Faculté des Sciences et Techniques de Limoges **2006-2007**

Examen partiel d'Algèbre de Master 1

Soit $\theta = \sqrt{3} + \sqrt[3]{3} \in \mathbb{R}$; on note $K = \mathbb{Q}(\sqrt{3})$ et $L = \mathbb{Q}(\theta)$

[K (resp.L) est le sous-corps de $\mathbb{C}$ engendré par $\sqrt{3}$ (resp. par θ)].

1) Montrer que $K = \{x + y\sqrt{3} \in \mathbb{C}; x, y \in \mathbb{Q}\}$.

2) Soient (a, a') et (b, b') deux couples d'entiers relatifs premiers entre eux.

a) Calculer le polynôme minimal sur $\mathbb{Q}$ de $\dfrac{a}{a'} + \dfrac{b}{b'}\sqrt{3} \in K$.

b) À quelles conditions est-il à coefficients entiers ?

c) En déduire que l'anneau des entiers de K est $\mathbb{Z}[\sqrt{3}]$.

d) Vérifier que le corps des fractions de $\mathbb{Z}[\sqrt{3}]$ est bien K.

3) Calculer $(2 + \sqrt{3})(2 - \sqrt{3})$ et montrer que l'anneau $\mathbb{Z}[\sqrt{3}]$ a une infinité d'éléments inversibles.

4) Calculer le polynôme minimal de $\sqrt[3]{3}$ sur $\mathbb{Q}$.

5a) Donner un polynôme à coefficients dans K, de degré 3, dont θ soit racine.

b) En déduire que $\sqrt{3} \in L$, puis que $\sqrt[3]{3} \in L$.

6a) Montrer que le degré $[L : \mathbb{Q}]$ est un multiple de 6.

b) En déduire le polynôme minimal de θ sur $\mathbb{Q}$.

c) Quels sont les conjugués de θ sur $\mathbb{Q}$?

7) Calculer la norme $N_{L/\mathbb{Q}}(1 + \theta)$ et la trace $Tr_{L/\mathbb{Q}}(1 + \theta)$ de $1 + \theta$ dans l'extension $L/\mathbb{Q}$.

8a) Décrire le groupe $\mathrm{Aut}(L)$.

b) L'extension L/K est-elle galoisienne ?

Soit $M = L(j)$ avec $j = e^{2i\pi/3} \in \mathbb{C}$.

9) Calculer $[M : \mathbb{Q}]$ et déterminer $M \cap \mathbb{R}$.

10) Montrer que le sous-groupe $\mathrm{Aut}_{\mathbb{Q}(j)}(M)$ du groupe $\mathrm{Aut}(M)$ est isomorphe au groupe cyclique $\mathbb{Z}/6\mathbb{Z}$.

11) Montrer comment construire un sous-groupe d'ordre 12 du groupe $\mathrm{GL}(12, \mathbb{Z})$ des matrices carrées inversibles à coefficients dans $\mathbb{Z}$ à 12 lignes et 12 colonnes.

Corrigé

1) Comme on a $\forall x, x', y, y' \in \mathbb{Q}$, $\quad (x + y\sqrt{3}) - (x' + y'\sqrt{3}) = (x - x') + (y - y')\sqrt{3}$,
$(x + y\sqrt{3})(x' + y'\sqrt{3}) = xx' + 3yy' + (xy' + yx')\sqrt{3}$ et
$(x + y\sqrt{3})^{-1} = x/(x^2 - 3y^2) - y/(x^2 - 3y^2)\sqrt{3}$,
l'ensemble $\{x + y\sqrt{3} \in \mathbb{C} \,; x, y \in \mathbb{Q}\}$ est un sous-corps de $\mathbb{C}$ qui contient $\sqrt{3}$ et comme tout sous-corps de $\mathbb{C}$ contenant $\sqrt{3}$ le contient, c'est bien le sous-corps K de $\mathbb{C}$ engendré par $\sqrt{3}$.

