Théorie des nombres

Michel Waldschmidt

code UE : MMAT4020 code Scolar : MM020

Examen du lundi 2 mai 2011
Durée : 4 heures
Seul le polycopié est autorisé

Exercice 1. Pour chacune des affirmations suivantes, dire si elle est vraie ou fausse, et justifier votre réponse.
(a) Toute extension finie d'un corps de caractéristique nulle est séparable.
(b) Toute extension finie d'un corps de caractéristique nulle est normale.
(c) Toute extension finie d'un corps fini est séparable.
(d) Toute extension finie d'un corps fini est normale.
(e) Toute extension quadratique est séparable.
(f) Toute extension quadratique est normale.

Exercice 2. Les questions a) et b) sont indépendantes.
a) Soit α une racine du polynôme $X^3 - X - 4$. On note $K := \mathbf{Q}(\alpha)$.
i) Quel est le degré de l'extension $K/\mathbf{Q}$? Quel est le rang du groupe des unités ?
ii) Calculer le discriminant de la famille $(1, \alpha, \alpha^2)$.
iii) Que peut-on en déduire sur l'indice de $\mathbf{Z}[\alpha]$ dans $\mathbf{Z}_K$?
iv) Montrer que $\dfrac{\alpha + \alpha^2}{2} \in \mathbf{Z}_K$.
v) Calculer $\mathbf{Z}_K$ et le discriminant D_K du corps K.
b) Soit β une racine du polynôme $X^3 - 3X^2 + 10X - 5$. On note $L := \mathbf{Q}(\beta)$.
i) Quel est le degré de l'extension $L/\mathbf{Q}$? Quel est le rang du groupe des unités ?
ii) Calculer le discriminant de la famille $(1, \beta, \beta^2)$.
iii) Calculer $\mathbf{Z}_L$ et le discriminant D_L du corps L.

Exercice 3. Soit G un groupe abélien fini. Soit m le ppcm des ordres des éléments de G (l'entier m est l'*exposant* du groupe G). Montrer que m est le plus petit entier strictement positif tel que $x^m = 1$ pour tout $x \in G$. Montrer qu'il existe un élément de G d'ordre m.

Exercice 4. Soit k un corps et soit $D \in k$. On note $\mathrm{M}_2(k)$ l'anneau des matrices carrées 2×2 à coefficients dans k.
a) Montrer qu'il existe un unique homomorphisme d'anneaux φ de $k[X]$ dans $\mathrm{M}_2(k)$ qui envoie

$$\alpha \in k \quad \text{sur} \quad \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix} \quad \text{et} \quad X \quad \text{sur} \quad \begin{pmatrix} 0 & D \\ 1 & 0 \end{pmatrix}.$$

Le noyau de φ est un idéal principal de $k[X]$: en donner un générateur.
On note $K = \varphi(k)$ et $E = \varphi(k[X])$.
b) On suppose que D n'est pas un carré dans k. Montrer que E est un corps, extension finie de K. Quel est le degré $[E : K]$ de E sur K ?
c) On suppose qu'il existe $d \in k$ tel que $D = d^2$. Montrer que l'anneau E n'est pas intègre. Montrer plus précisément que E est isomorphe à l'anneau

$$\begin{cases} k[\varepsilon] \quad \text{avec } \epsilon^2 = 0 & \text{si } 2D = 0, \\ k \times k & \text{si } 2D \neq 0. \end{cases}$$

Exercice 5.
Soient t_1 et t_2 deux nombres réels. On désigne par G le sous–groupe $\mathbf{Z}(1, t_1) + \mathbf{Z}(t_2, 1)$, c'est–à–dire

$$G = \big\{(a + bt_2, at_1 + b) \; ; \; (a, b) \in \mathbf{Z} \times \mathbf{Z}\big\}.$$

En distinguant plusieurs cas dépendant de t_1 et t_2, donner le rang ℓ de G, la dimension n de l'espace vectoriel engendré par G, décrire l'adhérence $\overline{G}$ de G dans $\mathbf{R}^2$, dire si G est fermé, donner la dimension d du plus grand sous–espace vectoriel V de $\mathbf{R}^2$ contenu dans $\overline{G}$, dire si G est dense dans $\mathbf{R}^2$ et si G est discret.

