

Théorie de Galois

Extension normale et séparable.

Exercice 1 — Extension de degré 2. Soient k un corps et K une extension de k de degré 2. Déterminer $\text{Aut}_k(K) = \text{Gal}(K/k)$. Attention à la caractéristique 2.

Exercice 2 — Extension de degré premier. Soient k un corps et $j : k \rightarrow K$ une extension de k de degré p avec p premier.

- Montrer que l'extension j est monogène.
- On note $\theta \in K$ un générateur de j c'est-à-dire $K = k(\theta)$. Donner une condition nécessaire et suffisante sur θ pour que l'extension j soit séparable.
- On se place dans le cas non séparable. Déterminer le nombre de racines du polynôme minimal π_θ de θ et la forme de π_θ . Montrer que l'extension j est normale et calculer le groupe de Galois de j .
- On se place dans le cas séparable. Déterminer le nombre de racines de π_θ et la forme du polynôme minimal de θ .
- On reste dans le cas séparable. Soit $\theta' \neq \theta$ une racine de π_θ dans une clôture algébrique de K . Montrer que si $\theta' \in K$ alors l'extension j est normale puis calculer son groupe de Galois.
- Montrer que, si $p = 2$, l'extension j est toujours normale.

Exercice 3 — Extension à groupe de Galois symétrique. Soient $P \in \mathbb{Q}[X]$ un polynôme de degré n , K le corps de décomposition de P sur $\mathbb{Q}$. On suppose que le groupe de Galois de l'extension $j : \mathbb{Q} \rightarrow K$ est isomorphe au groupe symétrique $\mathfrak{S}_n$.

- Montrer que P est irréductible sur $\mathbb{Q}$.
- Soit $\alpha \in K$ est une racine de P . Calculer le groupe de Galois de l'extension $j_\alpha : \mathbb{Q} \rightarrow \mathbb{Q}(\alpha)$.
- On suppose $n \geq 4$. Montrer que $\alpha^n \notin \mathbb{Q}$.

Exercice 4 — Décomposition d'un polynôme dans une extension. Soient k un corps, $j : k \rightarrow K$ une extension de degré m et $P \in k[X]$ un polynôme unitaire irréductible de degré n . On note $d = \text{pgcd}(m, n)$.

- Montrer que le degré de tout facteur irréductible de $P \in K[X]$ est un multiple de n/d et que P a au plus d facteurs irréductibles dans $E[X]$. Que se passe-t-il si $d = 1$?
- Montrer que si j est normale alors tous les facteurs irréductibles de P dans $E[X]$ de même degré. Quelle relation a-t-on entre d et le nombre de facteurs irréductibles de P dans $E[X]$.

Exercice 5 — Suite d'extension normale. Soient k un corps, $j : k \mapsto K$ et $j' : K \mapsto K'$ deux extensions de corps.

- Montrer que si j et j' sont normales alors $j' \circ j$ ne l'est pas forcément.
- Montrer que si $j' \circ j$ est normale alors j' l'est mais j ne l'est pas forcément.

Exercice 6 — Extension séparable et points fixes. Soient k un corps, $j : k \mapsto K$ une extension séparable et $x \in K$. Montrer que $x \in k$ si et seulement si $\sigma(x) = x$ pour tout k -morphisme de K dans $\overline{K}$.

Exercice 7 — Extension monogène. Déterminer $[\mathbb{Q}(\sqrt{2}, i, j) : \mathbb{Q}]$. Montrer que l'extension est monogène et déterminer un générateur de $\mathbb{Q}(\sqrt{2}, i, j)$ sur $\mathbb{Q}$.

Théorie de Galois.

Exercice 8 — Un tout petit peu de cyclotomie. Montrer que le polynôme $\Phi_7 = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$ est irréductible sur $\mathbb{Q}$. Déterminer un sous-corps K de $\mathbb{C}$ qui soit $\mathbb{Q}$ -isomorphe à $\mathbb{Q}[X]/\Phi_7$. Déterminer $\text{Gal}(K/\mathbb{Q}) = \text{Gal}(\mathbb{Q}[X]/\Phi_7/\mathbb{Q})$.

