Université P. et M. Curie (Paris VI), Michel Waldschmidt
Deuxième semestre 2007/2008

Master de sciences et technologies 1ère année - Mention : Mathématiques et applications
Spécialité : Mathématiques Fondamentales MO11 : Théorie des nombres (12 ECTS)

Contrôle du 29 Février 2008 : corrigé

Exercice 1.

a) On écrit

$$x^3 - 2y^3 = (x - \sqrt[3]{2}y)(x^2 + \sqrt[3]{2}xy + \sqrt[3]{4}y^2).$$

Supposons (i) vrai. La forme quadratique $X^2 + \sqrt[3]{2}X + \sqrt[3]{4}$ a un discriminant négatif $-3\sqrt[3]{4}$, elle est donc minorée par $(3/4)\sqrt[3]{4} > 1$. On en déduit

$$|x^3 - 2y^3| \ge |x - \sqrt[3]{2}y|y^2 \ge y^3 \left|\sqrt[3]{2} - \frac{x}{y}\right| \ge c_1|y|^{3-\theta},$$

ce qui est (ii) avec $c_2 = c_1$.
Supposons maintenant (ii) vrai. Prenons

$$c_1 = \min\{1/2,\ 2^{\theta-1},\ c_2/9\}.$$

Soit $p/q \in \mathbf{Q}$. Si

$$\left|\sqrt[3]{2} - \frac{p}{q}\right| \ge \frac{1}{2},$$

l'inégalité (i) est satisfaite pour $q \ge 2$ puisque $c_1 \le 2^{\theta-1}$ et aussi pour $q = 1$ puisque $c_1 \le 1/2$. Comme $2^4 < 3^3$, on a $\sqrt[3]{2} < 3/2$ et on peut donc supposer $0 < p < 2q$. Il en résulte

$$p^2 + \sqrt[3]{2}pq + \sqrt[3]{4}q^2 \le (4 + 2\sqrt[3]{2} + \sqrt[3]{4})q^2 \le 9q^2.$$

Ainsi

$$c_2 q^{3-\theta} \le |p^3 - 2q^3| \le 9q^2|p - \sqrt[3]{2}q|,$$

et (i) en résulte puisque $c_1 \le c_2/9$.

b) On sait par le principe des tiroirs (voir le lemme 1.4) qu'il existe une infinité de nombres rationnels p/q tels que $|q\sqrt[3]{2} - p| \le 1/q$ (et même $1/\sqrt{5}q$ par le lemme 1.5). Le résultat se déduit donc du fait que (i) ne peut avoir lieu avec $\theta < 1$. Plus précisément en prenant $x = p$, $y = q$ on obtient

$$|x^3 - 2y^3| \le 9y^2|x - \sqrt[3]{2}y| \le 9|y|.$$

Exercice 2.

On pose $G_0 = 0$, $G_1 = 1$, et par récurrence on définit $G_n = 2G_{n-1} + G_{n-2}$ pour $n \ge 2$. Montrons,

par récurrence, que pour tout $n \geq 1$, que le nombre $u_n = G_n^2 - 2G_nG_{n-1} - G_{n-1}^2$ vérifie $u_n = (-1)^{n-1}$. C'est vrai pour $n = 1$, et pour $n \geq 2$ on a

$$u_n = G_n(G_n - 2G_{n-1}) - G_{n-1}^2 = G_nG_{n-2} - G_{n-1}^2 = -u_{n-1}.$$

Par conséquent le polynôme homogène $g(X,Y) = X^2 - 2XY - Y^2$ de degré 2 dont le discriminant est 8 vérifie

$$\min\big\{|g(x,y)| \ ; \ (x,y) \in \mathbf{Z} \times \mathbf{Z}, \ (x,y) \neq (0,0)\big\} = 1.$$

Il suffit donc de poser $f(X,Y) = g(X,Y)\sqrt{\Delta/8}$.

