Feuille de TD 4

Nombres p-adiques

Exercice 1. Soit p un nombre premier impair.

(1) En utilisant le lemme de Hensel, montrer qu'un élément $v \in \mathbb{Q}_p^\times$, qu'on écrit sous la forme $v = p^r u$ avec $r \in \mathbb{Z}$ et $u \in \mathbb{Z}_p^\times$, est un carré si et seulement si r est pair et u est un carré modulo p.

(2) En déduire un isomorphisme $\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2} \simeq (\mathbb{Z}/2\mathbb{Z})^2$.

(3) Montrer que $\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2} \simeq (\mathbb{Z}/2\mathbb{Z})^3$.

(4) Quelles sont les extensions quadratiques de $\mathbb{Q}_p$?

Exercice 2. Soit p un nombre premier impair. Montrer que les racines de l'unité de $\mathbb{Q}_p$ sont les $p-1$ racines du polynômes $X^{p-1}-1$.

Corps finis

Exercice 3. (1) Montrer que X^2+X+1 est irréductible sur $\mathbb{F}_5$.

(2) Soit $P \in \mathbb{F}_5[X]$ un polynôme unitaire irréductible de degré 2. Montrer que l'anneau quotient $\mathbb{F}_5[X]/(P)$ est isomorphe au corps $\mathbb{F}_{25}$ et que P a deux racines dans $\mathbb{F}_{25}$.

(3) Soit α une racine de X^2+X+1 dans $\mathbb{F}_{25}$. Montrer que tout élément de $\mathbb{F}_{25}$ est de la forme $x\alpha + y$ avec $x, y \in \mathbb{F}_5$.

(4) Soit $P = X^5 - X + 1$. Montrer que P est irréductible sur $\mathbb{F}_5$. L'est-il encore sur $\mathbb{Q}$?

Exercice 4. On considère les polynômes $Q(X) = X^9 - X + 1$ et $P(X) = X^3 - X - 1$ à coefficients dans $\mathbb{F}_3$.

(1) Montrer que Q n'a pas de racines dans $\mathbb{F}_3$ et dans $\mathbb{F}_9$.

(2) Montrer que $\mathbb{F}_3[X]/(P)$ est isomorphe à $\mathbb{F}_{27}$.

(3) Montrer que toute racine $\alpha \in \mathbb{F}_{27}$ de P est racine de Q.

(4) Déterminer toutes les racines de Q dans $\mathbb{F}_{27}$.

(5) Factoriser le polynôme Q sur $\mathbb{F}_3$.

Exercice 5. (1) Donner tous les polynômes de degré au plus 4 sur $\mathbb{F}_2$.

(2) Quelle est la factorisation sur $\mathbb{F}_4$ d'un polynôme de $\mathbb{F}_2[X]$ irréductible de degré 4 ?

(3) En déduire le nombre de polynômes unitaires irréductibles de degré 2 sur $\mathbb{F}_4$, puis les expliciter.

Exercice 6. Soit $n \in \mathbb{N}$ un entier non nul.

(1) Soit $P \in \mathbb{F}_p[X]$ un polynôme de degré n et m un entier naturel. Donner une condition nécessaire et suffisante pour que P soit irréductible dans $\mathbb{F}_{p^m}$. Dans le cas où P est irréductible sur $\mathbb{F}_p$, préciser quels sont les degrés possibles des facteurs irréductibles de P sur $\mathbb{F}_{p^m}$.

(2) Déterminer l'entier naturel m minimal tel que tout polynôme de degré n à coefficients dans $\mathbb{F}_p$ soit totalement décomposé (respectivement possède une racine) sur $\mathbb{F}_{p^m}$.

Exercice 7. Montrer que $X^4 + 1$ est irréductible sur $\mathbb{Z}$ et réductible modulo tout nombre premier.

Exercice 8. On considère le polynôme $P = X^3 + 2X + 1$ et l'anneau $K = \mathbb{F}_3[X]/(P)$. Montrer que K est un corps de cardinal 27 et que X est un générateur du groupe multiplicatif $K^\times$. Trouver un entier k tel que $X^2 + X = X^k$.

Exercice 9 (Polynômes cyclotomiques). Soit p un nombre premier et $n \in \mathbb{N}^*$ un entier premier avec p. Notons d l'ordre de p dans $(\mathbb{Z}/n\mathbb{Z})^\times$.

(1) Montrer que $\Phi_{n,\mathbb{F}_p}$ est le produit de $\varphi(n)/d$ facteurs irréductibles de degré d.

(2) En déduire que ce polynôme est irréductible si et seulement si p engendre $(\mathbb{Z}/n\mathbb{Z})^\times$.

(3) Supposons $(\mathbb{Z}/n\mathbb{Z})^\times$ cyclique. Montrer qu'il existe une infinité de nombres premiers ℓ tels que $\Phi_{n,\mathbb{F}_\ell}$ est irréductible.
Indication. *Utiliser le* théorème de la progression arithmétique de Dirichlet *: pour tout entier n non nul et tout entier a premier avec n, il existe une infinité de nombres premiers congrus à a modulo n.*

Exercice 10 (Critère d'Eisenstein). Soit $P(X) = a_n X^n + \cdots + a_0$ un polynôme à coefficients dans $\mathbb{Z}$ et soit p un nombre premier tel que

(1) p ne divise pas a_n,

(2) pour chaque $i \in \{0, \ldots, n-1\}$, p divise a_i,

(3) p^2 ne divise pas a_0.

Montrer qu'alors P est irréductible dans $\mathbb{Q}$.
Application. Pour q premier, montrer que Φ_q est irréductible sur $\mathbb{Q}$.