École Polytechnique 2009-2010

Théorie de Galois

Feuille d'exercices 7

Exercice 1. (Une preuve par la théorie de Galois du théorème de d'Alembert-Gauss) Soit K une extension finie de $\mathbf{R}$, on veut montrer que $K = \mathbf{R}$ ou $\mathbf{C}$.

(i) Montrer que si $K/\mathbf{R}$ est de degré 2, alors $K \simeq \mathbf{C}$.

(ii) Montrer que si $K/\mathbf{R}$ est de degré impair, alors $K = \mathbf{R}$.

(iii) Montrer que $\mathbf{C}$ n'admet pas d'extension de degré 2.

(iv) Supposons $K/\mathbf{R}$ galoisienne finie. Montrer l'existence d'une tour d'extensions

$$\mathbf{R} \subset K_1 \subset K_2 \subset \cdots \subset K_n = K$$

telle que $[K_1 : \mathbf{R}]$ est impair et, pour $i = 1, \ldots, n-1$, $[K_{i+1} : K_i] = 2$.

On pourra utiliser les résultats suivants de théorie des groupes (voir la feuille précédente). Soient G un groupe fini et p un nombre premier. Écrivons $|G| = p^\alpha m$ où $(p, m) = 1$. Alors il existe un sous-groupe $P \subset G$ de cardinal p^α ("Théorème de Sylow"). De plus, si $m = 1$ il existe une suite de sous-groupes $G_1 \subset G_2 \subset \cdots \subset G_\alpha = G$, avec $|G_i| = p^i$ et G_i distingué dans G.

(v) Conclure.

Exercice 2. Si G est un groupe, on note $D(G)$ le sous-groupe de G engendré par les commutateurs $[x, y] = xyx^{-1}y^{-1}$ pour $x, y \in G$. Si $n \geq 1$, on pose $D^n(G) = D(D^{n-1}(G))$, $D^0(G) = G$, et on rappelle que G est dit résoluble si il existe un entier $n \geq 1$ tel que $D^n(G) = \{1\}$.

(i) Montrer que si $f : G \to G'$ est un morphisme de groupes, alors $f(D(G)) \subset D(G')$, cette inclusion étant une égalité si f est surjective.

(ii) En déduire que si $1 \to H \to G \to K \to 1$ est une suite exacte de groupes, alors G est résoluble si, et seulement si, K et H sont résolubles.

(iii) Montrer que $D(G)$ est distingué dans G. De plus, si H est un sous-groupe distingué de G, montrer que G/H est abélien si et seulement si H contient $D(G)$.

(iv) Montrer que G est résoluble si, et seulement si, il existe une suite de sous-groupes

$$G_0 = \{1\} \subset G_1 \subset G_2 \subset \cdots \subset G_n = G$$

avec G_i distingué dans G_{i+1} et G_{i+1}/G_i abélien si $0 \leq i < n$.

(v) Même question où l'on remplace "abélien" par "cyclique".

Exercice 3. (Extensions radicales et résolubles par radicaux) Soient k un corps de caractéristique 0, Ω une clôture algébrique de k, et $K \subset \Omega$ une extension finie de k. On suppose que K/k est galoisienne de groupe de Galois résoluble.

(i) Si k contient toutes les racines $[K : k]$-ièmes de l'unité de Ω, montrer que K/k est radicale (on pourra utiliser le (v) de l'exercice précédent).

(ii) Si $x \in \Omega$, montrer que $K(x)/k(x)$ est galoisienne de groupe de Galois résoluble.

(iii) En déduire que K/k est résoluble par radicaux.

Dans les exercices qui suivent, on se propose d'appliquer explicitement la méthode générale montrant qu'une extension galoisienne de groupe de Galois résoluble est résoluble par radicaux. On montre d'abord comment retrouver les formules de Cardan-Tartaglia en degré 3.

