Arithmétique et applications - L3 - MI

UBO – 25 juin 2009

examen - durée : 3 heures

CORRIGE

Partie II

Exercice III

Soit f le polynôme dans $\mathbb{Z}[x]$ défini par $f = x^4 - 2x^2 + 9$. Le but de cet exercice est de démontrer que le polynôme f est réductible modulo tout nombre premier p, mais irréductible dans $\mathbb{Q}[x]$.

1. Montrer que f n'admet pas de racine dans $\mathbb{Q}$.
   D'après le cours, si le nombre rationnel $\frac{a}{b}$, où $a \in \mathbb{Z}$, $b \in \mathbb{N}^\star$ et $\text{pgcd}(a, b) = 1$, est racine de f, alors b divise 1 et a divise 9. Les racines potentielles de f dans $\mathbb{Q}$ sont donc
   $$\pm 1, \pm 3, \pm 9.$$
   Or, en calculant avec sage :
   ```
   A=ZZ['x']
   x=A.gen()
   f=x^4-2*x^2+9
   map(f,[1,-1,3,-3,9,-9])
   ```
   on constate qu'aucun de ces nombres n'est racine de f. Il s'ensuit que f n'a pas de racine dans $\mathbb{Q}$.
2. Montrer que si g divise f dans $\mathbb{Q}[x]$, alors $g(-x)$ le divise également.
   Supposons que $g \in \mathbb{Q}[x]$ divise f. On peut donc écrire $f = gh$, où $h \in \mathbb{Q}[x]$. En substituant $-x$ pour x, on obtient
   $$g(-x)h(-x) = f(-x) = f(x).$$
   Cela montre que $g(-x)$ divise également f.
3. En déduire que f est irréductible dans $\mathbb{Q}[x]$.
   Supposons que f est réductible. Comme f n'a pas de racine dans $\mathbb{Q}$, et comme il est de degré 4, il s'écrit donc comme produit de deux polynômes g et h dans $\mathbb{Q}[x]$ de degré 2 et irréductibles. Comme f est à coefficients entiers, on peut supposer, d'après Gauss, que g et h en sont de même. De plus, comme f est unitaire, on peut supposer que g et h le sont également. D'après le 2, $g(-x)$ divise f aussi. D'après l'unicité de la décomposition en facteurs irréductibles, on a ou bien $g(-x) = g(x)$, ou bien $g(-x) = h(x)$.
   Si $g(-x) = h(x)$, écrivons $g = x^2 + ax + b$. Donc $h = x^2 - ax + b$ et
   $$f = gh = (x^2 + ax + b)(x^2 - ax + b) = x^4 + (2b - a^2)x^2 + b^2.$$
   Donc $2b - a^2 = -2$ et $b^2 = 9$. On obtient $b = \pm 3$ et $a^2 = 2b + 2$. Mais ni 8, ni -4 ne sont des carrés dans $\mathbb{Z}$.
   La seule possibilité est donc que $g(-x) = g(x)$, et de même $h(-x) = h(x)$. Dans ce cas $g = x^2 + a$ et $h = x^2 + b$, avec $a, b \in \mathbb{N}$. A nouveau, l'égalité $f = gh$ mène à une contradiction. Par conséquent, f est irréductible dans $\mathbb{Q}[x]$.

4. Montrer que f est réductible dans $\mathbb{F}_2[X]$.
   $\overline{f} = x^4 + 1 = (x^2 + 1)^2$ dans $\mathbb{F}_2[x]$.

5. Soit p un nombre premier impair tel qu'il existe $\delta \in \mathbb{F}_p$ avec $\delta^2 = -32$ dans $\mathbb{F}_p$. Montrer que le polynôme $x^2 - 2x + 9$ est réductible dans $\mathbb{F}_p[X]$.
   Le discriminant Δ du polynôme $x^2 - 2x + 9$ est égal à $4 - 36 = -32$. D'après l'hypoth'ese, il existe $\delta \in \mathbb{F}_p$ tel que $\delta^2 = -32$ dans $\mathbb{F}_p$. Comme p est impair, 2 est inversible dans $\mathbb{F}_p$, et on peut décomposer $x^2 - 2x + 9$ selon la formule habituelle :

$$x^2 - 2x + 9 = (x - 2^{-1}(2 + \delta))(x - 2^{-1}(2 - \delta)).$$

   Par conséquent, le polynôme $x^2 - 2x + 9$ est bien réductible dans $\mathbb{F}_p[x]$.

