TP : Corps finis sous SageMath

Exercice 1. Premières manipulations

1. Créer des corps finis de cardinaux $q = p^n$ non premiers pas trop gros. Comment les éléments de ces corps sont-ils représentés ?
   Trouver le polynôme utilisé pour définir l'extension. Quel est l'ordre de l'élément générateur choisi par SageMath ?
2. Créer un corps K à 81 éléments comme $\mathbb{F}_3[X]/(X^4 + X^2 + 2)$. Quel est l'ordre de la classe de X dans ce quotient ?
   Créer un autre corps L à 81 éléments et utiliser SageMath pour trouver les racines de X^4+X^2+2 dans `L`. Vérifier qu'elles se déduisent les unes des autres par l'automorphisme de Frobenius.
   Créer un isomorphisme explicite entre `K` et `L` et calculer l'image de (la classe de) $X^3 + X^2 + 1$.

Exercice 2. Créer un corps fini K, puis une extension L de ce corps fini. Générer un élément aléatoire de cette extension.
Écrire quelques lignes de code permettant de calculer le polynôme minimal sur K de cet élément et comparer le résultat avec la méthode native de SageMath.
Utiliser une autre méthode pour calculer ce polynôme minimal.

Exercice 3. Écrire un programme du type "crible d'Eratosthène" qui prend en argument deux entiers d et q (petits) et génère la liste de tous les polynômes unitaires irréductibles de $\mathbb{F}_q[X]$ de degré inférieur ou égal à d.

Exercice 4.

1. Écrire un programme testant si un polynôme $P \in \mathbb{F}_q[X]$ est scindé à racines simples. Vérifier expérimentalement que la probabilité qu'un polynôme aléatoire (i.e. tiré suivant une loi uniforme) de degré fixé d soit scindé à racines simples tend vers $1/d!$ quand q tend vers $+\infty$.
2. Idem en remplaçant "scindé à racines simples" par "scindé".

Exercice 5.

1. Exécuter les commandes suivantes :

```
K=GF(5^2); a=K.gen()
L=GF(5^3); b=L.gen()
M=GF(5^4); c=M.gen()
N=GF(5^6); d=N.gen()
O=GF(2^5); e=O.gen()
```

   Peut-on sommer/multiplier a et c ? a et b ? a et e ?

   (Remarque : tester aussi avec la syntaxe `K.<a> = GF(5^2); L.<b>=GF(5^3)` etc. Les résultats sont différents.)
2. SageMath a donc des plongements par défaut $\mathbb{F}_{p^d} \hookrightarrow \mathbb{F}_{p^n}$ quand $d \mid n$. Vérifier que ces plongements sont compatibles entre eux en calculant $(a + c) + d$, $(a + d) + c$ et $a + (d + c)$ par exemple.
3. Justifier que $d^{1+5^2+5^4}$ appartient à $\mathbb{F}_{5^4}$. Comment le faire voir à SageMath comme un élément de M ?
4. Vérifier (cf. exercice 1) que a, b, c et d sont bien des éléments primitifs dans leurs corps respectifs. En déduire les valeurs possibles du logarithme de a et de b en base d, puis déterminer ces logarithmes. Que constate-t-on ?