THÉORIE DE GALOIS

FICHE III : GROUPE DE GALOIS

Exercice 1 (indépendance de Dedekind)**.** Soient K et L deux corps.

(1) Soient $\sigma_1, \ldots, \sigma_n$ des morphismes de groupes distincts d'un groupe G dans L^*. Montrer qu'ils sont linéairement indépendants sur L en tant qu'applications de G dans L. On pourra commencer par montrer que si $\sum_1^n \lambda_i \sigma_i = 0$, alors pour tout $g \in G$, on a $\sum_2^n \lambda_i(\sigma_i(g) - \sigma_1(g))\sigma_i = 0$.

(2) En déduire que si $\phi_1, \ldots, \phi_n$ sont des morphismes de corps distincts de K vers L, ils sont linéairement indépendants sur L.

(3) En déduire finalement que si L est une extension de K, les éléments du groupe de Galois vus comme élément du L-espace vectoriel $\mathrm{Hom}_K(L, L)$ sont indépendants.

Exercice 2. Calculer le groupe de Galois du corps de décomposition du polynôme minimal sur $\mathbb{Q}$ de $\sqrt{3+\sqrt{3}}$.

Exercice 3. Soit P un polynôme irréductible de degré 3 sur un corps K de caractéristique 0 (on peut prendre $K = \mathbb{Q}$ pour simplifier). Montrer qu'à un changement de variables K-linéaire près, on peut supposer que P s'écrit $X^3 + pX - q$. On appelle x_1, x_2, x_3 ses racines et L son corps de décomposition.

(1) Montrer que si $L = K(x_1)$ alors le groupe de Galois est $\mathbb{Z}/3\mathbb{Z}$.

(2) Montrer que dans ce cas $(x_1 - x_2)(x_2 - x_3)(x_3 - x_1)$ est un élément de K.

(3) Montrer dans tous les cas que $\delta = (x_1 - x_2)(x_2 - x_3)(x_3 - x_1)$ vérifie $\delta^2 \in K$ et le calculer en fonction de p et q. Pour ce dernier calcul, on pourra remarquer que $-\delta^2 = P'(x_1)P'(x_2)P'(x_3)$.

(4) Montrer que si $\delta \in K$, c'est-à-dire si $-4p^3 - 27q^2$ est un carré dans K, alors $K(x_1)$ est bien normale sur K. On trouvera les autres racines en fonction de $x = x_1$, en écrivant ce que vaut $x_2 + x_3$ et $x_2 - x_3$ en fonction de δ et de x.

On suppose maintenant que $-4p^3 - 27q^2$ n'est pas un carré. Pour $K = \mathbb{Q}$ et $4p^3 + 27q^2 > 0$, on va trouver une racine réelle qui s'écrive avec des racines carrées et cubiques réelles.

(5) Montrer que L/K est une extension d'ordre 6 qui consiste à rajouter δ et une racine de P à K. Quel est son groupe de Galois et quels sont les corps intermédiaires ?

(6) On prend $K = \mathbb{Q}$. Montrer qu'il n'y a qu'une racine réelle.

(7) On pose $x = y - p/(3y)$, montrer que y^3 satisfait une équation de degré 2 dont les racines y_1^3 et y_2^3 sont dans $\mathbb{R}$, qu'on peut choisir y_1 et y_2 dans $\mathbb{R}$ tels que $y_1 y_2 = -p/3$ et enfin que $x = y_1 + y_2$ est bien la racine réelle de P.

(8) Montrer que les autres racines s'écrivent alors $jy_1 + j^2 y_2$ et $j^2 y_1 + jy_2$ où j est « la » racine cubique primitive de l'unité, en vérifiant par exemple que $x_2 x_3 = x^2 + p$.

Exercice 4. Calculer les degrés et les groupes de Galois des corps de décomposition des polynômes (de $\mathbb{Q}[X]$) suivants : X^3-1, X^6-1, X^4-7, X^3-X^2-X-2, $X^5+X^4+\cdots+X+1$, X^4+1.

Exercice 5. Soit P un polynôme irréductible sur $\mathbb{Q}$ de degré p premier qui admet deux racines non réelles seulement ; on va montrer que le groupe de Galois G de son corps de décomposition est isomorphe à S_p (tout entier).

(1) Dire pourquoi on peut injecter le groupe de Galois dans S_p.

On identifiera désormais par cette injection les éléments du groupe de Galois avec des éléments de S_p et les racines non réelles seront numérotées 1 et 2.

(2) Montrer que l'ordre de G est un multiple de p et qu'il contient un élément d'ordre p.

(3) Montrer que "cet" élément est un p-cycle (dans S_p) et en déduire qu'on a dans G un p-cycle de la forme $(1, 2, ...)$.

(4) Montrer qu'on peut alors supposer que $(1, 2, \ldots, p) \in G$.

(5) Montrer que la conjugaison complexe est dans G et trouver l'élément de S_p auquel elle correspond.

(6) Montrer (ou admettre) que le sous-groupe de S_p engendré par $(1, 2)$ et $(1, 2, , p)$ est S_p. On pourra montrer que ce sous-groupe contient successivement $(k, k+1)$ pour tout $k < p$ et finalement toute transposition (k, l) pour $1 \leq k < l \leq p$.

Application : Montrer que les racines des polynômes X^5-6X-3, $2X^p-2pX+1$ ne peuvent s'exprimer sous forme de radicaux pour p un nombre premier supérieur à 5.

Exercice 6. On veut voir comment et à quelles conditions, on peut obtenir (sur $\mathbb{Q}$ ou sur K de caractéristique différente de 2) une extension galoisienne de groupe de Galois $\mathbb{Z}/4\mathbb{Z}$. Soit L une telle extension.

(1) Montrer que L ne possède qu'une sous-extension de degré 2 qu'on note K_1.

(2) Montrer qu'on a donc un $d \in K$ tel $\sqrt{d} \notin K$ et $L_1 = K(\sqrt{d})$.

(3) Montrer que $L = L_1\big(\sqrt{u+v\sqrt{d}}\big)$ pour $u, v \in K$ et qu'on doit avoir $v \neq 0$.

(4) On pose $\alpha = \sqrt{u+v\sqrt{d}}$, montrer que $L = K(\alpha)$ et en déduire toutes les racines du polynôme minimal de α.

(5) Montrer qu'on a un élément σ du groupe de Galois qui envoie α sur $\beta \neq \pm\alpha$ et β sur $-\alpha$.

(6) En déduire que $\sigma(\sqrt{d}) = -\sqrt{d}$ et que $\sigma(\alpha\beta) = -\alpha\beta$.

(7) Montrer que $\alpha\beta \in L_1$ et que $\alpha\beta = \sqrt{d}w$; en déduire que $u^2 = d(v^2+w^2)$, donc que d est somme de 2 carrés sans être un carré (on pourra traiter à part le cas $u = 0$ car dans ce cas tout élément est somme de 2 carrés).

(8) Réciproquement : soit $d = x^2+y^2$, où $x, y \in K$ avec d qui n'est pas un carré dans K.

Montrer que $K(\sqrt{d+x\sqrt{d}})$ est galoisienne sur K de groupe de Galois $\mathbb{Z}/4\mathbb{Z}$.