Devoir de Théorie de nombres 2.

À rendre avant 12h00, le 8 avril 2021 sur Moodle.

Exercice 1. Soit m un entier positif sans facteur carré et $\equiv 1 \mod 9$, soit θ la racine cubique $\sqrt[3]{m}$ et K le corps de nombres $\mathbb{Q}(\theta)$.

1/ Montrer que

$$\sigma := (1 + \theta + \theta^2)/3$$

est un entier.

Correction. On calcule le polynôme caractéristique de σ. Dans la base $\{1, \theta, \theta^2\}$, on voit que σ est la matrice

$$\frac{1}{3}\begin{pmatrix} 1 & m & m \\ 1 & 1 & m \\ 1 & 1 & 1 \end{pmatrix}$$

Son poly car. est

$$X^3 - X^2 + \frac{1-m}{3}X - \frac{(m-1)^2}{27}.$$

□

2/ Montrer que $\Delta_K = -3^i m^2$ pour un certain $i \in \mathbb{N}$.

Correction. On sait que $\Delta_K(1, \theta, \theta^2) = -27m^2$. Si p est un facteur premier de m, le poly $X^3 - m$ est p-Eisenstein et donc $[\mathfrak{O}_K : \mathbb{Z}[\theta]]$ n'est pas divisible par p. En utilisant

$$\Delta_K \cdot [\mathfrak{O}_K : \mathbb{Z}[\theta]]^2 = -27m^2,$$

on déduit que $\Delta_K = -3^i m^2$. En effet, si $p \mid m$, alors $p^2 \mid m^2$ et donc $p^2 \mid \Delta_K$ par le lemme de Gauss. □

3/ Calculer Δ_K et en déduire que $\{\theta, \theta^2, \sigma\}$ est une base entière. Indication : On étudiera l'indice de $\mathbb{Z}[\theta]$ dans $A = \mathbb{Z}\theta + \mathbb{Z}\theta^2 + \mathbb{Z}\sigma$.

Correction. Soit $A = \theta\mathbb{Z} + \theta^2\mathbb{Z} + \sigma\mathbb{Z}$. Clairement $[A : \mathbb{Z}[\theta]] = 3$. Par conséquent,

$$\begin{aligned} [\mathfrak{O}_K : A]^2 \cdot 9 &= [\mathfrak{O}_K : \mathbb{Z}[\theta]]^2 \\ &= \frac{-27m^2}{\Delta_K} \\ &= 3^{3-i}. \end{aligned}$$

Donc,

$$[\mathfrak{O}_K : A]^2 = 3^{1-i}.$$

La seule option est ainsi que $i = 1$. Par conséquent, $\Delta_K = -3m^2$. Donc $[\mathfrak{O}_K : A] = 1$. □

Exercice 2. Soit $K = \mathbb{Q}(\sqrt{7})$. Déterminer les idéaux de norme 900 dans l'anneau $\mathfrak{O}_K$.

Correction. Soit $\mathfrak{a}$ un idéal de norme $900 = 2^2 \times 3^2 \times 5^2$. Si $\mathfrak{p} \mid \mathfrak{a}$, alors $\mathfrak{p}$ divise 2, 3 ou 5. On détermine les premiers qui divisent 2, 3 ou 5.

On a $\mathfrak{O}_K = \mathbb{Z}[\theta]$, avec $\theta = \sqrt{7}$. Le poly minimal de θ est $X^2 - 7$, et $X^2 - 7 \equiv (X+1)^2 \mod 2$. Donc $2\mathfrak{O}_K = \mathfrak{p}_2^2$ avec $\mathfrak{p}_2 = (2, \theta + 1)$; clairement $N\mathfrak{p}_2 = 2$. Ensuite, $X^2 - 7 \equiv X^2 - 1 \equiv (X-1)(X+1) \mod 3$ et $3\mathfrak{O}_K = \mathfrak{p}_3\mathfrak{q}_3$, où $\mathfrak{p}_3 = (3, \theta - 1)$ et $\mathfrak{q} = (3, \theta + 1)$. De plus, $N\mathfrak{p}_3 = N\mathfrak{q}_3 = 3$. Finalement, par les mêmes arguments, $\mathfrak{p}_5 = 5\mathfrak{O}_K$ et $N\mathfrak{p}_5 = 25$. Il suit que

$$\mathfrak{a} = \mathfrak{p}_2^i \cdot \mathfrak{p}_3^j \cdot \mathfrak{q}_3^k \cdot \mathfrak{p}_5^\ell,$$

d'où $i = 2$, $j + k = 2$, $\ell = 1$. Donc nous avons trois idéaux :

$$\mathfrak{p}_2^2\mathfrak{p}_3^2\mathfrak{p}_5, \quad \mathfrak{p}_2^2\mathfrak{q}_3^2\mathfrak{p}_5 \quad \mathfrak{p}_2^2\mathfrak{p}_3\mathfrak{q}_3\mathfrak{p}_5.$$

