Théorie des nbrs 2 2023/2024
T.D. 3

Exercice 1 (Équation de Pell–Fermat)**.** Soit $d > 0$ un entier qui n'est pas le carré d'un nombre entier. Rappelons que $\sqrt{d}$ est irrationnel.

(1) Montrer qu'il existe un entier $m \neq 0$ tel que l'équation $x^2 - dy^2 = m$ possède une infinité de solutions $x, y \in \mathbb{Z}$.

On fixe un tel entier dans la suite de l'exercice.

(2) Si $m > 1$,

(a) Montrer qu'il existe des solutions distinctes (a_1, b_1) et (a_2, b_2) de l'équation $x^2 - dy^2 = m$ telles que $a_1 \equiv a_2 \bmod m$ et $b_1 \equiv b_2 \bmod m$.

(b) Écrire la fraction $(a_1 + b_1\sqrt{d})/(a_2 + b_2\sqrt{d})$ sous la forme $x_3 + y_3\sqrt{d}$. Montrer que a_3 et b_3 sont entiers et satisfont à $a_3^2 - db_3^2 = 1$.

(3) Soit (a, b) une solutions de $x^2 - dy^2 = 1$ dans $\mathbb{Z}^2$ tel que $a + b\sqrt{d} > 1$. Montrer que $a \geq 2$ et $b \geq 1$.

(4) Soit (a_1, b_1), (a_2, b_2) deux solutions de $x^2 - dy^2 = 1$ dans $\mathbb{N}^2$. Notons $z_1 = a_1 + b_1\sqrt{d}$, $z_2 = a_2 + b_2\sqrt{d}$. Montrons que $z_1 < z_2 \Leftrightarrow a_1 < a_2 \Leftrightarrow b_1 < b_2$.

(5) Soit $(a_1, b_1) \in \mathbb{N}^2$ une solution de l'équation $x^2 - dy^2 = 1$, où $a_1 > 0$ est minimal. Montrer que les solutions de l'équation $x^2 - dy^2 = 1$ sont de la forme $\pm(a_n, b_n)$ pour $n \in \mathbb{Z}$, où a_n et b_n sont déterminés par la relation

$$a_n + b_n\sqrt{d} = (a_1 + b_1\sqrt{d})^n.$$

Commençons par rappeler la structure de l'anneau des entiers de $k := \mathbb{Q}(\sqrt{d}) \simeq \mathbb{Q}[\mathrm{T}]/\mathrm{T}^2 - d$: si $d \equiv 2, 3[4]$, $\mathrm{O}_k = \mathbb{Z}[\sqrt{d}]$ et si $d \equiv 1[4]$, $\mathrm{O}_k = \{\frac{1}{2}(a + b\sqrt{d}) \quad a - b \equiv 0[2]\}$. La norme $\mathrm{N} := \mathrm{N}_{k|\mathbb{Q}} : k \to \mathbb{Q}$, $x + y\sqrt{d} \mapsto x^2 - dy^2$ se restreint en $\mathrm{N}_{k|\mathbb{Q}} : \mathrm{O}_k \to \mathbb{Q}$ et induit des morphismes de groupes multiplicatifs $\mathrm{N}_{k|\mathbb{Q}} : k^\times \to \mathbb{Q}^\times$, et $\mathrm{N}_{k|\mathbb{Q}} : \mathrm{O}_k^\times \to^\times = \{\pm 1\}$. En particulier, $\mathrm{O}_k^\times = \mathrm{N}_{k|\mathbb{Q}}^{-1}(\{\pm 1\})$ (l'inclusion $\supset$ est immédiate). Comme $d > 0$, $r_1 = 2, r_2 = 0$ et les deux plongements réels de k sont $\sigma_+ : \mathbb{Q}[\mathrm{T}]/(\mathrm{T}^2 - d) \hookrightarrow \mathbb{R}$, $\bar{\mathrm{T}} \mapsto \sqrt{d}$, $\sigma_- : \mathbb{Q}[\mathrm{T}]/(\mathrm{T}^2 - d) \hookrightarrow \mathbb{R}$, $\bar{\mathrm{T}} \mapsto -\sqrt{d}$.

