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

Avertissement.

Sont autorisés: le polycopié du cours, les notes manuscrites du cours et des exercices traités en cours, les dictionnaires de langues papier.

Les réponses peuvent être rédigées en français ou en anglais.

Le sujet est très long; le barême sera adapté en conséquence (si vous traitez correctement l'un des deux exercices et une moitié du problème, vous êtes assurés d'avoir la note maximale). Prenez donc le temps de *justifier soigneusement* vos réponses. Vous pouvez bien sûr admettre certaines questions.

Exercice 1. Soit k un corps.

(1) Montrer que l'ensemble $A = \{P \in k[T] \mid P'(0) = 0\}$ est une sous-k-algèbre de $k[T]$.

(2) Montrer que A est engendrée comme k-algèbre par T^2, T^3 et qu'on a un isomorphisme canonique de k-algèbres $k[X,Y]/\langle X^3 - Y^2\rangle \tilde{\to} A$. En déduire que A est noethérien.

(3) Montrer que T^2 et T^3 sont irréductibles dans A.

(4) Donner deux factorisations en irréductibles de T^6 dans A. En déduire que A n'est pas factoriel.

(5) Exhiber un idéal non principal de A.

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 $\mathrm{End}_k(V)$ la k-algèbre des endomorphismes k-linéaires de V et $C(u) \subset \mathrm{End}_k(V)$ l'ensemble des $v \in \mathrm{End}_k(V)$ tels que $u \circ v = v \circ u$.

(1) Montrer que $C(u)$ est une sous-k-algèbre de $\mathrm{End}_k(V)$.

(2) Montrer que $k[u] \subset C(u)$. L'objectif de ce problème est de donner une condition nécessaire et suffisante sur u pour que $k[u] = C(u)$.

(3) On rappelle que V est muni d'une structure de $k[T]$-module V_u définie par $P(T) \cdot v = P(u)(v)$, $P \in k[T]$, $v \in V$. Rappeler pourquoi il existe une unique suite de polynômes unitaires (qu'on appelle la suite des invariants de similitude de u) $P_1 | P_2 | \cdots | P_r$ telle que

$$V_u \simeq k[T]/P_1 \oplus \cdots \oplus k[T]/P_r.$$

(4) Calculer le polynôme minimal Π et le polynôme caractéristique Ξ de u en fonction de $P_1, \ldots, P_r$.

(5) Soit $P, Q \in K[T]$. On note $\mathrm{Hom}_{k[T]}(k[T]/P, k[T]/Q)$ l'ensemble des morphismes de $k[T]$-modules de $k[T]/P$ dans $k[T]/Q$; on notera que c'est un $k[T]$-module donc, en particulier, un k-espace vectoriel. Montrer qu'on a un isomorphisme canonique de k-espaces vectoriels

$$\mathrm{Hom}_{k[T]}(k[T]/P, k[T]/Q) \tilde{\to} k[T]/gcd(P,Q).$$

(6) Montrer qu'on a un isomorphisme canonique de k-algèbres $C(u) \tilde{\to} \mathrm{End}_{k[T]}(V_u)$.

(7) En déduire la dimension de $C(u)$ en fonction du degré des invariants de similitudes de u.

(8) Déduire de ce qui précède que $C(u) = k[u]$ si et seulement si $r = 1$.

Problème. L'objectif de ce problème est d'introduire un nouvel outil - le discriminant - pour calculer le groupe de Galois G_P associé à un un polynôme irréductible P. Dans la Question (1), on introduit le discriminant $\Delta(P)$ et on le relie à la signature de G_P vu comme sous-groupe du groupe des permutations des racines de P. Dans la Question (2), on calcule de façon *ad-hoc* par une méthode un peu astucieuse le discriminant d'un polynôme irréductible de la forme $P = T^n + aT + b \in \mathbb{Q}[T]$. Dans la Question (3), on applique les résultats des Questions (1) et (2) à la détermination de groupes de Galois. Pour une méthode systématique du calcul de $\Delta(P)$ en fonction des coefficients de P, *cf.* la remarque finale.

(1) Soit k un corps, $P \in k[T]$ un polynôme unitaire de degré d et $K_P := D_k(P)/k$ un corps de décomposition de P. Sur K_P, on peut donc écrire $P(T) = \prod_{1\leq i\leq d}(T - x_i)$. On définit le discriminant $\Delta(P)$ de P par

$$\Delta(P) = \prod_{1\leq i<j\leq d}(x_j - x_i)^2 = (-1)^{\frac{d(d-1)}{2}} \prod_{1\leq i\neq j\leq d}(x_i - x_j).$$

(a) Montrer que $P \in k[T]$ est séparable si et seulement si $\Delta(P) \neq 0$.

(b) Exprimer $\Delta(P)$ en fonction de P' et de $x_1, \ldots, x_d$.

(c) Montrer que $\Delta(P) \in k$.

(d) Supposons $\Delta(P) \neq 0$. Rappeler pourquoi l'extension K_P/k est galoisienne. On note $G_P := Gal(K_P/k)$ son groupe de Galois. Notons $\mathcal{S}_d$ le groupe symétrique à $d!$ éléments et $\mathcal{A}_d \subset \mathcal{S}_d$ le groupe alterné *i.e.* le noyau du morphisme signature

$$\begin{array}{rccc} \epsilon: & \mathcal{S}_d & \to & \{\pm 1\} \\ & \sigma & \to & \prod_{1\leq i<j\leq d} \frac{\sigma(j)-\sigma(i)}{(j-i)} \end{array}$$

L'action de G_P sur $Z_k(P) = \{x_1, \ldots, x_d\}$ induit un morphisme de groupes injectif $G_P \hookrightarrow \mathcal{S}_d$ (qui envoie $\sigma \in G$ sur la permutation définie par $\sigma(x_i) = x_{\sigma(i)}$, $i = 1, \ldots, d$) permettant d'identifier G_P à un sous-groupe de $\mathcal{S}_d$. Montrer que $G_P \subset \mathcal{A}_d$ si et seulement si $\Delta(P)$ est un carré dans k.

