Sorbonne Université
Master Mathématiques et applications

UFR de Mathématiques
2021–2022

Théorie de Galois

Examen du 18 mai 2022, 8h30. Durée 3h00.
Pas de documents autorisés.

Exercice 1. Exemples et contre-exemples.

i. Donner un exemple d'extension finie de corps $k \subset K$ qui soit

(a) normale mais pas séparable, resp. séparable mais pas normale.

$k := \mathbb{F}_p(T^p) \subset K := \mathbb{F}_p(T)$ est normale car c'est le corps de décomposition de $X^p - T^p$ sur k. Non séparable car le polynôme minimal de T sur k est $X^p - T^p$ qui est non séparable. Attention (erreur constatée) : il n'est pas toujours vrai que l'extension de décomposition d'un polynôme inséparable est inséparable (par exemple en caractéristique 0 toutes les extensions sont séparables mais il y a plein de polynômes inséparables).

$k = \mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2})$ séparable (car. 0) mais non normale car $j\sqrt[3]{2} \notin \mathbb{Q}(\sqrt[3]{2})$.

(b) Galoisienne de groupe $\mathbb{Z}/6\mathbb{Z}$, resp. $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$

Pour $\mathbb{Z}/6\mathbb{Z}$, on peut penser à $\mathbb{F}_p \subset \mathbb{F}_{p^6}$ ou à $\mathbb{Q} \subset \mathbb{Q}(\mu_7)$. Pour $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ on peut penser à $\mathbb{Q} \subset \mathbb{Q}(\mu_{21})$ ou $\mathbb{Q} \subset \mathbb{Q}(\mu_{28})$, ou encore $\mathbb{Q} \subset \mathbb{Q}(\mu_7, \sqrt{2})$ (mais plus laborieux à justifier).

ii. Dans une tour d'extensions $k \subset K \subset L$, supposons que $K \supset k$ et $L \supset K$ soient Galoisiennes et abéliennes. Est-ce que $L \supset k$ est toujours Galoisienne ? (donner une preuve ou un contre-exemple).

Contre-exemple : $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[4]{2})$. Chaque extension intermédiaire est quadratique, donc Galoisienne, mais $\mathbb{Q} \subset \mathbb{Q}(\sqrt[4]{2})$ n'est pas normale car $i\sqrt[4]{2}$ est une racine du polynôme minimal $X^4 - 2$ de $\sqrt[4]{2}$ qui n'appartient pas à $\mathbb{Q}(\sqrt[4]{2})$.

iii. Soit $k \subset K$ une extension Galoisienne de degré pair. Est-il toujours vrai qu'elle contient une extension quadratique $k \subset k'$? (justifier).

Non. Par la correspondance de Galois, une extension quadratique $k \subset k'$ correspond à un sous-groupe d'indice 2 de $\mathrm{Gal}(K/k)$. On sait qu'un tel sous-groupe est toujours distingué de quotient $\mathbb{Z}/2\mathbb{Z}$. Or, par exemple $\mathfrak{A}_4$ ne possède aucun tel quotient, et on a vu en TD un exemple d'extension de groupe $\mathfrak{A}_4$. Autre exemple, $\mathfrak{A}_5$ est même simple (aucun sous-groupe distingué) et on a vu en cours une extension $\mathbb{Q} \subset \mathbb{Q}_f$ de groupe $\mathfrak{S}_5$, dont on déduit que l'extension $\mathbb{Q}(\sqrt{\mathrm{disc}(f)}) \subset \mathbb{Q}_f$ est de groupe $\mathfrak{A}_5$.

TSVP

Exercice 2. Soit p un nombre premier impair. On note $\mu_p := \{z \in \mathbb{C}, z^p = 1\}$.

i. Montrer que $\mathbb{Q}(\mu_p)$ contient une unique extension quadratique K de $\mathbb{Q}$. Montrer que $\mathrm{disc}(X^p - 1) = (-1)^{\frac{p(p-1)}{2}} p^p$ et en déduire que $K = \mathbb{Q}(\sqrt{(-1)^{\frac{p-1}{2}} p})$.