2a) Le nombre réel $x + y\sqrt{3}$ est racine du polynôme $X^2 - 2xX + x^2 - 3y^2 \in \mathbb{Q}[X]$ qui est irréductible sur $\mathbb{Q}$ si et seulement si $y \neq 0$ parce que $\sqrt{3} \notin \mathbb{Q}$: c'est donc le polynôme minimal de $x + y\sqrt{3}$ sur $\mathbb{Q}$ si et seulement si $y \neq 0$: dans ce dernier cas le polynôme minimal est $X-x$. Pour $x=a/a'$ (resp. $y=b/b'$) avec $a\in\mathbb{Z}, a'\in\mathbb{N}^*$ premiers entre eux (resp. $b\in\mathbb{Z}, b'\in\mathbb{N}^*$, premiers entre eux), le polynôme minimal de $z=\frac{a}{a'}+\frac{b}{b'}\sqrt{3}$ est donc $X^2-2\frac{a}{a'}X+\frac{a^2}{a'^2}-3\frac{b^2}{b'^2}$ si $b\neq 0$ sinon c'est $X-\frac{a}{a'}$.

2b) Il est à coefficients dans $\mathbb{Z}$ si $a'=1$ et $b=0$ ou si $a'\mid 2a$ et $\frac{a^2}{a'^2}-3\frac{b^2}{b'^2}\in\mathbb{Z}$; $a'\mid 2a\Rightarrow a'=1$ ou 2 car a et a' sont premiers entre eux et la deuxième condition devient $3\frac{b^2}{b'^2}\in\mathbb{Z}$ donc $b'^2\mid 3b^2$ si $a'=1$ et $\frac{a^2}{4}-3\frac{b^2}{b'^2}\in\mathbb{Z}$ donc $b'^2\mid 12b^2$ si $a'=2$. Comme b^2 et b'^2 sont premiers entre eux, dans le premier cas, b'^2 doit diviser 3, donc $b'=1$ ou 3; mais $b'\neq 3$ car sinon $9\mid 3b^2$ et $3\mid b$; dans le second cas, b'^2 doit diviser 12 donc $b'=1$, 2, 3 ou 6; mais $b'\neq 3$ ou 6 car sinon $9\mid 3b^2$ et $3\mid b$ et $b'\neq 2$ car sinon a et b sont impairs et $4\mid a^2-3b^2$ alors que a^2-3b^2 est $\equiv 2 \bmod 4$.

2c) Le nombre algébrique z est un entier algébrique si et seulement son polynôme minimal est à coefficients dans $\mathbb{Z}$. Dans tous les cas, la seule possibilité pour que z soit un entier algébrique est donc que $a'=b'=1$, donc l'anneau des entiers de $K=\mathbb{Q}(\sqrt{3})$ est $\mathbb{Z}[\sqrt{3}]$.

2d) Le corps des fractions de $\mathbb{Z}[\sqrt{3}]$ est $\subset K$ puisque K est un corps qui contient $\mathbb{Z}[\sqrt{3}]$; d'autre part il contient $\sqrt{3}$ et donc aussi le sous-corps de $\mathbb{C}$ engendré par $\sqrt{3}$ qui est K.

3) Comme $(2+\sqrt{3})(2-\sqrt{3})=1$, $2+\sqrt{3}$ et $2-\sqrt{3}$ sont deux éléments de l'anneau $\mathbb{Z}[\sqrt{3}]$ inverses l'un de l'autre; donc $(\,(2+\sqrt{3})^n\,)$ est une suite strictement croissante d'éléments inversibles de l'anneau $\mathbb{Z}[\sqrt{3}]$.