Exercice 3.

a) Les nombres 1, $\sqrt{2}$, $\sqrt{7}$ sont linéairement indépendants sur $\mathbf{Q}$. En effet une relation

$$a + b\sqrt{2} = c\sqrt{7}$$

avec a, b et c rationnels entraîne, en élevant au carré, $a^2 + 2b^2 - 7c^2 = -2ab\sqrt{2}$, donc $ab = 0$, puis $a = b = c = 0$. Il en résulte que $\sqrt{7}$ n'appartient pas au corps quadratique $\mathbf{Q}(\sqrt{2})$, d'où on déduit que le corps $\mathbf{Q}(\sqrt{2}, \sqrt{7})$ est de degré 4 sur $\mathbf{Q}$. Comme il est réel, il ne contient pas $i = \sqrt{-1}$, donc K est de degré 8 sur $\mathbf{Q}$. Une base de K comme $\mathbf{Q}$-espace vectoriel est

$$1, \ \sqrt{2}, \ \sqrt{7}, \ \sqrt{14}, \ i, \ i\sqrt{2}, \ i\sqrt{7}, \ i\sqrt{14}.$$

b) Le corps K est le corps de décomposition du $\mathbf{Q}$ du polynôme $(X^2-2)(X^2-7)(X^2+1)$, donc c'est une extension galoisienne de $\mathbf{Q}$. Pour $d = 2$, 7 ou -1, le nombre $\sqrt{d}$ a deux conjugués $\sqrt{d}$ et $-\sqrt{d}$ sur $\mathbf{Q}$. L'image des trois éléments $\sqrt{d}$ par un automorphisme σ de K détermine entièrement σ. Il en résulte que le groupe de Galois de K sur $\mathbf{Q}$ est isomorphe au produit $(\mathbf{Z}/2\mathbf{Z})^3$ de trois copies du groupe à deux éléments. Donc pour chacune des trois valeurs $d \in \{2, \ 7, \ -1\}$, il y a dans G un élément σ_d qui envoie $\sqrt{d}$ sur $-\sqrt{d}$ et qui laisse fixe les deux autres racines carrées. Par exemple σ_{-1} est la conjugaison complexe. Ainsi

$$G = \big\{1, \ \sigma_2, \ \sigma_7, \ \sigma_{-1}, \ \sigma_2\sigma_7, \ \sigma_2\sigma_{-1}, \ \sigma_7\sigma_{-1}, \ \sigma_2\sigma_7\sigma_{-1}\big\}$$

Chaque élément de G autre que l'élément neutre est d'ordre 2, il y a donc 7 sous-groupes d'ordre 2. Il y a aussi 7 sous-groupes d'ordre 4. Une des manières de le voir est de dire qu'il y a $\binom{7}{2} = 21$ façons de choisir deux éléments σ et τ d'ordre 2 dans G, cela donne un sous-groupe $\{\sigma, \ \tau, \ \sigma\tau\}$ d'ordre 4, et on trouve le même sous groupe pour les trois choix $\{\sigma, \ \tau\}$, $\{\sigma, \ \sigma\tau\}$, $\{\sigma\tau, \ \tau\}$.

Il y a donc 7 sous-corps de K quadratiques sur $\mathbf{Q}$ et 7 sous-corps biquadratiques (de degré 4) sur $\mathbf{Q}$, ce qui fait un total de 16 sous-corps (en comptant $\mathbf{Q}$ et K). Les 7 corps

quadratiques correspondent par la théorie de Galois aux sous-groupes d'ordre 4, ils sont engendrés respectivement par

$$\sqrt{2},\ \ \sqrt{7},\ \ i,\ \ \sqrt{14},\ \ i\sqrt{2},\ \ i\sqrt{7},\ \ i\sqrt{14}.$$

Les 7 sous-corps biquadratiques, correspondant par Galois aux sous-groupes d'ordre 2, sont engendrés par les couples

$$(\sqrt{2},\ \sqrt{7}),\ \ (\sqrt{2},\ i),\ \ (\sqrt{7},\ i),\ \ (i\sqrt{2},\ \sqrt{7}),\ \ (\sqrt{2},\ i\sqrt{7}),\ \ (\sqrt{14},\ i),\ \ (\sqrt{14},\ i\sqrt{2}).$$