Exercice 9 — Exemples. Soient k un corps et $P \in k[X]$. Déterminer le groupe de Galois de P sur k .

- $P = X^4 - 5$ sur $k = \mathbb{Q}$, $k = \mathbb{Q}(\sqrt{5})$, $k = \mathbb{Q}(i\sqrt{5})$, $k = \mathbb{Q}(i)$ et $k = \mathbb{Q}(i, \sqrt{5})$;

- b) $P = X^4 - a$ où $a \in \mathbb{Z}$ avec $a \neq 0$, $a \neq \pm 1$ sur $k = \mathbb{Q}$;
 c) $X^n - T$ sur $k = \mathbb{C}(T)$; $X^4 - T$ sur $k = \mathbb{R}(T)$.

Exercice 10 – Groupe de Galois d'un polynôme de degré 3.

- a) Soit $P \in k[X]$ un polynôme unitaire de degré n et $(\alpha_i)_{1 \leq i \leq n}$ les racines (comptées avec multiplicité) de P dans un corps de décomposition. Montrer que

$$D = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2 \in k$$

D s'appelle le discriminant de P .

Pour les questions **b**, **c** et **d**, on suppose P est séparable et car $k \neq 2$ et on note

$$d(P) = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j).$$

- b) Montrer que $\sigma(d(P)) = \varepsilon(\sigma)d(P)$ pour tout $\sigma \in \text{Gal}_k(P)$ où ε désigne la signature (de la permutation induite par σ sur les racines de P).
 c) Montrer que $k(d(P))$ est le sous-corps de $\text{Decomp}_k(P)$ associé au sous-groupe $\mathfrak{A}_n \cap \text{Gal}_k(P)$.
 d) Montrer que $\text{Gal}(P) \subset \mathfrak{A}_n$ si et seulement si D est un carré dans k si et seulement si $d(P) \in k$.
 e) Déterminer le groupe de Galois d'un polynôme de degré 3 en caractéristique différente de 2 et 3.
 f) Soit $P = X^3 + pX + q$. Calculer le discriminant D de P .
 g) En déduire le groupe de Galois sur $\mathbb{Q}$ des polynômes $P = X^3 - X - 1$, $X^3 - 10$, $X^3 + X + 1$ et $X^3 + X^2 - 2X - 1$.
 h) Déterminer le groupe de Galois $X^3 - 10$ sur $\mathbb{Q}(\sqrt{2})$, sur $\mathbb{Q}(i\sqrt{3})$, de $X^3 - X - 1$ sur $\mathbb{Q}(i\sqrt{23})$.

Exercice 11 – Suite d'extensions quadratiques. Soient k un corps de caractéristique différente de 2, $c \in k$ qui n'est pas un carré. On considère F l'extension quadratique de k associée au polynôme $X^2 - c$ et on note $x \in F$ tel que $x^2 = c$. On choisit ensuite $\alpha = a + bx \in F$ tel que $a, b \in k$. On note alors E le corps de décomposition de $X^2 - \alpha$ sur F .

- a) Montrer que les propositions suivantes sont équivalentes.

- (i) E est galoisienne sur k ;
- (ii) E est normale sur k ;
- (iii) E est le corps de décomposition sur F de $X^2 - \alpha'$ où $\alpha' = a - bx$;
- (iv) α' est un carré dans E ;
- (v) $\alpha\alpha' = a^2 - cb^2$ est un carré dans k ou $c\alpha\alpha'$ est un carré dans k .

Pour les questions **b** et **c**, on suppose que α n'est pas un carré dans F .

- b) Lorsque les conditions précédentes sont vérifiées, montrer que le groupe de Galois de E sur k est cyclique si et seulement si $c\alpha\alpha'$ est un carré dans k .
 c) En déduire le groupe de Galois de E sur k lorsque $\alpha\alpha'$ est un carré dans k .

