Feuille 11 – Calculs de groupes de Galois

Exercice 1. Montrer qu'un polynôme irréductible sur $\mathbb{Q}$ de degré p premier, ayant exactement deux racines complexes non réelles, a son groupe de Galois (sur $\mathbb{Q}$) isomorphe à $\mathfrak{S}_p$. Montrer que c'est le cas de $X^5 - 4X + 2$ par exemple ($p = 5$). Et si p n'est pas premier ?

Exercice 2. Soit $P \in \mathbb{Q}[X]$ dont le corps de décomposition est L. Soient x_1, …, x_r les racines de P, on pose $Q = \prod_{i=1}^{r}(X - x_i) = \sum_{j=1}^{r} a_j X^j$. Montrer que si $K = \mathbb{Q}(a_1, \ldots, a_r)$, alors L est le corps de décomposition de Q sur K, et $\mathrm{Gal}(Q/K) = \mathrm{Gal}(P/\mathbb{Q})$.

Exercice 3. On s'intéresse au groupe de Galois de polynômes réductibles.

1. Soit $P = (X^2 + 3)(X^3 - 3X + 1) \in \mathbb{Q}[X]$. Montrer que les groupes de Galois de $X^2 + 3$ et $X^3 - 3X + 1$ sur $\mathbb{Q}$ sont respectivement $\mathfrak{S}_2$ et $\mathfrak{A}_3$, puis que $\mathrm{Gal}(P/\mathbb{Q}) \simeq \mathfrak{S}_2 \times \mathfrak{A}_3 \simeq \mathbb{Z}/6\mathbb{Z}$.
2. Soit $P = (X^2 + 3)(X^3 - 5) \in \mathbb{Q}[X]$. Montrer que le groupe de Galois de $X^3 - 5$ sur $\mathbb{Q}$ est $\mathfrak{S}_3$, puis que $\mathrm{Gal}(P/\mathbb{Q}) \not\simeq \mathfrak{S}_2 \times \mathfrak{S}_3$.
3. Montrer que si L_1 et L_2 sont deux extensions galoisiennes de K, alors l'extension composée L_1L_2 est galoisienne sur K, de groupe de Galois isomorphe au sous-groupe de $\mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K)$ constitué des couples (σ, τ) tels que $\sigma(x) = \tau(x)$ pour tout $x \in L_1 \cap L_2$.
4. En déduire que $\mathrm{Gal}(L_1L_2/K) \simeq \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K)$ si, et seulement si $L_1 \cap L_2 = K$.

Exercice 4. Soient $K_1 = K_2 = \mathbb{Q}(\sqrt[3]{2})$, plongés respectivement dans $\bar{\mathbb{Q}}$ par les plongements $\sigma_1 : K_1 \hookrightarrow \bar{\mathbb{Q}}$ et $\sigma_2 : K_2 \hookrightarrow \bar{\mathbb{Q}}$.

1. Montrer que l'extension composée $K_1K_2/\mathbb{Q}$ est de degré 3 si, et seulement si $\sigma_1 = \sigma_2$.
2. Déterminer $K_1 \otimes_{\mathbb{Q}} K_2$.

Exercice 5. Par spécialisation, montrer que le polynôme $X^5 - X - 1$ est de groupe de Galois (sur $\mathbb{Q}$) isomorphe à $\mathfrak{S}_5$.

Exercice 6. Soit K un corps de caractéristique différente de 2. Soit $P \in K[X]$ un polynôme séparable unitaire de degré n, et $(\alpha_i)_{1 \leqslant i \leqslant n}$ ses racines (dans une clôture algébrique, comptées avec multiplicité). On rappelle que d'après le TD8, exercice 8,

$$D = \prod_{1 \leqslant i < j \leqslant n} (\alpha_i - \alpha_j)^2 = (-1)^{\frac{n(n-1)}{2}} \prod_{\substack{1 \leqslant i,j \leqslant n \\ i \neq j}} (\alpha_i - \alpha_j)$$

appartient à K. On rappelle également que

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

vérifie $\sigma(d(P)) = \varepsilon(\sigma) d(P)$ pour tout $\sigma \in \mathrm{Gal}_K(P)$, où ε désigne la signature (de la permutation induite par σ sur les racines de P).

1. Montrer que $\mathrm{Gal}_K(P) \subseteq \mathfrak{A}_n$ si, et seulement si D est un carré dans K, si et seulement si $d(P) \in K$.
2. (a) Déterminer le groupe de Galois d'un polynôme de degré 3 en caractéristique différente de 2 et 3.
   (b) Montrer, en reliant D au déterminant de Vandermonde, que D peut s'exprimer simplement à l'aide des sommes de Newton $s_j = \sum_{i=0}^{n} \alpha_i^j$.

(c) Soit $P = X^3 + pX + q$. Déduire de la question précédente le discriminant D de P.

(d) En déduire le groupe de Galois sur $\mathbb{Q}$ des polynômes $X^3 - X - 1$, $X^3 - 10$, et $X^3 + X + 1$.

