Correction Examen 2ème Session 2018/2019
4M002 - Algèbre et théorie de Galois
Anna Cadoret

Exercice 1. Soit k un corps.

(1) Il suffit de vérifier la stabilité par combinaison k-linéaire, composition et que $1 \in A$. Pas de difficultés.

(2) Clairement $T^2, T^3 \in A$ et par propriété universelle de la k-algèbre des polynômes à deux indéterminées, il existe un unique morphisme de k-algèbre $\phi := ev_{(T^2,T^3)} : k[X,Y] \to A$ tel que $\phi(X) = T^2$, $\phi(Y) = T^3$. On a donc $im(\phi) = k[T^2, T^3] \subset A$. Pour l'inclusion réciproque, on écrit $P(T) = a_d T^d + \cdots + a_0$. La condition $P(0) = 0$ s'écrit alors $a_1 = 0$. Or un entier $n \geq 2$ peut toujours s'écrire sous la forme $n = 2a+3b$ avec a, b des entiers ≥ 0 (effectuer la division euclidienne de n par 3 pour obtenir $n = 3q + r$ avec $r = 0, 1, 2$; si $r = 1$, écrire $n = 3(q-1) + 4...$). Donc ϕ est surjective. On a clairement $\langle X^3 - T^3 \rangle \subset \ker(\phi)$. Si $P(X,Y) \in \ker(\phi)$, en regardant P comme un polynôme dans $k[X][Y]$, on effectue la division euclidienne de P par Y^2 pour obtenir $P(X,Y) = Q(X,Y)Y^2 + A(X)Y + B(X)$. En appliquant ϕ, on en déduit $A(T^2)T^3 + B(T^2) = 0$, ce qui n'est possible que si $A = B = 0$ en comparant la parité des degrés des monômes dans $A(T^2)T^3$ (impaires) et $B(T^2)$ (paires). Donc $\ker(\phi) = \langle X^3 - T^3 \rangle$ et ϕ se factorise en un isomorphisme $k[X,Y]/\langle X^3 - Y^2 \rangle \tilde{\to} A$.

(3) Pour $a = 2, 3$ écrire $T^a = P(T)Q(T)$ avec $P = a_m T^m + \cdots + a_0, Q = b_n T^n + \cdots + b_0 \in A$ *i.e.* $a_1 = b_1 = 0$ et identifier les coefficients pour montrer que nécessairement $P = T^a$ ou $Q = T^a$.

(4) $T^6 = (T^3)^2 = (T^2)^3$; on n'a donc pas unicité de la décomposition de T^6 en irréductible.

(5) On sait que A n'est pas principal puisqu'il n'est pas factoriel. La question (2) suggère de considérer l'idéal image de $\langle X, Y \rangle$ *i.e.* $\langle T^2, T^3 \rangle \subset A$. S'il était principal, on aurait $P \in A$ de degré ≥ 2 tel que $T^2 = Q(T)P$ avec $Q \in A$, donc P de degré 2, ce qui force $P = a_2 T^2$ avec $0 \neq a_2$ (et $Q = 1$), et $T^3 = R(T)P$, ce qui force $R = a_2^{-1} T \notin A$: contradiction.

Exercice 2. Soit k un corps quelconque, V un k-espace vectoriel de dimension finie et $u : V \to V$ un endomorphisme du k-espace vectoriel V. On note $C(u) \subset \mathrm{End}_k(V)$ la sous-k-algèbre des endomorphismes qui commutent avec u.

(1) Il suffit de vérifier la stabilité par combinaison k-linéaire, composition et que $Id \in C(u)$. Pas de difficultés.

(2) Clairement $u \in C(u)$ et par propriété universelle de la k-algèbre des polynômes, il existe un unique morphisme de k-algèbre $ev_u : k[T] \to C(u)$ tel que $ev_u(T) = u$. On a donc $\mathrm{im}(ev_u) = k[u] \subset C(u)$.

(3) C'est le théorème de structure des modules de type fini sur l'anneau principal $k[T]$ appliqué à V_u, qui est de type fini et de torsion puisque de k-dimension finie.

