UNIVERSITÉ DE BORDEAUX I 2008-2009
MASTER DE MATHÉMATIQUES *1ère année*
Option : Théorie algébrique des nombres.

Corrigé DM 1

1. Le polynôme minimal de θ est X^2-3, d'Eisenstein en $p=2$ donc irréductible dans $\mathbb{Q}[X]$, moyennant quoi $[K:\mathbb{Q}]=3$. En outre θ est entier puisque X^2-3 est unitaire et à coefficients dans $\mathbb{Z}$. On a $\mathrm{Disc}\left(1,\theta,\theta^2\right)=\mathrm{Disc}X^2-3=-27\cdot 4$. Ainsi, en vertu de la relation $\mathrm{Disc}\left(1,\theta,\theta^2\right)=[\mathcal{O}_K:\mathbb{Z}[\theta]]^2 d_k$, l'indice $[\mathcal{O}_K:\mathbb{Z}[\theta]]$, s'il est différent de 1, ne peut être divisible que par 2 ou 3.
2. (a) Considérons la factorisation de l'idéal $\mathfrak{p}=\theta\mathcal{O}_K$ en produit d'idéaux maximaux, $\mathfrak{p}=\prod_{i=1}^t \mathfrak{p}_i^{\alpha_i}$, $\alpha_i\in\mathbb{N}$. Comme $\mathfrak{p}^3=\theta^3\mathcal{O}_K=2\mathcal{O}_K$, on conclut que $2\mathcal{O}_K=\prod_{i=1}^t \mathfrak{p}_i^{3\alpha_i}$. Si l'on note f_i le degré résiduel de $\mathfrak{p}_i$, on doit avoir
$$\sum_{i=1}^{t} 3\alpha_i f_i = 3.$$
Donc $t=1$ et $\mathfrak{p}=\mathfrak{p}_1$ est un idéal premier, de degré résiduel 1. En particulier, $\mathcal{O}_K/\mathfrak{p}\simeq\mathbb{F}_2$.

   (b) L'homomorphisme de $\mathbb{Z}[X]$ dans $\mathbb{F}_2$, qui à $Q(X)\in\mathbb{Z}[X]$ associe $Q(0) \mod 2$, est clairement surjectif, et il est identiquement nul sur l'idéal engendré par $P(X)=X^2-3$, puisque $P(0)=-2\equiv 0 \mod 2$. Par conséquent il induit, par le théorème de factorisation, un homomorphisme surjectif $\phi:\mathbb{Z}[\theta]\simeq\mathbb{Z}[X]/\left(X^2-3\right)\twoheadrightarrow\mathbb{F}_2$, défini explicitement par
$$\phi\left(\sum_{i=0}^{m} a_i\theta^i\right)=a_0 \mod 2.$$
Clairement, $\theta\mathbb{Z}[\theta]$ est contenu dans $\ker\phi$. Inversement, si $x=\sum_{i=0}^m a_i\theta^i$ appartient au noyau de ϕ, alors a_0 est divisible par $2=\theta^3$ et x appartient à $\theta\mathbb{Z}[\theta]$. Ainsi, $\ker\phi=\theta\mathbb{Z}[\theta]$ et $\mathbb{Z}[\theta]/\theta\mathbb{Z}[\theta]\simeq\mathbb{F}_2$ par le théorème de factorisation. En particulier $\theta\mathbb{Z}[\theta]$ est un idéal maximal de $\mathbb{Z}[\theta]$. Finalement, on observe que l'idéal $\mathfrak{p}\cap\mathbb{Z}[\theta]$ contient trivialement $\theta\mathbb{Z}[\theta]$, et lui est donc égal par maximalité.