4) Les racines du polynôme X^3-3 sont $\sqrt[3]{3}$, $j\sqrt[3]{3}$ et $j^2\sqrt[3]{3}$ où $j=e^{\frac{2i\pi}{3}}\in\mathbb{C}$ (comme on peut le voir en remarquant que le quotient de deux telles racines est une racine de X^3-1). Donc c'est un polynôme de degré $3\in\mathbb{Q}[X]$ qui n'a pas de racines dans $\mathbb{Q}$; il est bien irréductible et par suite, c'est le polynôme minimal de $\sqrt[3]{3}$ sur $\mathbb{Q}$.

5a) Comme $(\theta-\sqrt{3})^3=3$, θ est racine du polynôme $X^3-3\sqrt{3}X^2+9X-3\sqrt{3}\in K[X]$.

5b) $\sqrt{3}=\dfrac{\theta^3+9\theta-3}{3(\theta^2+1)}\in\mathbb{Q}(\theta)=L\;\Rightarrow\;\sqrt[3]{3}=\theta-\sqrt{3}\in\mathbb{Q}(\theta)=L$.

6a) Comme $L\supset K$ et $\mathbb{Q}(\sqrt[3]{3})$, d'après le théorème de multiplicativité des degrés, $[L:\mathbb{Q}]$ est multiple de $[K:\mathbb{Q}]=2$ et de $[\mathbb{Q}(\sqrt[3]{3}):\mathbb{Q}]=3$ (d'après la question 4) donc de 6.

6b) Comme $\left(\dfrac{\theta^3+9\theta-3}{3(\theta^2+1)}\right)^2=3$, θ est racine du polynôme $(X^3+9X-3)^2-27(X^2+1)^2\in\mathbb{Z}[X]$ dont on constate, sans qu'il soit nécessaire de le développer, qu'il est unitaire de degré 6. Comme, par ailleurs, $[\mathbb{Q}(\theta):\mathbb{Q}]\geq 6$, il est irréductible et c'est le polynôme minimal de θ sur $\mathbb{Q}$.

6c) Les conjugués de θ sur $\mathbb{Q}$ sont les images de θ par les 6 plongements distincts de L dans $\mathbb{C}$ qui appliquent $\sqrt{3}$ sur l'un de ses conjugués $\pm\sqrt{3}$ et $\sqrt[3]{3}$ sur l'un de ses conjugués $\sqrt[3]{3}, j\sqrt[3]{3}, j^2\sqrt[3]{3}$; d'où 6 conjugués possibles pour θ : $\sqrt{3}+\sqrt[3]{3}$, $\sqrt{3}+j\sqrt[3]{3}$, $\sqrt{3}+j^2\sqrt[3]{3}$, $-\sqrt{3}+\sqrt[3]{3}$, $-\sqrt{3}+j\sqrt[3]{3}$, $-\sqrt{3}+j^2\sqrt[3]{3}$ et comme θ est de degré 6, il n'est même pas nécessaire de vérifier qu'ils sont deux à deux distincts.

7)La norme $N_{L/\mathbb{Q}}(1+\theta)$ est le produit des conjugués de $1+\theta$ sur $\mathbb{Q}$; c'est aussi le terme constant du polynôme minimal de $1+\theta$ sur $\mathbb{Q}$; or si $P(X)$ est le polynôme minimal de

θ sur $\mathbb{Q}$, alors $P(X-1)$ est celui de $1+\theta$ sur $\mathbb{Q}$ parce que $1+\theta$ est aussi de degré 6 et racine de $P(X-1)$; il est facile de calculer ce terme constant, grâce à la question 6b) et sans même qu'il soit nécessaire de développer le polynôme. On trouve 61.
Pour la trace, c'est plus facile :
$Tr_{L/\mathbb{Q}}(1+\theta) =$

$$(1+\sqrt{3}+\sqrt[3]{3})+(1+\sqrt{3}+j\sqrt[3]{3})+(1+\sqrt{3}+j^2\sqrt[3]{3})+(1-\sqrt{3}+\sqrt[3]{3})+(1-\sqrt{3}+j\sqrt[3]{3},)+(1-\sqrt{3}+j^2\sqrt[3]{3})$$

