LES ANNEAUX D'ENTIERS DES EXTENSIONS QUADRATIQUES DE $\mathbb{Q}$

1. Les extensions quadratiques de $\mathbb{Q}$

Definition 1.1. Une *extension quadratique* K *de* $\mathbb{Q}$ est un sous-corps K de $\mathbb{C}$ (contenant forcément $\mathbb{Q}$) qui est un $\mathbb{Q}$-espace vectoriel de dimension 2.

1. Soit K une extension quadratique de $\mathbb{Q}$. Pour $d \in \mathbb{Q}$ on note $\sqrt{d} \in \mathbb{C}$ l'une des deux racines du polynôme $X^2 - d \in \mathbb{Q}[X]$ (l'autre est $-\sqrt{d}$).

(a) Montrer que tout élément de K est racine d'un polynôme de degré 2 à coefficients dans $\mathbb{Q}$.
(b) Montrer qu'il existe $\alpha \in \overline{\mathbb{Q}}$ tel que $K = \mathbb{Q}(\alpha)$.
(c) Montrer qu'il existe $d \in \mathbb{Q}$ tel que $K = \mathbb{Q}(\sqrt{d})$.
(d) Montrer qu'il existe $d \in \mathbb{Z}$ sans facteur carré (i.e. $d = -1$ ou $d = \pm p_1 \dots p_r$ avec $r \geq 1$, p_i premier et $p_i \neq p_j$ pour $i \neq j$) tel que $K = \mathbb{Q}(\sqrt{d})$.
(e) Soit $\alpha = x + y\sqrt{d} \in K$ avec $x, y \in \mathbb{Q}$. Donner $\mathrm{P}_{\min}(\alpha)$ en fonction de x, y.

(a) Soit $\alpha \in K$. Si $\alpha \in \mathbb{Q}$ alors $(X - \alpha)^2 \in \mathbb{Q}[X]$ annule α. Si $\alpha \notin \mathbb{Q}$ alors les éléments $1, \alpha, \alpha^2$ sont deux à deux distincts et $\dim_{\mathbb{Q}} K = 2 \Rightarrow (1, \alpha, \alpha^2)$ liés sur $\mathbb{Q}$. Soient $a_i \in \mathbb{Q}$ non tous nuls tels que $a_0 + a_1\alpha + a_2\alpha^2 = 0$; alors $\alpha \notin \mathbb{Q} \Rightarrow a_2 \neq 0$ donc $a_2X^2 + a_1X + a_0 \in \mathbb{Q}[X]$ est de degré 2 et annule α.
(b) D'après (a) on a $K \subset \overline{\mathbb{Q}}$ et $\deg \mathrm{P}_{\min}(\alpha) \leq 2$ pour tout $\alpha \in K$, avec $\deg \mathrm{P}_{\min}(\alpha) = 1 \Leftrightarrow \alpha \in \mathbb{Q}$. Comme $\dim_{\mathbb{Q}} K = 2$ il existe $\alpha \in K$ tel que $\dim_{\mathbb{Q}} \mathbb{Q}(\alpha) = \deg \mathrm{P}_{\min}(\alpha) = 2$, auquel cas $\mathbb{Q}(\alpha) \subseteq K \Rightarrow \mathbb{Q}(\alpha) = K$.
(c) Soit $\mathrm{P}_{\min}(\alpha)(X) = X^2 + aX + b$ avec $a, b \in \mathbb{Q}$. On a $X^2 + aX + b = (X + \frac{1}{2}a)^2 + b - \frac{1}{4}a^2$ d'où $\alpha = \frac{1}{2}(-a \pm \sqrt{a^2 - 4b})$. En prenant $d = a^2 - 4b \in \mathbb{Q}$ on obtient $\alpha = \frac{1}{2}(-a \pm \sqrt{d}) \Rightarrow \alpha \in \mathbb{Q}(\sqrt{d}) \Leftrightarrow \mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\sqrt{d})$ et aussi $\sqrt{d} = \pm(2\alpha + a) \Rightarrow \sqrt{d} \in \mathbb{Q}(\alpha) \Leftrightarrow \mathbb{Q}(\sqrt{d}) \subseteq \mathbb{Q}(\alpha)$. Donc $K = \mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{d})$.
(d) On a $d \in \mathbb{Q}^\times$ et $d \notin \mathbb{Q}^{\times 2} = \{x^2, x \in \mathbb{Q}^\times\}$ puisque $K \neq \mathbb{Q}$. Donc soit $d = -1$ soit $d = \pm p_1^{n_1} \dots p_r^{n_r}$ avec $r \geq 1$, $n_i \in \mathbb{Z} - \{0\}$ et p_i premiers deux à deux distincts. Dans le deuxième cas on a $d = c^2(\pm p_1^{\varepsilon_1} \dots p_r^{\varepsilon_r})$ avec $c \in \mathbb{Q}^\times$ et $\varepsilon_i = 0$ si $n_i \in 2\mathbb{Z}$, $\varepsilon_i = 1$ si $n_i \in 1 + 2\mathbb{Z}$, d'où $\sqrt{d} = \pm c\sqrt{d'}$ avec $d' = \pm p_1^{\varepsilon_1} \dots p_r^{\varepsilon_r}$ et donc $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{d'})$.
(e) On a $(x + y\sqrt{d})^2 = x^2 + dy^2 + 2xy\sqrt{d}$ d'où $(x + y\sqrt{d})^2 - 2x(x + y\sqrt{d}) + (x^2 - dy^2) = 0$. Donc α est racine de $X^2 - 2xX + (x^2 - dy^2) \in \mathbb{Q}[X]$. Si $\alpha \in \mathbb{Q}$ alors $\mathrm{P}_{\min}(\alpha)(X) = X - x$, si $\alpha \notin \mathbb{Q}$ alors $\mathrm{P}_{\min}(\alpha)(X) = X^2 - 2xX + (x^2 - dy^2)$.

