Corps finis II

Exercice 1. — Soit $P = X^4 + 1 \in \mathbf{F}_7[X]$.

a) P est-il sans facteur carré ?

b) En utilisant l'algorithme de Berlekamp, montrer que P n'est pas irréductible.

c) Factoriser P dans $\mathbf{F}_7[X]$.

Exercice 2. — Soit $P = X^4 + X^3 + X^2 + X + 1 \in \mathbf{F}_2[X]$ et $K = \mathbf{F}_2[X]/(P)$.

a) Montrer que K est un corps.

b) Pour chacun des éléments suivants, déterminer son polynôme minimal :

$$x_1 = \overline{X}, \qquad x_2 = \overline{X+1}, \qquad x_3 = \overline{X^3 + X^2}.$$

c) Déterminer l'ordre de chacun de ces éléments dans $K^\times$.

d) On a tapé les commandes Sage suivantes :

```
F.<x>=GF(16, modulus=x^4 + x^3 + x^2 + x + 1);
for y in F:
   if y<>0: print(y,y.minimal_polynomial(),y.multiplicative_order())
```

```
(x + 1, x^4 + x^3 + 1, 15)
(x^2 + 1, x^4 + x^3 + 1, 15)
(x^3 + x^2 + x + 1, x^4 + x^3 + x^2 + x + 1, 5)
(x^3 + x^2 + x, x^4 + x^3 + 1, 15)
(x^3 + x^2 + 1, x^2 + x + 1, 3)
(x^3, x^4 + x^3 + x^2 + x + 1, 5)
(x^2 + x + 1, x^4 + x + 1, 15)
(x^3 + 1, x^4 + x^3 + 1, 15)
(x^2, x^4 + x^3 + x^2 + x + 1, 5)
(x^3 + x^2, x^2 + x + 1, 3)
(x^3 + x + 1, x^4 + x + 1, 15)
(x, x^4 + x^3 + x^2 + x + 1, 5)
(x^2 + x, x^4 + x + 1, 15)
(x^3 + x, x^4 + x + 1, 15)
(1, x + 1, 1)
```

Quel est le sous-corps à 4 éléments de K ?
Combien de fois chaque polynôme minimal apparaît-il ? Etait-ce prévisible ?