Théorie des nombres

Michel Waldschmidt

code UE : MMAT4020 code Scolar : MM020

Examen du mardi 31 mai 2011
Durée : 3 heures
Seul le polycopié est autorisé

Exercice 1.
(a) Donner un exemple d'une extension finie qui n'est pas séparable.
(b) Donner un exemple d'une extension finie qui n'est pas normale.

Exercice 2. Soit x un nombre réel. On suppose que pour tout sous-corps K de $\mathbf{R}$, ou bien $x \in K$, ou bien x est transcendant sur K. En déduire que x est rationnel.

Exercice 3. Soit K un corps de nombres cubique, c'est–à–dire $[K : \mathbf{Q}] = 3$. Quelles sont les valeurs possibles pour le rang du groupe des unités de K ? Pour chaque valeur, en donner un exemple. Même question pour une extension quartique $[K : \mathbf{Q}] = 4$.

Exercice 4. Les questions (a) et (b) sont indépendantes.
(a) Soient $a, b, c \in \mathbf{Z}$ non carrés, tels que abc est un carré. Montrer que l'équation $x^6 - (a+b+c)x^4 + (ab+ac+bc)x^2 = abc$ n'a pas de solution dans $\mathbf{Q}$, mais qu'elle a des solutions dans tous les $\mathbf{F}_p$ (p premier) et dans $\mathbf{R}$.
(b) On cherche à montrer que l'équation $y^4 = 2x^2 + 17$ n'a pas de solution dans $\mathbf{Q}$. Soit $(x, y) \in \mathbf{Q}^2$ solution de cette équation.
i) Montrer qu'il existe $u, v, w \in \mathbf{Z}$ tels que $u^4 = 2v^2 + 17w^4$ et $(u, v) = 1$.
ii) Montrer que 2 n'est pas une puissance 4-ième modulo 17.
iii) En déduire que v n'est pas un carré modulo 17.
iv) En utilisant *i*), montrer que chaque diviseur premier de v est un carré modulo 17.
v) Conclure.

Exercice 5. Soient F un corps fini à q éléments et soit E une extension finie de F de degré n.
a) Quels sont les F–automorphismes de E ?
b) On pose

$$s = 1 + q + \cdots + q^{n-1} = \frac{q^n - 1}{q - 1}.$$

Montrer que la norme $\mathrm{N}_{E/F} : E^\times \longrightarrow F^\times$ est l'application $x \to x^s$.
c) Quel est le noyau G de $\mathrm{N}_{E/F}$? En déduire que $\mathrm{N}_{E/F}$ est une application surjective.
d) On suppose que s et $q - 1$ sont premiers entre eux. Montrer que le groupe cyclique $E^\times$ est isomorphe au produit de groupes cycliques $G \times F^\times$.

Théorie des nombres

Michel Waldschmidt

code UE : MMAT4020 code Scolar : MM020

Examen du mardi 31 mai 2011
Durée : 3 heures

Solutions

`Solution de l'exercice 1.`
a) Soit $E = \mathbf{F}_2(T)$ le corps des fractions rationnelles à coefficients dans le corps fini à deux éléments et K le sous-corps $\mathbf{F}_2(T^2)$. Alors l'extension quadratique E/K n'est pas séparable.
b) L'extension cubique $\mathbf{Q}(\sqrt[3]{2})/\mathbf{Q}$ n'est pas normale.

`Solution de l'exercice 2.`
Il s'agit de vérifier que si $x \in \mathbf{R}$ est irrationnel, il existe un sous–corps K de $\mathbf{R}$ qui ne contient pas x tel que x soit algébrique sur K. Si x est algébrique sur $\mathbf{Q}$, on prend $K = \mathbf{Q}$. Si x est transcendant sur $\mathbf{Q}$, on prend $K = \mathbf{Q}(x^2)$.
`N.B.` *Une version antérieure de ce corrigé disait de prendre* $K = \mathbf{Q}(\sqrt{x})$*, c'était une erreur !.*

