Universit P. et M. Curie (Paris VI)
Master de sciences et technologies 1re année - Mathématiques et applications — Mention :
Spécialité : Mathématiques Fondamentales — MO11 : (12 ECTS)
code UE : MMAT4020 — code Scolar : MM020

Théorie des nombres

Michel Waldschmidt

`Seul document autorisé : le polycopié du cours`

Examen du 11 mai 2009
Durée : 3 heures

Exercice 1. *a) Écrire la décomposition du polynôme $X^{12} - 1$ en facteurs irréductibles sur $\mathbb{Z}$.*
b) Écrire la décomposition du polynôme $X^{12} - 1$ en facteurs irréductibles sur le corps fini $\mathbb{F}_5$ à 5 éléments.
c) Quel est le nombre d'éléments du corps de décomposition sur $\mathbb{F}_5$ du polynôme $X^{12} - 1$?

Exercice 2. *Le groupe des unités d'un corps de nombres K a un rang égal à 4. Que pouvez-vous dire du degré de K sur $\mathbb{Q}$?*

Exercice 3. *On considère le polynôme $f(X) = X^3 + X - 1$*
a) Montrer que f est irréductible dans $\mathbb{Z}[X]$.
b) Quel est le discriminant de f ?
c) Montrer que f a une unique racine réelle α et que cette racine est dans l'intervalle $(0, 1)$
d) On considère le corps de nombres $k = \mathbb{Q}(\alpha)$. Quel est l'anneau des entiers de k ?
e) Donner un système d'unités indépendantes de k.
f) On désigne par N le corps de décomposition de f sur $\mathbb{Q}$. Donner la liste des sous-corps de N.

Exercice 4. *Soit $K = \mathbb{Q}(\theta)$ un corps de nombres de degré d. On suppose que son anneau d'entiers est $\mathcal{O}_K = \mathbb{Z}[\theta]$. On note $\mu_\theta \in \mathbb{Z}[X]$ le polynôme minimal de θ. Soit p un nombre premier. On factorise μ_θ en facteurs irréductibles dans $\mathbb{F}_p[X]$: soient $P_1(X), \ldots, P_r(X)$ des polynômes de $\mathbb{Z}[X]$ dont les images (que l'on note encore $P_i(X)$) dans $\mathbb{F}_p[X]$ sont des polynômes irréductibles de degré $f_1, \ldots, f_r$ respectivement tels que*

$$\mu_\theta(X) \equiv \prod_{i=1}^{r} P_i(X)^{e_i} \mod p.$$

1. *Pour tout $i = 1, \cdots, r$, quels sont les α_i tel que le corps fini $\mathbb{F}_{p^{\alpha_i}}$ possède une racine θ_i de P_i ?*
2. *Soit $\theta_i \in \overline{\mathbb{F}}_p$ une racine de P_i. Montrer qu'il existe un unique morphisme*

$$\varphi_i : \mathbb{Z}[\theta] \longrightarrow \mathbb{F}_p[\theta_i]$$

   tel que $\varphi_i(\theta) = \theta_i$. Montrer que ce morphisme est surjectif.
3. *On note $\mathcal{P}_i$ le noyau du morphisme φ_i de la question précédente. Montrez que $\mathcal{P}_i$ est un idéal premier de $\mathbb{Z}[\theta]$. Montrer que c'est l'idéal engendré par p et $P_i(\theta)$.*
4. *Vérifier $\prod_{i=1}^{r} \mathcal{P}_i^{e_i} \subset p\mathcal{O}_K$. En déduire qu'il existe des entiers $0 \leq e_i' \leq e_i$ pour tout $i = 1, \cdots, r$ tels que*

$$p\mathcal{O}_K = \prod_{i=1}^{r} \mathcal{P}_i^{e_i'}.$$

5. *Quelle est la norme de l'idéal $\mathcal{P}_i$?*
6. *Montrez en utilisant les questions précédentes que $p\mathcal{O}_K = \prod_{i=1}^{r} \mathcal{P}_i^{e_i}$.*

