TD5 : Théorie de Galois

23/10/2023

Exercice 1 : Exemples de groupes de Galois

1. Déterminer $\mathrm{Gal}(\mathbb{C},\mathbb{R})$ et $\mathrm{Gal}(\mathbb{R},\mathbb{Q})$.
2. Déterminer $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q})$.
3. Préciser les corps intermédiaires de L/K lorsque $K=\mathbb{Q}$ et $L=\mathbb{Q}(\sqrt{2}+\sqrt{3})$.
4. Préciser les corps intermédiaires de L/K lorsque $K=\mathbb{Q}$ et L est un corps de décomposition de X^3-2. Quels sont ceux qui sont normaux sur K ?
5. Soit α une racine dans $\mathbb{C}$ de $P(X)=X^3+X^2-2X-1$. Montrer que $\alpha'=\alpha^2-2$ est aussi racine de P. Calculer $\mathrm{Gal}(\mathbb{Q}(\alpha):\mathbb{Q})$ et montrer que l'extension $\mathbb{Q}(\alpha)/\mathbb{Q}$ est normale.

Exercice 2 : Corps cyclotomiques

1. Quel est le groupe de Galois de $\mathbb{Q}(exp(\frac{2i\pi}{35}))/\mathbb{Q}$? Est-il cyclique ?
2. Combien $\mathbb{Q}(exp(\frac{2i\pi}{35}))$ a-t-il de sous-corps de degré 12 ? De degré 6 ?

Exercice 3 : Le groupe de Galois comme groupe de permutations des racines d'un polynôme.

Soient K un corps de caractéristique $\neq 2$ et $P\in K[X]$. On note L un corps de décomposition de P sur K. On note $a_1,\dots,a_n$ les racines distinctes de P dans L. On note $G:=\mathrm{Gal}(L/K)$.
1. Montrer que G s'identifie naturellement à un sous-groupe de $\mathcal{S}_n$.
2. On suppose que G agit transitivement sur $\{a_1,\dots,a_n\}$. Montrer qu'alors il existe $Q\in K[X]$ irréductible tel que L est le corps de décomposition de Q sur K.
On rappelle que le discriminant de P est défini par

$$D=\Delta^2 \quad \text{avec} \quad \Delta:=(-1)^{\frac{n(n-1)}{2}}\prod_{i<j}(a_i-a_j). \tag{1}$$

On suppose que les racines de P dans L sont simples (on a alors $\deg P=n$).
3. Montrer que $D\in K$.
4. Montrer que $G\subset\mathcal{A}_n$ si et seulement si $\Delta\in K$.
5. On note $H:=G\cap\mathcal{A}_n$. Montrer que $L^H=K(\Delta)$.

Exercice 4 : Groupes de Galois et groupes symétriques

Soit p un nombre premier, P un polynôme irréductible sur $\mathbb{Q}$ de degré p. On suppose que P admet exactement deux zéros non réels.
1. Montrer que $\mathrm{Gal}_{\mathbb{Q}}(P)$ s'identifie à un sous-groupe de $\mathcal{S}_p$. Montrer qu'il contient un p-cycle et une transposition.
2. En déduire que $\mathrm{Gal}_{\mathbb{Q}}(P)\simeq\mathcal{S}_p$.

Exercice 5 : Groupe de Galois d'un polynôme de degré 3.

Soit $P=X^3+pX+q$ avec $p,q\in\mathbb{Q}$ et $K\subset\mathbb{C}$ l'extension de $\mathbb{Q}$ engendrée par es racines complexes (éventuellement confondues) z_1,z_2,z_3 de P. On note $G=Gal(K/\mathbb{Q})$.
1. Montrer la formule $\mathrm{disc}(P)=-\prod_i P'(z_i)$. En déduire la formule $\mathrm{disc}(P)=-4p^3-27q^2$.
2. Si P est réductible dans $\mathbb{Q}$, déterminer G en fonction du nombre de racines de P dans $\mathbb{Q}$.
On suppose désormais P sans racine dans $\mathbb{Q}$.
3. Montrer que les racines de P sont simples.
On plonge G dans S_3 en le faisant agir sur les racines.
4. Déterminer G en fonction des valeurs de $\mathrm{disc}(P)$.