(1) Par le théorème des unités de Dirichlet, $\mathrm{O}_k^\times \simeq \mathbb{Z} \times \mathbb{Z}/2$ (comme k n'a pas de plongement complexe, les seuls racines de 1 qu'il contient sont réelles). Notons $z = x + y\sqrt{d} \in \mathrm{O}_k^\times$ un générateur de la partie libre et, pour tout $n \in$, $z^n = x_n + y_n\sqrt{d}$. On a donc

$$x_{2n}^2 - dy_{2n}^2 = \mathrm{N}(z^{2n}) = 1.$$

Si $d \equiv 2, 3[4]$, on a $(x_{2n}, y_{2n}) \in \mathbb{Z}$, lesquels fournissent donc une infinité de solutions pour $m = 1$. Si $d \equiv 1[4]$, on a $(2x_{2n}, 2y_{2n}) \in \mathbb{Z}$, lesquels fournissent une infinité de solution pour $m = 4$.

(2) Supposons $m > 1$ et observons que si $(x, y \in \mathbb{Z})$ sont solutions de $x^2 - dy^2 = m$ alors $m \not| d$. Sinon, m serait sans facteur carré et $m|x^2$ donc $m|x$ donc $m^2|x^2$ donc $m|y^2$ donc $m^2|y^2$ donc $m|((\frac{x}{m})^2$ donc $m|\frac{x}{m}$ *etc.* : contrad. On peut donc réduire modulo m l'équation et obtenir $\bar{x}^2 - d\bar{2}^2 = 0$ dans $\mathbb{Z}/m$ avec $\bar{d} \neq 0$. Comme $\mathbb{Z}/m$ n'a qu'un nombre fini déléments, il existe au moins deux solutions (a_1, b_1), (a_2, b_2) de $x^2 - dy^2 = m$ qui se réduisent sur la même solution $(\bar{a}, \bar{b})$ de $x^2 - \bar{d}y^2 = 0$ dans $\mathbb{Z}/m$.

(3) Notons $z_i = a_i + b_i\sqrt{d}$. En écrivant $z_3 := z_1/z_2 = a_3 + b_3\sqrt{d}$, on a $a_3^2 - db_3^2 = \mathrm{N}(z_3) = \mathrm{N}(z_1)/\mathrm{N}(z_2) = 1$. En calculant explicitement $a_3 = (a_1a_2 - b_1b_2d)/m$, $b_3 = (b_1a_2 - a_1b_2)/m$. Mais on a $a_1a_2 - b_1b_2d \equiv a_1^2 - db_1^2[m] = m[m] = 0$ et $b_1a_2 - a_1b_2 \equiv b_1a_1 - a_1b_1 = 0[m]$ donc, en fait $a_3, b_3 \in \mathbb{Z}$.

(4) Soit (a, b) une solutions de $x^2 - dy^2 = 1$ dans $\mathbb{Z}^2$ tel que $a + b\sqrt{d} > 1$. Alors $a + b\sqrt{d} > 1 > a - b\sqrt{d} > 0$ donc $2b\sqrt{d} > 0$ donc $b > 0$ donc $b \geq 1$ donc $a \geq b\sqrt{d} \geq \sqrt{d} > 1$ donc $a \geq 2$.

(5) Soit (a_1, b_1), (a_2, b_2) deux solutions de $x^2 - dy^2 = 1$ dans $\mathbb{N}^2$. Notons $z_1 = a_1 + b_1\sqrt{d}$, $z_2 = a_2 + b_2\sqrt{d}$. Montrons que $z_1 < z_2 \Leftrightarrow a_1 < a_2 \Leftrightarrow b_1 < b_2$. En effet, on a $a_1^2 = 1 + db_1^2$, $a_2^2 = 1 + db_2^2$ donc en soustrayant, $(a_1 - a_2)(a_1 + a_2) = * = d(b_1 - b_2)(b_1 + b_2)$. En particulier, $a_1 < a_2 \Leftrightarrow * < 0 \Leftrightarrow b_1 < b_2 \Rightarrow z_1 < z_2$. Inversement, si $z_1 < z_2 \Leftrightarrow a_2 - b_2\sqrt{d} = \frac{1}{z_2} < \frac{1}{z_1} = a_1 - b_1\sqrt{d}$. Donc, en additionnant $z_1 < z_2$ et $\frac{1}{z_2} < \frac{1}{z_1}$, on a $(a_1 + a_2) + (b_1 - b_2)\sqrt{d} < (a_1 + a_2) + (b_2 - b_1)\sqrt{d} \Leftrightarrow b_1 < b_2$.