2. L'anneau des entiers de $\mathbb{Q}(\sqrt{d})$

Pour toute la suite on fixe un entier $d \in \mathbb{Z}$ sans facteur carré et on pose $K = \mathbb{Q}(\sqrt{d})$.

Definition 2.1. L'ensemble O_K est le sous-ensemble de K constitué des éléments qui sont racine d'un polynôme unitaire de degré 2 à coefficients dans $\mathbb{Z}$:

$$O_K \underset{\text{def}}{=} \big\{\alpha \in K \mid \exists\, n, m \in \mathbb{Z} \text{ tels que } \alpha^2 + n\alpha + m = 0\big\}.$$

2. Montrer que $a, b \in \mathbb{Z} \Rightarrow a + b\sqrt{d} \in O_K$ et que $\mathbb{Q} \cap O_K = \mathbb{Z}$.

Soient $a, b \in \mathbb{Z}$. D'après **1**(e) l'élément $a + b\sqrt{d}$ est racine de $X^2 - 2aX + (a^2 - db^2) \in \mathbb{Z}[X]$, d'où $a + b\sqrt{d} \in O_K$. En particulier $\mathbb{Z} \subseteq O_K$ ce qui équivaut à $\mathbb{Z} \subseteq \mathbb{Q} \cap O_K$. Soit $\alpha \in \mathbb{Q} \cap O_K$. Soient $r, s \in \mathbb{Z}$ tels que $s \neq 0$, $r\mathbb{Z} + s\mathbb{Z} = \mathbb{Z}$ (i.e. r, s premiers entre eux), et $\alpha = \frac{r}{s}$. Soient $n, m \in \mathbb{Z}$ tels que $\alpha^2 + n\alpha + m = 0$. Alors $r^2 + nrs + ms^2 = 0$, c'est-à-dire $r^2 = -(nr + ms)s$, d'où $nr + ms = 0$ ou $s \mid r^2$. Si $nr + ms = 0$ alors $r = 0$ i.e. $\alpha = 0$, sinon $s \mid r^2$ d'où $s = \pm 1$ i.e. $\alpha \in \mathbb{Z}$. Donc $\mathbb{Q} \cap O_K = \mathbb{Z}$.