✉clement.chivet@ens.fr

5. Montrer que P est irréductible sur $\mathbb{Q}(\sqrt{\text{disc}(P)})$.

Exercice 6 :

Soit $P = (X^2+3)(X^3-3X+1) \in \mathbb{Q}[X]$. Et G le groupe de Galois de P.
1. Montrer que G se plonge dans $\mathbb{Z}/2\mathbb{Z} \times \mathcal{S}_3$.
2. Déterminer G. Est-il commutatif ? cyclique ?

Exercice 7 :

On pose $a = \sqrt{5+\sqrt{21}}$ et on note $K = \mathbb{Q}(a)$.
1. Calculer $[K : \mathbb{Q}]$.
2. Montrer que $K/\mathbb{Q}$ est galoisienne.
3. Déterminer le groupe de Galois de l'extension $K/\mathbb{Q}$.
4. Déterminer les sous-corps de K.
5. L'extension $\mathbb{Q}(\sqrt{5+\sqrt{15}})/\mathbb{Q}$ est-elle galoisienne ?

Exercice 8 : Compositum de deux Corps

1. Soient $k \subset E, F \subset K$ des corps. On définit EF comme le plus petit sous-corps de K contenant E et F. On a $EF = E(F) = F(E)$.

a. Supposons que l'extension F/k est galoisienne. Montrer que EF/E et $F/F \cap E$ sont galoisienne et que $\text{res}_{|E} : \text{Gal}(EF/E) \to \text{Gal}(F/F \cap E)$ est un isomorphisme.

b. Dans ce cas, en déduire la relation sur les degrés :

$$[EF : k] = \frac{[F : k][E : k]}{[E \cap F : k]}$$

c. Supposons maintenant que E/k et F/k sont galoisiennes. Montrer que EF/k et $E \cap F/k$ sont galoisiennes et que l'application $\sigma \to (\sigma_{|E}, \sigma_{|F})$ de $\text{Gal}(EF/k) \to \text{Gal}(E/k) \times \text{Gal}(F/k)$ est un morphisme de groupe injectif et déterminer son image.

2. Soient m en n deux entiers naturels non nuls. On pose $N = ppcm(m,n)$ et $d = pgcd(m,n)$. Pour tout entier naturel non nul t, on désigne par ζ_t une racine primitive t-ème de l'unité dans $\mathbb{C}$.

a. Montrer que $\mathbb{Q}(\zeta_m)\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_N)$.
b. Montrer que $\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_d)$.

Exercice 9 : Méthode de Hilbert et Galois inverse

Soient K un corps de caractéristique nulle et $K \subseteq L$ une extension galoisienne de degré 3.
1. Déterminer le groupe de Galois de L/K.
2. Montrer qu'il existe un polynôme $P \in K[X]$ irréductible de degré 3 tel que L soit le corps de décomposition de P.
3. Donner l'exemple d'un corps K et d'un polynôme $P \in K[X]$ irréductible de degré 3 dont le corps de décomposition est de degré 6 sur K.

Soient σ l'automorphisme de corps qui fixe les éléments de K et qui envoie X sur $\dfrac{1}{1-X}$ et G le sous-groupe de $\text{Gal}(K(X)/K)$ engendré par σ.
4. Montrer que σ est un automorphisme d'ordre 3.
5. Montrer que le corps fixe $K(X)^G$ est de la forme $K(T)$, où l'extension $K(T) \subseteq K(X)$ est galoisienne de degré 3 et où T est une fraction rationnelle que l'on explicitera.

Supposons l'existence de $t \in K$ tel que le polynôme

$$P = X^3 - tX^2 + (t-3)X + 1 \in K[X]$$

soit irréductible.

