

TD $n^{\circ}4$: GROUPES DE GALOIS

Exercice 1. Pour chacun des polynômes P de degré n suivants, déterminer:

- le corps de décomposition N de P sur $\mathbb{Q}$ et le groupe de Galois $G := \text{Gal}(N|\mathbb{Q})$
- la correspondance entre sous-groupes de G et sous-extensions de N et la factorisation de P sur chacune des extensions intermédiaires,
- un sous-groupe de S_n isomorphe à G , en numérotant les racines.

1. $X^2 - 2$

3. $X^3 - 1$

5. $X^4 + 1$

2. $(X^2 - 2)(X^2 - 3)$

4. $X^3 + 2$

Exercice 2. Soit $P(X) = X^3 + pX + q$ dans $\mathbb{Q}[X]$. On note a, b, c ses racines et $d = (a - b)(b - c)(c - a)$. On rappelle que $d^2 = -4p^3 - 27q^2$.

1. Supposons P réductible sur $\mathbb{Q}$. Décrire en fonction de d les structures possibles de G .
2. Supposons P irréductible sur $\mathbb{Q}$.
 - (a) Décrire en fonction de d les structures possibles de G (On rappelle que $\mathbb{K}(a, b, c) = \mathbb{K}(a, d)$).
 - (b) Donner les extensions intermédiaires entre $\mathbb{Q}$ et $\mathbb{Q}(a, b, c)$.

Exercice 3. À l'aide de l'exercice précédent déterminer les groupes de Galois de :

1. $X^3 - 3X + 1$ sur $\mathbb{Q}$.

4. $X^3 - 2X + 2$ sur $\mathbb{Q}$ et $\mathbb{Q}(i\sqrt{19})$.

2. $X^3 - 4X + 1$ sur $\mathbb{Q}$.

5. $X^3 - 1$ sur $\mathbb{Q}$ et $\mathbb{Q}(j)$.

3. $X^3 - 2X - 1$ sur $\mathbb{Q}$ et $\mathbb{Q}(\sqrt{5})$.

6. $X^3 - 5$ sur $\mathbb{Q}$, $\mathbb{Q}(\sqrt[3]{5})$ et $\mathbb{Q}(i\sqrt{3})$.

Exercice 4. Soit $\mathbb{K}$ un corps intermédiaire entre $\mathbb{Q}$ et $\mathbb{C}$. Soit $\mathbb{L}$ une extension de degré 4 de $\mathbb{K}$ contenue dans $\mathbb{C}$.

1. On suppose qu'il existe a et b dans $\mathbb{K}$ tels que $\mathbb{L} = \mathbb{K}(\sqrt{a}, \sqrt{b})$, on dit alors que $\mathbb{L}$ est une *extension biquadratique* de $\mathbb{K}$.
 - (a) Montrer que $\mathbb{L}$ d'un corps $\mathbb{K}$ est une extension normale de $\mathbb{K}$ et donner son groupe de Galois.
 - (b) Décrire la correspondance de Galois entre sous-groupes de G et extensions intermédiaires entre $\mathbb{K}$ et $\mathbb{L}$.
2. On suppose que $\mathbb{L}$ est une extension normale de $\mathbb{K}$ de groupe de Galois G isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Montrer que $\mathbb{L}$ est une extension biquadratique de $\mathbb{K}$.

Exercice 5. On pose $\alpha = \sqrt{6 + \sqrt{11}}$, $\beta = \sqrt{6 - \sqrt{11}}$ et $N = \mathbb{Q}(\alpha)$.

1. Déterminer le polynôme minimal P de α sur $\mathbb{Q}$ et vérifier que $[N : \mathbb{Q}] = 4$.
2. (a) Montrer que $\sqrt{11}$ et β sont dans N et montrer que N est normale.
 (b) Donner les expressions de β et $\sqrt{11}$ dans la base $\{1, \alpha, \alpha^2, \alpha^3\}$.

3. (a) Décrire la structure du groupe de Galois $G = \text{Gal}(N|\mathbb{Q})$.
 (b) En déduire qu'il existe a et b rationnels tels que $N = \mathbb{Q}(\sqrt{a}, \sqrt{b})$. (On pourra utiliser l'exercice précédent.)
 (c) Vérifier que l'on peut choisir $a = (\alpha + \beta)^2$ et $b = (\alpha - \beta)^2$.
4. Déterminer les extensions intermédiaires entre $\mathbb{Q}$ et N et les sous-groupes de G correspondants.

Exercice 6. Soit $P := X^3 + 3X - 2$ et $u = \sqrt[3]{1 + \sqrt{2}}$ et $v = \sqrt[3]{1 - \sqrt{2}}$ deux nombres réels. On note d le discriminant de P , δ le nombre de partie imaginaire positive tel que $\delta^2 = d$ et N la clôture normale de $\mathbb{Q}(u)$ sur $\mathbb{Q}$.

1. Montrer que P a une racine réelle et deux racines complexes conjuguées. On note a la racine réelle et b, c les racines complexes, avec que $\text{Im } b > 0$. Déterminer a, b, c .
2. Soit G le groupe de Galois $\text{Gal}(\mathbb{Q}(a, b, c)|\mathbb{Q})$. Déterminer la structure de G .
3. (a) Déterminer le degré de u sur $\mathbb{Q}$.
 (b) Montrer que $N = \mathbb{Q}(u, j)$.
4. On note Γ le groupe de Galois $\text{Gal}(N|\mathbb{Q})$.
 (a) Déterminer l'ordre de Γ .
 (b) Soit σ, τ les éléments de Γ tels que $\sigma(u) = u$ et $\sigma(j) = j^2$ et $\tau(u) = jv$ et $\tau(j) = j^2$.
 i. Quels sont les ordres de σ et τ ?
 ii. Montrer que σ et τ engendrent Γ .
 iii. Calculer les images de δ et $\sqrt{2}$ par τ et σ .
 (c) Décrire la structure de Γ .
 (d) Quel est le sous-groupe de Γ laissant $\mathbb{Q}(u)$ invariant ? Est-il distingué dans Γ ?
 (e) Déterminer les extensions invariantes par les groupes $\langle \sigma, \tau^2 \rangle, \langle \tau\sigma, \tau^2 \rangle, \langle \tau \rangle$.
5. Décrire la correspondance de Galois entre sous-groupes de Γ et sous-corps de N .

Exercice 7. Soient K un corps, N une extension normale de K et soit $G = \text{Gal}(N|K)$.

1. Soient G' et G'' deux sous-groupes de G . Montrer que

$$I(G \cap G') = K(I(G) \cup I(G')) \quad \text{et} \quad I(\langle G, G' \rangle) = I(G) \cap I(G').$$

2. Soient L', L'' des extensions de K contenues dans N et $G' = \text{Gal}(N|L')$ et $G'' = \text{Gal}(N|L'')$.
 (a) Montrer que si L' et L'' sont des extensions normales de K telles que $K(L' \cup L'') = N$ et $L' \cap L'' = K$ alors $G \simeq G' \times G''$.
 (b) Montrer qu'alors on a :

$$\text{Gal}(N|K) \simeq \text{Gal}(L'|K) \times \text{Gal}(L''|K).$$

3. On suppose qu'il existe deux sous-groupes G' et G'' de G tels que $G \simeq G' \times G''$. Montrer que $I(G') \cup I(G'')$ engendre N et $I(G') \cap I(G'') = K$.
4. Déterminer le groupe de Galois de $X^5 + X^2 - 9X + 3$ sur $\mathbb{Q}$.