3. Soit $\alpha \in K$ et soient $x, y \in \mathbb{Q}$ tels que $\alpha = x + y\sqrt{d}$. Montrer que

$$\alpha \in O_K \quad \Leftrightarrow \quad \big(2x \in \mathbb{Z} \text{ et } x^2 - dy^2 \in \mathbb{Z}\big).$$

Si $\alpha \in \mathbb{Q}$ i.e. $\alpha = x$ alors $x \in O_K \Leftrightarrow x \in \mathbb{Z}$ par **2**, ce qui équivaut à $2x \in \mathbb{Z}$ et $x^2 \in \mathbb{Z}$. Si $\alpha \notin \mathbb{Q}$ i.e. $\mathrm{P}_{\min}(\alpha)(X) = X^2 - 2xX + (x^2 - dy^2)$ (par **1**(e)) alors $\alpha \in O_K \Leftrightarrow 2x \in \mathbb{Z}$ et $x^2 - dy^2 \in \mathbb{Z}$ puisque $\mathrm{P}_{\min}(\alpha)$ est l'unique polynôme unitaire de degré 2 dans $\mathbb{Q}[X]$ annulant α.

4. Montrer que

$$d \equiv 2 \text{ ou } 3 \bmod 4\mathbb{Z} \;\Rightarrow\; O_K = \big\{a + b\sqrt{d},\ a, b \in \mathbb{Z}\big\}$$

$$d \equiv 1 \bmod 4\mathbb{Z} \;\Rightarrow\; O_K = \Big\{\frac{a + b\sqrt{d}}{2},\ a, b \in \mathbb{Z} \text{ tels que } a \equiv b \bmod 2\mathbb{Z}\Big\}.$$

Remarque. d sans facteur carré $\Rightarrow d \equiv 1, 2$ ou $3 \bmod 4\mathbb{Z}$.
Soit $\alpha = x + y\sqrt{d} \in K$ avec $x, y \in \mathbb{Q}$; d'après **3** on a $\alpha \in O_K \Leftrightarrow 2x \in \mathbb{Z}$ et $x^2 - dy^2 \in \mathbb{Z}$. Posons $x = \frac{a}{2}$ avec $a \in \mathbb{Q}$ et $y = \frac{b}{c}$ avec $b, c \in \mathbb{Z}$, $c \geq 1$, et b, c premiers entre eux. Alors $2x \in \mathbb{Z} \Leftrightarrow a \in \mathbb{Z}$ et $x^2 - dy^2 \in \mathbb{Z} \Leftrightarrow \frac{a^2c^2 - 4db^2}{4c^2} \in \mathbb{Z} \Leftrightarrow 4c^2 \mid a^2c^2 - 4db^2$. Cette divisibilité implique $4 \mid a^2c^2$ et $c^2 \mid 4db^2$. On a $4 \mid a^2c^2 \Leftrightarrow 2 \mid ac \Leftrightarrow 2 \mid a$ ou $2 \mid c$, et $c^2 \mid 4db^2 \Leftrightarrow c^2 \mid 4d \Leftrightarrow c^2 \mid 4 \Leftrightarrow c \in \{1, 2\}$ puisque b et c sont premiers entre eux et que d est sans facteur carré. Si a est pair alors $4c^2 \mid a^2c^2 - 4db^2 \Leftrightarrow c^2 \mid db^2 \Leftrightarrow c^2 \mid d \Leftrightarrow c = 1$ (b, c premiers entre eux et d sans facteur carré), donc $x, y \in \mathbb{Z}$. Si a est impair alors c est pair, donc $c = 2$ et $x, y \in \frac{1}{2}\mathbb{Z}$. Dans ce cas $a \in (\mathbb{Z}/4\mathbb{Z})^\times$, et $x^2 - dy^2 = \frac{a^2}{4} - d\frac{b^2}{4} \in \mathbb{Z} \Leftrightarrow a^2 \equiv db^2 \bmod 4\mathbb{Z}$ implique $b, d \in (\mathbb{Z}/4\mathbb{Z})^\times$ et $d \equiv (ab^{-1})^2 \bmod 4\mathbb{Z}$. Comme la classe de 1 est le seul carré non nul dans $\mathbb{Z}/4\mathbb{Z}$ on en déduit $d \equiv 1 \bmod 4\mathbb{Z}$, d'où $a^2 \equiv b^2 \bmod 4\mathbb{Z} \Leftrightarrow 4 \mid (a + b)(a - b) \Leftrightarrow a \equiv b \bmod 2\mathbb{Z}$.