Théorie des nombres

Michel Waldschmidt

code UE : MMAT4020 code Scolar : MM020

Examen du lundi 2 mai 2011
Durée : 4 heures

Solutions

`Solution de l'exercice 1.`
(a) Toute extension finie d'un corps de caractéristique nulle est séparable : vrai (voir le polycopié).
(b) Toute extension finie d'un corps de caractéristique nulle est normale : faux (voir l'exemple de l'extension $\mathbf{Q}(\sqrt[3]{2})/\mathbf{Q}$ dans le polycopié).
(c) Toute extension finie d'un corps fini est séparable : vrai (voir le polycopié).
(d) Toute extension finie d'un corps fini est normale : vrai (voir le polycopié).
(e) Toute extension quadratique est séparable : faux (voir l'exemple de l'extension $\mathbf{F}_2(T)/\mathbf{F}_2(T^2)$ dans le polycopié).
(f) Toute extension quadratique est normale : vrai. Si un polynôme $aT^2+bT+c \in K[T]$ de degré 2 a une racine α dans le corps K, alors l'autre racine $(-b/a)-\alpha$ est aussi dans K.

`Solution de l'exercice 2`
a) i) Le polynôme X^3-X-4 est irréductible sur $\mathbf{Z}$ puisque se réduction modulo 3 n'a pas de racine. Comme il est unitaire, ce polynôme est irréductible dans $\mathbf{Q}[X]$. Un autre argument consiste à dire qu'il est irréductible sur $\mathbf{Q}$ car il est de degré 3 et n'a pas de racine rationnelle (étant unitaire, une racine rationnelle serait un entier, qui devrait diviser le terme constant, donc ce serait ±1, ±2 ou ±4, or aucun de ces six nombres n'est racine). Donc $[K:\mathbf{Q}]=3$.
Le polynôme X^3-X-4 a une racine réelle et deux racines complexes conjuguées, le nombre r_1 de plongements réels est 1, le nombre $2r_2$ de plongements complexes non réels est 2, le rang du groupe des unités $r=r_1+r_2-1$ est donc 1.
ii) On note $d_\alpha := \mathrm{disc}_{\mathbf{Z}}(1,\alpha,\alpha^2)$. On sait que d_α est égal au discriminant du polynôme X^3-X-4, donc $d_\alpha = -4(-1)^3-27.(-4)^2 = -428 = -4.107$.
iii) Puisque 107 est un nombre premier, et puisque le carré de l'indice de $\mathbf{Z}[\alpha]$ dans $\mathbf{Z}_K$ divise d_α, cet indice divise 2. Donc il vaut 1 ou 2.
iv) On pose $\gamma := \dfrac{\alpha+\alpha^2}{2}$. Alors $\gamma^2 = \dfrac{\alpha^2+3\alpha+4}{2}$ et $\gamma^3 = 2\alpha^2+3\alpha+4$. Donc on a $\gamma^3-\gamma^2-3\gamma-2 = 0$, donc $\gamma \in \mathbf{Z}_K$.
v) On a les inclusions suivantes : $\mathbf{Z}[\alpha] \subset \mathbf{Z}[\alpha,\gamma] \subset \mathbf{Z}_K$. Comme γ n'appartient pas à $\mathbf{Z}[\alpha]$, il en résulte que $\mathbf{Z}[\alpha]$ est d'indice 2 dans $\mathbf{Z}[\alpha,\gamma]$, donc la question c) assure que $\mathbf{Z}_K = \mathbf{Z}[\alpha,\gamma]$. En outre, on sait que $d_\alpha = [\mathbf{Z}_K : \mathbf{Z}[\alpha]]^2 D_K$, donc $D_K = -107$.
b) i) On remarque que le polynôme est irréductible en vérifiant par exemple que sa réduction modulo 2 n'a pas de racine. Donc $[L:\mathbf{Q}]=3$. Une autre solution consiste à vérifier que -1, 1, -5 et 5 ne sont pas racines de ce polynôme dans $\mathbf{Q}$. Le polynôme en question a une unique racine réelle et deux racines complexes conjuguées, donc $r_1=r_2=1$, par conséquent le théorème des