Bien entendu il y a d'autres façons de choisir ces couples, puisque

$$\mathbf{Q}(\sqrt{a},\sqrt{b}) = \mathbf{Q}(\sqrt{a},\sqrt{ab}) = \mathbf{Q}(\sqrt{ab},\sqrt{b}).$$

Dans le tableau ci-dessous les signes dans la ligne commençant par σ_2 signifient

$$\sigma_2(\sqrt{2}) = -\sqrt{2},\ \ \sigma_2(\sqrt{7}) = +\sqrt{7}\ \ \sigma_2(i) = +i,\ \ \sigma_2(\sqrt{14}) = -\sqrt{14},$$

$$\sigma_2(i\sqrt{2}) = -i\sqrt{2},\ \ \sigma_2(i\sqrt{7}) = +i\sqrt{7},\ \ \sigma_2(i\sqrt{14}) = -i\sqrt{14},$$

et la dernière colonne indique le sous-corps fixé par le sous-groupe de la première colonne ; ainsi pour $\{1,\sigma_2\}$ c'est $\mathbf{Q}(i,\ \sqrt{7})$ qu'on peut aussi écrire $\mathbf{Q}(i,\ i\sqrt{7})$ ou $\mathbf{Q}(\sqrt{7},\ i\sqrt{7})$. La dernière ligne indique le sous-groupe associé au corps quadratique engendré par la racine carrée de la première ligne. Ainsi $\mathbf{Q}(\sqrt{2})$ est le sous-corps fixé par le sous-groupe $\{1,\ \sigma_7,\ \sigma_{-1},\ \sigma_7\sigma_{-1}\}$, que l'on note simplement $<\sigma_7,\ \sigma_{-1}>$.

Il n'y a que 7 lignes et 7 colonnes car on n'a pas indiqué l'élément neutre du groupe de Galois ni les images par les éléments du groupe de Galois de l'unité 1 de K.

	$\sqrt{2}$	$\sqrt{7}$	i	$\sqrt{14}$	$i\sqrt{2}$	$i\sqrt{7}$	$i\sqrt{14}$	$K^{<\sigma>}$
σ_2	$-$	$+$	$+$	$-$	$-$	$+$	$-$	$(i,\ \sqrt{7})$
σ_7	$+$	$-$	$+$	$-$	$+$	$-$	$-$	$(i,\ \sqrt{2})$
σ_{-1}	$+$	$+$	$-$	$+$	$-$	$-$	$-$	$(\sqrt{2},\ \sqrt{7})$
$\sigma_2\sigma_7$	$-$	$-$	$+$	$+$	$-$	$-$	$+$	$(i,\ \sqrt{14})$
$\sigma_2\sigma_{-1}$	$-$	$+$	$-$	$-$	$+$	$-$	$+$	$(\sqrt{7},\ i\sqrt{2})$
$\sigma_7\sigma_{-1}$	$+$	$-$	$-$	$-$	$-$	$+$	$+$	$(\sqrt{2},\ i\sqrt{7})$
$\sigma_2\sigma_7\sigma_{-1}$	$-$	$-$	$-$	$+$	$+$	$+$	$-$	$(i\sqrt{2},\ \sqrt{14})$
	$<\sigma_7,\ \sigma_{-1}>$	$<\sigma_2,\ \sigma_{-1}>$	$<\sigma_2,\ \sigma_7>$	$<\sigma_{-1},\ \sigma_2\sigma_7>$	$<\sigma_7,\ \sigma_2\sigma_{-1}>$	$<\sigma_2,\ \sigma_7\sigma_{-1}>$	$<\sigma_2\sigma_7,\ \sigma_2\sigma_{-1}>$	

Un élément primitif de $\mathbf{Q}(\sqrt{a},\sqrt{b})$ (avec a et b deux éléments distincts de $\{2,\ 7,\ -1\}$) est $\sqrt{a}+\sqrt{b}$, et un élément primitif de K sur $\mathbf{Q}$ est $\sqrt{2}+\sqrt{7}+i$: ses huit images par les éléments du groupe de Galois sont distinctes.