1 Solutions

1 a) Les diviseurs de 12 sont $1, 2, 3, 4, 6$ et 12, donc

$$X^{12} - 1 = \Phi_1(X)\Phi_2(X)\Phi_3(X)\Phi_4(X)\Phi_6(X)\Phi_{12}(X)$$

avec

$$\Phi_1(X) = X - 1, \quad \Phi_2(X) = X + 1, \quad \Phi_3(X) = X^2 + X + 1,$$
$$\Phi_4(X) = \Phi_2(X^2) = X^2 + 1, \quad \Phi_6(X) = \Phi_3(-X) = X^2 - X + 1,$$
$$\Phi_{12} = \Phi_6(X^2) = X^4 - X^2 + 1.$$

b) Le polynôme $\Phi_n(X)$ se décompose dans le corps fini à q éléments en produit de polynômes irréductibles tous de même degré d, où d est l'ordre de q modulo n. On a

$$5 \equiv 1 \pmod 1, \quad 5 \equiv 1 \pmod 2, \quad 5 \equiv 1 \pmod 4,$$
$$5 \not\equiv 1 \pmod 3, \quad 5 \not\equiv 1 \pmod 6, \quad 5 \not\equiv 1 \pmod{12},$$
$$5^2 \equiv 1 \pmod 3, \quad 5^2 \equiv 1 \pmod 6, \quad 5^2 \equiv 1 \pmod{12},$$

ce qui signifie que 5 est d'ordre 1 modulo 1, 2 et 4, et qu'il est d'ordre 2 modulo 3, 6 et 12. Il en résulte que le polynôme $\Phi_4(X)$ est produit dans $\mathbb{F}_5[X]$ de deux polynômes de degré 1 :

$$X^2 + 1 = (X + 2)(X + 3) \quad \text{dans } \mathbb{F}_5[X],$$

que $\Phi_3(X)$, $\Phi_6(X)$ sont irréductibles dans $\mathbb{F}_5[X]$, et que $\Phi_{12}(X)$ est produit dans $\mathbb{F}_5[X]$ de deux polynômes irréductibles de degré 2 :

$$X^4 - X^2 + 1 = (X^2 + 2X - 1)(X^2 + 3X - 1).$$

Ainsi dans $\mathbb{F}_5[X]$ le polynôme $X^{12} - 1$ est produit de quatre polynômes de degré 1 et de quatre polynômes irréductibles de degré 2.
c) Soit K le corps de décomposition sur $\mathbb{F}_5$ de $X^{12} - 1$. Un quelconque des quatre facteurs irréductibles sur $\mathbb{F}_5$ de $X^{12} - 1$ de degré 2 a pour corps de rupture sur $\mathbb{F}_5$ l'unique extension quadratique de $\mathbb{F}_5$ contenue dans K. Dont $[K : \mathbb{F}_5] = 2$ et K a 25 éléments.

2 Désignons par r_1 le nombre de plongements de K dans $\mathbb{R}$, par $2r_2$ le nombre de plongements non réels de K dans $\mathbb{C}$ deux-à-deux conjugués, et par $n = [K : \mathbb{Q}]$ le degré de K sur $\mathbb{Q}$. On a $n = r_1 + 2r_2$ et le rang du groupe des unités est $r = r_1 + r_2 - 1$. Ici $r = 4$, donc $r_1 + r_2 = 5$. Les valeurs possibles pour r_1, r_2 et n sont données par le tableau ci-contre :

r_1	r_2	n
0	5	10
1	4	9
2	3	8
3	2	7
4	1	6
5	0	5

Par conséquent n peut prendre les valeurs 5, 6, 7, 8, 9 et 10.

3 On considère le polynôme $f(X) = X^3 + X - 1$
a) Le polynôme f est de degré 3, il n'a pas de racine rationnelle, donc il est irréductible sur $\mathbb{Q}$. Il a ses coefficients dans $\mathbb{Z}[X]$ premiers entre eux dans leur ensemble, donc il est irréductible sur $\mathbb{Z}$.
b) Le discriminant de $X^3 + pX + q$ est $-4p^3 - 27q^2$, ici $p = 1$ et $q = -1$, donc le discrimininant de f est $\Delta = -31$
c) Comme son discriminant Δ est négatif, f a une unique racine réelle, disons α, et deux racines complexes conjuguées, disons α' et $\overline{\alpha'}$. Cela résulte aussi du fait que la dérivée $f'(X) = 3X^2 + 1$ n'a pas de racine réelle, donc l'application polynomiale $f : \mathbb{R} \to \mathbb{R}$ est monotone. Comme $f(0) = -1$ et $f(1) = 1$, la racine α est dans l'intervalle $(0, 1)$.
d) Les seuls diviseurs de Δ dans $\mathbb{Z}$ sont $\pm\Delta$, donc l'anneau des entiers de k est $\mathbb{Z}[\alpha]$.
e) Le corps k est une extension cubique de $\mathbb{Q}$ avec un plongement réel et deux plongements complexes conjugués : $r_1 = 1$, $r_2 = 1$. Le rang du groupe des unités est $r = r_1 + r_2 - 1 = 1$ Comme α est une unité qui n'est pas une racine de l'unité (α est réel $\neq \pm 1$), un système d'unités indépendantes de k est $\{\alpha\}$.
f) Comme Δ n'est pas un carré dans $\mathbb{Q}$, le corps de décomposition $N = k(\sqrt{\Delta})$ de f sur $\mathbb{Q}$ est une extension quadratique de k, donc une extension de degré 6 de $\mathbb{Q}$, de groupe de Galois sur $\mathbb{Q}$ le groupe symétrique à 6 éléments. Les sous-groupes du groupe symétrique à 6 éléments sont au nombre de 6, il y en a un d'ordre 6, un d'ordre 1, un d'ordre 3 et trois d'ordre 2. Donc les sous-corps de N sont au nombre de 6, ce sont $\mathbb{Q}$, N, $\mathbb{Q}(\sqrt{\Delta})$, $k = \mathbb{Q}(\alpha)$, et les deux autres corps cubiques $k = \mathbb{Q}(\alpha')$ et $k = \mathbb{Q}(\overline{\alpha'})$.