unités assure que le rang du groupe des unités vaut $r = r_1 + r_2 - 1 = 1$.
ii) On note $d_\beta := \mathrm{disc}_{\mathbf{Z}}(1, \beta, \beta^2)$. On sait que d_β est égal au discriminant du polynôme $X^3 - 3X^2 + 10X - 5$. Or ce polynôme se réécrit sous la forme $(X-1)^3 + 7(X-1) + 3$, donc son discriminant est égal au discriminant du polynôme $Y^3 + 7Y + 3$, donc $d_\beta = -4.7^3 - 27.3^2 = -1615$. On peut aussi calculer ce discriminant en calculant les traces respectives des puissances de β.
iii) On remarque que le discriminant $d_\beta = -1615 = -5.17.19$, donc d_β est sans facteur carré. Donc on en déduit que $\mathbf{Z}_L = \mathbf{Z}[\beta]$ et que $D_L = -1615$.

`Solution de l'exercice 3.`
Rappelons que l'ordre de $x \in G$ est le générateur positif de l'idéal $\mathfrak{I}_x = \{\ell \in \mathbf{Z}\ ;\ x^\ell = 1\}$ de $\mathbf{Z}$. L'exposant de G est le générateur positif de l'idéal

$$\{\ell \in \mathbf{Z}\ ;\ x^\ell = 1 \text{ pour tout } x \in G\} = \bigcap_{x \in G} \mathfrak{I}_x,$$

c'est donc à la fois le ppcm des générateurs des $\mathfrak{I}_x$ (donc le ppcm des ordres des éléments de G) et le plus petit entier positif dans cet idéal (donc le plus petit entier m tel que $x^m = 1$ pour tout $x \in G$).

D'autre part, un groupe abélien fini est isomorphe à un produit de groupes cycliques dont les ordres $a_1, \ldots, a_s$ vérifient : a_1 divise a_2,..., a_{s-1} divise a_s. Alors $x^{a_s} = 1$ pour tout x dans G, de plus G possède au moins un élément d'ordre a_s, donc l'exposant de G est a_s.

`Solution de l'exercice 4.`
L'application ϕ de k dans $\mathrm{M}_2(k)$ qui envoie $\alpha \in k$ sur

$$\begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix}$$

est un homomorphisme d'anneaux. L'image de ϕ dans $\mathrm{M}_2(k)$ est

$$K = \phi(k) = \left\{ \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix}\ ;\ \alpha \in k \right\},$$

et ϕ induit un isomorphisme de corps $k \to K$. Quand A est un anneau, k un corps, ϕ un homomorphisme de k dans A et γ un élément de A, il existe un unique homomorphisme d'anneaux de $k[X]$ dans A qui prolonge ϕ et envoie X sur γ. D'où l'existence de l'homomorphisme φ recherché, avec $\varphi(k) = \phi(k) = K$. L'image par φ d'un polynôme $a_0 + a_1X + \cdots + a_nX^n$ est $a_0 + a_1\varphi(X) + \cdots + a_n\varphi(X)^n$ avec

$$\varphi(X) = \begin{pmatrix} 0 & D \\ 1 & 0 \end{pmatrix}.$$

Comme cette matrice vérifie

$$\varphi(X)^2 = \begin{pmatrix} 0 & D \\ 1 & 0 \end{pmatrix}^2 = \begin{pmatrix} D & 0 \\ 0 & D \end{pmatrix} = \phi(D),$$

on a

$$\varphi(X^{2m}) = \varphi(X^2)^m = \phi(D^m) = \begin{pmatrix} D^m & 0 \\ 0 & D^m \end{pmatrix} \quad \text{et} \quad \varphi(X^{2m+1}) = \varphi(X)\varphi(X^{2m}) = \begin{pmatrix} 0 & D^{m+1} \\ D^m & 0 \end{pmatrix}.$$