(e) Déterminer le groupe de Galois de $X^3 - 10$ sur $\mathbb{Q}(\sqrt{2})$ puis sur $\mathbb{Q}(i\sqrt{3})$, et de $X^3 - X - 1$ sur $\mathbb{Q}(i\sqrt{23})$.

Exercice 7. Soit $P = X^4 + aX^2 + b$ un polynôme irréductible sur $\mathbb{Q}$. On note $\pm\alpha$, $\pm\beta$ ses racines dans un corps de décomposition K.

1. Montrer que $\mathrm{Gal}(K/\mathbb{Q})$ est isomorphe à un sous-groupe du groupe diédral $\mathrm{D}_4 = \mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$. En déduire qu'il est isomorphe à $\mathbb{Z}/4\mathbb{Z}$, $(\mathbb{Z}/2\mathbb{Z})^2$ ou D_4.
2. Montrer qu'on a $\alpha^2 - \beta^2 \notin \mathbb{Q}$.
3. Montrer que $\mathrm{Gal}(K/\mathbb{Q}) = \mathbb{Z}/4\mathbb{Z}$ si, et seulement si $\frac{\alpha}{\beta} - \frac{\beta}{\alpha} \in \mathbb{Q}$, et $\mathrm{Gal}(K/\mathbb{Q}) = (\mathbb{Z}/2\mathbb{Z})^2$ si, et seulement si $\alpha\beta \in \mathbb{Q}$.
4. Montrer par des exemples explicites que tous ces cas de figure peuvent se produire.

Exercice 8. Le groupe $\mathfrak{S}_n$ agit naturellement sur $\mathbb{Q}[X_1, \ldots, X_n]$ par permutation des indéterminées. Pour $\varphi \in \mathbb{Q}[X_1, \ldots, X_n]$, on pose

$$\mathfrak{S}_\varphi = \{\sigma \in \mathfrak{S}_n \mid \varphi(X_{\sigma(1)}, \ldots, X_{\sigma(n)}) = \varphi(X_1, \ldots, X_n)\} \subseteq \mathfrak{S}_n,$$

qui n'est rien d'autre que le stabilisateur de φ pour cette action.

1. Décrire $\mathfrak{S}_\varphi \subseteq \mathfrak{S}_4$ pour $\varphi = X_1X_2 + X_3X_4$.

Si $P = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[X]$ est un polynôme unitaire, dont les racines sont notées $(\alpha_i)_{1 \leqslant i \leqslant n}$, on pose :

$$\mathrm{Res}(\varphi, P) = \prod_{\tau \in \mathfrak{S}_n \cdot \varphi} (X - \tau(\alpha_1, \ldots, \alpha_n)).$$

2. Montrer que $\mathrm{Res}(\varphi, P)$ est un polynôme à coefficients entiers.
3. Supposons que $\mathrm{Res}(\varphi, P)$ n'a pas de racines multiples. Montrer que le groupe de Galois de P sur $\mathbb{Q}$ est contenu dans un des $\mathfrak{S}_{\varphi_i}$ si, et seulement si $\mathrm{Res}(\varphi, P)$ a une racine entière.
4. Application : soit $P = X^4 + a_3X^3 + a_2X^2 + a_1X + a_0$ un polynôme irréductible de degré 4 et $\varphi = X_1X_2 + X_3X_4$.
   (a) Montrer que
   $$\mathrm{Res}(\varphi, P) = X^3 - a_2X^2 - (a_1a_3 - 4a_0)X - a_0a_3^2 - 4a_0a_2 - a_1^2,$$
   et en déduire que $\mathrm{Res}(\varphi, P)$ n'a pas de racine multiple.
   (b) Montrer que si $\mathrm{Res}(\varphi, P)$ n'a pas de racine entière, alors le groupe de Galois de P sur $\mathbb{Q}$ égale $\mathfrak{A}_4$ ou $\mathfrak{S}_4$: comment lever l'indétermination par un calcul pratique ? Montrer par des exemples explicites que ces deux cas de figure peuvent se produire.
   (c) Montrer que si $\mathrm{Res}(\varphi, P)$ a une racine entière, alors le groupe de Galois de P sur $\mathbb{Q}$ est isomorphe à $\mathbb{Z}/4\mathbb{Z}$, $(\mathbb{Z}/2\mathbb{Z})^2$ ou D_4. Par quel calcul pratique peut-on déterminer s'il s'agit de $(\mathbb{Z}/2\mathbb{Z})^2$ ou non ?
5. Montrer que si $P \in \mathbb{Z}[X]$ est un polynôme irréductible de degré n et $G \subseteq \mathfrak{S}_n$ un sous-groupe quelconque, alors il existe une fonction $\varphi \in \mathbb{Z}[X_1, \ldots, X_n]$ telle que $\mathfrak{S}_\varphi = G$, avec $\mathrm{Res}(\varphi, P)$ sans racine multiple.