Corps finis

Exercice 1. Dans `sage`, les corps finis se définissent à l'aide de la commande `GF`.

1. Calculer les carrés des éléments de $\mathbb{F}_4$.
2. Calculer les ordres (pour la multiplication) des éléments non nuls de $\mathbb{F}_9$.
3. La méthode `polynomial` permet d'obtenir le polynôme unitaire et irréductible choisi automatiquement par `sage` pour définir un corps composé. Déterminer le polynôme choisi par `sage` pour définir $\mathbb{F}_4$. Vérifier que ce polynôme est irréductible dans $\mathbb{F}_2[x]$.
4. Déterminer la liste des polynômes irréductibles de degré 2 de $\mathbb{F}_2[x]$ et la liste des polynômes irréductibles de degré 3 de $\mathbb{F}_2[x]$. *On pourra utiliser la méthode* `polynomials` *des objets anneaux de polynômes.*
5. L'option `modulus` de `GF` permet d'imposer un choix de polynôme unitaire irréductible dans la définition d'un corps composé. Définir $\mathbb{F}_8$ en utilisant deux polynômes irréductibles différents.
6. Déterminer les élements a de $\mathbb{F}_8$ vérifiant $a^{2^2} = a$.

Exercice 2 (Algorithme de Cipolla)**.** Le but de cet exercice est l'étude et l'implantation de l'algorithme de Cipolla d'extraction de racines carrées modulo p. Soit p un nombre premier *impair* et a un élément de $\mathbb{F}_p$ *qui est un carré non nul.*

1. Soit $t \in \mathbb{F}_p$. À quelle condition sur t et a le polynôme $P = X^2 - tX + a$ est-il irréductible sur $\mathbb{F}_p$?
2. Écrire une fonction `trouve_t(a,p)` qui à l'entrée (a, p) associe t tel que P est irréductible. Pour tester si un élément est un carré dans $\mathbb{F}_p$, on pourra utiliser la commande `is_square` ou la commande `kronecker(a,p)` qui calcule le symbole de Legendre $(\frac{a}{p})$. Pour choisir un élément aléatoire, on pourra utiliser `random_element()`. Écrire une nouvelle version de la fonction précédente qui renvoie également le nombre de tirages nécessaires pour trouver t.
3. Implémenter une fonction `cipolla(a,p)` renvoyant une racine de a modulo p si a est un carré modulo p ou un message d'erreur sinon.
4. Que dire du cas $p = 2$.
5. Montrer que, en moyenne sur les carrés non nuls a de $\mathbb{F}_p$, la probabilité qu'un élément $t \in \mathbb{F}_p$ choisi uniformément au hasard donne lieu à un polynôme P irréductible est $(1/2) \times (1 - (1/p))$.

Exercice 3.

1. Justifier que $P = U^2 - 2 \in \mathbb{F}_5[U]$ est irréductible en utilisant `sage` et sans utiliser `sage`. On note $K = \mathbb{F}_5[U]/(P)$.
2. Justifier de même que $Q = V^3 + V + 1 \in \mathbb{F}_5[V]$ est irréductible. On note $L = \mathbb{F}_5[V]/(Q)$.
3. Montrer que $R = W^3 + W + 1$ est irréductible sur $K[W]$ en utilisant `sage` et sans utiliser `sage`. On note M le corps $K[W]/(R)$.
4. Expliquer pourquoi M est une extension de K et de L.
5. Déterminer le degré de M sur $\mathbb{F}_5$ sans utiliser `sage`. Déterminer les sous-corps de M.
6. On note u et w les classes de U et W dans M. Sans utiliser `sage`, montrer que $x = u + w$ engendre M sur $\mathbb{F}_5$.

7. À l'aide de `sage`, déterminer un polynôme minimal de x sur $\mathbb{F}_5$. En déduire (à nouveau) que $M = \mathbb{F}_5(x)$.
8. Déterminer la matrice dont la i-ème colonne ($0 \leqslant i \leqslant 5$) donne les coordonnées de x^i dans la base $(1, w, w^2, u, uw, uw^2)$.
9. En déduire une expression de u et w comme polynômes en x de degré inférieur à 5.
10. Sans utiliser `sage`, justifier que $x + x^{5^2} + x^{5^4} \in K$ et que $x + x^{125} \in L$.

Exercice 4.

1. Soit p un nombre premier et $f \in \mathbb{F}_p[x]$, non constant, de degré k. Montrer que les assertions suivantes sont équivalentes
   (a) f est irréductible
   (b) $\text{pgcd}(f, x^{p^j} - x) = 1$ pour $j = 1, 2, \ldots, \lfloor k/2 \rfloor$
   (c) $x^{p^k} \equiv x[f]$ et $\text{pgcd}(f, x^{p^{k/q}} - x) = 1$ pour tout premier q divisant k.
2. Déduire de la question précédente (au moins) un test d'irreductibilité sur $\mathbb{F}_p$. L'implanter avec `sage`.
3. Implanter avec `sage` un algorithme probabiliste prenant en entrée un nombre premier p et un entier n et renvoyant un polynôme irréductible unitaire de degré n. Modifier votre algorithme pour renvoyer également le nombre d'essai effectués.