École polytechnique 2012-2013
Théorie de Galois

Feuille d'exercices 5

Soient k un corps parfait et Ω une clôture algébrique de k. On rappelle qu'une sous-extension finie K/k de Ω est *galoisienne* si pour chaque $x \in K$, tous les k-conjugués de x dans Ω appartiennent à K. D'après un résultat du cours, il est équivalent de demander que l'inclusion naturelle $\mathrm{Hom}_k(K,K) \subset \mathrm{Hom}_k(K,\Omega)$ soit une égalité, de sorte que $|\mathrm{Hom}_k(K,K)| = [K:k]$. Le groupe $\mathrm{Gal}(K/k) = \mathrm{Hom}_k(K,K)$ est appelé *groupe de Galois* de K/k. Si $x \in K$, les k-conjugués de x sont alors permutés transitivement par $\mathrm{Gal}(K/k)$.

Si $P \in k[X]$, on note R_P l'ensemble de ses racines dans Ω et $\mathrm{Gal}(P,k)$ le groupe de Galois de l'extension galoisienne $k(R_P)$ sur k.

Exercice 1. Soient $K_1 \subset \Omega$ et $K_2 \subset \Omega$ des extensions galoisiennes de k. Montrer que $K_1 \cap K_2$ et K_1K_2 sont aussi galoisiens sur k.

Exercice 2. Soit K une extension galoisienne de k et soient $k \subseteq L \subseteq K, k \subseteq F \subseteq K$ des sous-extensions de K. Montrer que $\mathrm{Gal}(K/LF) = \mathrm{Gal}(K/L) \cap \mathrm{Gal}(K/F)$ et que $\mathrm{Gal}(K/L \cap F)$ est le sous-groupe de $\mathrm{Gal}(K/k)$ engendré par $\mathrm{Gal}(K/L)$ et $\mathrm{Gal}(K/F)$.

Que peut-on en conclure si $\mathrm{Gal}(K/L) \cap \mathrm{Gal}(K/F) = 1$?

Exercice 3. Soit K un extension galoisienne de k et soit $k \subseteq F \subseteq K$ une sous-extension de K. Notons L la plus petite sous-extension normale de K contenant L . Montrer que

$$\mathrm{Gal}(K/L) = \bigcap_{\sigma \in \mathrm{Gal}(K/k)} \sigma \mathrm{Gal}(K/F) \sigma^{-1}.$$

Exercice 4. Soit $P \in k[X]$ un polynôme irréductible de degré n et soit $G = \mathrm{Gal}(P,k)$.

(i) Rappeler pourquoi $|R_P| = n$.

(ii) En déduire que n divise $|G|$ et que $|G|$ divise $n!$.

Exercice 5. Soit $g \in \mathbf{Q}[X]$ le polynôme cubique unitaire dont les racines réelles sont $x_1 = 2\cos(2\pi/7)$, $x_2 = 2\cos(4\pi/7)$ et $x_3 = 2\cos(6\pi/7)$.

(i) Vérifier que $g = X^3 + X^2 - 2X - 1$.

(ii) Montrer que g est irréductible.

(iii) Montrer que $\mathbf{Q}(x_1)$ est un corps de décomposition de g.

(iv) En déduire $\mathrm{Gal}(g)$.

(v) Indiquer une méthode pour calculer le *discriminant* de g, $\Delta = \prod_{i<j}(x_i - x_j)^2$.

Exercice 6. Soient $f = X^4 - 4X^2 - 1 \in \mathbf{Q}[X]$ et $g = Y^2 - 4Y - 1 \in \mathbf{Q}[Y]$.

(i) Pourquoi le groupe $\mathrm{Gal}(g,\mathbf{Q})$ est-il un quotient de $G = \mathrm{Gal}(f,\mathbf{Q})$?

(ii) Montrer que G est un sous-groupe de $\mathfrak{S}_{R_f}$ *compatible* avec la partition

$$\{\{\sqrt{2+\sqrt{5}}, -\sqrt{2+\sqrt{5}}\}, \{\sqrt{2-\sqrt{5}}, -\sqrt{2-\sqrt{5}}\}\}$$

de R_f. (On dit qu'une permutation σ d'un ensemble fini E est *compatible* avec une partition de E lorsque $x \sim y$ implique $\sigma(x) \sim \sigma(y)$ pour $\sim$ la relation d'équivalence dont les classes sont la partition considérée.)

(iii) En déduire que G est contenu dans le groupe diédral du carré.

(iv) Montrer qu'il existe un élément $\sigma \in G$ tel que $\sigma(\sqrt{2+\sqrt{5}})$ est égal à $\sqrt{2-\sqrt{5}}$ ou $-\sqrt{2-\sqrt{5}}$.

(v) Montrer qu'il existe un élément $\tau \in G$ échangeant $\sqrt{2-\sqrt{5}}$ et $-\sqrt{2-\sqrt{5}}$ mais fixant $\sqrt{2+\sqrt{5}}$.

(vi) En déduire que G est le groupe diédral tout entier.

Exercice 7. Soit K une extension galoisienne de k et $P \in k[X]$ un polynôme unitaire irréductible. Soient $Q, R \in K[X]$ des facteurs unitaires irréductibles de P. Montrer qu'il existe $\sigma \in \mathrm{Gal}(K/k)$ tel que $Q = \sigma(P)$ (on étend l'action de σ à $K[X]$ de façon évidente).