(4) L'action de u sur V_u s'identifie à l'action de T sur $k[T]/P_1 \oplus \cdots \oplus k[T]/P_r$. En notant ϵ_i la base $1, \overline{T}, \ldots, \overline{T}^{\deg(P_i)-1}$ de $k[T]/P_i$, $i = 1, \ldots, r$ et $\epsilon = \epsilon_1, \ldots, \epsilon_r$ la base résultante de $k[T]/P_1 \oplus \cdots \oplus k[T]/P_r$, la matrice de T dans ϵ est la matrice diagonale par bloc des matrices compagnons $C(P_i)$, $i = 1, \ldots, r$ des P_i. Or pour un polynôme P donné, le polynôme minimal et le polynôme caractéristique de $C(P)$ sont tous deux égaux à P. On en déduit que $\Xi = P_1 \cdots P_r$ et que $\Pi = ppcm(P_1, \ldots, P_r) = P_r$.

(5) On sait que si A est un anneau principal, les A-modules indécoposables sont les A-modules de la forme A/p^n, $a \in A$ irréductible, $n \geq 1$. Donc déjà u est indŕecomposable si et seulement si $r = 1$ et $\Pi_u = \Xi_u$ est une puissance d'un polynôme irréductible.

(6) Immédiat.

(7) Observons qu'un élément $f \in \mathrm{Hom}_{k[T]}(k[T]/P, k[T]/Q)$ est entièrement déterminé par $f(\overline{1})$. Donc on a un morphisme injectif $\Phi : \mathrm{Hom}_{k[T]}(k[T]/P, k[T]/Q) \hookrightarrow k[T]/Q$, $f \to \Phi(f) := f(\overline{1})$. Notons $D := gcd(P, Q)$ et $P = R_P D$ $Q = R_Q D$. Il existe $A, B \in k[T]$ tels que $AR_P + BR_Q = 1$. On vérifie immédiatement que l'image de Φ est le sous $k[T]$-module des $R \in k[T]/Q$ tels que $\overline{RP} = 0$ ou encore $RR_P = R_Q C$ *i.e.* $R \in R_Q k[T]$. On a donc

$$(\Phi) = R_Q k[T]/Q \simeq R_Q k[T]/R_Q D \simeq k[T]/D.$$

(8) Par définition

$$C(u) = \mathrm{Hom}_{k[T]}(\bigoplus_{1\leq i\leq r} k[T]/P_i, \bigoplus_{1\leq i\leq r} k[T]/P_i) \simeq \bigoplus_{1\leq i,j\leq r} \mathrm{Hom}_{k[T]}(k[T]/P_i, k[T]/P_j).$$

Donc si on note d_i le degré de P_i, en utilisant que $P_1|P_2|\cdots|P_r$, on obtient

$$\dim(C(u)) = \sum_{1\leq i\leq r} d_i + 2\sum_{1\leq i\leq r}(r-i)d_i = (2r-1)d_1 + (2r-3)d_2 + \cdots + 3d_{r-1} + d_r$$

.

(9) Comme $k[u] \subset C(u)$, $k[u] = C(u)$ si et seulement si $\dim(k[u]) = \dim(C(u))$ *i.e.* si et seulement si $d_1 + \cdots + d_r = (2r-1)d_1 + (2r-3)d_2 + \cdots + 3d_{r-1} + d_r$. Donc $k[u] = C(u)$ si et seulement si $r = 1$ ou encore $\Pi = \Xi$; on dit qu'un tel endomorphisme est cyclique).

Problème.

(1) (a) C'est la définition: $P \in k[T]$ est séparable si et seulement si il a $\deg(P) = d$ racines distinctes dans K_P *i.e.* si et seulement si $x_i - x_j \neq 0$, $1 \leq i \neq j \leq d$, ce qui équivaut bien à $\Delta(P) \neq 0$ puisque K_P est intègre.