Le groupe de Galois d'un corps quadratique $\mathbf{Q}(\sqrt{d})$ est cyclique d'ordre 2, l'élément différent de l'élément neutre envoie $\sqrt{d}$ sur $-\sqrt{d}$.

Le groupe de Galois sur $\mathbf{Q}$ d'un corps biquadratique $\mathbf{Q}(\sqrt{a},\ \sqrt{b})$ est d'ordre 4, produit de deux groupes cycliques d'ordre 2, un élément envoie $\sqrt{a}$ sur $-\sqrt{a}$ et laisse $\sqrt{b}$ fixe, un autre laisse $\sqrt{a}$ fixe et envoie $\sqrt{b}$ sur $-\sqrt{b}$, leur produit envoie $\sqrt{a}$ sur $-\sqrt{a}$ et $\sqrt{b}$ sur $-\sqrt{b}$ (il fixe $\sqrt{ab}$).

c) Les racines du polynôme Y^2+2Y-7 sont $\alpha=2\sqrt{2}-1$ et $\beta=-2\sqrt{2}-1$. On a bien sûr $\alpha+\beta=-2$ et $\alpha\beta=-7$. Aussi $\mathbf{Q}(\alpha)=\mathbf{Q}(\gamma)=\mathbf{Q}(\sqrt{2})$.

Posons $\gamma=\sqrt{\alpha}$ et $\delta=\sqrt{|\beta|}$ en prenant les racines positives. Alors les racines de $f(X)=X^4+2X^2-7$ sont γ, $-\gamma$, $i\delta$, $-i\delta$. Remarquons que $\gamma\delta=\sqrt{7}$.

Comme il n'y a pas de couple (a,b) de nombres rationnels satisfaisant $(a+b\sqrt{2})^2=2\sqrt{2}-1$, le nombre α n'est pas un carré dans $\mathbf{Q}(\sqrt{2})$ et le le polynôme f est irréductible sur $\mathbf{Q}$. Un corps de rupture de f sur $\mathbf{Q}$ est $F=\mathbf{Q}(\gamma)$ qui est de degré 4 sur $\mathbf{Q}$ et de degré 2 sur $\mathbf{Q}(\sqrt{2})$. Ce corps F est réel, donc il ne contient pas $i\delta$, par conséquent le corps de décomposition de f sur $\mathbf{Q}$ est une extension quadratique de F :

$$E=\mathbf{Q}(\gamma,i\delta)=\mathbf{Q}(\gamma,i\sqrt{7})$$

qui est donc de degré 8 sur $\mathbf{Q}$.

Comme l'extension $F/\mathbf{Q}$ n'est pas galoisienne (le polynôme f a une racine dans F sans y être totalement décomposé), l'extension $E/\mathbf{Q}$ n'est pas abélienne (le groupe de Galois contient un sous-groupe qui n'est pas normal). Mais l'extension $K/\mathbf{Q}$ est abélienne, il en résulte que le corps E n'est pas un sous-corps de K. Par conséquent le corps de décomposition de f sur K, qui est le compositum de K et E, est l'extension $\mathbf{Q}(\gamma,\ \sqrt{7},\ i)$, qui est une extension quadratique de K, donc de degré 16 sur $\mathbf{Q}$.

Exercice 4.

a) C'est du cours ; on paramètre le cercle $u^2+v^2=1$ avec $u>0$ et $v>0$ en prenant t la pente de la droite joignant (u,v) à $(-1,0)$ dont l'équation est donc $v=t(u+1)$ ce qui donne le résultat.

