{T}]dT_i$, pour toute A-dérivation $\delta : A[\underline{T}] \to M$ il existe un unique morphisme de $A[\underline{T}]$-modules $\phi : \oplus_{1\le i\le r} A[\underline{T}]dT_i \to M$ tel que $\phi(dT_i) = \delta(T_i)$, $i = 1, \ldots, r$ et la relation (*) montre que cela implique automatiquement $\phi \circ d = \delta$. On conclut par unicité de l'objet universel à unique isomorphisme près.

(4) Soit $\psi : B \to C$ un morphisme de A-algèbre.

(a) Comme $d_{C|A} \circ \psi : B \to \Omega^1_{C|A}$ est une A-dérivation, il existe un unique morphisme de B-modules $\gamma : \Omega^1_{B|A} \to \Omega^1_{C|A}$ tel que $\gamma \circ d_{B|A} = d_{C|A} \circ \psi$. Cela permet de définir l'application $\Omega^1_{B|A} \times C \to \Omega^1_{C|A}$, $(\omega, c) \mapsto c\gamma(\omega)$, dont on vérifie immédiatement qu'elle est B-bilinéaire donc, par propriété universelle de $\otimes_B$ se factorise en un morphisme de B-modules $g : \Omega^1_{B|A} \otimes_B C \to \Omega^1_{C|A}$, qui, par construction, est aussi un morphisme de C-modules quand on munit $\Omega^1_{B|A} \otimes_B C$ de la structure de C-module $c_0 \cdot (\omega \otimes c) = \omega \otimes (c_0 c)$. Explicitement $g(d_{B|A}b \otimes c) = c d_{C|A}(\psi(b))$. Comme $d_{C|B} : C \to \Omega^1_{C|B}$ est une B-dérivation donc *a fortiori* une A-dérivation, il existe un unique morphisme de C-modules $h : \Omega^1_{C|A} \to \Omega^1_{C|B}$ tel que $h \circ d_{C|A} = d_{C|B}$.

(b) On veut montrer que la suite de C-modules

$$\Omega^1_{B|A} \otimes_B C \xrightarrow{g} \Omega^1_{C|A} \xrightarrow{h} \Omega^1_{C|B} \to 0$$

est exacte.

- On a $h \circ d_{C|A} = d_{C|B}$ donc comme $\Omega^1_{C|B}$ (resp. $\Omega^1_{C|A}$) est engendré comme C-module par les $d_{C|B}c$, $c \in C$ (resp. les $d_{C|A}c$, $c \in C$), le morphisme de C-modules $h : \Omega^1_{C|A} \to \Omega^1_{C|B}$ est surjectif.

- On a $h \circ g((d_{B|A}b) \otimes 1) = d_{C|B}(\psi(b)) = 0$ puisque $d_{C|B} : C \to \Omega^1_{C|B}$ est une B-dérivation. Comme les éléments $d_{B|A}b) \otimes 1$, $b \in B$ engendrent $\Omega^1_{B|A} \otimes_B C$ comme C-module, on en déduit

$im(g) \subset \ker(h)$.

- Notons $I := im(g)$. Comme $I \subset \ker(h)$, le morphisme surjectif de C-modules $h : \Omega^1_{C|A} \twoheadrightarrow \Omega^1_{C|B}$ se factorise en $\overline{h} : \Omega^1_{C|A}/I \twoheadrightarrow \Omega^1_{C|B}$ et on a $I = \ker(h)$ ssi $\overline{h} : \Omega^1_{C|A}/I \twoheadrightarrow \Omega^1_{C|B}$ est un isomorphisme. Construisons donc un inverse de $\overline{h} : \Omega^1_{C|A}/I \twoheadrightarrow \Omega^1_{C|B}$. Par propriété universelle du C-module libre $\oplus_{c\in C} Cdc$, il existe un unique morphisme de C-modules $f : \oplus_{c\in C} Cdc \to \Omega^1_{C|A}/I$ tel que $f(dc) = d_{C|A}(c)[I]$. De plus, on a $f(cc') - cf(c') - c'f(c) = d_{C|A}(cc') - cd_{C|A}c' - c'd_{C|A}(c)[I] = 0$ puisque $d_{C|A} : C \to \Omega^1_{C|A}$ est une A-dérivation et $f(\phi(b)) = d_{C|A}(\psi(b))[I] = g(d_{B|A}b \otimes 1)[I] = 0$, par définition de $I = im(g)$. Cela montre que $f : \oplus_{c\in C} Cdc \to \Omega^1_{C|A}/I$ se factorise en un morphisme de C-modules $\overline{f} : \Omega^1_{C|B} \to \Omega^1_{C|A}/I$, dont on vérifie immédiatement que c'est un inverse de $\overline{h} : \Omega^1_{C|A}/I \twoheadrightarrow \Omega^1_{C|B}$.

