Corps finis I

Exercice 1. Définition des corps finis avec sage. Dans `sage`, les corps finis se définissent à l'aide de la commande `GF`. Par exemple `GF(5)` définit le corps à 5 éléments. Dans le cas d'un corps fini de cardinal p^k avec p premier et $k > 1$, $\mathbb{F}_{p^k}$ est isomorphe à un quotient $\mathbb{F}_p[X]/(P)$ où $P \in \mathbb{F}_p[X]$ est unitaire et irréductible de degré k ; et on peut dans ce cas indiquer à `sage` un nom pour le générateur naturel de l'extension corps, c'est à dire la classe d'équivalence du polynôme X. Par exemple, `F4.<u> = GF(4)` permet de définir simultanément `F4` comme un corps à 4 éléments et `u` comme variable correspondant au générateur.

1. Faire afficher les éléments de $\mathbb{F}_{16}$.
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.

Exercice 2. Symbole de Legendre. L'objectif de cet exercice est d'illustrer à l'aide de `sage` les propriétés du symbole de Legendre.

1. En utilisant `random_prime`, choisir un nombre premier p au hasard entre 3 et 100.
2. Faire la liste des carrés non nuls de $\mathbb{Z}/p\mathbb{Z}$ de sorte que chaque carré n'apparaisse qu'une seule fois dans la liste.
3. De même, faire la liste des éléments de $\mathbb{Z}/p\mathbb{Z}$ qui ne sont pas des carrés.
4. Vérifier la valeur prise par le symbole de Legendre sur les éléments de chacune des listes obtenues en 2. et 3.
5. (a) Montrer que le produit de deux éléments de $\mathbb{Z}/p\mathbb{Z}$ qui ne sont pas des carrés est un carré.
   (b) Examiner les autres possibilités.
   (c) Illustrer (a) et (b) à l'aide de `sage`.
6. Pour quelles valeurs de p, -1 est-il un carré dans $\mathbb{Z}/p\mathbb{Z}$? Vérifier cela avec `sage` pour tous les nombres premiers p entre 3 et 1000.

Exercice 3. Polynômes de degré 2 sur un corps fini.

1. Soit $P = X^2 + bX + c \in k[X]$ où k est un corps de caractéristique différente de 2. Montrer que P est irréductible sur k si et seulement si $b^2 - 4c$ n'est pas un carré de k.
2. Déduire de la question précédente et de l'exercice 2 la liste des nombres premiers p entre 3 et 1000 tels que $X^2 + X + 1$ soit irréductible dans $(\mathbb{Z}/p\mathbb{Z})[X]$.
3. Vérifier à l'aide de `sage` que tous les polynômes unitaires de degré 2 de $\mathbb{F}_{11}$ sont scindés sur $\mathbb{F}_{121}$.
4. On se place maintenant sur $\mathbb{F}_{p^2} = \mathbb{F}_p[X]/(P)$ où p est un nombre premier impair et $P = X^2 + bX + c$ est irréductible de degré 2.
   (a) Montrer que $t = b^2 - 4c$ est un carré de $\mathbb{F}_{p^2}$.
   (b) En déduire que tous les éléments de $\mathbb{F}_p$ sont des carrés dans $\mathbb{F}_{p^2}$ (indication : si x n'est pas un carré dans $\mathbb{F}_p$, que peut-on dire de x/t dans $\mathbb{F}_p$?).
   (c) Montrer que tout polynôme unitaire de $\mathbb{F}_p$ de degré 2 est scindé sur $\mathbb{F}_{p^2}$.
5. Donner une autre preuve de 4.(c), en utilisant l'unicité (à isomorphisme près) du corps à p^2 éléments.