Corps finis, théorie de Galois II (TD8)

FIMFA Algèbre 2 (Tony Ly), Avril 2014

Exercice 1 (Théorème de Chevalley-Warning)

Soient p un nombre premier, q une puissance de p et $n \geq d \geq 1$ des entiers. Soit $f \in \mathbb{F}_q[X_0, \ldots, X_n]$ un polynôme homogène de degré d.

a) Calculer $\sum f(x_0, \ldots, x_n)^{q-1}$ pour $(x_0, \ldots, x_n)$ parcourant $\mathbb{F}_q^{n+1}$.

b) En déduire que f possède un zéro autre que $(0, \ldots, 0)$.

Exercice 2 (Réciprocité quadratique)

Soit $p > 2$ un nombre premier et $\overline{\mathbb{F}}_p$ une clôture algébrique fixée de $\mathbb{F}_p$. Pour $x \in \mathbb{F}_p^\times$, on note $\left(\frac{x}{p}\right) = x^{\frac{p-1}{2}} \in \{\pm 1\}$ le symbole de Legendre.

a) Montrer que, pour tout $x \in \mathbb{F}_p^\times$, $\left(\frac{x}{p}\right)$ est égal à 1 si et seulement si x est un carré dans $\mathbb{F}_p$.

b) En considérant $\alpha + \alpha^{-1}$ avec $\alpha \in \overline{\mathbb{F}}_p$ une racine primitive 8-ème de l'unité, montrer l'égalité $\left(\frac{2}{p}\right) = (-1)^{\frac{(p-1)(p+1)}{8}}$.

Soit $\ell > 2$ un nombre premier distinct de p. Soit $\xi \in \overline{\mathbb{F}}_p$ une racine ℓ-ème primitive de l'unité. On note $S = \sum_{x \in \mathbb{F}_\ell^\times} \left(\frac{x}{\ell}\right) \xi^x$ la somme de Gauss correspondante.

c) Calculer, pour $y \in \mathbb{F}_\ell$, la quantité $\sum_{t \in \mathbb{F}_\ell^\times} \left(\frac{1 - yt^{-1}}{\ell}\right)$.

d) Montrer l'égalité $S^2 = (-1)^{\frac{\ell-1}{2}} \ell$.

e) En déduire la loi de réciprocité quadratique

$$\left(\frac{\ell}{p}\right)\left(\frac{p}{\ell}\right) = (-1)^{\frac{(p-1)(\ell-1)}{4}}.$$

Exercice 3 (Cyclotomie sur $\mathbb{F}_q$)

Soient p un nombre premier, q une puissance de p et $r \geq 1$ un entier.

a) Déterminer le groupe $\mu_{p^r}(\mathbb{F}_q)$ des racines p^r-èmes de l'unité dans $\mathbb{F}_q$.

b) Montrer que toute extension finie de $\mathbb{F}_q$ est cyclotomique, c'est-à-dire engendrée par des racines de l'unité.

Soient $n \geq 1$ un entier et $\Phi_n \in \mathbb{Z}[X]$ le n-ème polynôme cyclotomique sur $\mathbb{C}$. On note $\overline{\Phi}_n^{(p)}$ la réduction de Φ_n modulo p, que l'on peut voir comme un polynôme sur $\mathbb{F}_q$.

Supposons n premier à p.

c) Montrer que les racines de $\overline{\Phi}_n^{(p)}$ sont exactement les racines primitives n-èmes de l'unité dans $\mathbb{F}_q$.

d) Montrer que si $(\mathbb{Z}/n\mathbb{Z})^\times$ n'est pas cyclique, alors $\overline{\Phi}_n^{(p)}$ n'est pas irréductible sur $\mathbb{F}_p$.

e) En déduire que la réduction de Φ_8 modulo p est réductible pour tout p.

f) Montrer que $\overline{\Phi}_n^{(p)}$ est irréductible sur $\mathbb{F}_q$ si et seulement si q est un générateur de $(\mathbb{Z}/n\mathbb{Z})^\times$.

Exercice 4

Soient K un sous-corps de $\mathbb{R}$, $p > 2$ un nombre premier et $a \in K$ qui n'est pas une puissance p-ème dans K. Soit $x \in \mathbb{R}$ vérifiant $x^p = a$.

a) Montrer que $K \subseteq K(x)$ n'est pas galoisienne.