(6) Notons $z_1 = a_1 + b_1\sqrt{d}$ et S_d l'ensemble des solutions de $x^2 - dy^2 = 1$ dans $\mathbb{Z}^2$. On sait déjà que $\{(a_n, b_n),\ 0 \neq n \in \mathbb{Z} \subset \mathrm{S}_d$. Inversement, soit $1 \neq z = a + b\sqrt{d} \in \mathrm{S}_d$ avec $a, b \geq 0$ (donc > 0). Comme la suite z_1^n, $n \geq 1$ est strictement croissante et tend vers $+\infty$, il existe un unique $n \geq 1$ tel que $z_1^n \leq z < z_1^{n+1}$. Montrons que $z_n = z$. On a $1 \leq \frac{z}{z_1^n} < z_1$ avec $\frac{z}{z_1^n} = u + v\sqrt{d} \in \mathrm{S}_d$ et, si $\frac{z}{z_1^n} > 1$, on aurait $u \geq 2$, $v \geq 1$ par la question (4), ce qui contredirait la minimalité de z_1. Supposons maintenant que (a, b) est une solution quelconque de $x^2 - dy^2 = 1$ dans $\mathbb{Z}^2$. Il reste 3 cas :
— $a > 0$, $b < 0$: $a + b\sqrt{d} = (a - b\sqrt{d})^{-1} = z_1^{-n}$ pour un certain $n \geq 1$;
— $a < 0$, $b > 0$: $a + b\sqrt{d} = -(-a + b\sqrt{d})^{-1} = z_1^{-n}$ pour un certain $n \geq 1$;
— $a < 0$, $b < 0$: $a + b\sqrt{d} = -(-a - b\sqrt{d}) = -z_1^n$ pour un certain $n \geq 1$.

Exercice 2. Soit d un entier > 1 sans facteurs carrés et $\mathrm{K} := \mathbb{Q}(\sqrt{d})$. Posons

$$\omega = \begin{cases} \frac{1+\sqrt{d}}{2} & \text{si } d \equiv 1 \bmod 4, \\ \sqrt{d} & \text{sinon,} \end{cases}$$

de sorte que l'anneau des entiers de K soit égal à $\mathrm{O_K} = \mathbb{Z}[\omega]$.

(1) Soit $\mathfrak{P}$ un idéal maximal de $\mathrm{O_K}$ contenant un nombre premier p. Montrer que $\mathrm{N_K}(\mathfrak{P})$ vaut p ou p^2. Si $\mathrm{N_K}(\mathfrak{P}) = p^2$, montrer que $\mathfrak{P} = p\mathrm{O_K}$ et que p est un élément irréductible de $\mathrm{O_K}$.

(2) On suppose que $\mathrm{N_K}(\mathfrak{P}) = p$. Démontrer qu'il existe un entier $a \in \{0, \ldots, p-1\}$ tel que

$$\mathfrak{P} = (p, a - \omega).$$

(3) On suppose que $\mathfrak{P}$ n'est pas principal. Démontrer l'inégalité : pour tout $n \in \mathbb{Z}$,

$$|\mathrm{N_K}(a - \omega - np)| \geq 2p$$

(4) Montrer que pour $d = 101$, l'anneau $\mathrm{O_K}$ est principal.

