Sorbonne Université
Master Mathématiques et applications

UFR de Mathématiques
2022–2023

Théorie de Galois

Partiel du 16 mars 2023. Durée 2h00.
Pas de documents autorisés.

Exercice 1. Soit k un corps et K une extension finie de k

i. Donner un exemple où K n'est pas séparable sur k.

Par exemple, $K = \mathbb{F}_p(T)$ et $k = \mathbb{F}_p(T^p)$.

ii. Si k est de caractéristique nulle, et K est un corps de décomposition d'un polynôme non séparable dans $k[X]$, montrer que c'est aussi le corps de décomposition d'un polynôme séparable dans $k[X]$.

Comme k est de caractéristique 0, tout polynôme irréductible est séparable donc tout élément de K est séparable, et K est Galoisienne, donc est le corps de décomposition d'un polynôme séparable.

iii. Si K est un corps de décomposition d'un polynôme irréductible de degré n, montrer que n divise $[K : k]$, et $[K : k]$ divise $n!$. Donner un exemple où $[K : k] = n!$ et un exemple où $[K : k] = n$.

K contient une racine α de f et l'évaluation en α fournit un isomorphisme $\mathrm{ev}_\alpha : k[X]/(f) \xrightarrow{\sim} k(\alpha)$, donc $n = [k(\alpha) : k]$ divise $[K : k]$. Si K est séparable, et donc Galoisienne, on sait que son groupe de Galois agit fidèlement sur les n racines de f dans K et donc $[K : k] = |\mathrm{Gal}(K/k)|$ divise $n!$. En général, on peut le montrer par récurrence sur n pour n'importe quel polynôme f de degré n. En effet, si f se factorise $f = f_1 f_2$, avec f_i de degré n_i, alors $[K_f : k] = [K_f : K_{f_1}][K_{f_1} : k]$ qui, par hypothèse de récurrence (observer que K_f est un corps de décomposition de f_2 sur K_{f_1}), divise $n_2! \cdot n_1!$, qui divise $n!$. Si f est irréductible, posons $K_1 = k(\alpha)$ où α est une racine de f. Alors f se factorise $f = (X - \alpha) f_1$ dans $K_1[X]$, et K est donc un corps de décomposition de f_1 sur K_1. Utilisant l'hypothèse de récurrence, on a alors que $[K_f : k] = [K_f : K_1][K_1 : k]$ divise $(n-1)! \cdot n = n!$.

Pour $k = \mathbb{Q}(\Sigma_1, \cdots, \Sigma_n)$, le polynôme $f = X^n - \Sigma_1 X^{n-1} + \cdots + (-1)^n \Sigma_n$ vérifie $[K_f : k] = n!$
Pour $k = \mathbb{C}(T)$, le polynôme $f = X^n - T$ vérifie $[K_f : k] = n$ (on a $K_f = \mathbb{C}(T^{1/n})$).

iv. Si $[K : k] = 2$ et k n'est pas de caractéristique 2, montrer que K est Galoisienne et calculer son groupe de Galois.

Soit $\alpha \in K \setminus k$. On a $k(\alpha) = K$, donc $\deg f_\alpha = 2$ et f_α est séparable car k n'est pas de caractéristique 2. Par ailleurs, f_α a une racine (α) dans K, donc est scindé dans $K[X]$, et K est donc normale. Le groupe de Galois est un groupe d'ordre 2, donc isomorphe à $\mathbb{Z}/2\mathbb{Z}$.

TSVP

v. Donner un exemple où K est Galoisienne sur k de groupe $\mathfrak{S}_n$.

cf plus haut.

vi. Donner un exemple où $k = \mathbb{Q}$ et K est Galoisienne de groupe $\mathfrak{S}_3$, resp. $\mathbb{Z}/6\mathbb{Z}$, resp. $\mathbb{Z}/3\mathbb{Z}$.

