École Polytechnique 2009-2010

Théorie de Galois

Feuille d'exercices 6

Soient k un corps parfait et Ω un corps algébriquement clos contenant k. Soit $K \subset \Omega$ une extension finie de k. On rappelle que K/k est dite *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. Par exemple, si $P \in k[X]$ (non nécessairement irréductible) et si $x_1, x_2, \ldots, x_n$ sont les racines de P dans Ω, alors $k[x_1, \ldots, x_n] \subset \Omega$ est une extension galoisienne de k.

Exercice 1. Soit $x = \sqrt{1+\sqrt{2}} \in \mathbf{R}$.

(i) Montrer que $[\mathbf{Q}[x] : \mathbf{Q}] = 4$.

(ii) Montrer que $\mathbf{Q}[x]/\mathbf{Q}$ n'est pas galoisienne, bien que $\mathbf{Q}[x]/\mathbf{Q}[\sqrt{2}]$ et $\mathbf{Q}[\sqrt{2}]/\mathbf{Q}$ le soient. (Pour le premier point, on pourra remarquer que $\pm\sqrt{1-\sqrt{2}}$ est un conjugué de x sur $\mathbf{Q}$.) Vérifier que $\mathbf{Q}[x,i]$ est galoisienne sur $\mathbf{Q}$ de degré 8. [1]

(iii) Montrer qu'en revanche, $\mathbf{Q}[\sqrt{2+\sqrt{2}}]$ est galoisienne sur $\mathbf{Q}$, de degré 4.

Exercice 2. (Retour sur un exercice de PC) Soient $x = \sqrt[3]{2}$, $j = e^{2i\pi/3}$ et $K = \mathbf{Q}[x,j] \subset \mathbf{C}$.

(i) Montrer que K est galoisienne sur $\mathbf{Q}$, que $[K : \mathbf{Q}] = 6$, puis que $\mathrm{Gal}(K/\mathbf{Q})$ est isomorphe à $\mathfrak{S}_3$ (considerer l'action sur les conjugués de x sur $\mathbf{Q}$).

(ii) Expliciter la correspondance de Galois dans l'extension $K/\mathbf{Q}$.

Exercice 3. Soient q une puissance d'un nombre premier p et $n \geq 1$ un entier.

(i) Montrer que l'extension $\mathbf{F}_{q^n}/\mathbf{F}_q$ est galoisienne de groupe de Galois cyclique d'ordre n engendré par $x \mapsto x^q$.

(ii) Expliciter la correspondance de Galois pour cette extension.

Exercice 4. (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 le théorème de Sylow, énoncé et démontré dans l'exercice 5, ainsi que le résultat de l'exercice 6.)

(v) Conclure.

[1] On pourrait montrer que $\mathrm{Gal}(\mathbf{Q}[x,i])/\mathbf{Q})$ est isomorphe au groupe des isométries d'un carré, ou ce qui revient au même au commutant de la double transposition (13)(24) dans $\mathfrak{S}_4$ (ce dernier groupe a par ailleurs été étudié dans le dernier exercice de la PC5, où il est noté D).

Exercice 5. (L'existence des p-Sylow par dévissage) Soit G un groupe fini et p un nombre premier divisant $|G|$. Écrivons $|G| = p^\alpha m$ où $(p, m) = 1$. On se propose de montrer qu'il existe un sous-groupe $P \subset G$ de cardinal p^α (*Théorème de Sylow).*

(i) Démontrer le résultat si G est un groupe cyclique.

(ii) En déduire que si G est abélien et p divise $|G|$, alors G contient un élément d'ordre p. (Si on note d_x l'ordre d'un élément $x \in G$, on pourra d'abord construire un morphisme surjectif bien choisi

$$\prod_{x \in G} (\mathbf{Z}/d_x\mathbf{Z}) \longrightarrow G.$$

En déduire que l'un au moins des d_x est divisible par p puis conclure par le (i).)

Nous allons maintenant démontrer le théorème par récurrence sur $|G|$. Il est évident si $|G| = p$. Pour $x \in G$, on note $\mathrm{conj}(x) = \{gxg^{-1}, g \in G\}$ sa classe de conjugaison, et $G_x = \{g \in G, gx = xg\}$ son commutant. Enfin, $Z = \{g \in G, gh = hg \ \forall h \in G\}$ est le centre de G.

(iii) Vérifier que Z et G_x sont des sous-groupes de G, et que $|G_x||\mathrm{conj}(x)| = |G|$. De plus, vérifier que $x \in Z$ si et seulement si $|\mathrm{conj}(x)| = 1$.

(iv) Conclure dans le cas où il existe un $x \in G \backslash Z$ tel que $|\mathrm{conj}(x)|$ est premier à p.

(v) Supposons donc que p divise $|\mathrm{conj}(x)|$ pour tout $x \in G \backslash Z$. En écrivant G comme réunion disjointe de classes de conjugaison, montrer que $|G| \equiv |Z| \bmod p$.

(vi) En déduire qu'il existe un élément $z \in Z$ d'ordre p.

(vii) Soit $H = \langle z \rangle$. Montrer que H est distingué dans G, puis que G/H admet un sous-groupe d'ordre $p^{\alpha-1}$.

(viii) Conclure.

Exercice 6. Soit p un nombre premier. On rappelle qu'un p-groupe est un groupe fini de cardinal une puissance de p. Cet exercice fait suite à l'exercice précédent.

(i) (*Le centre d'un p-groupe est non trivial*) Montrer que si G est un groupe fini alors

$$|G| = |Z| + \sum_{i=1}^{r} |\mathrm{conj}(x_i)|$$

pour certains éléments $x_1, \ldots, x_r \in G \backslash Z$ bien choisis. En déduire que le centre d'un p-groupe est non trivial, puis qu'il contient un élément d'ordre p.

(ii) Montrer que si $|G| = p^n$, alors il existe une suite de sous-groupes $G_1 \subset G_2 \subset \cdots \subset G_n$, avec $|G_i| = p^i$ et G_i distingué dans G. On pourra d'abord montrer l'existence de G_1 puis considérer le groupe quotient G/G_1 (principe de preuve "par dévissage").

Exercice 7. * (Retour sur la constructibilité) En utilisant la correspondance de Galois et l'exercice précédent (ii), montrer qu'un nombre algébrique $x \in \mathbf{C}$ est constructible à la règle et au compas si, et seulement si, l'extension engendrée par x *et ses conjugués* est de degré une puissance de 2.

Exercice 8. Démontrer la proposition 6.9.4 du poly et faire l'exercice 6.10.2.