4 (1) Pour que le corps fini $\mathbb{F}_{p^{\alpha_i}}$ possède une racine θ_i de P_i, il faut et il suffit que $\mathbb{F}_{p^{\alpha_i}}$ contienne $\mathbb{F}_p(\theta_i) \simeq \mathbb{F}_{p^{f_i}}$ et ceci est vérifié si et seulement si f_i divise α_i.

(2) Il existe un unique morphisme $\mathbb{Z}[X] \to \mathbb{F}_p[\theta_i]$ tel que $X \mapsto \theta_i$; ce morphisme est surjectif, et son noyau contient $\mu_\theta(X)$, puisque $\mu_\theta(\theta_i) = 0$. Par passage au quotient on obtient le morphisme φ_i cherché.

(3) Comme l'image de φ_i est un anneau intègre on en déduit que son noyau $\mathcal{P}_i$ est un idéal premier (maximal même, car un anneau intègre fini est toujours un corps). Par ailleurs $\mathcal{P}_i$ contient p et $P_i(\theta)$. Des isomorphismes

$$\mathbb{Z}[\theta]/(p, P_i(\theta)) \simeq \mathbb{Z}[X]/(p, P_i(X)) \simeq \mathbb{F}_p[X]/(P_i(X)) \simeq \mathbb{F}_p[\theta_i] = \mathbb{F}_p(\theta_i)$$

il résulte que l' idéal $(p, P_i(\theta))$ est maximal, comme il est contenu dans $\mathcal{P}_i$ il est égal à $\mathcal{P}_i$.

(4) Un élément de $\mathcal{P}_i$ s'écrit $cp + dP_i(\theta)$ avec c et d dans $\mathcal{O}_K$. Un élément x de $\prod_{i=1}^r \mathcal{P}_i^{e_i}$ est une combinaison linéaire de produits de tels elements avec e_1 facteurs dans $\mathcal{P}_1$, ..., e_r facteurs dans $\mathcal{P}_r$. Le nombre $\prod_{i=1}^r P_i(\theta)^{e_i}$ est dans $\mathbb{Z}$ et congru modulo p à $\mu_\theta(\theta) = 0$, donc il est multiple de p. Il en résulte que x est dans $p\mathcal{O}_K$. Ainsi l'écriture de $p\mathcal{O}_K$ en produit d'idéaux premiers est $\prod_{i=1}^r \mathcal{P}_i^{e'_i}$ avec $0 \leq e'_i \leq e_i$.

(5) La norme de $\mathcal{P}_i$ est par définition le cardinal de $\mathcal{O}_K/\mathcal{P}_i \simeq \mathbb{F}_p[\theta_i]$ et donc égale à p^{f_i}.

(6) De l'égalité $p\mathcal{O}_K = \prod_{i=1}^r \mathcal{P}_i^{e_i'}$ en prenant la norme on déduit

$$p^d = p^{\sum_{i=1}^r e_i' f_i}, \quad \text{donc} \quad d = \sum_{i=1}^r e_i' f_i.$$

Ainsi comme $d = \sum_{i=1}^r e_i f_i$ et $0 \leq e_i' \leq e_i$, on en déduit que $e_i' = e_i$ pour tout $i = 1, \cdots, r$.