Théorie des nombres

Michel Waldschmidt

code UE : MMAT4020 code Scolar : MM020

Examen Partiel 23 Février 2011

Solutions

`Solution de l'exercice 1.`
Si G est un sous–groupe fini d'ordre n de $K^\times$, alors G est l'ensemble des racines du polynôme X^n-1, donc ce polynôme a n racines distinctes dans K, par conséquent sa dérivée n'est pas nulle, ce qui implique que p ne divise pas n.

`Solution de l'exercice 2.`

1. On calcule
$$\beta(\beta-2\alpha^2)=(\alpha+\alpha^2)(\alpha-\alpha^2)=\alpha^2-\alpha^4=\alpha^2-8\,.$$
Par conséquent, on en déduit que $\alpha^2=\dfrac{8+\beta^2}{1+2\beta}$, donc $\alpha^2\in\mathbf{Q}(\beta)$. Donc $\alpha=\beta-\alpha^2\in\mathbf{Q}(\beta)$. Donc $\mathbf{Q}(\alpha)\subset\mathbf{Q}(\beta)$. L'inclusion réciproque est évidente.
2. On peut par exemple montrer que le polynôme P est irréductible dans $\mathbf{Z}[X]$ (donc dans $\mathbf{Q}[X]$ puisqu'il est unitaire). Il est clair que P n'a pas de racine dans $\mathbf{Z}$. Par conséquent, s'il n'est pas irréductible dans $\mathbf{Z}[X]$, il existe des entiers $a,b,c,d\in\mathbf{Z}$ tels que $P(X)=(X^2+aX+b)(X^2+cX+d)$. On identifie alors les coefficients, et on obtient $c=-a$, $b+d=a^2$, $a(b-d)=0$ et $bd=-8$. On déduit facilement de ces conditions que 8 ou -8 est un carré dans $\mathbf{Z}$, ce qui n'est pas. Donc P est irréductible dans $\mathbf{Z}[X]$, donc dans $\mathbf{Q}[X]$ (lemme de Gauss). Donc $[\mathbf{Q}(\alpha):\mathbf{Q}]=4$.
3. Les racines de P dans $\mathbf{C}$ sont exactement $\alpha, i\alpha, -\alpha$ et $-i\alpha$. Par conséquent, un corps de décomposition L de P sur $\mathbf{Q}$ est donné par
$$L=\mathbf{Q}(i,\alpha)\,.$$
4. L'extension $L/\mathbf{Q}(\alpha)$ est de degré au plus 2 (puisque $L=\mathbf{Q}(\alpha)(i)$ et $i^2\in\mathbf{Q}$). Or cette extension n'est pas triviale car $\mathbf{Q}(\alpha)\subset\mathbf{R}$ et $i\notin\mathbf{R}$. Donc finalement $[L:\mathbf{Q}(\alpha)]=2$, et on conclut par multiplicativité des degrés que
$$[L:\mathbf{Q}]=[L:\mathbf{Q}(\alpha)][\mathbf{Q}(\alpha):\mathbf{Q}]=8\,.$$

`Solution de l'exercice 3.`
L'application exponentielle $\exp:\mathbf{R}\longrightarrow\mathbf{R}^\times$ qui envoie x sur e^x est un homomorphisme d'image $\mathbf{R}_+^\times$.
L'application exponentielle $\exp:\mathbf{C}\longrightarrow\mathbf{C}^\times$ qui envoie z sur $e^{2i\pi z}$ est un homomorphisme surjectif de noyau $\mathbf{Z}$.

L'application $\vartheta \longmapsto e^{2i\pi\vartheta}$ est un homomorphisme de $\mathbf{R}$ dans $\mathbf{C}^\times$, de noyau $\mathbf{Z}$ et d'image $\mathbf{U}$, d'où l'isomorphisme $\mathbf{R}/\mathbf{Z} \longrightarrow \mathbf{U}$. Cela donne une définition de $e^{2i\pi\theta}$ pour $\theta \in \mathbf{R}/\mathbf{Z}$.
Le sous–groupe de torsion de $\mathbf{R}/\mathbf{Z}$ est $\mathbf{Q}/\mathbf{Z}$, celui de $\mathbf{U}$ est $\boldsymbol{\mu}$, d'où l'isomorphisme $\mathbf{Q}/\mathbf{Z} \longrightarrow \boldsymbol{\mu}$.
L'application $(x,u) \longmapsto xu$ est un isomorphisme de $\mathbf{R}_+^\times \times \mathbf{U}$ sur $\mathbf{C}^\times$ (l'isomorphisme inverse est $z \longmapsto (|z|, z/|z|)$), en la composant avec l'isomorphisme précédent $\mathbf{R}/\mathbf{Z} \longrightarrow \mathbf{U}$ on obtient un isomorphisme $(x,\theta) \longmapsto xe^{2i\pi\vartheta}$ de $\mathbf{R}_+^\times \times \mathbf{R}/\mathbf{Z}$ sur $\mathbf{C}^\times$.

