École polytechnique 2011-2012
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. 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 4. Montrer que pour tout entier $d \geq 1$, il existe un polynôme irréductible de degré d dans $\mathbf{F}_p[X]$. (Indication : on pourra utiliser l'exercice 1.)

Exercice 5. On note $\mathscr{P}$ l'ensembles des polynômes irréductibles unitaires de $\mathbf{F}_p[X]$ et $\mathscr{P}_d$ ceux de degré d.

(i) Soit $q = p^n$ une puissance de p. Montrer que

$$X^q - X = \prod_{\substack{d|n \\ P \in \mathscr{P}_d}} P.$$

En particulier, $p^n = \sum_{d|n} d|\mathscr{P}_d|$ ($\star$). D'après la *formule d'inversion de Möbius*, on a donc

$$n|\mathscr{P}_n| = \sum_{d|n} \mu(\frac{n}{d}) p^d,$$

où μ est est la fonction de Möbius, valant 1 (resp. -1) en les entiers produit d'un nombre pair (resp. impair) de nombres premiers distincts et 0 sinon.

(iii) En déduire une seconde démonstration du résultat de l'exercice précédent.

(iv) Soit $A = \mathbf{F}_p[X]$. Montrer que la « fonction zêta » de A

$$\zeta_A(s) := \sum_{\substack{f \in A \\ \text{unitaire}}} \frac{1}{|f|^s},$$

où $|f| = p^{\deg(f)}$, est égale au produit eulérien $\prod_{P \in \mathscr{P}} \frac{1}{1-|P|^{-s}}$. (Dans cet exercice, on pourra ignorer les problèmes de convergence en s.[1])

(v) Montrer que $\zeta_A(s) = \frac{1}{1-p\cdot p^{-s}}$. En déduire une seconde démonstration de la formule de ($\star$). (Indication : on pourra poser $T = p^{-s}$ et considérer la dérivée logarithmique de $\frac{1}{1-pT}$ par rapport à T.)

Exercice 6. (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.

Exercice 7. 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 $\mathrm{Frob}^d(x) = x$.

(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 $\mathrm{Frob}^n(x)$ avec $0 \leq n < d_x$.

Exercice 8. (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 9. (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 $\Phi_p(X+1)$.)

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

(ii) 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 7.)

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

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

(v) 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.)

1. C'est un fait général que ces fonctions zêta sont analytiques pour $\Re(s) \gg 0$.