Arithmétique et applications - L3 - MI

UBO – 25 mai 2009

examen - durée : 3 heures

CORRIGE

Partie II

Exercice 1

Soit f le polynôme dans $\mathbb{Q}[x]$ défini par

$$f = x^5 - x^3 + 3x^2 - 2x + 1.$$

En utilisant l'algorithme de Schubert-Kronecker, décomposer f en facteurs irréductibles dans $\mathbb{Q}[x]$.

Si f est réductible, il admet un facteur de degré ≤ 2 qu'on peut supposer être à coefficients entiers d'après Gauss. En évaluant f en $-1, 0, 1$, on saura que les valeurs en $-1, 0, 1$ d'un tel facteur sont des diviseurs de $f(-1), f(0), f(1)$, respectivement. On pourra donc déterminer de tels facteurs en effectuant l'interpolation de Lagrange.

```
A=ZZ['x']
B=QQ['x']
x=A.gen()
f=x^5-x^3+3*x^2-2*x+1
vals=[f(-1),f(0),f(1)]
```

Dressons les listes des diviseurs des valeurs de f en $-1, 0, 1$, et déterminons d'éventuels polynômes g dans $\mathbb{Z}[x]$ non constants de degré ≤ 2 divisant f :

```
divdevals=[val.divisors()+map(lambda x:-x,val.divisors()) for val in
  vals]
for divs in cartesian_product_iterator(divdevals):
  g=B.lagrange_polynomial([(-1,divs[0]),(0,divs[1]),(1,divs[2])])
  if g.degree()>=1 and g.denominator()==1 and f%g==0: print g
```

On a trouvé un seul—à signe près—facteur non trivial de f de degré ≤ 2, à savoir $g = x^2 - x + 1$. Le polynôme g est donc forcément irréductible.

```
g=x^2-x+1
h=f//g
```

On a $h = x^3 + x^2 - x + 1$, et montrons qu'il est irréductible. Si h était réductible, h serait forcément divisible par g, car g est le seul facteur non trivial de f de degré ≤ 2. Or, le reste dans la division euclidienne de h par g est $-1 \neq 0$. Par conséquent, h est irréductible. La décomposition en facteurs irréductibles de f est donc

$$f = (x^2 - x + 1)(x^3 + x^2 - x + 1).$$

Exercice 2

Soit $m = x^7 + x + 1 \in \mathbb{F}_2[x]$.

1. Montrer que m est irréductible dans $\mathbb{F}_2[x]$.
   Si m était réductible, il serait divisible par un polynôme irréductible de degré ≤ 3. Comme m n'a pas de racine dans $\mathbb{F}_2$, le polynôme m n'est pas divisible par un polynôme de degré 1. Il reste à vérifier si m est divisible par un polynôme irréductible de degré 2 ou 3. Ces derniers sont

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

   Calculons les restes dans la division euclidienne de m par g_1, g_2, g_3 :

   ```
   A=GF(2)['x']
   x=A.gen()
   m=x^7+x+1
   g1=x^2+x+1
   g2=x^3+x+1
   g3=x^3+x^2+1
   ```

   Comme les restes $m\%g1 = 1$, $m\%g2 = x$, $m\%g3 = x$ sont tous non nuls, m est irréductible.
2. Soit $K = \mathbb{F}_2[x]/m$, et notons $\alpha = x \bmod m$. Quel est le cardinal de K ?
   Comme $\deg(m) = 7$, le nombre d'éléments de K est égal à $2^7 = 128$.
3. L'élément α de $K^\star$ est-il générateur ?

   ```
   K=GF(128,name='alpha',modulus=m)
   alpha=K.gen()
   alpha.multiplicative_order()
   ```

   L'ordre multiplicatif de α est egal à $127 = 128 - 1$. L'élément α est donc bien générateur de $K^\star$.
4. Déterminer les sous-corps de K.
   Comme l'extension K/F_2 est de degré 7, et donc premier, les seuls sous-corps de K sont les sous-corps triviaux $\mathbb{F}_2$ et K.
5. Déterminer les racines de m dans K.
   Par construction, α est racine de m dans K. Par Frobenius, α^2, α^4, α^8, α^{16}, α^{32}, α^{64} sont également racines de m dans K. Comme α est d'ordre 127, ces 7 racines sont toutes distinctes. Comme m est de degré 7, m ne possède pas d'autre racine dans K.
6. Décomposer m dans $K[x]$.
   D'après ce qui précède,

   $$m = (x + \alpha)(x + \alpha^2)(x + \alpha^4)(x + \alpha^8)(x + \alpha^{16})(x + \alpha^{32})(x + \alpha^{64}).$$

7. Quel est le polynôme minimal n de α^3 sur $\mathbb{F}_2$?
   En posant

   ```
   n=(alpha^3).minpoly()
   ```

   on trouve que le polynôme minimal de α^3 est égal à $x^7 + x^5 + x^3 + x + 1$.