Exercice 12 – Polynôme bicarré de degré 4. Soit $P = X^4 + aX^2 + b \in \mathbb{Q}[X]$ un polynôme irréductible dont on note $\pm\alpha, \pm\beta$ les racines dans un corps de décomposition de P .

- a) Majorer et minorer le cardinal du groupe de Galois G de P . Montrer que G est isomorphe à un sous-groupe de D_8 .
 b) En déduire que G est isomorphe à $\mathbb{Z}/4\mathbb{Z}$ ou $(\mathbb{Z}/2\mathbb{Z})^2$ ou à D_8 .
 c) Montrer que $G \simeq \mathbb{Z}/4\mathbb{Z}$ si et seulement si $(\alpha/\beta - \beta/\alpha) \in \mathbb{Q}$.
 d) Montrer que $G \simeq (\mathbb{Z}/2\mathbb{Z})^2$ si et seulement si $\alpha\beta \in \mathbb{Q}$ ou $\alpha^2 - \beta^2 \in \mathbb{Q}$.
 e) Montrer que sinon G est isomorphe à D_8 .
 f) Soit $P = X^4 - 4X^2 - 1$. Déterminer le corps de décomposition de P , son groupe de Galois et la correspondance de Galois associée.
 g) Même question pour les polynômes $X^4 + 30X^2 + 45$ et $X^4 + 4X^2 + 2$.

Exercice 13 – Complément à la correspondance de Galois. Soient k un corps et $j : k \rightarrow K$ une extension galoisienne finie de groupe G .

- a) Soit F un sous-corps de K contenant k . Montrer que $\{\sigma \in G, \sigma(F) = F\}$ est le normalisateur du groupe de Galois $\text{Gal}(K, F)$ de K sur F . Décrire le quotient.
- b) Soient F' un sous-corps de K contenant k qui est k -isomorphe à F . Montrer que cet isomorphisme est la restriction d'un élément de G . En déduire le nombre de sous-corps de K contenant k et isomorphe à F .
- c) Soit H un sous-groupe de G . Calculer son normalisateur H et le quotient N/H .

Exercice 14 – Groupe de Galois d'un polynôme non irréductible. Soit $P = (X^2 + 3)(X^3 - 3X + 1) \in \mathbb{Q}[X]$ et G le groupe de Galois de P sur $\mathbb{Q}$.

- a) Montrer que G est isomorphe à un sous-groupe de $\mathbb{Z}/2\mathbb{Z} \times \mathfrak{S}_3$.
- b) Calculer $|G|$.
- c) Le groupe G est-il commutatif? Cyclique?
- d) Reprendre l'exercice avec $P_1 = (X^2 + 3)(X^3 - 5)$.

Exercice 15 – Correspondance de Galois. Soient $P = X^6 - 11 \in \mathbb{Q}[X]$, $j = \exp(2i\pi/3)$, $K = \mathbb{Q}(j)$, $L = \mathbb{Q}(\sqrt[6]{11})$ et M le corps de décomposition de P sur $\mathbb{Q}$.

- a) Calculer $[L : \mathbb{Q}]$, $[K : \mathbb{Q}]$, $\text{Gal}(L | \mathbb{Q})$ et $\text{Gal}(K | \mathbb{Q})$.
- b) L'extension $\mathbb{Q} \subset L$ est-elle galoisienne? normale? séparable?
- c) Montrer que $K \subset M$ et calculer $\text{Gal}(M | K)$.
- d) Calculer $[M : \mathbb{Q}]$ et montrer que $\text{Gal}(M | \mathbb{Q})$ est isomorphe au groupe diédral D_6 (c'est-à-dire au groupe des isométries d'un hexagone régulier ou à un produit semidirect non commutatif de $\mathbb{Z}/6\mathbb{Z}$ par $\mathbb{Z}/2\mathbb{Z}$).
- e) Donner les extensions de degré 6 sur $\mathbb{Q}$ contenues dans M en précisant pour chacune si elles sont galoisiennes ou non. Donner un élément primitif de chacune de ces extensions.
- f) Donner les extensions de degré 3 sur $\mathbb{Q}$ contenues dans M en précisant pour chacune si elles sont galoisiennes ou non. Donner un élément primitif de chacune de ces extensions.
- g) Donner les extensions de degré 4 sur $\mathbb{Q}$ contenues dans M en précisant pour chacune si elles sont galoisiennes ou non. Donner un élément primitif de chacune de ces extensions.
- h) Donner les extensions de degré 2 sur $\mathbb{Q}$ contenues dans M en précisant pour chacune si elles sont galoisiennes ou non. Donner un élément primitif de chacune de ces extensions.