(b) En dérivant $P(T) = \prod_{1\leq i\leq d}(T - x_i)$ on obtient $P'(T) = \sum_{1\leq i\leq d}\prod_{1\leq j\neq i\leq d}(T - x_j)$ et en évaluant en x_i, $P'(x_i) = \prod_{1\leq j\neq i\leq d}(x_i - x_j)$ donc

$$\Delta(P) = (-1)^{\frac{d(d+1)}{2}} \prod_{1\leq i\leq d} P'(x_i).$$

(c) Si $\Delta(P) \neq 0$, P est séparable donc K_P/k est galoisienne comme corps de décomposition d'un polynôme séparable. De plus, tout $\sigma \in G_P := Gal(K_P/k)$ induit une permutation $\sigma \in \mathcal{S}_d$ en posant $\sigma(x_i) = x_{\sigma(i)}$, $i = 1, \ldots, d$. Mais, puisque σ est un automorphisme du corps K_P on a

$$\sigma\Delta(P) \overset{(1)}{=} \prod_{1\leq i<j\leq d} (\sigma(x_j) - \sigma(x_i))^2 \overset{(2)}{=} \prod_{1\leq i<j\leq d} (x_{\sigma(j)} - x_{\sigma(i)})^2 \overset{(3)}{=} \prod_{1\leq i<j\leq d} (x_j - x_i)^2 = \Delta(P),$$

où (1) résulte du fait que σ est un morphisme de corps, (2) est par définition de la permutation associée à σ et (3) est parce que $\Delta(P)$ est symétrique en les $x_1, \ldots, x_d$. On a donc $\Delta(P) \in K_P^{G_P} = k$.

(d) Notons $\tilde{\Delta}(P) := \prod_{1\leq i<j\leq d}(x_j - x_i)$ (de sorte que $\Delta(P) = \tilde{\Delta}(P)^2$. On a alors comme dans la question précédente, pour tout $\sigma \in G_P$,

$$\sigma(\tilde{\Delta}(P)) = \prod_{1\leq i<j\leq d} (\sigma(x_j) - \sigma(x_i)) = \prod_{1\leq i<j\leq d} (x_{\sigma(j)} - x_{\sigma(i)}) = \epsilon(\sigma) \prod_{1\leq i<j\leq d} (x_j - x_i) = \epsilon(\sigma)\tilde{\Delta}(P).$$

Puisque $-1 \in k$, $\Delta(P)$ est un carré dans k si et seulement si $\tilde{\Delta}(P) \in k$. Mais $k = K_P^{G_P}$ donc $\tilde{\Delta}(P) \in k$ si et seulement si $\sigma\tilde{\Delta}(P) = \epsilon(\sigma)\tilde{\Delta}(P) = \tilde{\Delta}(P)$, $\sigma \in G_P$ si et seulement si $G_P \subset \mathcal{A}_d$.

(e) Si $\Delta(P)$ n'est pas un carré dans k, on vient de voir que $G_P \not\subset \mathcal{A}_d$, ce qui équivaut à $G_P \cap \mathcal{A}_d \not\subseteq G_P$ ou encore, $\epsilon|_{G_P} : G_P \twoheadrightarrow \{\pm 1\}$. De plus, $G_P \cap \mathcal{A}_d = \ker(\epsilon|_{G_P})$ donc $\epsilon|_{G_P} : G_P \twoheadrightarrow \{\pm 1\}$ se factorise en $G_P/G_P \cap \mathcal{A}_d \tilde{\to} \{\pm 1\}$. Enfin, soit x une racine du polynôme $T^2 - \Delta(P) \in k[t]$; quitte à remplacer x par $-x$, on peut supposer que $x = \prod_{1\leq i<j\leq d}(x_j - x_i)$. En particulier, $x \in K_P$ et $x \notin k$ par hypothèse donc $[k(x) : k] = 2$. On a également pour tout $\sigma \in G_P \cap \mathcal{A}_d$, $\sigma(x) = \prod_{1\leq i<j\leq d}(\sigma(x_j) - \sigma(x_i)) =$

$\epsilon(\sigma)x = x$ donc $k(x) \subset K_P^{G_P \cap \mathcal{A}_d}$, donc, puisque $[K_P^{G_P \cap \mathcal{A}_d} : k] = [G_P : G_P \cap \mathcal{A}_d] = 2$, $k(x) = K_P^{G_P \cap \mathcal{A}_d}$.

(2) On suppose ici que P est irréductible dans $\mathbb{Q}[T]$ et de la forme $P = T^n + aT + b \in \mathbb{Q}[T]$.