5. Montrer que O_K est un sous-anneau unitaire de K avec $O_K = \mathbb{Z}[\sqrt{d}]$ si $d \equiv 2$ ou $3 \bmod 4\mathbb{Z}$ et $O_K = \mathbb{Z}\big[\frac{1+\sqrt{d}}{2}\big]$ si $d \equiv 1 \bmod 4\mathbb{Z}$.

Si $d \equiv 2$ ou $3 \bmod 4\mathbb{Z}$ alors $O_K = \{a + b\sqrt{d},\ a, b \in \mathbb{Z}\}$ d'après **4**, donc O_K est stable par $+$ et $\times$; comme il contient 1 c'est un sous-anneau unitaire de K et $O_K = \mathbb{Z}[\sqrt{d}]$ (= le sous-anneau unitaire de K engendé par $\sqrt{d}$). Si $d \equiv 1 \bmod 4\mathbb{Z}$ alors $O_K = \{\frac{a+b\sqrt{d}}{2},\ a, b \in \mathbb{Z}, a \equiv b \bmod 2\mathbb{Z}\} = \{\frac{a-b}{2} + b\frac{1+\sqrt{d}}{2},\ a, b \in \mathbb{Z}, a \equiv b \bmod 2\mathbb{Z}\} = \{a + b\frac{1+\sqrt{d}}{2},\ a, b \in \mathbb{Z}\}$ d'après **4**, donc O_K est stable par $+$ et $\times$; comme il contient 1 c'est un sous-anneau unitaire de K et $O_K = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$.

Definition 2.2. On appelle O_K *l'anneau des entiers de* K.

3. Unités

6. Montrer que l'application appelée norme de K sur $\mathbb{Q}$

$$\begin{aligned} N_{K/\mathbb{Q}} : K^\times &\longrightarrow \mathbb{Q}^\times \\ x + y\sqrt{d} &\longmapsto x^2 - dy^2 \end{aligned}$$

est un morphisme de groupes.

Remarque. $x + y\sqrt{d} \neq 0 \Leftrightarrow (x, y) \neq (0, 0)$ puisque $(1, \sqrt{d})$ est une $\mathbb{Q}$-base de K, et $(x, y) \neq (0, 0) \Rightarrow x^2 - dy^2 \neq 0$ puisque d est sans facteur carré.
Soit $\alpha = x + y\sqrt{d} \in K^\times$ avec $x, y \in \mathbb{Q}$. L'application de multiplication par α

$$\begin{aligned} \mu_\alpha : K &\longrightarrow K \\ \xi &\longmapsto \alpha\xi \end{aligned}$$

est $\mathbb{Q}$-linéaire. On a $\mu_\alpha(1) = x + y\sqrt{d}$ et $\mu_\alpha(\sqrt{d}) = dy + x\sqrt{d}$, donc la matrice de μ_α dans la base $(1, \sqrt{d})$ est

$$\begin{pmatrix} x & dy \\ y & x \end{pmatrix} \quad \text{et} \quad \det(\mu_\alpha) = x^2 - dy^2 = N_{K/\mathbb{Q}}(\alpha).$$

On en déduit $N_{K/\mathbb{Q}}(\alpha\beta) = \det(\mu_{\alpha\beta}) = \det(\mu_\alpha \circ \mu_\beta) = \det(\mu_\alpha)\det(\mu_\beta) = N_{K/\mathbb{Q}}(\alpha)N_{K/\mathbb{Q}}(\beta)$ pour tous $\alpha, \beta \in K^\times$. De plus $N_{K/\mathbb{Q}}(1) = 1$, donc $N_{K/\mathbb{Q}}$ est un morphisme de groupes.