   (c) L' homomorphisme naturel de $\mathbb{Z}[\theta]$ dans $\mathcal{O}_K/\mathfrak{p}$ obtenu en composant l'injection canonique de $\mathbb{Z}[\theta]$ dans $\mathcal{O}_K$ et la surjection canonique de $\mathcal{O}_K$ sur $\mathcal{O}_K/\mathfrak{p}$ a pour noyau $\mathfrak{p}\cap\mathbb{Z}[\theta]=\theta\mathbb{Z}[\theta]$. On en déduit (théorème de factorisation), un homomorphisme injectif de $\mathbb{Z}[\theta]/\theta\mathbb{Z}[\theta]$ dans $\mathcal{O}_K/\mathfrak{p}$, qui est nécessairement surjectif puisque $\mathbb{Z}[\theta]/\theta\mathbb{Z}[\theta]$ et $\mathcal{O}_K/\mathfrak{p}$ sont tous les deux isomorphes à $\mathbb{F}_2$. Cela signifie que tout élément de $\mathcal{O}_K$ est équivalent modulo $\mathfrak{p}$, à un élément de $\mathbb{Z}[\theta]$, ou autrement dit que $\mathcal{O}_K=\mathbb{Z}[\theta]+\mathfrak{p}=\mathbb{Z}[\theta]+\theta\mathcal{O}_K$, d'où l'on tire
$$\mathcal{O}_K=\mathbb{Z}[\theta]+\theta\mathcal{O}_K=\mathbb{Z}[\theta]+\theta(\mathbb{Z}[\theta]+\theta\mathcal{O}_K)=\mathbb{Z}[\theta]+\theta^2\mathcal{O}_K$$
puis finalement
$$\mathcal{O}_K=\mathbb{Z}[\theta]+\theta^2(\mathbb{Z}[\theta]+\theta\mathcal{O}_K)=\mathbb{Z}[\theta]+\theta^3\mathcal{O}_K=\mathbb{Z}[\theta]+2\mathcal{O}_K.$$
3. Démonstration strictement identique à la précédente.
4. Supposons que p divise $|G|$. Alors G contient au moins un élément x_0 d'ordre p. En particulier, l'application de G dans lui-même $x\mapsto x^p$ n'est pas injective (si e désigne l'élément neutre de G, x_0 et e ont même image). Elle n'est donc pas non plus surjective (une application d'un ensemble fini dans lui-même est surjective si et seulement si elle est injective), d'où la conclusion.

5. Considérons le groupe abélien fini $G = \mathcal{O}_K/\mathbb{Z}[\theta]$. Les relations

$$\mathcal{O}_K = \mathbb{Z}[\theta] + 2\mathcal{O}_K. \tag{1}$$

et

$$\mathcal{O}_K = \mathbb{Z}[\theta] + 3\mathcal{O}_K. \tag{2}$$

obtenues précédemment signifient exactement que $2G = G$ et $3G = G$. Le lemme précédent montre alors que $[\mathcal{O}_K : \mathbb{Z}[\theta]]$ n'est divisible ni par 2, ni par 3. Vu le résultat obtenu à la question 1, on conclut que $\mathcal{O}_K = \mathbb{Z}[\theta]$.

Exercice 1. *Un théorème de Stickelberger.*

1. On développe le déterminant $\det((\sigma_i(e_j))_{1\leq i,j\leq n}$ selon la formule

$$\begin{aligned}\det((\sigma_i(e_j))_{1\leq i,j\leq n} &= \sum_{\phi\in S_n} \epsilon(\phi)\sigma_1(e_{\phi(1)})\cdots\sigma_n(e_{\phi(n)}) \\ &= \sum_{\phi\in A_n} \sigma_1(e_{\phi(1)})\cdots\sigma_n(e_{\phi(n)}) - \sum_{\phi\in S_n\setminus A_n} \sigma_1(e_{\phi(1)})\cdots\sigma_n(e_{\phi(n)}) \\ &= P - N.\end{aligned}$$

2. $P + N$ et PN sont entiers sur $\mathbb{Z}$, puisqu'ils sont obtenus par sommes et produits d'éléments entiers sur $\mathbb{Z}$.
3. Soit $\tau \in \mathrm{Gal}(L/\mathbb{Q})$. Pour tout $i = 1\ldots n$, $\tau\circ\sigma_i$ est un plongement de K dans $\mathbb{C}$. Autrement dit, il existe une permutation $\rho \in S_n$ telle que $\tau\circ\sigma_i = \sigma_{\rho(i)}$ pour $i = 1\ldots n$. On en déduit que

$$\tau(P) = \sum_{\phi\in A_n}\prod_{i=1}^{n} \tau\circ\sigma_i(e_{\phi(i)}) = \sum_{\phi\in A_n}\prod_{i=1}^{n} \sigma_{\rho(i)}(e_{\phi(i)}) = \sum_{\phi\in A_n}\prod_{i=1}^{n} \sigma_i(e_{\phi\rho^{-1}(i)}).$$

Par conséquent $\tau(P) = \begin{cases} P \text{ si } \rho\in A_n \\ N \text{ sinon}\end{cases}$. De la même façon, $\tau(N) = \begin{cases} N \text{ si } \rho\in A_n \\ P \text{ sinon}\end{cases}$. Dans tous les cas $\tau(P+N) = P+N$ et $\tau(PN) = PN$. Comme ceci vaut pour tout $\tau \in \mathrm{Gal}(L/\mathbb{Q})$, on conclut que $P + N$ et PN sont dans $\mathbb{Q}$. Comme ils sont par ailleurs entiers sur $\mathbb{Z}$, on conclut qu'ils sont dans $\mathbb{Z}$.
4. En résumé, $d_K = (P-N)^2 = (P+N)^2 - 4PN \equiv (P+N)^2 \mod 4$ d'où finalement $d_K \equiv 0$ ou $1 \mod 4$ car pour tout $n \in \mathbb{Z}$, on a $n^2 \equiv 0$ ou $1 \mod 4$.