(c) Supposons que $\psi : B \twoheadrightarrow C$ est surjective; on note $I := \ker(\psi) \subset B$ son noyau, qui est un idéal de B de sorte que $\psi : B \twoheadrightarrow C$ s'identifie au morphisme quotient $p_I : B \twoheadrightarrow B/I$.

(i) Comme $\psi : B \twoheadrightarrow C$, $\Omega^1_{C|B}$ est engendré comme C-module par les $d_{C|B}\psi(b)$, $b \in B$. Mais comme $d_{C|B} : C \to \Omega^1_{C|B}$ est une B-dérivation, on a, par définition, $d_{C|B}\psi(b) = 0$, $b \in B$.

(ii) La structure naturelle de B-module sur I/I^2 passe au quotient en une structure de $B/I = C$-module. Notons $\widetilde{f} : I \to \Omega^1_{B|A} \otimes C$ le morphisme de A-modules défini par $\widetilde{f}(a) = d_{B|A}a \otimes 1$. Comme pour tout $a, b \in I$, $\widetilde{f}(ab) = d_{B|A}b \otimes a + d_{B|A}a \otimes b$ et $a = b = 0[I]$, $\widetilde{f} : I \to \Omega^1_{B|A} \otimes C$ se factorise en un morphisme de A-modules $f : I/I^2 \to \Omega^1_{B|A} \otimes C$. En outre, pour tout $a \in I$, $b \in B$ on a $f(ba[I^2]) = d_{B|A}(ba) \otimes 1 = d_{B|A}a \otimes b + d_{B|A}b \otimes a = d_{B|A}a \otimes b = b \cdot f(a[i^2])$ donc $f : I/I^2 \to \Omega^1_{B|A} \otimes C$ est bien C-linéaire.

(iii) On veut montrer que la suite de C-modules

$$I/I^2 \xrightarrow{f} \Omega^1_{B|A} \otimes_B C \xrightarrow{g} \Omega^1_{C|A} \to 0$$

est exacte. D'après (4) (b) et (4) (c) (i) on sait déjà que $g : \Omega^1_{B|A} \otimes_B C \to \Omega^1_{C|A}$ est surjective. On a $g \circ f(a) = d_{C|A}d_{B|A}\psi(a) = 0$ puisque $I = \ker(\psi)$. Donc $J := im(f) \subset \ker(g)$ et $g : \Omega^1_{B|A} \otimes_B C \twoheadrightarrow \Omega^1_{C|A}$ se factorise donc en un morphisme de C-modules $\overline{g} : \Omega^1_{B|A} \otimes_B C/J \twoheadrightarrow \Omega^1_{C|A}$. Comme en (4) (b), on construit un inverse de $\overline{g} : \Omega^1_{B|A} \otimes_B C/J \twoheadrightarrow \Omega^1_{C|A}$ comme suit. Fixons un section (ensembliste) $s : C = B/I \to B$ de $\psi : B \twoheadrightarrow C$. Par propriété universelle de $\oplus_{c\in C} Cdc$ il existe un unique morphisme de C-modules $k : \oplus_{c\in C} Cdc \to \Omega^1_{B|A} \otimes_B C/J$ tel que $k(dc) = d_{B|A}s(c) \otimes 1[J]$. Cette définition est indépendante de $s : C = B/I \to B$ car si $b, b' \in B$ sont tels que $b - b' \in I$ on a $d_{B|A}b \otimes 1 - d_{B|A}b' \otimes 1 = d_{B|A}(b - b') \otimes 1 \in J$. En particulier, pour tout $c = \psi(b)$, $c' = \psi(b')$,

$$\begin{aligned} k(d(cc') - cdc' - c'dc) &= (d_{B|A}s(cc') \otimes 1 - d_{B|A}s(c') \otimes c - d_{B|A}s(c) \otimes c')[J] \\ &= (d_{B|A}bb' \otimes 1 - bd_{B|A}b' \otimes 1 - b'd_{B|A}b \otimes 1)[J] \\ &= ((d_{B|A}(bb') - bd_{B|A}b' - b'd_{B|A}b) \otimes 1)[J] = 0. \end{aligned}$$

Enfin, pour tout $a \in A$ on a $k(d\psi\phi(a)) = d_{B|A}(\phi(a)) \otimes 1[J] = 0$ puisque $d_{B|A} : B \to \Omega^1_{B|A}$ est une A-dérivation. Cela montre que $k : \oplus_{c\in C} Cdc \to \Omega^1_{B|A} \otimes_B C/J$ se fcatorise en un morphisme de C-modules $\overline{k} : \Omega^1_{B|A} \to \Omega^1_{B|A} \otimes_B C/J$ dont on vérifie immédiatement que c'est un inverse de $\overline{g} : \Omega^1_{B|A} \otimes_B C/J \twoheadrightarrow \Omega^1_{C|A}$.