On sait que $\mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q}) = (\mathbb{Z}/p\mathbb{Z})^\times \simeq \mathbb{Z}/(p-1)\mathbb{Z}$ est un groupe cyclique d'ordre pair. Un tel groupe possède un unique sous-groupe d'indice 2. Concrètement, si σ est un générateur (donc d'ordre $p-1$), l'unique sous-groupe d'indice 2 est le sous-groupe engendré par σ^2. Pour le discriminant δ, on peut utiliser la formule vue en cours ou la retrouver dans ce cas simple. Le calcul montre que ce discriminant δ n'est pas un carré dans $\mathbb{Q}$. Par ailleurs le cours nous dit que $\mathbb{Q}(\mu_p)$ contient les racines carrées de δ. Donc l'extension $\mathbb{Q} \subset \mathbb{Q}(\sqrt{\delta})$ est bien quadratique contenue dans $\mathbb{Q}(\mu_p)$. On conclut par unicité.

ii. Montrer que $\mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$ contient un unique élément τ d'ordre 2, que celui-ci est induit par la conjugaison complexe, et que sa signature (comme permutation des racines primitives) est $(-1)^{\frac{p-1}{2}}$.

Comme ci-dessus, $\mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$ contient un unique sous-groupe d'ordre 2, donc un unique élément d'ordre 2, et celui-ci est $\tau = \sigma^{\frac{p-1}{2}}$. Par ailleurs, la conjugaison complexe induit certainement un automorphisme c de $\mathbb{Q}(\mu_p)$ d'ordre au plus 2. Comme $c(e^{2i\pi/p}) = e^{-2i\pi/p} \neq e^{2i\pi/p}$, cet automorphisme est non trivial, donc d'ordre 2, et $c = \tau$. Son action sur les racines de $X^p - 1$ est donnée par $c(e^{2ik\pi/p}) = e^{-2ik\pi/p}$. Comme p est impair, τ est donc un produit de $\frac{p-1}{2}$ transpositions, d'où la signature.

iii. Montrer que $\mathbb{Q}(\mu_p) \cap \mathbb{R} = \mathbb{Q}(\cos(\frac{2\pi}{p}))$.

On a certainement $\cos(\frac{2\pi}{p}) = \frac{e^{2i\pi/p} + e^{-2i\pi/p}}{2} \in \mathbb{Q}(\mu_p) \cap \mathbb{R}$. Par ailleurs, $\mathbb{Q}(\mu_p)$ a pour $\mathbb{Q}$-base $(e^{2ik\pi/p})_{1 \leqslant k \leqslant p-1}$. Pour $\alpha := \sum_k a_k e^{2ik\pi/p}$, on a alors $\alpha \in \mathbb{R} \Leftrightarrow \forall k, a_k = a_{p-k}$, auquel cas $\alpha = \sum_{k=1}^{\frac{p-1}{2}} \cos(\frac{2k\pi}{p})$. Mais on sait (ou on redémontre par récurrence) que $\cos(kx)$ est un polynôme en $\cos(x)$. D'où $\mathbb{Q}(\mu_p) \cap \mathbb{R} \subset \mathbb{Q}(\cos(\frac{2\pi}{p}))$.

Exercice 3 (Problème de Galois inverse pour les groupes abéliens)**.** On admet le théorème de Dirichlet : *pour tout entier $a \geqslant 1$, l'ensemble des nombres premiers p tel que $p \equiv 1$ mod a est non vide, et même infini.*

i. Montrer que tout groupe cyclique est quotient d'un groupe de la forme $(\mathbb{Z}/p\mathbb{Z})^\times$ pour un p premier.

Soit a un entier. Choisissons grâce à Dirichlet un p tel que $a | p-1$, et donc $a\mathbb{Z} \supset (p-1)\mathbb{Z}$. Alors $\mathbb{Z}/a\mathbb{Z} = (\mathbb{Z}/(p-1)\mathbb{Z})/(a\mathbb{Z}/(p-1)\mathbb{Z})$, donc on conclut puisque $(\mathbb{Z}/p\mathbb{Z})^\times \simeq \mathbb{Z}/(p-1)\mathbb{Z}$

ii. Montrer que tout groupe abélien fini est quotient d'un groupe de la forme $(\mathbb{Z}/n\mathbb{Z})^\times$ pour un entier $n \geqslant 1$.