`Solution de l'exercice 4.`
Le groupe $(\mathbf{Z}/7\mathbf{Z})^\times$ est cyclique d'ordre 6, il y a $\varphi(6) = 2$ éléments qui sont générateurs, ce sont les classes de 3 et de 5. Les classes de 2 et 4 modulo 7 sont d'ordre 3, la classe de 6 est d'ordre 2, celle de 1 est d'ordre 1. Donc

- Si $q \equiv 3$ ou 5 mod 7, alors Φ_7 est irréductible dans $\mathbf{F}_q[X]$,
- Si $q \equiv 2$ ou 4 mod 7, alors Φ_7 se décompose en un produit de 2 polynômes irréductibles de degrés 3 dans $\mathbf{F}_q$,
- Si $q \equiv 6$ mod 7, alors Φ_7 se décompose en un produit de 3 polynômes irréductibles de degrés 2 dans $\mathbf{F}_q[X]$,
- Si $q \equiv 1$ mod 7, alors Φ_7 est totalement décomposé dans $\mathbf{F}_q[X]$,
- Si q est une puissance de 7, alors $\Phi_7 = (X-1)^6$ dans $\mathbf{F}_q[X]$.

Par exemple

- Sur $\mathbf{F}_2$, on a $\Phi_7(X) = (X^3+X^2+1)(X^3+X+1)$,
- Sur $\mathbf{F}_3$ et sur $\mathbf{F}_5$, le polynôme $\Phi_7(X)$ est irréductible,
- Sur $\mathbf{F}_7$, on a $\Phi_7(X) = (X-1)^6$,
- Sur $\mathbf{F}_8$, on a $\Phi_7(X) = \prod_{x\in\mathbf{F}_8^\times,\, x\neq 1}(X-x)$.

`Solution de l'exercice 5.`
a) Dans le cas $p = q = 3$, $s = 1$, on a $F = \mathbf{F}_3$, tout élément α de $F^\times$ (il y en a 2, à savoir 1 et -1) satisfait la propriété $F = \mathbf{F}_p(\alpha)$. Le groupe $F^\times$ est cyclique d'ordre 2, il y a un seul générateur, c'est -1.

Supposons maintenant $q-1 = p^s-1$ premier impair. Alors $p = 2$ et s est un nombre premier (et $q-1$ est un nombre premier de Mersenne). Comme s est premier, les seuls sous–corps de F sont $\mathbf{F}_2$ et F. Donc tout élément α de F autre que 0 et 1 est un générateur du groupe cyclique $F^\times$ et vérifie $\mathbf{F}_2(\alpha) = F$. Pour chacune des deux questions, le nombre d'éléments demandé est donc $q-2 = 2^s-2$ (et ce sont les mêmes éléments qui répondent à la question).
b) Comme l'ordre de p modulo n est s, le polynôme cyclotomique Φ_n se décompose sur $\mathbf{F}_p$ en facteurs irréductibles tous de même degré $s = [F : \mathbf{F}_p]$, et il se décompose complètement dans le corps F. Soit $\alpha \in F$ une racine de Φ_n ; alors α est de degré s, donc $\mathbf{F}_p(\alpha) = F$, et α est d'ordre n dans le groupe multiplicatif $F^\times$.
c) Montrons que si $q-1$ n'est pas un nombre premier, il existe un entier $n \neq p^s-1$ tel que l'ordre de p modulo n soit égal à s (cf. un exercice du polycopié § 2.3, après le Corollaire 2.22). Si p est impair, on prend $n = (p^s-1)/(p-1)$. Si $p = 2$ et s est premier, on prend pour n est un diviseur de 2^s-1. Si s possède un diviseur strict d, alors 2 est d'ordre s modulo n pour $n = (2^s-1)/(2^d-1)$. Ce qui précède montre que dans ce cas ($q-1$ n'est pas un nombre premier), il existe un élément α dans $F^\times$, qui n'est pas un générateur du groupe cyclique $F^\times$, tel que $\mathbf{F}_p(\alpha) = F$.
`Référence:` Claire Tête, Cyclotomie et corps finis, Revue de la filière mathématique RMS 121 n°1, 34–41. `http://www.rms-math.com/`
`Remarque` : l'énoncé a été corrigé avec $\alpha \in F^\times$ dans (i) et non $\alpha \in F$ à cause du cas $p = q = 2$.