8. Déterminer les racines de n dans K.
   Comme ci-dessus, les racines de n dans K sont
   $$\alpha^3, \alpha^6, \alpha^{12}, \alpha^{24}, \alpha^{48}, \alpha^{96}, \alpha^{192} = \alpha^{65}.$$

9. Décomposer n dans $K[x]$.

   $$n = (x+\alpha^3)(x+\alpha^6)(x+\alpha^{12})(x+\alpha^{24})(x+\alpha^{48})(x+\alpha^{96})(x+\alpha^{65}).$$

10. Quel est le nombre de polynômes irréductibles de degré 7 dans $\mathbb{F}_2[x]$?
    Tout élément β de $K \setminus \mathbb{F}_2$ est de degré 7 d'après le 4, et possède donc un polynôme minimal de degré 7 dans $\mathbb{F}_2[x]$. Un tel polynôme est forcément irréductible dans $\mathbb{F}_2[x]$. Les racines du polynome minimal ℓ de β sont β^{2^i}, pour $i = 0, \ldots, 6$. Le polynôme ℓ est aussi polynôme minimale de ces 7 éléments de K. On obtient ainsi $(128-2)/7 = 18$ polynomes irréductibles dans $\mathbb{F}_2[x]$. Il n'y en a pas d'autres. En effet, si $f \in \mathbb{F}_2[x]$ est irréductible de degré 7, il définit un corps L à 128 éléments. D'après le cours, L est isomorphe à K, et K contient, tout comme L, un élément dont la polynôme minimal sur $\mathbb{F}_2$ est égal à f. Par conséquent, $\mathbb{F}_2[x]$ contient exactement 18 polynômes irréductibles de degré 7.

Exercice 3

Déterminer le plus petit corps $\mathbb{F}_q$ de la forme $\mathbb{F}_2[\alpha]$ où α n'est pas générateur du groupe multiplicatif $\mathbb{F}_q^\star$.

On cherche tout d'abord des puissances $q = 2^n$ de 2 pour lequel $q-1$ n'est pas premier :

```
for n in range(10):
  if not (2^n-1).is_prime() : print 2^n
```

On obtient la liste $1, 2, 16, 64, 256, 512$. La valeur $q = 1$ ne correspond pas au cardinal d'un corps, bien-sûr. La valeur $q = 2$ correspond au corps $\mathbb{F}_2$, mais tout élément $\alpha \in \mathbb{F}_2^\star = \{1\}$ est évidemment générateur de $\mathbb{F}_2^\star$. La valeur suivante $q = 16$ correspond au corps $\mathbb{F}_{16}$. Son groupe multiplicatif est isomorphe à $\mathbb{Z}/15\mathbb{Z}$ et contient notamment un élément α d'ordre 5. Les sous-corps de $\mathbb{F}_{16}$ sont $\mathbb{F}_2$, $\mathbb{F}_4$ et $\mathbb{F}_{16}$. Les groupes multiplicatifs correspondants sont $\mathbb{F}_2^\star$, $\mathbb{F}_4^\star$ et $\mathbb{F}_{16}^\star$, de cardinal 1, 3 et 15, respectivement. Comme l'ordre de α est égal à 5, α ne peut être un élément de $\mathbb{F}_2^\star$ ou de $\mathbb{F}_4^\star$. Par conséquent, le plus petit sous corps $\mathbb{F}_2[\alpha]$ de $\mathbb{F}_{16}$ est $\mathbb{F}_{16}$ même. Pourtant, α nést pas générateur de $\mathbb{F}_{16}^\star$. Le plus petit corps $\mathbb{F}_q$ de la forme $\mathbb{F}_2[\alpha]$ où α n'est pas générateur du groupe multiplicatif $\mathbb{F}_q^\star$ est donc $\mathbb{F}_{16}$