(1) Comme $p\mathrm{O_K} \subset \mathfrak{P}$, $(\mathbb{Z}/p)^{\oplus 2} \simeq \mathrm{O_K}/p\mathrm{O_K} \twoheadrightarrow \mathrm{O_K}/\mathfrak{P}$. En particulier, $|\mathrm{O_K}/\mathfrak{P}| = p, p^2$ et $|\mathrm{O_K}/\mathfrak{P}| = p^2$ ssi $p\mathrm{O_K} = \mathfrak{P}$. De plus, comme $\mathfrak{P}$ est un idéal maximal de $\mathrm{O_K}$, $\mathrm{O_K}/\mathfrak{P}$ est un corps fini donc, plus précisément $\mathrm{O_K}/\mathfrak{P} \simeq \mathbb{F}_p, \mathbb{F}_{p^2}$ et $\mathrm{O_K}/\mathfrak{P} \simeq \mathbb{F}_{p^2}$ ssi $|\mathrm{O_K}/\mathfrak{P}| = p^2$.

(2) On suppose que $\mathrm{N_K}(\mathfrak{P}) = p$. Cela signifie que le polynôme minimal $\mathrm{P}_\omega \in \mathbb{Z}[\mathrm{T}]$ se scinde modulo p sous la forme $\overline{\mathrm{P}}_\omega = (\mathrm{T} - \alpha)(\mathrm{T} - \beta)$ et que $\mathfrak{P} = \langle p, \omega - a\rangle$ ou $\langle p, \omega - b\rangle$, avec $a, b \in \{0, \ldots, p-1\}$ tq $\overline{a} = \alpha$, $\overline{b} = \beta$.

(3) Si $\mathfrak{P}$ n'est pas principal, pour tout $n \in \mathbb{Z}$, $(\omega-(a+np))\mathrm{O_K} \subsetneq \mathfrak{P}$ donc

$$\mathrm{N_K}(\omega-(a+np)) = \mathrm{N_K}((\omega-(a+np))\mathrm{O_K}) = \mathrm{N_K}(\mathfrak{P})\mathrm{N_K}((\omega-(a+np))\mathrm{O_K}\mathfrak{P}^{-1}) \geq 2\mathrm{N_K}(\mathfrak{P}).$$

(4) On a $r_1 = 2$, $r_2 = 0$ et comme $101 \equiv 1[4]$, $(\mathrm{K}) = 101$. Donc $\mathrm{M_K} = \frac{1}{2}\sqrt{101} \sim 5, ...$ et $Cl(\mathrm{K})$ est engendré par les idéaux maximaux de normes $2, 2^2, 3$ ou 5. Comme $\mathrm{P}_\omega = \mathrm{T}^2 - \mathrm{T} - 25$ est irréductible modulo 2 et 3, les seuls générateurs éventuellement non-triviaux de $Cl(\mathrm{K})$ sont les idéaux de norme 5. Comme $\overline{\mathrm{P}}_\omega = \mathrm{T}^2 - \mathrm{T} = \mathrm{T}(\mathrm{T}-1)$, on a deux idéaux maximaux de norme 5, à savoir $\mathfrak{P}_5 = \langle 5, \omega\rangle$ et $\mathfrak{P}'_5 = \langle 5, \omega - 1\rangle$. Or

$$\mathrm{N_K}(\omega-5n) = \frac{1}{4}(10n+1+\sqrt{101})(10n+1-\sqrt{101}) = \frac{1}{4}((10n+1)^2-101) = \frac{1}{4}(100n^2+20n+1-101) = 25n^2+5n-25$$

Pour $n = 1$, on a $\mathrm{N_K}(\omega - 5) = 5 < 2 \times 5$ donc $\mathfrak{P}_5$ est principal et comme $5\mathrm{O_K} = \mathfrak{P}_5\mathfrak{P}'_5$, $5\mathrm{O_K} \sim \mathfrak{P}'_5$. Donc $Cl(\mathrm{K}) = 1$ et $\mathrm{O_K}$ est principal.

Exercice 3. Soit d un entier > 1 sans facteurs carrés et $\mathrm{K} := \mathbb{Q}(\sqrt{d})$.

