TD n°7 : Corps finis, symboles de Legendre

Exercice 1. Pour $q = 3, 11, 17$, établir pour n'importe quel nombre premier p quand est-ce que q est un carré modulo p.

Exercice 2. En utilisant la loi de réciprocité quadratique, calculer $\left(\frac{13}{37}\right)$, $\left(\frac{45}{109}\right)$ et $\left(\frac{11}{199}\right)$.

Exercice 3. Le but de cet exercice est de montrer que le polynôme $X^4 + 1$ est irréductible dans $\mathbb{Z}[X]$ mais que pour tout nombre premier p, son image dans $\mathbb{Z}/p\mathbb{Z}[X]$ n'est pas irréductible.

1. Montrer que $X^4 + 1$ est irréductible dans $\mathbb{Z}[X]$.
2. Montrer que dans un corps fini k, l'ensemble des éléments de $k^\times$ qui sont des carrés est un sous-groupe de $k^\times$ d'indice 2.
3. Montrer qu'au moins un élément parmi -1, 2 et -2 est un carré modulo p, et en déduire que $X^4 + 1$ n'est pas irréductible dans $\mathbb{Z}/p\mathbb{Z}[X]$.

Exercice 4. [Polynômes irréductibles sur $\mathbb{F}_p$]

1. Montrer que $X^q - X$ est scindé à racines simples dans $\mathbb{F}_q$.
2. Soit P un facteur irréductible de $X^q - X$. Montrer que le degré de P divise n.
3. Réciproquement, soit P un polynôme unitaire irréductible dans $\mathbb{F}_p[X]$ dont le degré divise n. Montrer que P est un facteur simple de $X^q - X$.
4. Pour tout $d \in \mathbf{N}$ on note $\mathcal{I}(p, d)$ l'ensemble des polynômes unitaires irréductibles dans $\mathbf{F}_p[X]$ de degré d. Montrer que dans $\mathbf{F}_p[X]$ on a
$$X^q - X = \prod_{d|n} \prod_{P \in \mathcal{I}(p,d)} P$$
5. On note $I(p, d)$ le cardinal de $\mathcal{I}(p, d)$. Montrer que $p^n = \sum_{d|n} dI(p, d)$. En déduire que l'ensemble $\mathcal{I}(p, d)$ est non vide.
6. Montrer que $\frac{p^n - p^{\lfloor n/2 \rfloor + 1}}{n} \leq I(n, p) \leq \frac{p^n}{n}$ En déduire qu'un polynôme unitaire de degré n "assez grand" choisi au hasard a au moins une chance sur n d'être irréductible.

Exercice 5. [Polynômes irréductibles sur un corps fini] Soit $k = \mathbb{F}_q$ un corps fini de cardinal q, et soit $P \in k[X]$ un polynôme de degré $d \geq 1$. Montrer que P est irréductible si, et seulement si, $P | X^{q^d} - X$ et que pour tout nombre premier ℓ divisant d, les polynômes $X^{q^{\frac{d}{\ell}}} - X$ sont premiers entre eux.

Exercice 6. Soit p un nombre premier et soit $q = p^n$. Montrer que $GL_m(\mathbb{F}_q)$ contient un élément d'ordre $p^{nm} - 1$.

Exercice 7. [Corps à huit, neuf et seize éléments]

On se propose dans cet exercice de construire tous les corps à 8, 9 et 16 éléments qui peuvent être obtenus comme corps de rupture de polynômes irréductibles sur $\mathbb{F}_2$ et $\mathbb{F}_3$.

1. Donner tous les polynômes irréductibles de degré inférieur à 4 sur $\mathbb{F}_2$ et inférieurs à 3 sur $\mathbb{F}_3$.
2. Utiliser un polynôme irréductible de degré 3 pour construire une extension $\mathbb{F}_8/\mathbb{F}_2$ de degré 3, et en donner la table de multiplication.
3. Montrer que les extensions obtenues pour les différents polynômes irréductibles choisis sont isomorphes, en exhibant un isomorphisme explicite.
4. Montrer que $\mathbb{F}_8^\times$ est cyclique en en exhibant un générateur.
5. Dans chacun des corps $\mathbb{F}_8$ précédemment obtenus, dire si l'élément primitif canonique est un générateur du groupe multiplicatif $K^\star$.
6. Choisir un corps $\mathbb{F}_8$ parmi les précédents, et donner le polynôme minimal de tous ses éléments sur $\mathbb{F}_2$.
7. Adapter et reprendre ces cinq dernières questions pour une extension $\mathbb{F}_9/\mathbb{F}_3$ de degré 2, et une extension $\mathbb{F}_{16}/\mathbb{F}_2$ de degré 4.