On peut bien évidemment aussi noter que $\mathfrak{p}_2^2\mathfrak{p}_5 = (10)$ et développer $\mathfrak{p}_3^2$, $\mathfrak{q}_3^2$ et $\mathfrak{p}_3\mathfrak{q}_3$ pour obtenir une expression plus nette. □

Exercice 3. Faire les questions 3 à 5 de l'exercice 2 de la séance 6 des TDs (attention aux hypothèses : n est une puissance d'un premier ℓ, qui est différent de p).

`https://webusers.imj-prg.fr/~joao-pedro.dos-santos/Theorie_de_nombres_2/TDs_Seance6_26mars_2021_Corrigee.pdf`

3/ Soit $K = \mathbb{Q}(\mu_n)$. Montrer que $p\mathfrak{O}_K$ n'est pas ramifié, c'est-à-dire, il existe des premiers $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ deux-à-deux distincts de K tels que

$$p\mathfrak{O}_K = \mathfrak{p}_1 \cdots \mathfrak{p}_r.$$

Correction. On peut appliquer directement le théorème de Dedekind : comme Δ_K est une puissance de ℓ et $p \neq \ell$, le premier p ne ramifie pas. Mais il est possible de travailler d'une autre façon : On note la réduction modulo p par un tilde. Ceci étant, on considère la décomposition de $\widetilde{\Phi}_n$ en polynômes irréductibles $\widetilde{\Phi}_n = \widetilde{P}_1^{e_1} \cdots \widetilde{P}_r^{e_r}$ avec $\{P_1, \dots, P_r\}$ des polynômes unitaires de $\mathbb{Z}[X]$ deux-à-deux distincts. Dans ce cas, on sait que

$$p\mathfrak{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$$

où $\mathfrak{p}_i = (p, P_i(\zeta))$. Comme $\widetilde{\Phi}_n \mid X^n - \widetilde{1}$ et ce dernier n'a pas de racines multiples (en $\overline{\mathbb{F}}_p$), on déduit que $e_i = 1$ pour chaque i. La décomposition de $p\mathfrak{O}_K$ en premiers distincts sans facteur carré en découle. □

4/ On garde les notations de la question précédente. Prouver que le degré de chaque $\mathfrak{p}_i$ (qui vaut $[\mathbb{F}_{\mathfrak{p}_i} : \mathbb{F}_p]$), est l'ordre de p dans $(\mathbb{Z}/n)^*$. Indication : Faire appel à la question 2. En déduire que si $p \equiv 1 \mod n$, alors p est totalement décomposé en K.

Correction. Pour simplifier la notation, on choisit $\mathfrak{p}$ parmi $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$; le poly irréductible correspondant est P. Comme $\widetilde{P}$ divise $\widetilde{\Phi}_n$, $\widetilde{P}$ est le polynôme minimal d'une racine de $\widetilde{\Phi}_n$. Or, en $\mathbb{F}_\mathfrak{p}$ on sait que

$$\widetilde{\Phi}_n = \prod_{\omega \in \not\!\mu'_n} (X - \widetilde{\omega})$$

et donc $\widetilde{P}$ est le poly minimal d'un $\widetilde{\omega}$, qui est racine primitive n-ème de l'unité d'après la question 2. Par conséquent, en employant la question 1, son degré est l'ordre de p en $(\mathbb{Z}/n)^*$. □

5/ On suppose $n = 8$ et $p = 3$. Décomposer l'idéal $p\mathfrak{O}_K$ en premiers.

Correction. On note la réduction modulo 3 par un tilde. On considère la décomposition de $\widetilde{\Phi}_8$ en polynômes irréductibles $\widetilde{\Phi}_8 = \widetilde{P}_1 \cdots \widetilde{P}_r$ avec $\{P_1, \ldots, P_r\}$ des polynômes unitaires de $\mathbb{Z}[X]$ deux-à-deux distincts. Dans ce cas, on sait que $3\mathfrak{O}_K = \mathfrak{p}_1 \cdots \mathfrak{p}_r$ et que chaque $\mathfrak{p}_i$ a degré égal à l'ordre de 3 en $(\mathbb{Z}/8)^*$. Par conséquent, $\deg(\mathfrak{p}_i) = 2$. En utilisant, d'près le cours que,

$$\varphi(8) = \sum_{i=1}^{r} \deg(\mathfrak{p}_i),$$

on déduit que $r = 2$. De plus, on sait que $\mathfrak{p}_i = (3, P_i(\zeta))$.On doit ainsi trouver P_1 et P_2. Or, $X^2 + X + \widetilde{2}$ est irréductible et en faisant la division, $X^4 + \widetilde{1} = (X^2 + X + \widetilde{2})(X^2 + \widetilde{2}X + \widetilde{2})$. Il suit que $\mathfrak{p}_1 = (3, \zeta^2 + \zeta + 2)$ et $\mathfrak{p}_2 = (3, \zeta^2 + 2\zeta + 2)$ conviennent. □