Une extension $K \subseteq L$ est dite *radicale réelle* s'il existe une tour d'extensions

$$K = K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_n \subseteq \mathbb{R}$$

telle que $L \subseteq K_n$ et, pour tout i, $K_{i+1} = K_i(x_i)$ avec $x_i^{n_i} \in K_i$ pour un certain entier $n_i \geq 1$. Un polynôme est dit *résoluble par radicaux réels* si son corps de décomposition l'est.

Soit $K \subseteq L$ une extension galoisienne radicale réelle.

b) En se ramenant à une tour avec degrés successifs premiers, montrer que $[L : K]$ est une puissance de 2.

c) Donner un exemple de telle extension.

d) Montrer que l'extension $\mathbb{Q} \subseteq \mathbb{Q}\big(\cos(\frac{2\pi}{7})\big)$ est radicale mais pas radicale réelle.

Soit $P \in K[X]$ un polynôme irréductible de degré 3.

e) Montrer que si P a trois racines réelles x, y, z, alors aucune des extensions $K(x)/K$, $K(y)/K$ et $K(z)/K$ n'est radicale réelle (résultat dû à Hölder).

On rappelle les formules de Tartaglia-Cardan : les zéros du polynôme $X^3 + bX + c$ sont les

$$\xi \sqrt[3]{-\frac{c}{2} + \sqrt{\frac{c^2}{4} + \frac{b^3}{27}}} + \xi^2 \sqrt[3]{-\frac{c}{2} - \sqrt{\frac{c^2}{4} + \frac{b^3}{27}}}$$

pour ξ parcourant les racines 3-èmes de l'unité.

f) Montrer que si P n'a qu'une racine réelle x, alors $K(x)/K$ est radicale réelle.

Exercice 5

Soient $n \geq 2$ un entier et $P \in \mathbb{Z}[X]$ un polynôme unitaire irréductible de degré n. Soient p un nombre premier, $\overline{\mathbb{F}}_p$ une clôture algébrique de $\mathbb{F}_p$ et $\overline{P}$ la réduction modulo p de P. Soient K un corps de décomposition de P et $x_1, \ldots, x_n$ les racines de P dans K. On note $A = \mathbb{Z}[x_1, \ldots, x_n]$ le sous-anneau de K engendré par les racines.

a) Montrer que $\mathbb{Z}[x_1]$ est un $\mathbb{Z}$-module libre de rang fini.

b) En déduire qu'il existe un corps fini $k \subseteq \overline{\mathbb{F}}_p$ et un morphisme surjectif d'anneaux $\varphi : A \to k$.

c) Montrer que tout automorphisme de corps de K stabilise A.

Soit $\mathfrak{P} = \operatorname{Ker} \varphi$: c'est un idéal maximal de A contenant pA. Soit $D_{\mathfrak{P}}$ le sous-groupe de $G := \operatorname{Gal}(K/\mathbb{Q})$ fixant $\mathfrak{P}$, que l'on appelle le *groupe de décomposition* en $\mathfrak{P}$.

d) Montrer que $g^{-1}(\mathfrak{P})$ est un idéal maximal de A pour tout $g \in G$, et que l'on a l'isomorphisme d'anneaux

$$A \Big/ \Big(\bigcap_{g \in D_{\mathfrak{P}} \backslash G} g^{-1}(\mathfrak{P}) \Big) \xrightarrow{\sim} \prod_{g \in D_{\mathfrak{P}} \backslash G} A/g^{-1}(\mathfrak{P}).$$

e) Montrer que l'application naturelle $D_{\mathfrak{P}} \to \operatorname{Gal}(k/\mathbb{F}_p)$ est surjective.

Supposons que $\overline{P}$ possède n racines simples dans $\overline{\mathbb{F}}_p$.

f) Montrer que φ induit une bijection entre les racines de P et les racines de $\overline{P}$.

g) En déduire que l'application $D_{\mathfrak{P}} \to \operatorname{Gal}(k/\mathbb{F}_p)$ est un isomorphisme compatible aux plongements dans le groupe symétrique.

Supposons $n = [K : \mathbb{Q}]$ et $\overline{P}$ irréductible sur $\mathbb{F}_p$.

h) Montrer que l'idéal pA est un idéal maximal de A, et que l'on peut renuméroter les racines de P de sorte que, pour tout $1 \leq i \leq n$, il existe $y_i \in A$ vérifiant $x_i = x_1^{p^{i-1}} + py_i$.