On a vu en cours que $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q}) = \mathfrak{S}_3$ et $\mathrm{Gal}(\mathbb{Q}(\zeta_7)/\mathbb{Q}) = (\mathbb{Z}/7\mathbb{Z})^\times \simeq \mathbb{Z}/6\mathbb{Z}$. La conjugaison complexe c induit un sous-groupe d'ordre 2 de $\mathrm{Gal}(\mathbb{Q}(\zeta_7)/\mathbb{Q})$, dont le quotient est $\mathrm{Gal}(\mathbb{Q}(\zeta_7)^c/\mathbb{Q}) \simeq \mathbb{Z}/3\mathbb{Z}$. On voit que $\cos(2\pi/7) \in \mathbb{Q}(\zeta_7)^c \setminus \mathbb{Q}$, donc $\mathbb{Q}(\zeta_7)^c = \mathbb{Q}(\cos(2\pi/7))$.

vii. Donner un exemple où K n'est pas une extension monogène de k, en justifiant sans trop de détails.

On a vu en TD que l'extension $K = \mathbb{F}_p(X, Y) \supset k = \mathbb{F}_p(X^p, Y^p)$ n'est pas monogène. On calcule en effet que son degré est p^2, mais que pour tout élément $\alpha \in K$, on a $\alpha^p \in k$, donc α est de degré p ou 1, mais pas p^2.

viii. Supposons ici K algébrique *infinie*. Si K/k est séparable, montrer que K contient des éléments de degré arbitrairement grand. Construire un exemple (non séparable !) où les degrés sont bornés.

Soit N un entier. Par hypothèse, K contient sous-k-ev de dimension N, lequel engendre donc un corps L de degré supérieur à N sur k. Étant sépable sur k, ce corps admet un élément primitif, dont le degré est donc supérieur à N.

Un exemple d'extension infinie où les degrés sont bornés : $K = \mathbb{F}_p(T_1, T_2, \cdots, T_n, \cdots)$ et $k = K^p = \mathbb{F}_p((T_1)^p, (T_2)^p, \cdots, (T_n)^p, \cdots)$.

Exercice 2. On considère la propriété suivante sur un corps k :

(C) : toutes les extensions Galoisiennes finies de k sont cycliques.

i. Donner deux exemples non algébriquement clos de corps k ayant la propriété (C).

$k = \mathbb{F}_P$ et $k = \mathbb{R}$.

ii. Montrer que si k vérifie (C), toute extension finie séparable de k est Galoisienne.

Soit K une extension finie séparable de k. Notons $\tilde{K}$ une clôture normale de K (par exemple, on peut tout plonger dans une clôture algébrique de k). Alors $\tilde{K}$ est une extension Galoisienne de k, donc son groupe de Galois $\mathrm{Gal}(\tilde{K}/k)$ est cyclique, et son sous-groupe $\mathrm{Gal}(\tilde{K}/K)$ est distingué. Par la correspondance de Galois, il s'ensuit que K/k est Galoisienne.

iii. Montrer que si k vérifie (C), toute extension finie séparable de k vérifie (C) aussi.

Soit k' une extension finie de séparable de k et K' une extension Galoisienne de k'. Par la question précédente, c'est aussi une extension Galoisienne de k. Donc $\mathrm{Gal}(K'/k')$ est un sous-groupe du groupe cyclique $\mathrm{Gal}(K'/k)$, donc est cyclique.

iv. Montrer que k vérifie (C) si et seulement si k admet au plus une extension séparable finie de degré m dans $\overline{k}$ pour tout $m \in \mathbb{N}$.

Supposons que k vérifie (C) et soient K, K' deux sous-extensions séparables de degré m dans $\overline{k}$. Alors le corps composé $L = KK'$ est une extension séparable finie, donc Galoisienne, et K, resp. K', est le corps des points fixes d'un sous-groupe H, resp. H', d'indice m dans $\mathrm{Gal}(L/k)$. Or, comme $\mathrm{Gal}(L/k)$ est cyclique, il a un unique sous-groupe d'indice m, donc $H = H'$ et $K = K'$.