(1) Montrer que $\mathrm{O_K}$ est principal pour $d = -19$, -43, -67 et -163 sont principaux ;

(2) Montrer que $Cl(\mathrm{K}) \simeq \mathbb{Z}/2$ pour $d = -5$;

(3) Montrer que $Cl(\mathrm{K}) \simeq \mathbb{Z}/4$ pour $d = -14$;

Dans tout cet exercice, $d < 0$ donc $r_1 = 0$, $r_2 = 1$ et la borne de Minkowski est $\mathrm{M_K}\frac{2}{\pi}\sqrt{disc(\mathrm{K})}$. On sait que $Cl(\mathrm{K})$ est engendré par les idéaux maximaux $\mathfrak{P}$ de norme $\mathrm{N_K}(\mathfrak{P}) = |\mathrm{O_K}/\mathfrak{P}| \leq \mathrm{M_K}$. Il faut donc déterminer ces idéaux et les relations entre eux. On retient la notation ω de l'exercice précédent. Avant de se lancer dans l'exercice, rappelons que pour tout premier p, on a une décomposition unique

$$p\mathrm{O_K} = \prod_{\mathfrak{P}\in spec(\mathrm{O_K})} \mathfrak{P}^{v_\mathfrak{P}(p)}$$

d'où, par le thm. Chinois et en utilisant les isomorphismes canoniques $\mathrm{A}/(\mathrm{I}+\mathrm{J}) \tilde{\to} (\mathrm{A}/\mathrm{I})/((\mathrm{I}+\mathrm{J})/\mathrm{I})$, des isomorphismes canoniques

$$\prod_{\mathfrak{P}\in spm(\mathrm{O_K})} \mathrm{O_K}/\mathfrak{P}^{v_\mathfrak{P}(p)} \tilde{\leftarrow} \mathrm{O_K}/p \tilde{\leftarrow} ([\mathrm{T}]/\mathrm{P}_\omega)/p \tilde{\to} \mathbb{F}_p[\mathrm{T}]/\overline{\mathrm{P}}_\omega \tilde{\to} \prod_{1\leq i\leq r} \mathbb{F}_p[\mathrm{T}]/\overline{\mathrm{P}}_i^{\alpha_i} \tilde{\leftarrow} \prod_{1\leq i\leq r} \mathbb{Z}[\mathrm{T}]/\langle p, \mathrm{P}_i\rangle^{\alpha_i},$$

où l'on a noté $\overline{\mathrm{P}} := \mathrm{P}[p] \in \mathbb{F}_p[\mathrm{T}]$, $\overline{\mathrm{P}} = \prod_{1\leq i\leq r} \overline{\mathrm{P}}_i^{\alpha_i}$ sa décomposition en produit d'irréductibles dans $\mathbb{F}_p[\mathrm{T}]$ et $\mathrm{P}_i \in \mathbb{Z}[\mathrm{T}]$ un polynôme (disons unitaire de même degré que $\overline{\mathrm{P}}_i$ pour fixer les idées) relevant $\overline{\mathrm{P}}_i$, $i = 1, \ldots, r$. En particulier, si on regarde l'anneau réduit associé à $\mathrm{O_K}/p$ (*i.e.* en quotientant par $\sqrt{0}$), on obtient un isomorphisme canonique

$$\prod_{\mathfrak{P}\in spec(\mathrm{O_K})} \mathrm{O_K}/\mathfrak{P} \tilde{\to} \prod_{1\leq i\leq r} \mathbb{F}_p[\mathrm{T}]/\overline{\mathrm{P}}_i,$$

d'où une bijection entre idéaux maximaux de $\mathrm{O_K}$ de norme p^f et facteurs irréductibles de $\overline{\mathrm{P}}$ de degré f. En prenant en compte les indices de nilpotence de l'unique idéal maximal dans les anneaux locaux $\mathrm{O_K}/\mathfrak{P}^{v_\mathfrak{P}(p)}$ et $\mathbb{F}_p[\mathrm{T}]/\overline{\mathrm{P}}_i^{\alpha_i}$ (pour $\mathfrak{P}$ correspondant à $\overline{\mathrm{P}}_i$ dans la bijection précédente), on obtient de plus $v_\mathfrak{P}(p) = \alpha_i$. Donc, concrètement, en posant $\mathfrak{P}_i := \langle p, \mathrm{P}_i\rangle$, on a $p\mathrm{O_K} = \prod_{1\leq i\leq r} \mathfrak{P}_i^{\alpha_i}$. Ces observations permettent en général de déterminer assez facilement les générateur de $Cl(\mathrm{K})$. Établir des relations entre ces générateurs est en général plus subtil mais le principe de base est que si $\mathfrak{P}_i$ est un idéal maximal de $\mathrm{O_K}$ de norme $p_i^{f_i}$, $i = 1, \ldots, r$ et que l'on veut monter une relation du type