(a) Soit x une racine de P et notons $y := P'(x)$. On a $y = dx^{d-1} + a$ et, puisque $x^d + ax + b = 0$, $x^{d-1} = -a - bx^{-1}$ donc

$$y = dx^{d-1} + a = -d(a + bx^{-1}) + a = -(d-1)a - dbx^{-1}.$$

(b) On a $y = dx^{d-1} + a \in \mathbb{Q}(x)$ donc $\mathbb{Q}(y) \subset \mathbb{Q}(x)$. Inversement, $x = -db(y + (d-1)a)^{-1} \in \mathbb{Q}(y)$ donc $\mathbb{Q}(x) \subset \mathbb{Q}(y)$.

(c) En mettant au même dénominateur - $(Y + (d-1)a)^d - d$, on a

$$P(\frac{-db}{Y + (d-1)a}) = \frac{(-db)^d - dba(Y + (d-1)a)^{d-1} + b(Y + (d-1)a)^d}{(Y + (d-1)a)^d}$$

$$= b\frac{(Y + (d-1)a)^d - da(Y + (d-1)a)^{d-1} + (-d)^d b^{d-1}}{(Y + (d-1)a)^d}$$

Le polynôme

$$Q = (Y + (d-1)a)^d - da(Y + (d-1)a)^{d-1} + (-d)^d b^{d-1}$$

est unitaire de degré d et vérifie

$$Q(y) = (y + (d-1)a)^d P(\frac{-db}{y + (d-1)a}) = (y + (d-1)a)^d P(x) = 0$$

donc $Q(y) = 0$ puisque $(y + (d-1)a)^d = (-dbx^{-1})^d \neq 0$ ($b \neq 0$ car P est irréductible). C'est donc un polynôme annulateur de y. Mais comme P est irréductible sur $\mathbb{Q}$ on a $deg(Q) = d = deg(P) = [\mathbb{Q}(x) : \mathbb{Q}]$ donc d'après la question précédente $deg(Q) = [\mathbb{Q}(y) : \mathbb{Q}]$, ce qui assure que Q est en fait le polynôme minimal de y sur $\mathbb{Q}$.

(d) Puisque $Q(0)$ est le terme constant de Q, on a

$$Q(0) = (-1)^d \prod_{z \in Z_{K_Q}} z.$$

Mais comme Q est le polynôme minimal de y sur $\mathbb{Q}$, ses racines sont exactement les conjugués sur $\mathbb{Q}$ de y *i.e.* les $\sigma(y) = \sigma(P'(x)) = P'(\sigma(x))$, $\sigma : \mathbb{Q}(y) = \mathbb{Q}(x) \hookrightarrow \overline{\mathbb{Q}}$. Mais comme P est le polynôme minimal de x sur $\mathbb{Q}$, les $\sigma(x)$, $\sigma : \mathbb{Q}(x) \hookrightarrow \overline{\mathbb{Q}}$ sont exactement les racines $x_1, \ldots, x_d$ de P. On a donc

$$Q(0) = (-1)^d \prod_{1 \leq i \leq d} P'(x_i).$$

(e) D'après (1) (b) et (4) (e), $Q(0) = (-1)^{\frac{d(d+1)}{2}} \Delta(P)$. Par ailleurs

$$Q(0) = ((d-1)a)^d - da((d-1)a)^{d-1} + (-d)^d b^{d-1} = -(d-1)^{d-1} a^d + (-d)^d b^{d-1}.$$

D'où:

$$\Delta(P) = (-1)^{\frac{d(d-1)}{2}}((1-d)^{d-1} a^d + d^d b^{d-1}).$$

(3) On va maintenant appliquer ce qui précède à la détermination de groupes de Galois de polynômes. On reprend les notations de la Question (1).

(a) Considérons le polynôme $P = T^3 - T - 1 \in \mathbb{Q}[T]$.