Réciproquement, si k possède au plus une extension séparable de degré m, alors le groupe de Galois G d'une extension Galoisienne de k possède au plus un sous-groupe d'indice m pour tout m. Il faut voir qu'un tel groupe est nécessairement cyclique. Pour p premier, les p-Sylow de G on tous le même indice, donc ils sont égaux, i.e. il y a un unique p-Sylow, qui est donc distingué. Il s'ensuit que G est le produit de ses sous-groupes de Sylow, et il suffit de montrer que chacun de ces sous-groupes de Sylow est cyclique. On est donc ramené au cas où G est un p-groupe. Dans ce cas, G admet un sous-groupe d'indice p, et celui-ci est l'unique sous-groupe maximal parmi les sous-groupes propres de G. Par la question v(b) ci-dessous, G est donc cyclique.

v. Soient $\alpha \in \overline{\mathbb{Q}} \setminus \mathbb{Q}$ et k un sous-corps de $\overline{\mathbb{Q}}$ qui est maximal (pour l'inclusion) parmi les sous-corps de $\overline{\mathbb{Q}}$ ne contenant pas α.

(a) Montrer que $k(\alpha)$ est une extension Galoisienne de k dont le groupe de Galois n'a aucun sous-groupe propre non-trivial. En déduire que $\mathrm{Gal}(k(\alpha)/k)$ est isomorphe à $\mathbb{Z}/p\mathbb{Z}$ pour un premier p inférieur à $[\mathbb{Q}(\alpha) : \mathbb{Q}]$.

Soit $g_\alpha \in k[X]$ le polynôme minimal de α sur k, et soit α' une autre racine de g_α dans $\overline{\mathbb{Q}}$. On a $[k(\alpha) : k] = [k(\alpha') : k]$, donc si $\alpha' \notin k(\alpha)$, alors $\alpha \notin k(\alpha')$, ce qui contredit la maximalité de k. Donc g_α est scindé dans $k[X]$, et $k(\alpha)$ est un corps de décomposition de g_α sur k. Soit H un sous-groupe propre de $\mathrm{Gal}(k(\alpha)/k)$. Alors $k(\alpha)^H$ est un corps contenant strictement k. Par maximalité de k, ce corps doit contenir α, donc $k(\alpha)^H = k(\alpha)$ et $H = \{id\}$. Les seuls groupes qui ne contiennent aucun sous-groupe propre non trivial sont les $\mathbb{Z}/p\mathbb{Z}$, pour p premier.

(b) Montrer qu'un groupe G qui admet un unique sous-groupe propre maximal est cyclique d'ordre une puissance d'un nombre premier. En déduire que k a la propriété (C) et que toutes ses extensions séparables finies sont de degré une puissance de p.

Supposons que G admette un unique sous-groupe propre maximal, noté H, et soit $x \in G \setminus H$. Le sous-groupe $\langle x \rangle$ n'est pas contenu dans H, donc il n'est pas propre, donc $G = \langle x \rangle$ est cyclique. Par ailleurs, pour $n = p_1^{\nu_1} \cdots p_r^{\nu_r}$, les sous-groupes propres maximaux de $\mathbb{Z}/n\mathbb{Z}$, sont les r sous-groupes d'indice p_i, $i = 1, \cdots, r$. Donc l'ordre de G est une puissance d'un nombre premier.

Soit maintenant K une extension Galoisienne finie de k de groupe de Galois noté G. Toute extension non-triviale de k doit contenir α, donc K possède une unique sous-extension non triviale minimale, à savoir $k(\alpha)$. Par la correspondance de Galois, G possède un unique sous-groupe propre maximal, donc est cyclique d'ordre une puissance d'un nombre premier et divisible par p.

TSVP

vi. (facultatif) Soit $\mathbb{C}[[T]] := \{f(T) = \sum_{n\geqslant 0} a_n T^n\}$ l'anneau des séries formelles à coefficients dans $\mathbb{C}$.

(a) Montrer que pour $f \in \mathbb{C}[[T]]$, on a $f \in \mathbb{C}[[T]]^\times \Leftrightarrow a_0 \neq 0$.

(b) Montrer que $\mathbb{C}[[T]]$ est un anneau local principal d'idéal maximal (T). En déduire que son corps des fractions est

$$\mathbb{C}((T)) := \mathbb{C}[[T]][T^{-1}] = \{f = \sum_{n\in\mathbb{Z}} a_n T^n,\ a_n = 0 \text{ pour } n << 0\}.$$

(c) On admet que toute extension finie de $\mathbb{C}((T))$ est contenue dans $\mathbb{C}((T^{1/n}))$ pour un $n \in \mathbb{N}$. En déduire que $\mathbb{C}((T))$ a la propriété (C).