Le théorème de classification des groupes abéliens finis nous dit qu'un tel groupe est de la forme $H = \mathbb{Z}/a_1\mathbb{Z} \times \cdots \times \mathbb{Z}/a_r\mathbb{Z}$ avec $a_1 | \cdots | a_r$. Choisissons grâce à Dirichlet des p_i *deux*

TSVP

à deux distincts tels que $a_i | p_i - 1$. Donc H est quotient de $(\mathbb{Z}/p_1\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_r\mathbb{Z})^\times = (\mathbb{Z}/n\mathbb{Z})^\times$ avec $n = p_1 \cdots p_r$ par le théorème des restes chinois (les p_i sont distincts).

iii. Montrer que tout groupe abélien fini est le groupe de Galois d'une extension de $\mathbb{Q}$.

On applique la correspondance de Galois à l'extension $\mathbb{Q} \subset \mathbb{Q}(\mu_n)$ et la question précédente.

Exercice 4 (Problème de Galois inverse pour les groupes symétriques)**.** Soit $n > 2$ un entier et p, q deux premiers distincts.

i. Montrer que pour tout entier m, il existe un polynôme irréductible de degré m dans $\mathbb{F}_p[X]$.

On sait que le corps $\mathbb{F}_{p^m}$ est de degré m sur $\mathbb{F}_p$ et qu'il admet un élément primitif (par exemple un générateur du groupe cyclique $\mathbb{F}_{p^m}^\times$). Le polynôme minimal de cet élément primitif est donc de degré m.

ii. Montrer qu'il existe un polynôme unitaire irréductible $f \in \mathbb{Z}[X]$ de degré n tel que :

- $(f \bmod p)$ possède un facteur irréductible de degré $n-1$ dans $\mathbb{F}_p[X]$ et
- $(f \bmod q)$ soit séparable et possède un unique facteur irréductible de degré pair, ce degré étant égal à 2, dans $\mathbb{F}_q[X]$.

On commence par choisir $f_p \in \mathbb{F}_p[X]$ et $f_q \in \mathbb{F}_q[x]$ unitaires de la forme voulue grâce à la question 1. Puis on utilise le théorème des restes Chinois pour trouver $f \in \mathbb{Z}[X]$ se réduisant respectivement sur f_p et f_q. Le problème est qu'on veut aussi f irréductible. Pour cela, on peut par exemple choisir un troisième nombre premier ℓ et demander que la réduction de f mod ℓ soit un polynôme irréductible $f_\ell \in \mathbb{F}_\ell[X]$ préalablement choisi.

iii. Pour un tel f, montrer que $G_f = \mathfrak{S}_n$.

Puisque f est irréductible, G_f est un sous-groupe transitif de $\mathfrak{S}_n$. Par le théorème de spécisalisation en p, G_f contient un $(n-1)$-cycle c. Par le même théorème en q, il contient un élément $\sigma = \tau\sigma'$ avec τ transposition de support disjoint de celui de σ' qui est produit de cycles disjoints impairs. Donc si k désigne le ppcm des longueurs des cycles de σ', on voit que $\tau = \sigma^k$ appartient à G_f.

Grâce à la transitivité, il existe $g \in G_f$ tel que le support de $g\tau g^{-1}$ n'est pas contenu dans celui de c. Quitte à renuméroter les racines, on peut supposer $g\tau g^{-1} = (1, 2)$ et $c = (2, 3, \cdots, n-1)$. Mais alors, G_f contient $c^k g\tau g^{-1} c^{-k} = (1, k+1)$. Or, on sait que $\mathfrak{S}_n$ est engendré par les $(1, i)$, $2 \leqslant i \leqslant n$.

Exercice 5. On veut montrer que le corps $\mathbb{C}(X)$ peut être plongé dans $\mathbb{C}$. Pour cela, notons $\Theta \subset \mathbb{C}$ une base de transcendance de $\mathbb{C}$ sur $\mathbb{Q}$.

i. Expliquer pourquoi $\mathbb{C}$ est une clôture algébrique de $\mathbb{Q}(\Theta)$.

