École polytechnique 2012-2013
Théorie de Galois

Feuille d'exercices 4

On note p un nombre premier, $\mathbf{F}_p$ le corps fini $\mathbf{Z}/p\mathbf{Z}$ et Ω une clôture algébrique de $\mathbf{F}_p$. Enfin, on désignera par $\mathrm{Frob}_p : \Omega \to \Omega$ l'élévation à la puissance p (morphisme de Frobenius).

Exercice 1. Montrer que tout sous-groupe fini G du groupe multiplicatif $K^\times$ des inversibles d'un corps K est *cyclique*. (Indication : utilisant la commutativité de G, on pourra montrer que si n est son *exposant* — c'est-à-dire le *ppcm* des ordres de ses éléments —, il existe un élément d'ordre n.)

Exercice 2.

(**i**). Rappeler pourquoi $\mathbf{F}_p = \{x \in \Omega, x^p = x\}$.

(**ii**). (p impair) Montrer qu'il existe $\zeta \in \Omega$ tel que $\zeta^2 = -1$. En déduire que -1 est un carré dans $\mathbf{F}_p$ si et seulement si $p \equiv 1 \bmod 4$.

(**iii**). (p impair) Montrer qu'il existe $\zeta \in \Omega$ tel que $\zeta^4 = -1$. En considérant l'élément $\zeta + \zeta^{-1}$, montrer que 2 est un carré dans $\mathbf{F}_p$ si et seulement si $p \equiv \pm 1 \bmod 8$.

Exercice 3.

(**i**). Montrer que pour tout entier $d \geq 1$, il existe un polynôme irréductible de degré d dans $\mathbf{F}_p[X]$.

(**ii**). Supposons $p \geq 3$. Montrer plus précisément que la proportion des polynômes unitaires de degré d dans $\mathbf{F}_p[X]$ qui sont irréductibles est au moins égale à $\frac{1}{2d}$.

Exercice 4. Soit $\mathbf{F}$ un corps fini de cardinal q.

(**i**). Montrer que si $r < q - 1$, $\sum_{x \in \mathbf{F}} x^r = 0$. (On fait la convention que $0^0 = 1$.)

(**ii**). En déduire que si $P \in \mathbf{F}[X_1, \ldots, X_n]$ est un polynôme de degré $d < n$, le nombre d'éléments $(x_1, \ldots, x_n) \in \mathbf{F}^n$ tels que $P(x_1, \ldots, x_n) = 0$ est divisible par p. (Indication : on pourra considérer le polynôme P^{q-1}.)

(**iii**). On suppose de plus que P est homogène. Montrer l'équation $P(x_1, \ldots, x_n) = 0$ admet un zéro non trivial.

Exercice 5. Soit $x \in \Omega^\times$ et soit $d_x = [\mathbf{F}_p(x) : \mathbf{F}_p]$ son degré sur $\mathbf{F}_p$. (On rappelle que c'est aussi le degré de son polynôme minimal $\Pi_{\mathbf{F}_p, x}$ sur $\mathbf{F}_p$.)

(**i**). Montrer d_x est le plus petit entier $d \geq 1$ tel que $\mathrm{Frob}_p^d(x) = x$.

(**ii**). Montrer que l'ordre N de x dans $\Omega^\times$ est premier à p.

(**iii**). Montrer que d_x est l'ordre de p dans $(\mathbf{Z}/N\mathbf{Z})^\times$.

(**iv**). Montrer que les $\mathbf{F}_p$-conjugués de x dans Ω sont exactement les $\mathrm{Frob}_p^n(x)$ avec $0 \leq n < d_x$.

Exercice 6. (Polynôme d'Artin-Schreier) Montrer que si p est premier et $a \in \mathbf{F}_p^\times$, alors $X^p - X + a$ est irréductible dans $\mathbf{F}_p[X]$. (On pourra utiliser l'exercice précédent.)

Exercice 7.

(**i**). Montrer que $\Phi_p(X) = X^{p-1} + \cdots + X + 1$ est irréductible dans $\mathbf{Q}[X]$. (Indication : on pourra appliquer le critère d'Eisenstein au polynôme $\Phi_p(X + 1)$.)