$$\prod_{1\leq i\leq r} \mathfrak{P}_i^{\alpha_i} = 1$$

dans $cl(\mathrm{K})$, il faut chercher un élément $z \in \mathrm{O_K}$ de norme $p_1^{f_1} \cdots p_r^{f_r}$ tq $z \in \cap_{1 \leq i \leq r} \mathfrak{P}_i^{\alpha_i}$.

(1) $-19 \equiv 1[4]$ donc $disc(\mathrm{K}) = 19$, $\mathrm{M_K} \sim 2,77$. En particulier, $Cl(\mathrm{K})$ est engendré par les idéaux maximaux de norme 2 ou 2^2. Si on note $\omega = \frac{1+\sqrt{-19}}{2}$, on a $\mathrm{P}_\omega = \mathrm{T}^2 - \mathrm{T} + 5$, qui est irréductible modulo 2. Donc $\mathrm{O_K}$ contient un unique idéal maximal contenant 2, qui est de norme 2^2 donc principal. De même
— $-43 \equiv 1[4]$, $\mathrm{M_K} \sim 4,17$, $\mathrm{P}_\omega = \mathrm{T}^2 - \mathrm{T} + 11$, qui reste irréductible modulo 2, 3.
— $-67 \equiv 1[4]$, $\mathrm{M_K} \sim 5,21$, $\mathrm{P}_\omega = \mathrm{T}^2 - \mathrm{T} + 17$, qui reste irréductible modulo 2, 3, 5.
— $-163 \equiv 1[4]$, $\mathrm{M_K} \sim 8,13$, $\mathrm{P}_\omega = \mathrm{T}^2 - \mathrm{T} + 41$, qui reste irréductible modulo 2, 3, 5, 7.

(2) $-5 \equiv 3[4]$ donc $|disc(\mathrm{K})| = 4 \times 5 = 20$, $\mathrm{M_K} \sim 2,97$, $\mathrm{P}_\omega = \mathrm{T}^2 + 5 \equiv \mathrm{T}^2 + 1 = (\mathrm{T}-1)^2[2]$. Donc $Cl(\mathrm{K})$ est engendré par l'idéal $\mathfrak{P} = \langle 2, \omega - 1 \rangle$, qui est de norme 2 et n'est pas principal. Sinon, il existerait $x = a + b\omega \in \mathrm{O_K} = \mathbb{Z}[\omega]$ tq $2 = \mathrm{N_K}(\mathfrak{P}) = \mathrm{N_K}(x) = a^2 + 5b^2$, ce qui n'est pas possible. Par contre, $\mathfrak{P}^2 = \langle 4, 2\omega - 2, (\omega-1)^2 \rangle$ avec $(\omega-1)^2 = \omega^2 - 2\omega + 1 = 2\omega - 4$ donc

$$\mathfrak{P}^2 = \langle 4, 2\omega - 2, 2\omega - 4 \rangle = \langle 4, 2\omega - 2, 2\omega \rangle = \langle 2, 2\omega \rangle = 2\mathbb{Z}[\omega] = 2\mathrm{O_K}.$$