`Solution de l'exercice 3.`
Les décompositions possibles $3 = r_1 + 2r_2$ avec r_1 et r_2 entiers ≥ 0 sont $3 = 3 + 0$ et $3 = 1 + 2$ avec (r_1, r_2) égal respectivement à $(3, 0)$ et $(1, 1)$. Le rang du groupe des unités est $r = r_1 + r_2 - 1$, c'est donc 2 si $(r_1, r_2) = (3, 0)$ et 1 si $(r_1, r_2) = (1, 1)$

Le premier cas $(r_1, r_2) = (3, 0)$, $r = 2$ est celui d'un corps cubique totalement réel (avec trois plongements réels), ce sont les corps de rupture des polynômes cubiques irréductibles ayant 3 racines réelles. Un exemple est $X^3 - 3X + 1$.

Le second cas $(r_1, r_2) = (1, 1)$, $r = 1$ est celui d'un corps cubique ayant un plongement réel et deux plongements imaginaires conjugués, ce sont les corps de rupture des polynômes cubiques irréductibles ayant une seule racine réelle, comme $X^3 - 2$. Ainsi le rang du groupe des unités du corps $\mathbf{Q}(\sqrt[3]{2})$ est 1.

Les décompositions possibles $4 = r_1 + 2r_2$ avec r_1 et r_2 entiers ≥ 0 sont $4 = 4 + 0$, $4 = 2 + 2$ et $4 = 0 + 4$ avec (r_1, r_2) égal respectivement à $(4, 0)$, $(2, 1)$ et $(0, 2)$. Le rang $r = r_1 + r_2 - 1$ du groupe des unités est 3 si $(r_1, r_2) = (4, 0)$, c'est 2 si $(r_1, r_2) = (2, 1)$ et c'est 1 si $(r_1, r_2) = (0, 2)$.

Le premier cas $(r_1, r_2) = (4, 0)$, $r = 3$ est celui d'un corps quartique totalement réel (avec quatre plongements réels), ce sont les corps de rupture des polynômes de degré 4 irréductibles ayant 4 racines réelles. Un exemple est

$$(X - \sqrt{2} - \sqrt{3})(X - \sqrt{2} + \sqrt{3})(X + \sqrt{2} - \sqrt{3})(X + \sqrt{2} + \sqrt{3}) = X^4 - 10X^2 + 1.$$

Le second cas $(r_1, r_2) = (2, 1)$, $r = 2$ est celui d'un corps quartique ayant deux plongements réels et deux plongement imaginaires conjugués, ce sont les corps de rupture des polynômes de degré

4 irréductibles ayant 2 racines réelles et deux racines complexes conjuguées. Un exemple de tel polynôme est X^4-2, donc le rang du groupe des unités du corps $\mathbf{Q}(\sqrt[4]{2})$ est $r=2$.

Le troisième cas $(r_1,r_2)=(0,2)$, $r=1$ est celui d'un corps quartique totalement imaginaire, avec quatre plongements imaginaires deux à deux conjugués, ce sont les corps de rupture des polynômes de degré 4 irréductibles ayant quatre racines complexes deux à deux conjuguées. Un exemple de tel polynôme est le polynôme cyclotomique $\Phi_8=X^4+1$.

`Solution de l'exercice 4.`

(a) On voit que l'équation à résoudre n'est autre que $(x^2-a)(x^2-b)(x^2-c)=0$. Puisque a,b,c ne sont pas des carrés d'entiers, il est clair que cette équation n'a pas de solution dans $\mathbf{Z}$, donc dans $\mathbf{Q}$. En outre, puisque $abc>0$, l'un au moins des trois a, b ou c est positif, donc c'est un carré dans $\mathbf{R}$, donc l'équation admet une solution dans $\mathbf{R}$. Soit p un nombre premier. Si p divise abc, il est clair que 0 est solution de l'équation dans $\mathbf{F}_p$. Sinon, on a par hypothèse $\left(\frac{abc}{p}\right)=1$, donc $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\left(\frac{c}{p}\right)=1$. Donc l'un au moins des trois symboles parmi $\left(\frac{a}{p}\right)$, $\left(\frac{b}{p}\right)$ et $\left(\frac{c}{p}\right)$ est égal à 1, ce qui signifie que l'un au moins des trois entiers a, b, c est un carré modulo p, donc l'équation a une solution dans $\mathbf{F}_p$.