b) Si D est congruent, on écrit $D=ab/2$ avec $a^2+b^2=c^2$, puis $a=c(1-t^2)/(1+t^2)$, $b=2ct/(1+t^2)$. On pose $x=-t$, $y=(1+t^2)/c$ et on a

$$D=\frac{ab}{2}=c^2\cdot\frac{t(1-t^2)}{(1+t^2)^2}=\frac{x^3-x}{y^2}\cdot$$

Inversement, si (x,y) est une solution rationnelle de l'équation $Dy^2=x^3-x$ avec $y\neq 0$, on pose $t=-x$, $c=(1+t^2)/y$, $b=2tc/(1+t^2)$, $a=c(1-t^2)/(1+t^2)$ et on vérifie $D=ab/2$ avec $a^2+b^2=c^2$.

c) La courbe $C_D(\mathbf{R})$ a deux composantes connexes : un ovale dans la région $-1\leq x\leq 0$ et une courbe avec direction asymptotique verticale dans la région $x\geq 1$. L'intersection d'une droite avec $C_D(\mathbf{R})$ donne une équation de degré 3 : $x^3-\sigma_1x^2+\sigma_2x-\sigma_3$. Si celle-ci possède 2 solutions x_1,x_2 alors elle en possède 3 la dernière étant donnée par $x_3=\sigma_1-x_1-x_2\in\mathbf{Q}$. On en déduit ainsi que l'application qui à un point $P\in C_D(\mathbf{R})$ associe l'intersection P'

de la droite passant par P et $(-1,0)$, échange les deux composantes connexes et préserve $C_D(\mathbf{Q})$, d'où le résultat.

d i) On écrit $x = a/b$ avec $a \wedge b = 1$; on obtient alors $b^4y^2 = ab(a-b)(a+b)$ et donc comme a (resp. b) est premier à $b(a-b)(a+b)$ (resp. $a(a-b)(a+b)$), a et b sont des carrés dans $\mathbf{N}$ et donc x est un carré dans $\mathbf{Q}$.

d ii) En outre $(a-b) \wedge (a+b)|2$ de sorte que $a \pm b$ sont soient des carrés soit des doubles de carrés et donc $x \pm 1$ sont soit des carrés soit des doubles de carrés.

d iii) On vérifie $x-1 = (t+u)(u+v)$ et $x+1 = (t+v)(u+v)$, de sorte que f est bien à valeurs dans $C_1(\mathbf{Q})$.

Soit $(x,y) \in C_1(\mathbf{Q})$ avec $y \neq 0$. Posons

$$t = \frac{x^2+1}{2y}, \quad u = \frac{x^2-2x-1}{2y}, \quad v = \frac{x^2+2x-1}{2y}.$$

On a

$$t+u = \frac{x^2-x}{y}, \quad t+v = \frac{x^2+x}{y}, \quad u+v = \frac{x^2-1}{y},$$

ce qui permet de vérifier $(t+u)(t+v) = x$ et $(t+u)(t+v)(u+v) = y$. L'égalité $f \circ g(x,y) = (x,y)$ en résulte, donc f est surjective. Il reste à montrer que f est injective, c'est à dire qu'étant donné $(x,y) \in C_1(\mathbf{Q}) \setminus \{(-1,0),(0,0),(1,0)\}$, il y a un unique $(t,u,v) \in X(\mathbf{Q})$ tel que $f(t,u,v) = (x,y)$. En effet de $u+v = y/x$ et $v^2-u^2 = 2$ on déduit $v-u = 2x/y$ puis

$$2u = \frac{y}{x} - \frac{2x}{y} = \frac{x^2-2x-1}{y} \quad \text{et} \quad 2v = \frac{y}{x} + \frac{2x}{y} = \frac{x^2+2x-1}{y}.$$

Chacune des conditions $t^2-u^2 = 1$ et $v^2-t^2 = 1$ montre que t est fixé au signe près. Enfin comme $(t+u)(t+v) - (-t+u)(-t+v) = 2t(u+v) \neq 0$ une seule des valeurs de $(t+u)(t+v)$ et $(-t+u)(-t+v)$ peut être égale à x.

e) Que 1 n'est pas un nombre congruent équivaut, d'après ce qui précède, au fait qu'il n'y a pas de couple rationnel (x,y) avec $y \neq 0$ vérifiant $y = x^3 - x$.