(3) $-14 \equiv 2[4]$ donc $|disc(\mathrm{K})| = 4 \times 14 = 56$, $\mathrm{M_K} \sim 4,76$, $\mathrm{P}_\omega = \mathrm{T}^2 + 14$ donc $\mathrm{P}_\omega \equiv \mathrm{T}^2[2]$ et $\mathrm{P}_\omega \equiv \mathrm{T}^2 + 2 = (\mathrm{T}+1)(\mathrm{T}+2)[3]$. Donc $Cl(\mathrm{K})$ est engendré par l'idéal $\mathfrak{P}_2 = \langle 2, \omega \rangle$, qui est de norme 2 et $\mathfrak{P}_3 = \langle 3, \omega + 1 \rangle$ (ou son inverse, $\mathfrak{P}_3' = \langle 3, \omega + 2 \rangle$), qui est de norme 3. Notons que $\mathfrak{P}_2$ n'est pas principal car $a^2 + 14b^2 = 2$ n'a pas de solution dans $\mathbb{Z}^2$. Par contre, $\mathfrak{P}_2^2 = \langle 4, 2\omega, \omega^2 \rangle = \langle 4, 2\omega, -14 \rangle = \langle 2, 2\omega \rangle = 2\mathbb{Z}[\omega] = 2\mathrm{O_K}$. Montrons que $\mathfrak{P}_3^2 = \mathfrak{P}_2$. Pour cela, considérons $z = 2 + \omega$. On a $\mathrm{N_K}(z) = 4 + 14 = 18 = 2 \times 3^2$. Donc $z\mathrm{O_K} = \mathfrak{P}_2 \mathfrak{P}_3^{\alpha_3} \mathfrak{P}_3'^{\alpha_3'}$ avec $\alpha_3 + \alpha_3' = 2$. Mais on ne peut pas avoir $\alpha_3 = \alpha_3' = 1$ car sinon, $z\mathrm{O_K} = 3\mathfrak{P}_2$ donc il existerait $a + b\omega \in \mathfrak{P}_2$ tq $z = 2 + \omega = 3a + 3b\omega$: contradiction. Donc $z\mathrm{O_K} = \mathfrak{P}_2 \mathfrak{P}_3^2$, ou encore $\mathfrak{P}_3^2 \sim \mathfrak{P}_2^{-1} \sim \mathfrak{P}_2$.

Exercice 4. Soit K un corps quadratique de discriminant Δ. Posons

$$\omega = \begin{cases} \frac{1+\sqrt{\Delta}}{2} & \text{si } \Delta \equiv 1 \bmod 4, \\ \sqrt{\Delta} & \text{sinon,} \end{cases}$$

de sorte que l'anneau des entiers de K soit égal à $\mathrm{O_K} = \mathbb{Z}[\omega]$.

(a) Soit P un idéal maximal de $\mathrm{O_K}$ contenant un nombre premier p. Montrer que $\mathrm{N_K}(\mathrm{P})$ vaut p ou p^2. Si $\mathrm{N_K}(\mathrm{P}) = p^2$, montrer que $\mathrm{P} = (p)$ et que p est un élément irréductible de $\mathrm{O_K}$.

(b) On suppose que $\mathrm{N_K}(\mathrm{P}) = p$. Démontrer qu'il existe un entier $a \in \{0, \ldots, p-1\}$ tel que

$$\mathrm{P} = (p, a - \omega).$$

(c) On suppose que P n'est pas principal. Démontrer l'inégalité : pour tout $n \in \mathbb{Z}$,

$$|\mathrm{N_K}(a - \omega - np)| \geq p^2.$$

(d) Démontrer que, si $\Delta = 101$, l'anneau $\mathrm{O_K}$ est principal.

Exercice 5. Soient K un corps de nombres et $\mathrm{A} := \mathrm{O_K}$ son anneau d'entiers. On veut montrer que tout idéal I de A est engendré par au plus deux éléments. On rappelle que I s'écrit de façon unique sous la forme

$$\mathrm{I} = \prod_{\mathfrak{P} \in spec(\mathrm{A})} \mathfrak{P}^{v_\mathfrak{P}(\mathrm{I})}$$

et que $\mathrm{I} \subset \mathrm{J}$ ssi $v_\mathfrak{P}(\mathrm{J}) \leq v_\mathfrak{P}(\mathrm{I})$, $\mathfrak{P} \in spec(\mathrm{A})$.