Exercice 4. Soit K un corps de nombres, $\theta \in K$ un entier algébrique et p un nombre premier *qui ne divise pas* l'indice

$$m := [\mathfrak{O}_K : \mathbb{Z}[\theta]].$$

Soit f le polynôme minimal de θ et soient $f_1, \ldots, f_r \in \mathbb{Z}[X]$ des polynômes *unitaires* tels que, utilisant un tilde pour désigner la réduction modulo p, on ait :

i) $\tilde{f}_1, \ldots, \tilde{f}_r$ sont *irréductibles*, et

ii) $\tilde{f} = \tilde{f}_1^{e_1} \cdots \tilde{f}_r^{e_r}$ est la décomposition de $\tilde{f}$ en facteurs irréductibles dans $\mathbb{F}_p[X]$.

1/ Montrer que $\mathfrak{p}_i = (p, f_i(\theta))$ est un premier de $\mathfrak{O}_K$ de norme p^{d_i}, où $d_i = \deg f_i$. Indication : On étudiera le morphisme naturel d'anneaux $\varphi : \mathbb{Z}[\theta]/(p) \to \mathfrak{O}_K/(p)$ induit par l'inclusion $\mathbb{Z}[\theta] \subset \mathfrak{O}_K$.

Correction. Le morphisme d'anneaux $\mathbb{Z}[\theta]/(p) \to \mathfrak{O}_K/(p)$ est un isomorphisme. Il est surjective, car pour $x \in \mathfrak{O}_K$, on sait que $mx \in \mathbb{Z}[\theta]$. Prenant $n \in \mathbb{Z}$ tel que $nm = 1+pk$, on déduit que $nmx = x + pkx$ et $x \equiv n(mx) \mod p$. Ensuite, si $x \in \mathbb{Z}[\theta]$ est tel que $x = py$, avec $y \in \mathfrak{O}_K$, alors on a $x + pkx = nmpy$, d'où $x = p(nmy - kx)$ avec $nmy - kx \in \mathbb{Z}[\theta]$.

Donc, $\mathbb{Z}[\theta]/(p, f_i(\theta)) \simeq \mathfrak{O}_K/(p, f_i(\theta))$, mais puisque $\mathbb{Z}[\theta] \simeq \mathbb{Z}[X]/(f)$, on déduit que

$$\begin{aligned}\mathbb{Z}[\theta]/(p, f_i(\theta)) &\simeq \mathbb{Z}[X]/(f, f_i, p)\\ &= \mathbb{Z}[X]/(p, f_i)\\ &= \mathbb{F}_p[X]/(\tilde{f}_i)\end{aligned}$$

et $\mathfrak{O}_K/(p, f_i(\theta))$ est un corps et $\mathfrak{p}_i$ est maximal.

Finalement, la norme de $\mathfrak{p}_i$ est le cardinal $\#\mathbb{F}_p[X]/(\tilde{f}_i) = p^{d_i}$. □

2/ Montrer que si $\mathfrak{a}, \mathfrak{b}_1, \mathfrak{b}_2$ sont des idéaux de $\mathfrak{O}_K$, alors $(\mathfrak{a} + \mathfrak{b}_1)(\mathfrak{a} + \mathfrak{b}_2) \subset \mathfrak{a} + \mathfrak{b}_1\mathfrak{b}_2$. En déduire que $\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r} \subset p\mathfrak{O}_K$.

3/ En considérant les normes, montrer que

$$\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r} = p\mathfrak{O}_K.$$

Correction. On écrit $p\mathfrak{O}_K = \mathfrak{p}_1^{k_1} \cdots \mathfrak{p}_r^{k_r}$. En effet, si $\mathfrak{p} \mid p$ alors $\mathfrak{p} \mid \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$ et donc $\mathfrak{p} \in \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$. Clairement, $k_i \leqslant e_i$. Prenant les normes :

$$p^{\sum e_i d_i} = p^{\sum k_i d_i}.$$

Donc $\sum e_i d_i = \sum k_i d_i$ et il faut que $e_i = k_i$. □

Exercice 5. Soit $\theta = \sqrt[3]{7}$ et K le corps de nombres $\mathbb{Q}(\theta)$.