Exercice 8. Soit $f = X^d + a_1X^{d-1} + \cdots + a_d \in K[X]$ un polynôme (unitaire, de degré d) séparable à coefficients dans un corps K, et $\xi_1, \ldots, \xi_d$ ses racines dans un corps de décomposition noté L (de sorte que $f = \prod_{i=1}^d (X - \xi_i)$). On définit la *résolvante de Kronecker* de f comme

$$R = \prod_{\sigma \in \mathfrak{S}_d} \Big(X - \sum_{i=1}^{d} Y_i \xi_{\sigma(i)}\Big) \in L[X, Y_1, \ldots, Y_d]$$

(**i**). Montrer que le polynôme R est, en fait, à coefficients dans K, et il est invariant par $\mathfrak{S}_d$ agissant par permutation sur les variables $Y_1, \ldots, Y_d$.

(**ii**). Soit h un facteur irréductible quelconque de R dans $K[X, Y_1, \ldots, Y_d]$, choisi unitaire comme polynôme en X ; et soit S_h le sous-groupe de $\mathfrak{S}_d$ formé des permutations $\sigma \in \mathfrak{S}_d$ (permutant les Y_i) qui laissent h invariant. Montrer que S_h est de cardinal $\deg_X(h)$ et conjugué, dans $\mathfrak{S}_d$, au groupe de Galois $G = \mathrm{Gal}(L/K)$ de f sur K vu comme un groupe de permutations sur $\{\xi_i\}$. (Indication : on pourra montrer que si $(X - \sum_i Y_i \xi_i)$ est un facteur de h sur L, alors $h = \prod_{g \in G} \big(X - \sum_i Y_i g(\xi_i)\big)$.)

(**iii**). Soit $f = X^3 + X^2 - 2X - 1$ (*cf.* exercice 3). On admet que

$$\begin{aligned}
R = \Big(&X^3 + (Y_1 + Y_2 + Y_3)X^2 \\
&+\big(-2(Y_1^2 + Y_2^2 + Y_3^2) + 3(Y_1Y_2 + Y_2Y_3 + Y_3Y_1)\big)X \\
&+\big(-(Y_1^3 + Y_2^3 + Y_3^3) - 3(Y_1^2Y_2 + Y_2^2Y_3 + Y_3^1Y_1) \\
&\quad +4(Y_1Y_2^2 + Y_2Y_3^2 + Y_3Y_1^2) + Y_1Y_2Y_3\big)\Big) \\
\cdot\Big(&X^3 + (Y_1 + Y_2 + Y_3)X^2 \\
&+\big(-2(Y_1^2 + Y_2^2 + Y_3^2) + 3(Y_1Y_2 + Y_2Y_3 + Y_3Y_1)\big)X \\
&+\big(-(Y_1^3 + Y_2^3 + Y_3^3) + 4(Y_1^2Y_2 + Y_2^2Y_3 + Y_3^1Y_1) \\
&\quad -3(Y_1Y_2^2 + Y_2Y_3^2 + Y_3Y_1^2) + Y_1Y_2Y_3\big)\Big)
\end{aligned}$$

Que peut on en déduire sur le groupe de Galois de f sur $\mathbf{Q}$?

(**iv**). On considère à nouveau le cas général. Montrer que le discriminant de R (par rapport à la variable X) est un polynôme non nul dans $K[Y_1, \ldots, Y_d]$.

Exercice 9. Soit p premier et soient σ, τ respectivement une transposition et un p-cycle dans $\mathfrak{S}_p$. On note $G \subseteq \mathfrak{S}_p$ le sous-groupe engendré par τ et σ. Sans perte de généralité on pourra supposer que $\tau = (1, 2 \cdots, p)$ et $\sigma = (i, i + l)$ avec $1 \leq i < i + l \leq p$. Dans la suite, on considérera tous les entiers modulo p.

(i) Montrer que $(i + l, i + 2l)$ appartient à G, puis qu'il en est de même pour $(i, i + 2l)$.

(ii) Montrer que $(i, i + kl) \in G$ pour tout $k \in \mathbf{N}$.

(iii) En déduire que $G = \mathfrak{S}_p$.

Exercice 10. Soient $P = X^5 - 4X + 2 \in \mathbf{Q}[X]$ et $G = \mathrm{Gal}(P, \mathbf{Q})$.

(i) Vérifier que P est irréductible sur $\mathbf{Q}$.

(ii) Montrer que P a exactement trois racines réelles. En déduire que G, vu comme groupe de permutations des racines de P dans $\mathbf{C}$, contient une transposition.

(iii) Montrer que G contient un 5-cycle.

(iv) Montrer que $G = \mathfrak{S}_5$. (On pourra utiliser l'exercice précédent.)

(v) Modulo 257, P se décompose sous la forme $P = (X + 91)\,(X - 53)\,(X - 31)\,(X^2 - 7X - 118)$. Indiquer une méthode pour montrer que le dernier facteur est irréductible. (On verra plus tard que cela force G à contenir une transposition.)

Exercice 11. Soit k un corps parfait et Ω une clôture algébrique de k. On dit que k est *quasi-fini* si pour tout entier $n > 0$ il existe exactement une extension de k de degré n dans Ω.

(**i**). Soit G un groupe fini ayant la propriété suivante : pour tout diviseur d de $|G|$ il existe au plus un sous-groupe de G de cardinal d. Montrer que pour tout diviseur d de $|G|$ il existe au plus $\phi(d)$ éléments de G d'ordre d.

(**ii**). En utilisant la formule $\sum_{d|n} \phi(d) = n$ montrer que G est cyclique.

(**iii**). En conclure que toute extension finie d'un corps quasi-fini est galoisienne cyclique.