6. En déduire que f est réductible dans $\mathbb{F}_p[x]$ lorsque p est un nombre premier impair tel qu'il existe $\delta \in \mathbb{F}_p$ avec $\delta^2 = -32$ dans $\mathbb{F}_p$.
   On substitue x^2 pour x dans la décomposition ci-dessus, et on trouve

$$f = x^4 - 2x^2 + 9 = (x^2 - 2^{-1}(2 + \delta))(x^2 - 2^{-1}(2 - \delta)),$$

   i.e., f est réductible dans $\mathbb{F}_p[x]$.

Dans la suite, p désignera un nombre premier impair pour lequel il n'existe pas de $\delta \in \mathbb{F}_p$ avec $\delta^2 = -32$ dans $\mathbb{F}_p$.

7. Montrer qu'il existe un élément $\beta \in \mathbb{F}_{p^2}$ tel que $\beta^2 = -1$.
   D'après le cours, le groupe multiplicatif $\mathbb{F}_{p^2}^\star$ est cyclique d'ordre $p^2 - 1$. Soit ε un générateur de ce groupe. Comme $-1 \in \mathbb{F}_{p^2}^\star$, il existe $e \in \mathbb{Z}$ tel que $-1 = \varepsilon^e$. Du coup, $1 = (-1)^2 = \varepsilon^{2e}$, et $2e$ est divisible par $p^2 - 1$. Comme p est impair, $p^2 - 1 = (p - 1)(p + 1)$ est divisible par 4, et donc $2e$ aussi. Cela montre que e est pair. Ecrivons donc $e = 2d$, avec $d \in \mathbb{Z}$, et soit $\beta = \varepsilon^d$. On a

$$\beta^2 = (\varepsilon^d)^2 = \varepsilon^{2d} = \varepsilon^e = -1.$$

8. Montrer qu'il existe un élément $\gamma \in \mathbb{F}_{p^2}$ tel que $\gamma^2 = 2$
   De même, il existe $e \in \mathbb{Z}$ tel que $\varepsilon^e = 2$. Comme $2 \in \mathbb{F}_p$, l'ordre c de 2 est un diviseur de $(p - 1)$. Comme $1 = 2^c = \varepsilon^{ce}$, l'entier ce est divisible par $p^2 - 1 = (p - 1)(p + 1)$. Il s'ensuit que e est pair, et on conclut comme ci-dessus.

9. Montrer que $\alpha = \beta + \gamma$ est une racine de f dans $\mathbb{F}_{p^2}$.
   On calcule, en utilisant que $\beta^2 = -1$ et $\gamma^2 = 2$,

$$\begin{aligned} f(\beta + \gamma) = (\beta + \gamma)^4 - 2(\beta + \gamma)^2 + 9 = \\ \beta^4 + 4\beta^3\gamma + 6\beta^2\gamma^2 + 4\beta\gamma^3 + \gamma^4 - 2\beta^2 - 4\beta\gamma - 2\gamma^2 + 9 = \\ 1 - 4\beta\gamma - 12 + 8\beta\gamma + 4 + 2 - 4\beta\gamma - 4 + 9 = 0 \end{aligned}$$

10. En déduire que f est réductible dans $\mathbb{F}_p[x]$ lorsque p est un nombre premier impair pour lequel il n'existe pas de $\delta \in \mathbb{F}_p$ avec $\delta^2 = -32$.
    Soit m le polynôme minimal de α sur $\mathbb{F}_p$. Comme le degré de $\mathbb{F}_{p^2}/\mathbb{F}_p$ est égal à 2, le degré de m est ≤ 2. Effectuons la division euclidienne de f par m : $f = qm + r$, où $q, r \in \mathbb{F}_p[x]$ avec $\deg(r) < \deg(m)$. Evaluons en α :

$$0 = f(\alpha) = q(\alpha) \cdot m(\alpha) + r(\alpha) = q(\alpha) \cdot 0 + r(\alpha) = r(\alpha).$$

Comme m est le polynôme non nul de plus bas degré dans $\mathbb{F}_p[x]$ annulant α, on en tire que $r = 0$. Il vient que m divise f dans $\mathbb{F}_p[x]$. Comme $1 \leq \deg(m) \leq 2 < 4 = \deg(f)$, le polynôme f est réductible.