(e) Si $\Delta(P)$ n'est pas un carré dans k, montrer que $G_P \cap \mathcal{A}_d$ est un sous-groupe normal d'indice 2 de G_P. Décrire la sous-extension quadratique de K_P/k correspondante en fonction des racines $x_1, \ldots, x_d$ de P.

(2) L'objectif de cette question est de calculer $\Delta(P)$ pour $P = T^d + aT + b \in \mathbb{Q}[T]$ *irréductible* dans $\mathbb{Q}[T]$.

(a) Soit x une racine de P et notons $y := P'(x)$. Montrer que $y = -(d-1)a - dbx^{-1}$.

(b) En déduire que $\mathbb{Q}(y) = \mathbb{Q}(x)$.

(c) En écrivant $P(\frac{-db}{Y+(d-1)a})$ comme quotient de deux polynômes dans $\mathbb{Q}[Y]$, montrer que le polynôme minimal de y sur $\mathbb{Q}$ est

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

(d) Exprimer $Q(0)$ en fonction de P' et des racines $x_1, \ldots, x_d$ de P.

(e) Déduire de (1) (b) et (2) (d) que

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

(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) Montrer que P est irréductible sur $\mathbb{Q}$ (penser à la méthode de réduction). En déduire que $3||G_P|$.

(ii) Montrer que G_P n'est pas un sous-groupe de $\mathcal{A}_3$ et déterminer G_P.

(iii) Décrire les sous-extensions de corps de $K_P/\mathbb{Q}$ en fonction des racines x_1, x_2, x_3 de P. Dans chaque cas, on donnera le degré de la sous-extension et on précisera si la sous-extension correspondante est galoisienne ou non et si elle l'est, on donnera son groupe de Galois.

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

(i) Montrer que P est irréductible sur $\mathbb{Q}$. En déduire que $4||G_P|$.

(ii) Montrer que G_P n'est pas un sous-groupe de $\mathcal{A}_4$.

(iii) En réduisant P modulo 7, montrer que G_P contient un 3-cycle.

(iv) Déterminer G_P.

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

(i) Montrer que P est irréductible sur $\mathbb{Q}$. En déduire que $5||G_P|$.

(ii) Montrer que G_P est un sous-groupe de $\mathcal{A}_5$.

(iii) En réduisant P modulo 7, montrer que G_P contient un 3-cycle.

(iv) On rappelle que $\mathcal{A}_5$ est un groupe simple. Soit $H \subsetneq \mathcal{A}_5$ un sous-groupe strict de $\mathcal{A}_5$. En faisant agir $\mathcal{A}_5$ par translation sur $\mathcal{A}_5/H$ montrer qu'on définit un morphisme de groupes injectif $\mathcal{A}_5 \hookrightarrow \mathcal{S}(\mathcal{A}_5/H)$. En déduire qu'un sous-groupe strict de $\mathcal{A}_5$ est d'ordre < 15.

(v) Déterminer G_P.

Remarque culturelle. Le problème précédent montre que le discriminant d'un polynôme donne des informations très pratiques pour déterminer le groupe de Galois. La méthode décrite pour calculer $\Delta(P)$ en (2) est *ad-hoc*. En général, on dispose d'une méthode systématique pour calculer $\Delta(P)$ comme déterminant d'une matrice dont les coefficients ne font intervenir que ceux de P et P'. Plus précisément, étant donné un entier $d \geq 0$ et un corps k on note $k[T]_{\leq d}$ le k-espace vectoriel des polynômes à coefficients dans k de degré $\leq d$ en l'indéterminée T. Soit $P = a_0T^m + a_1T^{m-1} + \cdots + a_m$, $Q = b_0T^n + b_1T^{n-1} + \cdots + b_n \in k[T]$; on suppose $a_0, b_0 \neq 0$. On considère l'application k-linéaire

$$\begin{array}{rccc} \phi_{P,Q}: & k[T]_{\leq n-1} \times k[T]_{\leq m-1} & \to & k[T]_{\leq m+n-1} \\ & (U, V) & \to & UP + VQ \end{array}$$

Le déterminant $Res(P, Q) = \det(\phi_{P,Q})$ est par définition le résultant de P et Q. Vous pouvez écrire la matrice de $\phi_{P,Q}$ dans les bases $(1, 0), \ldots (T^{n-1}, 0), (0, 1), \ldots, (0, T^{m-1})$ de $k[T]_{\leq n-1} \times k[T]_{\leq m-1}$ et $1, \ldots, T^{m+n-1}$ de $k[T]_{\leq m+n-1}$ pour voir à quoi cela ressemble. On peut montrer que, si P est un polynôme unitaire de degré d, $\Delta(P) = (-1)^{\frac{d(d-1)}{2}} Res(P, P')$. Cette description de $\Delta(P)$ est 'la' méthode pour calculer sur machine $\Delta(P)$ en fonction des coefficients de P (on dispose d'algorithmes très performants de calcul de déterminant). Mais si vous essayez de mener ce genre de calcul à la main, vous verrez vite que c'est en général impossible dès que $d \geq 3, 4$...

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