(5) Soit $P \in A[\underline{T}] \setminus A$; notons $I := A[\underline{T}]P$ et $\psi : A[\underline{T}] \twoheadrightarrow C := A[\underline{T}]/I$ l'anneau quotient. En appliquant (4) (c) (iii) on obtient une suite exacte de C-modules

$$I/I^2 \xrightarrow{f} \Omega^1_{A[\underline{T}]|A} \otimes_{A[\underline{T}]} C \xrightarrow{g} \Omega^1_{C|A} \to 0.$$

D'après (3), $\Omega^1_{A[\underline{T}]|A} = \oplus_{1\leq i\leq r} A[\underline{T}dT_i)$ donc en utilisant que $\otimes$ et $\oplus$ commutent et que $A[\underline{T}]\otimes_{A[\underline{T}]} C = C$, on déduit $\Omega^1_{A[\underline{T}]|A}\otimes_{A[\underline{T}]} C = \oplus_{1\leq i\leq r} CdT_i)$. Enfin, le morphisme $f : I/I^2 \to \Omega^1_{A[\underline{T}]|A}\otimes_{A[\underline{T}]} C = \oplus_{1\leq i\leq r} CdT_i$ est explicitement donné par $f(QP[I^2]) = d_{A[\underline{T}]|A}(QP)\otimes 1 = d_{A[\underline{T}]|A}P\otimes Q + d_{A[\underline{T}]|A}Q\otimes P = d_{A[\underline{T}]|A}P\otimes Q$. En aparticulier, l'image de f s'identifie au sous-C-module $CdP \subset \oplus_{1\leq i\leq r} CdT_i)$.

(6) Soit K/k une extension de corps finie.

(a) On construit K^s inductivement en utilisant la transitivité de la séparabilité. Si $K \setminus k$ ne contient aucun élément séparable, on pose $K^s = k$. Sinon, on fixe un élément séparable $a_1 \in K \setminus k$ séparable sur k et on pose $K_1 := k(a_1)$, qui est séparable sur k puisque a_1 l'est. Si $K \setminus K_1$ ne contient aucun élément séparable sur k, on pose $K^s = K_1$. Sinon, on fixe un élément séparable $a_2 \in K \setminus K_1$ séparable sur k donc sur K_1 et on pose $K_2 := K_1(a_2)$, qui est séparable sur K_1 puisque a_2 l'est. Par transitivité de la séparabilité K_2 est séparable sur k. On itère le procédé, qui s'arrête au bout d'un nombre fini d'itération puisque K/k est finie.

(b) Par définition / construction les éléments de $K \setminus K^s$ ne sont pas séparables. Rappelons que $x \in K$ n'est pas séparable sur k signifie que son polynôme minimal $P = T^n + \sum_{0\leq i\leq n-1} a_i T \in k[T]$ vérifie $P' = 0$. Cela ne peut se produire que si k est de car. $p > 0$, auquel cas, P s'écrit sous la forme $P(T) = P_1(T^p)$ avec $P_1 \in k[T_1]$ irréductible. En itérant, on obtient $P(T) = P_r(T^{p^r})$ avec $P_r \in k[T_r]$ irréductible, séparable. En particulier, $x^{p^r} \in K^s$ et le polynôme minimal de a sur K^s divise $T^{p^r} - x^{p^r} = (T-x)^{p^r}$. Comme K/k est finie, on peut écrire $K = K_0(x)$ avec $K^s \subset K_0 \subset\neq K$. Le polynôme minimal $P_0(T) \in K_0[T]$ de a sur K_0 divise le polynôme minima de x sur K^s donc, d'après ce qu'on vient de voir, divise un polynôme de la forme $T^{p^r} - x^{p^r}$ donc n'est pas séparable.

(c) Supposons K/k séparable. Par l'élément primitif, $K = k(x)/k$ est monogène donc si on note $P \in k[T]$ le polynôme minimal de x sur k, $K \simeq k[T]/P$. D'après (5), $\Omega^1_{K|k} = KdT/KdP = KdT/KP'(T)dT$. Mais comme P' et P sont premiers entre eux, par Bézout, $P'(T)$ est inversible (*i.e.* non nul) dans $K = k[T]/P$ donc $\Omega^1_{K|k} = 0$. Inversement, si K/k n'est pas séparable, d'après (6) (b), on peut écrire $K = K_0(x)$ avec le polynôme minimal P de x sur K_0 de dérivée nulle. Donc $\Omega^1_{K|K_0} \simeq (K_0[T]/P)dT = KdT \neq 0$ (même calcul que ci-dessus). Mais d'après la suite exacte de (4) (b) (appliquée avec $A = k \subset B = K_0 \subset C = K$), on a un morphisme surjectif de K-modules $\Omega^1_{K|k} \twoheadrightarrow \Omega_{K|K^1_0} \neq 0$.

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