Exercice IV

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

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 voir 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^6 + x^5 + x^4 + x^2 + 1
   g1=x^2+x+1
   g2=x^3+x+1
   g3=x^3+x^2+1
   ```

   Comme les restes $m\%g1 = x$, $m\%g2 = 1$, $m\%g3 = x^2 + x + 1$ 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 $\deg(m) = 6$, le nombre d'éléments de K est égal à $2^6 = 64$.
3. Montrer que l'élément α de $K^\star$ n'est pas générateur

   ```
   K=GF(64,name='alpha',modulus=m)
   alpha=K.gen()
   alpha.multiplicative_order()
   ```

   L'ordre multiplicatif de α est egal à $21 \neq 64 - 1$. L'élément α n'est donc pas générateur de $K^\star$.
4. Déterminer un générateur β de $K^\star$.
   On cherche un élément $\beta \in K$ d'ordre 63

   ```
   for beta in list(K):
     if beta!=0 and beta.multiplicative_order()==63: print beta
   ```

   Par exemple, $\beta = \alpha + 1$ convient.
5. Déterminer les sous-corps de K.
   Si $\gamma \in K$, le sous-corps $\mathbb{F}_2[\gamma]$ de K est une extension de $\mathbb{F}_2$ de degré égal au degré du polynôme minimal de γ sur $\mathbb{F}_2$. Comme ce degré doit être un diviseur du degré de $K/\mathbb{F}_2$, il est égal à 1, 2, 3 ou 6. Comptons les éléments de K de degré $1, 2, 3, 6$:

```
degres=map(lambda gamma:gamma.minpoly().degree(),list(K))
nombre_elts_degre=dict([(n,degres.count(n)) for n in 6.divisors()])
```

On constate que K contient 2 éléments de degré 1, 2 éléments de degré 2, 6 éléments de degré 3, et 54 éléments de degré 6. Cela fait bien un total de $2+2+6+54=64$ éléments.

Les 2 éléments de degré 2 dans K sont, bien-sûr, 0 et 1. Ils engendrent le sous-corps trivial $\mathbb{F}_2$. Les 54 éléments de degré 6 dans K engendrent le sous-corps trivial K de K. Les 2 éléments de degré 2 engendrent tous les deux un sous-corps non trivial de K de degré 2 sur $\mathbb{F}_2$, i.e., un sous-corps à 4 éléments. Un tel sous-corps contient 2 éléments de degré 2. Il s'ensuit que les 2 éléments de degré 2 de K engendrent le même sous-corps à 4 éléments de K. Notons-le par $\mathbb{F}_4$. De même, les 6 éléments de K de degré 3 engendrent le même sous-corps de K de cardinal 8. Notons-le $\mathbb{F}_8$. Le corps K ne contient pas d'autre sous-corps.

6. Pour chaque sous-corps L de K, préciser un générateur de $L^\star$.

   Un générateur de $\mathbb{F}_2^\star$ est 1. Un générateur de $K^\star$ est $\beta=\alpha+1$, d'après le 4. En particulier, β est d'ordre 63. Afin de déterminer un générateur de $\mathbb{F}_3^\star$ qui est cyclique de cardinal $8-1=7$, il convient de considérer l'élément β^9, puisqu'il est d'ordre 7. Mais appartient-il bien à $\mathbb{F}_3^\star$? Calculons son degré :

   ```
   beta=alpha+1
   (beta^9).minpoly().degree()
   ```

   L'élément β^9 est bien de degré 3 sur $\mathbb{F}_2$, il appartient donc à $\mathbb{F}_8$. Comme il est d'ordre 7, c'est un générateur de $\mathbb{F}_8^\star$.

   De même, β^{21} est générateur de $\mathbb{F}_4^\star$.