Par définition de base de transcendance, $\mathbb{C}$ est algébrique sur $\mathbb{Q}(\Theta)$. Comme $\mathbb{C}$ est algébriquement clos, c'en est donc une clôture algébrique.

ii. Soit k un corps au plus dénombrable.

(a) Montrer qu'une clôture algébrique de k est au plus dénombrable.

Remarquons que $k[X]$ est en bijection avec $k^{(\mathbb{N})}$ donc est dénombrable. Regardons l'application $\bar{k} \longrightarrow k[X]$ qui a α associe son polynôme minimal f_α. Ses fibres sont finies, d'où une partition $\bar{k} = \bigsqcup_f \{\alpha, f_\alpha = f\}$ par des sous-ensembles finis indexés par le sous-ensemble dénombrable des polynômes irréductibles dans $k[X]$. Il s'ensuit que $\bar{k}$ est dénombrable.

(b) Montrer que $k(X)$ est au plus dénombrable.

L'application $k[X] \times k[X] \setminus \{0\} \longrightarrow k(X)$, $(f, g) \mapsto f/g$ est surjective, donc $k(X)$ est au plus dénombrable.

iii. (a) Montrer que le degré de transcendance de $\mathbb{C}$ sur $\mathbb{Q}$ est infini.

D'après ii(b), un corps de degré de transcendance fini sur $\mathbb{Q}$ est dénombrable, ce qui n'est pas le cas de $\mathbb{C}$.

(b) En déduire que Θ est en bijection avec $\Theta \sqcup \{X\}$, puis construire un isomorphisme de corps $\mathbb{Q}(\Theta) \xrightarrow{\sim} \mathbb{Q}(\Theta)(X)$.

On vient de voir que Θ est infini. En particulier, il contient un sous-ensemble Σ en bijection avec $\mathbb{N}$, disons $\Sigma = \{X_n\}_{n\in\mathbb{N}}$. Notons $X_0 := X$. La bijection $\mathbb{N} \setminus \{0\} \xrightarrow{\sim} \mathbb{N}$, $n \mapsto n-1$ induit une bijection $\Sigma \xrightarrow{\sim} \Sigma \sqcup \{X_0\}$, que l'on prolonge en une bijection $\Theta \xrightarrow{\sim} \Theta \sqcup \{X_0\}$ en prenant l'identité sur $\Theta \setminus \Sigma$. Cette bijection induit, par propriété universelle des polynômes, un isomorphisme $\mathbb{Q}[\Theta] \xrightarrow{\sim} \mathbb{Q}[\Theta \sqcup \{X\}] = \mathbb{Q}[\Theta][X]$ de $\mathbb{Q}$-algèbres, lequel induit un isomorphisme des corps de fractions comme souhaité.

iv. Montrer que $\mathbb{C}(X)$ est isomorphe à un sous-corps de $\mathbb{C}$.

Puisque $\mathbb{C}$ est algébrique sur $\mathbb{Q}(\Theta)$ et X est évidemment algébrique sur $\mathbb{Q}(\Theta)(X)$, on a que $\mathbb{C}(X)$ est algébrique sur $\mathbb{Q}(\Theta)(X)$. Via l'isomorphisme précédent, on obtient donc une extension algébrique $\mathbb{Q}(\Theta) \hookrightarrow \mathbb{C}(X)$. Par la propriété des clôtures algébriques, on peut donc plonger cette extension algébrique dans $\mathbb{C}$, vu comme clôture algébrique de $\mathbb{Q}(\Theta)$.

v. Est-ce que $\overline{\mathbb{Q}}(X)$ est isomorphe à un sous-corps de $\overline{\mathbb{Q}}$?

L'élément X de $\overline{\mathbb{Q}}(X)$ est transcendant sur $\mathbb{Q}$. Tout morphisme de corps de caractéristique nulle est $\mathbb{Q}$-linéaire. Or, $\overline{\mathbb{Q}}$ ne contient aucun élement transcendant sur $\mathbb{Q}$. Donc on ne peut pas plonger $\overline{\mathbb{Q}}(X)$ dans $\overline{\mathbb{Q}}$.