Exercice 4. Soient k un corps parfait et $P = X^3+pX+q \in k[X]$ un polynôme irréductible. On note K l'extension de k engendrée par les racines x_1, x_2, x_3 de P dans une clôture algébrique Ω de k, et $j \in \Omega$ une racine primitive cubique de l'unité. On pose $\delta = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3) \in K$, de sorte que $\delta^2 = \mathrm{disc}(P) = -4p^3 - 27q^2 \in k$.

(i) Montrer que K/k est galoisienne de groupe de Galois $\mathcal{A}_3$ ou $\mathfrak{S}_3$, selon que $-4p^3 - 27q^2$ est ou non un carré dans k. Donner un exemple dans les deux cas pour $k = \mathbf{Q}$.

(ii) Montrer que $K(j)/k(\delta, j)$ est une extension de Kummer de degré 3, de groupe de Galois engendré par un élément σ tel que $\sigma(x_i) = x_{i+1}$ (les indices étant pris modulo 3).

(iii) Diagonaliser explicitement l'élément $\sigma \in \mathrm{End}_{k(\delta,j)}(K(j))$.

Soit A (resp. B) un vecteur propre de σ pour la valeur propre j (resp. j^2).

(iv) En déduire que $A^3 \in k(\delta, j)$ et que $K(j) = k(\delta, j, \sqrt[3]{A^3})$ (idem pour B).

(v) Retrouver la formule de Cardan-Tartaglia pour les racines x_i de P.

Calculs : $(x_1 + j^{-1}x_2 + j^{-2}x_3)^3 = \frac{-3\sqrt{-3}\delta - 27q}{2}$ et $(x_1 + j^{-2}x_2 + j^{-1}x_3)^3 = \frac{3\sqrt{-3}\delta - 27q}{2}$.

Exercice 5. Soit $P := X^4 + 4X^3 + 12X^2 + 24X + 24 \in \mathbf{Q}[X]$. On note $x_1, \ldots, x_4$ ses racines dans $\mathbf{C}$ et on pose $K := \mathbf{Q}(x_1, x_2, x_3, x_4)$.

(i) Montrer que P est irréductible dans $\mathbf{Q}[X]$. En déduire que les x_i sont distincts et que $\mathrm{Gal}(K/\mathbf{Q})$ s'identifie à un sous-groupe transitif de $\mathcal{A}_4$.

Données : la réduction modulo 5 de P est $(X^3 + 2X + 1)(X + 4)$ et $\mathrm{disc}(P) = 331776 = 2^{12}3^4$.

(ii) On pose $Q := (X - y_1)(X - y_2)(X - y_3) \in K[X]$ avec

$$y_1 = x_1x_2 + x_3x_4,\ y_2 = x_2x_3 + x_1x_4,\ \text{et}\ \ y_3 = x_3x_1 + x_2x_4.$$

Montrer que $Q \in \mathbf{Q}[X]$ et donner une méthode théorique pour calculer ses coefficients. Un calcul montrerait en fait que $Q = X^3 - 12X^2 + 192$.

(iii) Montrer que Q est irréductible dans $\mathbf{Q}[X]$, puis que $\mathrm{Gal}(K/\mathbf{Q}) \simeq \mathcal{A}_4$.

(iv) Soit $L := \mathbf{Q}(y_1, y_2, y_3) \subset K$. Montrer que $L/\mathbf{Q}$ est galoisienne cyclique de degré 3, que c'est l'unique sous-corps de degré 3 de $\mathbf{Q}(e^{2i\pi/9})$, i.e. $\mathbf{Q}(\cos(2\pi/9))$, et que

$$\{y_1, y_2, y_3\} = \{4 + 2\cos(2\pi/9),\ 4 + 2\cos(8\pi/9),\ 4 + 2\cos(6\pi/9)\}.$$

Donnée : $\mathrm{disc}(Q) = 2^{12}3^4$, si $z = y_1 + jy_2 + j^2y_3$ alors $z^3 = 1728j = 12^3j$.

(v) Donner une écriture explicite des x_i comme sommes de radicaux emboîtés de rationnels. (On pourra d'abord les écrire comme sommes de radicaux d'éléments de L.)