Par conséquent l'image de φ est

$$E = \left\{ \begin{pmatrix} a & bD \\ b & a \end{pmatrix} \ ; \ (a,b) \in k \times k \right\}$$

et le noyau de φ contient $X^2 - D$. Comme $\varphi(X) \notin K$, le noyau de φ ne contient pas de polynôme de degré 1, donc $\ker \varphi$ est l'idéal principal engendré par $X^2 - D$. On en déduit que l'anneau E est isomorphe au quotient $k[X]/(X^2 - D)$.
b) Si D n'est pas un carré dans k, le polynôme quadratique $X^2 - D$ est irréductible dans $k[X]$, donc E est un corps, extension quadratique de K, isomorphe à $k(\sqrt{D})$.
c) Supposons $D = d^2$ avec $d \in k$. L'anneau E n'est pas intègre puisque

$$\begin{pmatrix} 0 & D \\ 1 & 0 \end{pmatrix}^2 - \begin{pmatrix} d & 0 \\ 0 & d \end{pmatrix}^2 = \left(\begin{pmatrix} 0 & D \\ 1 & 0 \end{pmatrix} - \begin{pmatrix} d & 0 \\ 0 & d \end{pmatrix} \right) \left(\begin{pmatrix} 0 & D \\ 1 & 0 \end{pmatrix} + \begin{pmatrix} d & 0 \\ 0 & d \end{pmatrix} \right) = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

L'anneau E est isomorphe à $k[X]/(X-\delta)(X+\delta)$. Si les deux polynômes $X-\delta$ et $X+\delta$ sont premiers entre eux, c'est–à–dire si la caractéristique de k est différente de 2 et $D \neq 0$, alors par le théorème des restes chinois $k[X]/(X-\delta)(X+\delta)$ est isomorphe au produit des quotients $k[X]/(X-\delta)$ et $k[X](X+\delta)$, et chacun de ces deux facteurs est isomorphe à k. Si au contraire $X - \delta$ et $X + \delta$ ne sont pas premiers entre eux, c'est–à–dire si $2D = 0$, alors $X - \delta = X + \delta$, donc

$$k[X]/(X-\delta)(X+\delta) = k[X]/(X-\delta)^2,$$

et si on désigne par ϵ la classe de $X - \delta$, on conclut que E est isomorphe à $k[\varepsilon]$ avec $\epsilon^2 = 0$.

`Solution de l'exercice 5`
Une condition nécessaire et suffisante pour que G contienne une base de $\mathbf{R}^2$ est que $(1, t_1)$ et $(t_2, 1)$ soient linéairement indépendants sur $\mathbf{R}$, donc que le déterminant

$$\begin{vmatrix} 1 & t_2 \\ t_1 & 1 \end{vmatrix}$$

soit non nul, ce qui s'écrit $t_1 t_2 \neq 1$.

Si t_1 est rationnel non nul et $t_2 = 1/t_1$, alors $\ell = 1$, $n = 1$, $\overline{G} = G$, G est fermé, $d = 0$, G n'est pas dense dans $\mathbf{R}^2$, G est discret.

Si t_1 est irrationnel et $t_2 = 1/t_1$, alors $\ell = 2$, donc $n = 1$, $\overline{G} = \mathbf{R}(1, t_1)$, G n'est pas fermé, $d = 1$, G n'est pas dense dans $\mathbf{R}^2$, G n'est pas discret.

Si $t_1 t_2 \neq 1$, alors $\ell = 2$, $n = 2$, $\overline{G} = G$, G est fermé, $d = 0$, G n'est pas dense dans $\mathbf{R}^2$, G est discret : c'est un réseau de $\mathbf{R}^2$.