$= 6.$

8a) Comme $L=\mathbb{Q}(\theta)$ tout plongement σ de L dans $\mathbb{C}$ est déterminé par $\sigma(\theta)$ et pour que σ soit un automorphisme de L il faut et il suffit que $\sigma(\theta)\in L$. Or il n'y a que deux conjugués de θ qui sont réels : θ et $-\sqrt{3}+\sqrt[3]{3}$; ils sont dans L d'où deux automorphismes de L : id_L et $\theta \mapsto -\sqrt{3}+\sqrt[3]{3}$, c'est à dire : $\sqrt{3}\mapsto -\sqrt{3}, \sqrt[3]{3}\mapsto \sqrt[3]{3}$.
8b) Comme id_L est le seul K-automorphisme de L, L/K n'est sûrement pas galoisienne.
9) Comme $M\supset L$, $[M:\mathbb{Q}]$ est un multiple de $[L:\mathbb{Q}]=6$; comme $L\subset\mathbb{R}$ et que $j\in M\smallsetminus\mathbb{R}$, $M\neq L$ et donc $[M:\mathbb{Q}]\geq 12$; mais j est de degré ≤ 2 sur L (puisque racine de $X^2+X+1\in L[X]$) donc $[M:L]\leq 2$ et $[M:\mathbb{Q}]\leq 12$, d'où $[M:\mathbb{Q}]=12$. Comme $L\subset M\cap\mathbb{R}\subsetneq M$ avec $[M:L]=2$, on a $L=M\cap\mathbb{R}$.
10) L'extension $M/\mathbb{Q}$ est galoisienne parceque M est le corps des racines du polynôme minimal de θ sur $\mathbb{Q}$. D'autre part $[M:\mathbb{Q}(j)]=\dfrac{[M:\mathbb{Q}]}{[\mathbb{Q}(j):\mathbb{Q}]}=6$ et $\{1,\sqrt{3},\sqrt[3]{3},\sqrt{3}\sqrt[3]{3},\sqrt[3]{9},\sqrt{3}\sqrt[3]{9}\}$ est une base de M sur $\mathbb{Q}(j)$; donc $\sqrt{3}\mapsto-\sqrt{3}$, $\sqrt[3]{3}\mapsto j\sqrt[3]{3}$ détermine un $\mathbb{Q}(j)$-automorphisme σ de M. Calculons : $\sigma(\sqrt{3})=-\sqrt{3}$, $\sigma^3(\sqrt{3})=-\sqrt{3}$, $\sigma^5(\sqrt{3})=-\sqrt{3}$ et $\sigma^2(\sqrt[3]{3})=j^2\sqrt[3]{3}$, $\sigma^4(\sqrt[3]{3})=j^2\sqrt[3]{3}$; donc $\sigma,\sigma^2,\sigma^3,\sigma^4,\sigma^5\neq\mathrm{id}_M$ et $\sigma^6=\mathrm{id}_M$. Le sous-groupe de $\mathrm{Aut}(M)$ engendré par σ est donc un groupe cyclique d'ordre 6 et comme $[M:\mathbb{Q}(j)]=6$ c'est le groupe de Galois $\mathrm{Gal}(M/\mathbb{Q}(j))$.
11) Il suffit de calculer les matrices des éléments de $\mathrm{Aut}(M)$ dans la base

$$(1,\sqrt{3},j,j\sqrt{3},\sqrt[3]{3},\sqrt[3]{9},\sqrt{3}\sqrt[3]{3},\sqrt{3}\sqrt[3]{9},j\sqrt[3]{3},j\sqrt[3]{9},j\sqrt{3}\sqrt[3]{3},j\sqrt{3}\sqrt[3]{9})$$

(ou dans toute autre base de M sur $\mathbb{Q}$). Elles constituent un groupe pour la multiplication.