(**ii**). La suite de cet exercice est consacrée à l'étude de la réduction de Φ_p modulo un nombre premier $\ell \neq p$.

(**iii**). Montrer que la réduction modulo ℓ de Φ_p est de la forme $P_1 \dots P_g$ où tous les P_i sont des irréductibles unitaires distincts de même degré, égal à l'ordre de ℓ dans $\mathbf{F}_p^\times$. (On pourra utiliser l'exercice 5.)

(**iv**). En déduire que Φ_p est irréductible sur $\mathbf{F}_\ell$ si et seulement si ℓ engendre $\mathbf{F}_p^\times$.

(**v**). Montrer que Φ_p admet une racine dans $\mathbf{F}_\ell$ si et seulement si $\ell \equiv 1 \bmod p$.

(**vi**). Déduire du (iv) qu'il existe une infinité de nombres premiers ℓ tels que $\ell \equiv 1 \bmod p$. (Indication : on pourra s'inspirer de la preuve d'Euclide de l'infinité des nombres premiers.)

Exercice 8. Soit $n \geq 0$ un entier. Montrer que le quotient

$$K_n = \mathbf{F}_2[X_i : 0 \leq i < n]/(X_i^2 + X_i + \prod_{j<i} X_j, 0 \leq i < n)$$

est une extension de $\mathbf{F}_2$ de degré 2^n.

(Indication : on pourra montrer par récurrence sur n que les monômes $\prod_{i \in I} x_i$, où I parcourt les sous-ensembles de $\{0, \dots, n-1\}$, forment une base sur $\mathbf{F}_2$ de K_n.)

Exercice 9. Soit $f \in \mathbf{F}_p[X]$ un polynôme non nul. Montrer que le nombre de facteurs irréductibles de f est la dimension du noyau de $\mathrm{Frob}_p - \mathrm{Id} : A \to A$, où $A = \mathbf{F}_p[X]/(f)$. (On pourra d'abord considérer le cas où f est sans facteur carré.)

Exercice 10. Soit $P \in \mathbf{F}_p[X]$ un polynôme de degré d.

(**i**). Montrer que P est irréductible dans $\mathbf{F}_p[X]$ si et seulement si P n'a pas de racine dans $\mathbf{F}_{p^r}$ pour tout $r \leq \frac{d}{2}$.

(**ii**). (Application) Montrer que $\mathbf{F}_4 = \{0, 1, j, j^2\}$ avec $j^2 = 1 + j$. En déduire que les polynômes $1+X^2+X^5$, $1+X^3+X^5$, $1+X+X^2+X^3+X^5$, $1+X+X^2+X^4+X^5$, $1+X+X^3+X^4+X^5$ et $1 + X^2 + X^3 + X^4 + X^5$ sont les polynômes irréductibles de degré 5 de $\mathbf{F}_2[X]$.

(**iii**). (Une variante) Supposons $d \leq 5$. Montrer que P est irréductible dans $\mathbf{F}_p[X]$ si et seulement si $(P, X^{p^2} - X) = 1$.

Exercice 11.

(**i**). Vérifier les factorisations dans $\mathbf{C}[X]$

$$X^4+1 = (X^2+i)(X^2-i) = (X^2-\sqrt{2}X+1)(X^2+\sqrt{2}X+1) = (X^2+i\sqrt{2}X-1)(X^2-i\sqrt{2}-1).$$

(**ii**). En déduire que $X^4 + 1$ est irréductible dans $\mathbf{Q}[X]$.

(**iii**). On suppose p impair. Montrer que l'ensemble des carrés de $\mathbf{F}_p^\times$ est un sous-groupe d'indice 2. En déduire que si $a, b \in \mathbf{F}_p$, alors a, b ou ab est un carré dans $\mathbf{F}_p$.

(**iv**). Montrer que $X^4 + 1$ est réductible dans $\mathbf{F}_p[X]$ pour tout nombre premier p.