(i) En réduisant modulo 2 on obtient $P = T^3 + T + 1$, dont on vérifie immédiatement qu'il n'a pas de racine dans $\mathbb{F}_2$; il est donc irréductible sur $\mathbb{F}_2$. Cela assure que P est irréductible dans $\mathbb{Z}[T]$ donc dans $\mathbb{Q}[T]$ puisqu'il est de contenu 1. En particulier, si x est une racine de P, on a

$$3 = deg(P) = [\mathbb{Q}(x) : \mathbb{Q}] | [K_P : \mathbb{Q}] = |G_P|.$$

(ii) En utilisant (2) (e), $\Delta(P) = -5$ n'est pas un carré dans $\mathbb{Q}$. Donc G_P n'est pas un sous-groupe de $\mathcal{A}_3$. Or les seuls sous groupes de $\mathcal{S}_3$ sont le sous-groupe trivial, $\mathcal{A}_3$ (d'ordre 3), les 3 sous-groupes d'ordre 2 engendrés respectivement par $(1,2)$, $(1,3)$, $(2,3)$ et $\mathcal{S}_3$ lui-même. Comme $3||G_P|$ et $G_P \not\subset \mathcal{A}_3$, la seule possibilité est $G_P = \mathcal{S}_3$.

(iii) Par la correspondance de Galois, $K_P/\mathbb{Q}$ on sait que $K_P/\mathbb{Q}$ a trois sous-extensions non galoisiennes de degré 3 et une sous-extension galoisienne de degré 2. Plus précisément, on a immédiatement, en notant $\delta = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$:

$\mathbb{Q} \subset K_P^H \subset K_P$	H	$[G_P : H] = [K_P^H : k]$	Galoisienne	$G_P/H = Gal(K_P^H\|\mathbb{Q})$
$\mathbb{Q}(x_1 - x_2) = \mathbb{Q}(x_2 - x_3) = \mathbb{Q}(x_3 - x_1)$	$\{1\}$	1	oui	$\mathcal{S}_3$
$\mathbb{Q}(x_1)$	$\langle(2,3)\rangle$	3	non	
$\mathbb{Q}(x_2)$	$\langle(1,3)\rangle$	3	non	
$\mathbb{Q}(x_3)$	$\langle(1,2)\rangle$	3	non	
$\mathbb{Q}(\delta)$	$\mathcal{A}_3$	2	oui	$\mathbb{Z}/2$
$\mathbb{Q}$	$\mathcal{S}_3$	1	oui	$\{1\}$

(b) Considérons le polynôme $P(T) = T^4 - T - 1$.

(i) Là encore, en réduisant modulo 2 on obtient $P \equiv T^4 + T + 1$, dont on vérifie immédiatement qu'il n'a pas de racine dans $\mathbb{F}_2$; s'il est réductible sur $\mathbb{F}_2[T]$, ile ne peut donc se factoriser qu'en un produit $P = QR$ de deux polynômes unitaires $Q, R \in \mathbb{F}_2[T]$ de degré 2. En écrivant $Q = T^2 + aT + b$, $R = T^2 + cT + d$ et en identifiant les coefficients dans $P = QR$, on obtient $a + c = b + d + ac = 0$, $ad + bc = bd = 1$. Mais $bd = 1$ équivaut à $b = d = 1$ alors que $a + c = 0$ équivaut à $a = c = 1$ ou $a = c = 0$, or $a = c = 0$ n'est pas possible puisque $ad + bc = 1$. Donc $a = b = c = d = 1$. Mais alors $ad + bc = 0$: contradiction. Cela assure que $T^4 + T + 1$ est irréductible dans $\mathbb{F}_2[T]$ donc que P est irréductible dans $\mathbb{Z}[T]$ donc dans $\mathbb{Q}[T]$ puisqu'il est de contenu 1. En particulier, si x est une racine de P, on a

$$4 = deg(P) = [\mathbb{Q}(x) : \mathbb{Q}]|[K_P : \mathbb{Q}] = |G_P|.$$

(ii) En utilisant (2) (e), $\Delta(P) = -43$ n'est pas un carré dans $\mathbb{Q}$. Donc G_P n'est pas un sous-groupe de $\mathcal{A}_4$.

(iii) Sur $\mathbb{F}_7$, P a 3 comme racine donc s'écrit sous la forme $P = (T - 3)(T^3 + 3T^2 + 2T - 2)$. Comme $T^3 + 3T^2 + 2T - 2$ n'a pas de racines dans $\mathbb{F}_7$ et est de degré 3, il est irréductible sur $\mathbb{F}_7$. Donc G_P contient un 3-cycle.

