École Polytechnique 2009-2010

Théorie de Galois

Feuille d'exercices 1

Exercice 1. (Rappel de cours) (i) Soit k un corps. Rappeler pourquoi tout idéal non nul de $k[X]$ est engendré par un unique polynôme unitaire.

Soient $k \subset K$ une extension de corps et $x \in K$ un élément algébrique sur k. Notons $I_x \subset k[X]$ l'ensemble des polynômes $P \in k[X]$ annulateurs de x, *i.e.* tels que $P(x) = 0$.

(ii) Montrer que I_x est un idéal non nul.

On note Π_x le générateur unitaire de I_x ("le polynôme minimal de x sur k").

(iii) Montrer que Π_x est irréductible dans $k[X]$.

On pose $k[x] = \{P(x), P \in k[X]\} \subset K$.

(iv) Vérifier que $k[x]$ est une sous-k-algèbre de K et que $[k[x] : k] = \deg(\Pi_x)$. On pourra montrer que $1, x, x^2, \ldots, x^{\deg(\Pi_x)-1}$ est une base de $k[x]$ sur k.

(v) Montrer que $k[x]$ est un corps et donner une méthode pour exprimer l'inverse d'un élément non nul de $k[x]$ comme polynôme en x de degré $< \deg(\Pi_x)$.

Exercice 2. (i) Montrer que $\sqrt{7}$, $e^{2i\pi/17}$, $\sqrt{2} + \sqrt[3]{5}$ sont des nombres algébriques sur $\mathbf{Q}$.

(ii) Montrer que tout nombre complexe est algébrique sur $\mathbf{R}$.

Exercice 3. (i) Montrer que $X^3 - 2$ est irréductible dans $\mathbf{Q}[X]$.

(ii) En déduire que $\sqrt[3]{2}$ n'est pas de la forme $a + b\sqrt{c}$ où $a, b, c \in \mathbf{Q}$.

(iii) Trouver des rationnels a, b, c tels que $\frac{1}{\sqrt[3]{4}-1} = a + b\sqrt[3]{2} + c\sqrt[3]{4}$.

Exercice 4. (Rappels de cours bis) Soit K/k une extension de corps.

(i) (Base téléscopique) Soit L une K-algèbre. Montrer que $[L : k] < \infty$ si et seulement si $[L : K] < \infty$ et $[K : k] < \infty$, auquel cas on a l'égalité $[L : k] = [L : K][K : k]$.

(ii) Pour $x, y \in K$, on pose $k[x, y] = \{P(x, y), P \in k[X, Y]\} = (k[x])[y]$. Si x, y sont algébriques sur k, montrer que $[k[x, y] : k] \leq [k[x] : k][k[y] : k]$. En déduire que $x + y$ et xy sont algébriques sur k.

Exercice 5. (Extensions quadratiques) Soit k un corps de caractéristique différente de 2 et $k \subset K$ une extension quadratique, c'est à dire telle que $[K : k] = 2$.

(i) Montrer qu'il existe $x \in K \backslash k$ tel que $x^2 \in k^*$ et $K = k[x]$.

(ii) Vérifier que si un autre élément $y \in K$ a cette propriété, alors $y = \lambda x$ pour $\lambda \in k^*$.

(iii) En déduire que toute extension quadratique de $\mathbf{Q}$ dans $\mathbf{C}$ s'écrit de manière unique $\mathbf{Q}(\sqrt{n})$ où $n \neq 1$ est un entier relatif sans facteur carré.

Exercice 6. (*Constructions à la règle et au compas*) Soit k un sous-corps de $\mathbf{R}$.

(i) Montrer qu'une droite $D \subset \mathbf{R}^2$ contenant deux points de k^2 admet une équation de la forme $ax + by + c = 0$ avec a, b, c dans k. On dit que D est définie sur k.

Montrer qu'un cercle C de $\mathbf{R}^2$ dont le centre est dans k^2 et qui contient un point de k^2 admet une équation de la forme $x^2 + y^2 + ax + by + c = 0$ avec a, b, c dans k. On dit que C est défini sur k.

(ii) Supposons qu'un point $(x, y) \in \mathbf{R}^2$ est dans l'intersection d'un cercle et d'une droite, ou bien de deux cercles distincts, définis sur k. Montrer que $[k[x] : k] \leq 2$ et $[k[y] : k] \leq 2$.

(iii) Soit (x, y) un point du plan $\mathbf{R}^2$. On dira que ce point est *constructible* (à la règle et au compas) si l'on peut trouver une tour finie de sous-corps de $\mathbf{R}$

$$\mathbf{Q} = k_0 \subset k_1 \subset \cdots \subset k_n \subset \mathbf{R}$$

avec $[k_i : k_{i-1}] = 2$ pour $i = 1, \ldots, n$ et $(x, y) \in k_n^2$. Montrer que cette définition coïncide avec la définition du cours (2.1.1).

(iv) Montrer que l'ensemble des coordonnées des points constructibles est un sous corps de $\mathbf{R}$, algébrique sur $\mathbf{Q}$. Montrer que les degrés sur $\mathbf{Q}$ des éléments de ce corps sont des puissances de 2.

(v) (*Condition nécessaire de constructibilité du polygone régulier à un nombre premier p de côtés*) Montrer que si le point $(\cos \frac{2\pi}{p}, \sin \frac{2\pi}{p})$ est constructible alors p est "de Fermat", *i.e.* $p - 1$ est une puissance de 2 (on admettra pour cette question le résultat du (iii) de l'exercice suivant).

On rappelle le *critère d'Eisenstein* : *Soit $P = a_0 + a_1X + \cdots + a_nX^n \in \mathbf{Z}[X]$ un polynôme non constant. Supposons qu'il existe un nombre premier p tel que p divise $a_0, a_1, \cdots, a_{n-1}$, p ne divise pas a_n, et p^2 ne divise pas a_0. Alors P est irréductible dans $\mathbf{Q}[X]$.* (On le démontrera plus tard.)

Exercice 7. (i) Montrer que pour tout entier $n \geq 1$, $X^n - 19$ est irréductible dans $\mathbf{Q}[X]$. (En particulier, il existe des nombres algébriques sur $\mathbf{Q}$ de tout degré.)

(ii) (*Polynômes cyclotomiques pour p premier*) Soit p un nombre premier. Montrer que $\Phi_p(X) = X^{p-1} + \cdots + X + 1$ est irréductible dans $\mathbf{Q}[X]$. (On appliquera le critère d'Eisenstein au polynôme $\Phi_p(X + 1)$).

(iii) En déduire $[\mathbf{Q}[e^{2i\pi/p}] : \mathbf{Q}]$ et montrer que $[\mathbf{Q}[\cos(2\pi/p)] : \mathbf{Q}] = \frac{p-1}{2}$ si $p > 2$.

Exercice 8. (i) Soit $k \subset K$ une extension de corps de degré premier, montrer que les seuls corps intermédiaires entre k et K sont k et K.

(ii) Soient $k \subset K$ une extension de corps et $x \in K$ algébrique sur k de degré impair. Montrer que $k[x^2] = k[x]$.

(iii) Soient $P \in \mathbf{Q}[X]$ de degré n et $x_1, \ldots, x_n$ ses racines dans $\mathbf{C}$. Montrer que $[\mathbf{Q}[x_1, x_2, \ldots, x_n] : \mathbf{Q}] \leq n!$.

Exercice 9. (Difficile) Montrer que pour tout entier $n > 1$, $\sqrt{2} + \sqrt{3} + \sqrt{4} + \cdots + \sqrt{n}$ n'est pas un entier.