(1) Montrer que $v_\mathfrak{P}(\mathrm{IJ}) = v_\mathfrak{P}(\mathrm{I}) + v_\mathfrak{P}(\mathrm{J})$, $v_\mathfrak{P}(\mathrm{I} + \mathrm{J}) = min(v_\mathfrak{P}(\mathrm{I}), v_\mathfrak{P}(\mathrm{J}))$, $v_\mathfrak{P}(\mathrm{I} \cap \mathrm{J}) = max(v_\mathfrak{P}(\mathrm{I}), v_\mathfrak{P}(\mathrm{J}))$ et $\mathrm{IJ} = (\mathrm{I} \cap \mathrm{J})(\mathrm{I} + \mathrm{J})$.

(2) Soit I un idéal non nul de A et $0 \neq a \in \mathrm{I}$. Notons $a\mathrm{A} = \prod_{1\leq i\leq r} \mathfrak{P}_i^{\mathrm{N}_i} \subset \mathrm{I} = \prod_{1\leq i\leq r} \mathfrak{P}_i^{n_i}$ avec $n_i \leq \mathrm{N}_i$, $i = 1, \ldots, r$. Pour $i = 1, \ldots, n$, soit $b_i \in \mathfrak{P}_i^{n_i} \prod_{1\leq i\neq j\leq r} \mathfrak{P}_j^{n_j+1} \backslash \prod_{1\leq j\leq r} \mathfrak{P}_j^{n_j+1}$ et posons $b = b_1 + \cdots + b_n$. Montrer que $\mathrm{I} = \langle a, b\rangle$.

(1) $\mathrm{IJ} = (\mathrm{I}\cap\mathrm{J})(\mathrm{I}+\mathrm{J})$ résulte immédiatement des 3 autres égalités. $v_{\mathfrak{P}}(\mathrm{IJ}) = v_{\mathfrak{P}}(\mathrm{I}) + v_{\mathfrak{P}}(\mathrm{J})$, $v_{\mathfrak{P}}(\mathrm{I}+\mathrm{J}) \geq min(v_{\mathfrak{P}}(\mathrm{I}), v_{\mathfrak{P}}(\mathrm{J}))$ et $v_{\mathfrak{P}}(\mathrm{I}\cap\mathrm{J}) \leq max(v_{\mathfrak{P}}(\mathrm{I}), v_{\mathfrak{P}}(\mathrm{J}))$ sont immédiats. Comme $\mathrm{I}, \mathrm{J} \subset \mathrm{I}+\mathrm{J}$, on a $v_{\mathfrak{P}}(\mathrm{I}+\mathrm{J}) \leq v_{\mathfrak{P}}(\mathrm{I}), v_{\mathfrak{P}}(\mathrm{J})$ donc $v_{\mathfrak{P}}(\mathrm{I}+\mathrm{J}) \leq min(v_{\mathfrak{P}}(\mathrm{I}), v_{\mathfrak{P}}(\mathrm{J}))$. De même, comme $\mathrm{I}\cap\mathrm{J} \subset \mathrm{I}, \mathrm{J}$ on a $v_{\mathfrak{P}}(\mathrm{I}), v_{\mathfrak{P}}(\mathrm{J}) \leq v_{\mathfrak{P}}(\mathrm{I}\cap\mathrm{J})$ donc $max(v_{\mathfrak{P}}(\mathrm{I}), v_{\mathfrak{P}}(\mathrm{J})) \leq v_{\mathfrak{P}}(\mathrm{I}\cap\mathrm{J})$.

(2) Par construction $b \in \mathrm{I}$ donc $\mathrm{J} := \langle a, b\rangle \subset \mathrm{I}$. Réciproquement, toujours par construction, $b_j \in \mathfrak{P}_j^{n_i+1}$, $1 \leq i \neq j \leq n$ et $b_i \in \mathfrak{P}_i^{n_i}$ mais $b_i \notin \mathfrak{P}_i^{n_i+1}$ donc $v_{\mathfrak{P}_i}(b) = n_i$. Or $\mathrm{A}a \subset \mathrm{J} = \mathrm{A}a + \mathrm{A}b = \prod_{1\leq i\leq n} \mathfrak{P}_i^{min(\mathrm{N}_i, n_i)} = \mathrm{I}$ (la première inclusion montre que les seuls idéaux qui apparaissent dans la décomposition de J apparaissent dans celle de $\mathrm{A}a$).