Extension et fraction rationnelle.

Exercice 16 – Un premier résultat. Soient k un corps et $k(X)$ le corps des fractions rationnelles sur k .

- a) Soit σ un automorphisme de corps de k . Montrer qu'il existe un unique automorphisme de corps σ' de $k(X)$ tel que $\sigma'(x) = \sigma(x)$ pour tout $x \in K$ et $\sigma(X) = X$.
- b) Soit G un sous-groupe du groupe des automorphismes de k . Pour $g \in G$, on note g' le prolongement de g à $k(X)$ donné dans la question a et $G' = \{g', g \in G\}$. Montrer que G' est un sous-groupe d'automorphisme de $k(X)$ isomorphe à G .
- c) On note k^G le sous-corps de k fixé par G et $k(X)^{G'}$ le sous-corps de $k(X)$ fixé par G' . Comparer $k(X)^{G'}$ et $k^G(X)$.

Exercice 17 – Automorphisme de $k(X)$. Soient k un corps et $k(X)$ le corps des fractions rationnelles sur k . Pour $F \in k(X)$, on écrit $F = P/Q$ avec $P, Q \in k[X]$ et P et Q premier entre eux et on pose $\deg F = \max(\deg P, \deg Q)$.

- a) Montrer que, si F n'est pas une constante, alors $[k(X) : k(F)] = \deg F$.
- b) Montrer que tout k -automorphisme de $k(X)$ est déterminé par une fraction rationnelle de degré 1.
- c) Montrer que le groupe G des k -automorphismes de $k(X)$ est isomorphe à $\text{PGL}(2, k) = \text{GL}(2, k)/k^\times \text{id}$.
- d) Montrer G est engendré par les automorphismes déterminés par les fractions rationnelles $X + b$ ($b \in k$), aX ($a \in k^\times$) et X^{-1} .
- e) On suppose que k est infini. Montrer que G est infini et déterminer $k(X)^G$.
- f) Montrer que l'extension $\mathbb{C}(X^3 + 1/X^3) \subset \mathbb{C}(X)$ est galoisienne, déterminer son groupe de Galois, les extensions intermédiaires et des éléments primitifs pour chacune.

Dans la suite, on suppose que k est fini de cardinal q .

- g) Déterminer l'ordre de G .
- h) Montrer que $k(X)^G = k(F)$ pour $F = (X^{q^2} - X)^{q+1} / (X^q - X)^{q^2+1}$.

- i)** Soit H_1 le sous-groupe de G formé par les automorphismes déterminées par les fractions rationnelles $aX + b$ ($a \in k^\times, b \in k$). Montrer que $k(X)^{H_1} = k(Y)$ où $Y = (X^q - X)^{q-1}$.
- j)** Soit H_2 le sous-groupe de G formé par les automorphismes déterminées par les fractions rationnelles $X + b$ ($b \in k$). Montrer que $k(X)^{H_2} = k(Z)$ où $Z = X^q - X$.
- k)** Soit H_3 le sous-groupe de G formé par les automorphismes déterminées par les fractions rationnelles aX ($a \in k^\times$). Montrer que $k(X)^{H_3} = k(T)$ où $T = X^{q-1}$.
- l)** Soit H_4 le sous-groupe de G formé par les automorphismes déterminées par les fractions rationnelles X et X^{-1} . Montrer que $k(X)^{H_4} = k(U)$ où $U = X + 1/X$.