(b)

i) On écrit $x=\frac{a}{b}$ et $y=\frac{u}{w}$ comme des fractions irréductibles. Alors la relation $y^4=2x^2+17$ devient $u^4=\frac{2a^2w^4}{b^2}+17w^4$, donc $b^2|2a^2w^4$, donc $b^2|2w^4$ (car $(a,b)=1$), donc $b^2|w^4$, donc $b|w^2$. Donc il existe $k\in\mathbf{Z}$ tel que $w^2=kb$. Alors l'équation devient $u^4=2(ak)^2+17w^4$, d'où le résultat avec $v:=ak\in\mathbf{Z}$. Il suffit maintenant de vérifier que $(u,v)=1$, ce qui est clair puisque $(u,w)=1$ et tout diviseur commun à u et v doit diviser w.

ii) La liste des puissances quatrième dans $\mathbf{F}_{17}$ est $0,1,4,13,16$, donc il est clair que 2 n'est pas une puissance 4-ième modulo 17. On peut aussi remarquer que les deux racines carrées 6 et -6 de 2 modulo 17 ne sont pas des carrés modulo 17.

iii) Réduisons l'égalité de la question (b) *i*) précédente modulo 17 : il reste $u^4\equiv 2v^2\ [17]$, et v n'est pas divisible par 17 (sinon u le serait aussi). Si v est un carré modulo 17, on en déduit que 2 est une puissance quatrième dans $\mathbf{F}_{17}$, ce qui contredit la question (b) *ii*). Donc v n'est pas un carré modulo 17.

iv) Soit p un diviseur premier de v. Alors modulo p, on a $u^4\equiv 17w^4\ [p]$, donc puisque p ne divise pas u, p ne divise pas w et $\left(\frac{17}{p}\right)=1$. Or $17\equiv 1\ [4]$, donc la loi de réciprocité quadratique assure que $\left(\frac{p}{17}\right)=1$

v) D'après la réponse à la question (b) *iv*), tout facteur premier p de v est un carré modulo 17, donc $\left(\frac{v}{17}\right)=1$ et v est un carré modulo 17. Ceci contredit la réponse à la question (b) *iii*), donc il n'existe pas de solution $(x,y)\in\mathbf{Q}^2$ de l'équation $y^4=2x^2+17$.

`Solution de l'exercice 5.`

a) Les F–automorphismes de E sont $\{1,\mathrm{Frob}_q,\dots,\mathrm{Frob}_q^{n-1}\}$, où $\mathrm{Frob}_q : x\longmapsto x^q$ est le Frobenius de E sur F.

b) Par conséquent

$$\mathrm{N}_{E/F}(x) = x\mathrm{Frob}_q(x)\cdots\mathrm{Frob}_q^{n-1}(x) = x\cdot x^q\cdots x^{q^{n-1}} = x^{1+q+\cdots+q^{n-1}} = x^s.$$

c) Comme s divise q^n-1, le groupe cyclique $E^\times$ d'ordre q^n-1 possède un unique sous-groupe d'ordre s, qui est l'ensemble des x dans E tels que $x^s=1$: c'est donc le noyau G de $\mathrm{N}_{E/F}$. Le nombre d'éléments du groupe quotient $E^\times/G$ est $(q^n-1)/s = q-1$, donc l'application injective $E^\times/G \to F^\times$ est surjective. Par conséquent la norme $\mathrm{N}_{E/F}$ est surjective.
d) Comme s et $q-1$ sont premiers entre eux, le groupe cyclique $E^\times$ est isomorphe au produit de ses deux groupes cycliques d'ordres respectivement s et $q-1$, le premier est G, le second est isomorphe à $F^\times$.