Arithmétique - L3 - MI
Contrôle n^{0}3 - 2009
CORRIGE

Question

Soit $m = x^6 + x^5 + x^4 + x^2 + 1 \in \mathbb{F}_2[x]$.

1. Montrer que m n'a pas de racine dans $\mathbb{F}_2$.
   On vérifie sans problème que $m(0) = 1$ et $m(1) = 1$. En particulier, m n'a pas de racine dans $\mathbb{F}_2$.
2. Déterminer la dérivée $m'(X)$, et la décomposer en facteurs irréductibles dans $\mathbb{F}_2[X]$.
   La dérivée $m' = x^4$, ce qui est également sa décomposition en facteurs irréductibles.
3. Montrer que m n'a pas de facteur irréductible multiple.
   Comme le polynôme x ne divise pas m, les polynômes m et m' sont premiers entre eux. Cela implique que m n'a pas de facteur multiple.
4. Montrer que m est irréductible dans $\mathbb{F}_2[x]$.
   Si m était réductible, m serait divisible par un polynôme sans racine de degré 2 ou 3. Ces derniers sont

   $$g_1 = x^2 + x + 1$$
   $$g_2 = x^3 + x + 1$$
   $$g_3 = x^3 + x^2 + 1$$

   On calcule les restes dans la division euclidienne de m par g_1, g_2 et g_3 pour vérifier qu'aucun de ces polynômes ne divise m :

   ```
   x=GF(2)['x'].gen()
   m=x^6+x^5+x^4+x^2+1
   g1=x^2+x+1
   g2=x^3+x+1
   g3=x^3+x^2+1
   m%g1
   m%g2
   m%g3
   ```

   Comme les restes $m\%g1 = x$, $m\%g2 = 1$, $m\%g3 = x^2 + x + 1$ sont tous non nuls, m est irréductible.
5. Soit $K = \mathbb{F}_2[x]/m$, et notons $\alpha = x \bmod m$. Quel est le cardinal de K ?
   Comme $\deg(m) = 6$,

   $$K = \{a_0 + a_1 x + \cdots + a_5 x^5 \mid a_0, \ldots, a_5 \in \mathbb{F}_2\}.$$

   Il s'ensuit que K contient $2^6 = 64$ éléments.
6. L'élément α de $K^\star$ est-il générateur ?
   Déterminons l'ordre multiplicatif de α à l'aide de sage :

```
K=GF(2^6,name='alpha',modulus=m)
alpha=K.gen()
alpha.multiplicative_order()
```

Comme l'ordre de α est égal à $21 \neq 2^6 - 1 = 63$, l'élément α n'est pas générateur de $K^\star$.

7. Déterminer un sous-corps de K de cardinal 4.

   Si L est un sous-corps de K de cardinal 4, le groupe multiplicatif $L^\star$ est cyclique d'ordre 3. Or, α étant d'ordre 21, l'élément $\beta = \alpha^7$ de K est d'ordre 3.

   Montrons que $\mathbb{F}_2[\beta]$ est un sous-corps de cardinal 4.

   ```
   beta=alpha^7
   beta.minpoly().degree()
   ```

   Comme le polynôme minimal $x^2 + x + 1$ de β sur $\mathbb{F}_2$ est de degré 2,

   $$\mathbb{F}_2[\beta] = \{a + b\beta \mid a, b \in \mathbb{F}_2\}$$

   est bien un sous-corps de K de cardinal 4.

8. Déterminer un sous-corps de K de cardinal 8.

   De même, on prend $\gamma = \alpha^3$ qui est d'ordre $7 = 8 - 1$.

   ```
   gamma=alpha^3
   gamma.minpoly().degree()
   ```

   Comme le degré de γ est égal à 3, le sous-corps $\mathbb{F}_2[\gamma]$ contient $2^3 = 8$ éléments.