(iv) On a $4||G_P|$ par (i), $3||G_P|$ par (iii) donc $12||G_P|||\mathcal{S}_4| = 24$ donc les seules possibilités sont $|G_P| = 12$ ou 24. Mais si $|G_P| = 12$, G_P est d'indice 2 dans $\mathcal{S}_4$ or le seul sous-groupe d'indice 2 dans $\mathcal{S}_4$ est $\mathcal{A}_4$, ce qui n'est pas possible par (ii). Donc $G_P = \mathcal{S}_4$.

(c) Considérons le polynôme $P(T) = T^5 + 20T + 16$.

(i) Cette fois-ci, en réduisant modulo 3 on obtient $P \equiv T^5 + 2T + 1$, dont on vérifie immédiatement qu'il n'a pas de racine dans $\mathbb{F}_3$; s'il est réductible sur $\mathbb{F}_3[T]$, ile ne peut donc se factoriser qu'en un produit $P = QR$ de deux polynômes unitaires $Q, R \in \mathbb{F}_3[T]$ de degré 3 et 2 respectivement. En écrivant $Q = T^3 + aT^2 + bT + c$, $R = T^2 + dT + e$ et en identifiant les coefficients dans $P = QR$, on obtient $d + a = e + ad + b = ae + bd + c = 0$, $cd + be = 2$, $ce = 1$. Or $ce = 1$ équivaut à $c = e = 1$ ou $c = e = -1$. Si $c = e = 1$, on a $d + a = 1 + ad + b = a + bd + 1 = 0$, $d + b = 2$ donc $d = -a$, $b = 2 - d = 2 + a$, $a(1 - a) = 0$ et $1 - a(a + 1) = 0$. Mais $1 - a(a + 1) = 0$ n'a pas de solution dans $\mathbb{F}_3$: contradiction. On argumente de même pour $c = e = -1$. Cela assure que $T^5 + 2T + 1$ est irréductible dans $\mathbb{F}_3[T]$ donc que P est irréductible dans $\mathbb{Z}[T]$ donc dans $\mathbb{Q}[T]$ puisqu'il est de contenu 1. En particulier, si x est une racine de P, on a

$$5 = deg(P) = [\mathbb{Q}(x) : \mathbb{Q}]|[K_P : \mathbb{Q}] = |G_P|.$$

(ii) En utilisant (2) (e), $\Delta(P) = 2^{16}5^6$ (sic!) est un carré dans $\mathbb{Q}$. Donc G_P est un sous-groupe de $\mathcal{A}_5$.

(iii) Sur $\mathbb{F}_7$, $P \equiv T^5 - T + 2$ a pour racines 4 et 5 donc s'écrit sous la forme $P = (T-4)(T-5)(T^3+2T^2-2T-2)$. Comme T^3+2T^2-2T-2 n'a pas de racines dans $\mathbb{F}_7$ et est de degré 3, il est irréductible sur $\mathbb{F}_7$. Donc G_P contient un 3-cycle.

(iv) Soit $H \subsetneq \mathcal{A}_5$ un sous-groupe. En faisant agir $\mathcal{A}_5$ par translation sur $\mathcal{A}_5/H$, on définit un morphisme de groupes $\phi : \mathcal{A}_5 \to \mathcal{S}(\mathcal{A}_5/H)$ qui est non trivial puisque $H \subsetneq \mathcal{A}_5$ donc, en particulier $\ker(\phi) \subsetneq \mathcal{A}_5$ est un sous-groupe normal strict de $\mathcal{A}_5$ donc $\ker(\phi) = \{1\}$ puisque $\mathcal{A}_5$ est simple. Cela implique notamment que $60 = |\mathcal{A}_5| \leq |\mathcal{S}(\mathcal{A}_5/H)| = [\mathcal{A}_5 : H]!$ or cette inégalité n'est possible que si $[\mathcal{A}_5 : H] > 4$ *i.e.* $|H| < 15$.

(v) On a $5||G_P|$ par (i), $3||G_P|$ par (ii) donc $15||G_P|$. D'après (iv) cela force $G_P = \mathcal{A}_5$.

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