1/ Soient $u = \theta - 1$ et $v = \theta + 2$. Calculer leur norme. Existe-t-il un entier de K ayant norme 3 ou -3 ?

Correction. On a vu en TD que $\{1, \theta, \theta^2\}$ est une base entière de $\mathfrak{O}_K$: il suffit de prendre, dans la notation de la séance 5 des TDs de 2021, $m = 1$ et $n = 7$. On a aussi vu que la norme d'un élément $a + b\theta + c\theta^2$ est

$$a^3 + 7b^3 + 49c^3 - 21abc.$$

Il suit que $\mathrm{N}u = 6$ et $\mathrm{N}v = 15$.

Ensuite, un élément $a + b\theta + c\theta^2$ de norme 3 doit satisfaire

$$a^3 + 7b^3 + 49c^3 - 21abc = 3.$$

En regardant modulo 7, on obtient $a^3 \equiv 3 \mod 7$. Or, $1^3 \equiv 1 \mod 7$, $2^3 \equiv 1 \mod 7$, $3^3 \equiv 6 \mod 7$ et $4^3 \equiv 1 \mod 7$, $5^3 \equiv 6 \mod 7$ et $6^3 \equiv 6 \mod 7$. Donc 3 n'est pas un cube. Clairement, si $a + b\theta + c\theta^2$ est de norme -3, l'élément $-a - b\theta - c\theta^2$ est de norme 3. □

2/ Déterminer le groupe de classes Cl_K.

Correction. On sait que $\mathfrak{O}_K = \mathbb{Z}[\theta]$. Puis, $M_K < 10,29$ et Cl_K est engendré par les premiers qui divisent $2, 3, 5, 7$. On sait que

$$\begin{aligned} X^3 - 7 &\equiv (X+1)(X^2+X+1) \mod 2 \\ &\equiv (X-7)^3 \mod 3 \\ &\equiv (X+2)(X^2-2X-1) \mod 5 \\ &\equiv X^3 \mod 7. \end{aligned}$$

Il suit que

$$\begin{aligned} 2\mathfrak{O}_K &= \underbrace{(2, \theta+1)}_{\mathfrak{p}_2}\underbrace{(2, \theta^2+\theta+1)}_{\mathfrak{q}_2} \\ 3\mathfrak{O}_K &= \underbrace{(3, \theta-7)^3}_{\mathfrak{p}_3} \\ 5\mathfrak{O}_K &= \underbrace{(5, \theta+2)}_{\mathfrak{p}_5}\underbrace{(5, \theta^2-2\theta-1)}_{\mathfrak{q}_5} \\ 7\mathfrak{O}_K &= (7, \theta)^3 \\ &= (\theta)^3 \end{aligned}$$

Le groupe Cl_K est engendré par $\{[\mathfrak{p}_2], [\mathfrak{p}_3], [\mathfrak{p}_5]\}$. De plus, on note que $\mathrm{N}\mathfrak{p}_2 = 2$, $\mathrm{N}\mathfrak{p}_3 = 3$ et $\mathrm{N}\mathfrak{p}_5 = 5$. De même, $\mathrm{N}\mathfrak{q}_2 = 4$ et $\mathrm{N}\mathfrak{q}_5 = 25$.

Soit $\mathfrak{P}$ un premier qui divise u. Il suit que $\mathrm{N}\mathfrak{P}$ divise aussi 6 et donc $\mathfrak{P} \mid 2$ ou $\mathfrak{P} \mid 3$. Donc, $(u) = \mathfrak{p}_2^i \mathfrak{q}_2^j \mathfrak{p}_3^k$. En prenant la norme, on voit que $i = 1$, $j = 0$ et $k = 1$. De ce fait, $[\mathfrak{p}_2]$ appartient au groupe engendré par $[\mathfrak{p}_3]$. Ensuite, si $\mathfrak{P} \mid v$, alors $\mathrm{N}\mathfrak{P} \mid 15$ et donc $\mathfrak{P} \mid 3$ ou $\mathfrak{P} \mid 5$. Donc, $(v) = \mathfrak{p}_3^i \mathfrak{p}_5^j \mathfrak{q}_5^k$. Prenant les normes, on voit que $i = 1$ et $j = 1$ et $k = 0$. Donc $[\mathfrak{p}_5]$ appartient à $\langle [\mathfrak{p}_3] \rangle$. Le groupe Cl_K est engendré par $[\mathfrak{p}_3]$. Or, si $\mathfrak{p}_3 = (w)$, on aurait $\mathrm{N}w = 3$ ou $\mathrm{N}w = -3$, et ceci est exclu par la question précédente. Finalement, $\mathrm{Cl}_K \simeq \mathbb{Z}/3$. □

.