6. Montrer que le corps de décomposition de P est une extension galoisienne de degré 3 de K.

Exercice 10 : Encore des exemples

Calculer les groupes de Galois suivants :

(i) $X^3 - 3X + 1$ sur $\mathbb{Q}$,

(ii) $X^3 - 3TX - T - T^2$ sur $\mathbb{C}(T)$,

(iii) $X^6 - 3X^2 - 1$,

(iv) $X^3 + 2X^2 + 3X + 2$ sur $\mathbb{Q}$, $\mathbb{Q}(\sqrt{7})$, et $\mathbb{Q}(i\sqrt{7})$.

Exercice 11 : Equation non résoluble par radicaux

On considère le polynôme

$$P(X) = X^5 - 5X^2 + 1 \in \mathbb{Q}[X] \tag{2}$$

et G le groupe de Galois de P sur $\mathbb{Q}$.

1. Montrer que G se plonge dans S_5.

Soit $\bar{P}$ la réduction de P dans $\mathbb{F}_2[X]$.

2. Montrer que $\bar{P}$ est irréductible dans $\mathbb{F}_2[X]$.

3. En déduire que P est irréductible dans $\mathbb{Z}[X]$ puis dans $\mathbb{Q}[X]$.

4. Montrer que G possède un élément d'ordre 5.

On note σ la conjugaison complexe.

5. Montrer que $\sigma \in G$ et déterminer le type de l'image de σ dans S_5.

6. Déterminer le cardinal de G. L'équation $P(x) = 0$ est-elle résoluble par radicaux ?

Exercice 12 : Groupe de Galois mod p

Soit $P(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_0 \in \mathbb{Z}[X]$ un polynôme unitaire à coefficients entiers. Notons $z_1, \ldots, z_n$ ses racines complexes et $K := \mathbb{Q}(z_1, \ldots, z_n) \subset \mathbb{C}$ le corps de décomposition de P, et $G = \mathrm{Gal}(K/\mathbb{Q})$. Soit p un nombre premier, $\overline{P}$ la réduction de P dans $\mathbb{F}_p[X]$ et $\overline{G}$ le groupe de Galois de $\overline{P}$.

On note $A = \mathbb{Z}[z_1, \ldots, z_n]$ sous-anneau de K.

1.

a. Montrer que l'action de G sur K laisse A stable.

b. Pour $a \in A, N(a) := \prod_{g \in G} g(a)$. Montrer que $N(a) \in \mathbb{Z}$.

c. Montrer que l'idéal pA est distinct de A.

d. Soit $\mathfrak{m}$ un idéal maximal de A contenant pA. Montrer que $k := A/\mathfrak{m}$ est un corps de décomposition de $\overline{P}$.

2. On pose $D_\mathfrak{m} := \{g \in G, g(\mathfrak{m}) = \mathfrak{m}\}$, et on note $\{\mathfrak{m}_1, \ldots, \mathfrak{m}_i\} = \{g(\mathfrak{m}), g \in G \backslash D_\mathfrak{m}\}$ l'ensemble des idéeaux distincts conjugués à $\mathfrak{m}$.

a. Montrer que $D_\mathfrak{m}$ est un sous-groupe de G.

b. Montrer que pour tout i, $\mathfrak{m}_i + \mathfrak{m} = A$, puis que $\mathfrak{m} + \mathfrak{m}_1 \ldots \mathfrak{m}_r = A$.

c. Montrer qu'il existe $x \in A$ tel que $\overline{x} \in k$ engendre l'extension $k/\mathbb{F}_p$. Montrer qu'il existe $z \in A$ tel que $\overline{z} = \overline{x}$ et $g(z) \in \mathfrak{m}$ pour tout $g \in G \backslash D_\mathfrak{m}$.

d. Montrer que le polynôme $\mu(X) := \prod_{g \in G}(X - g(z))$ est à coefficients dans $\mathbb{Z}$.

e. Si $g \in D_\mathfrak{m}$, expliquer pourquoi g induit un élément $\overline{g} \in \overline{G}$. Montrer que le morphisme $\psi : g \in D_\mathfrak{m} \to \overline{g} \in \overline{G}$ est un isomorphisme.

f. Si $\overline{P}$ est séparable, montrer que ψ est surjectif.

3. Quelle est la nature de $\overline{G}$?