7. Montrer que $O_K^\times = O_K \cap N_{K/\mathbb{Q}}^{-1}\big(\{\pm 1\}\big)$.

Soient $\alpha, \beta \in O_K^\times$ tels que $\alpha\beta = 1$. Alors $N_{K/\mathbb{Q}}(\alpha\beta) = N_{K/\mathbb{Q}}(\alpha)N_{K/\mathbb{Q}}(\beta) = 1$ d'après **6** d'où $N_{K/\mathbb{Q}}(\alpha) = \pm 1$. Donc $O_K^\times \subseteq O_K \cap N_{K/\mathbb{Q}}^{-1}(\mathbb{Z}^\times)$. Réciproquement soit $\alpha \in O_K$ tel que $N_{K/\mathbb{Q}}(\alpha) = \pm 1$. Alors $X^2 + nX \pm 1$ annule α avec $n \in \mathbb{Z}$ d'après **1**(e), d'où $\alpha(\alpha + n) = \pm 1$ ce qui implique $\alpha \in O_K^\times$. Donc $O_K \cap N_{K/\mathbb{Q}}^{-1}(\mathbb{Z}^\times) \subseteq O_K^\times$.

8. On suppose $d < 0$.

(a) Montrer que $O_K^\times = \{\alpha \in O_K \mid N_{K/\mathbb{Q}}(\alpha) = 1\}$.
(b) Montrer que l'application $\iota : K \to \mathbb{R} \oplus \mathbb{R}$ donnée par $x + y\sqrt{d} \mapsto (x, y)$ est injective.
(c) Montrer que $\iota(O_K^\times) \subseteq \big(\frac{1}{2}\mathbb{Z} \oplus \frac{1}{2}\mathbb{Z}\big) \cap E(1, -d)$ où $E(1, -d)$ est l'ellipse d'équation $X^2 + (-d)Y^2 = 1$ dans $\mathbb{R} \oplus \mathbb{R}$.
(d) Montrer que $E(1, -d)$ est compact dans $\mathbb{R} \oplus \mathbb{R}$.
(e) En déduire que $O_K^\times$ est fini.

(a) Soit $\alpha = x + y\sqrt{d} \in O_K$, $x, y \in \mathbb{Q}$. On a $N_{K/\mathbb{Q}}(\alpha) = x^2 - dy^2 \geq 0$ puisque $d < 0$, donc $O_K^\times = O_K \cap N_{K/\mathbb{Q}}^{-1}(\{1\})$ par **7**.
(b) L'application ι est injective car $(1, \sqrt{d})$ est une base de K sur $\mathbb{Q}$ (et $\operatorname{Im}\iota = \mathbb{Q} \oplus \mathbb{Q}$).
(c) D'après **4** on a $\iota(O_K) \subset \frac{1}{2}\mathbb{Z} \oplus \frac{1}{2}\mathbb{Z}$ et par (a) et (b) on obtient $\iota(O_K^\times) = \iota(O_K \cap N_{K/\mathbb{Q}}^{-1}(\{1\})) = \iota(O_K) \cap \iota(N_{K/\mathbb{Q}}^{-1}(\{1\})) \subset (\frac{1}{2}\mathbb{Z} \oplus \frac{1}{2}\mathbb{Z}) \cap E(1, -d)$ avec $E(1, -d) = \{(x, y) \in \mathbb{R} \oplus \mathbb{R} \mid x^2 - dy^2 = 1\}$.
(d) L'ensemble $E(1, -d)$ est l'image réciproque du fermé $\{1\}$ par l'application continue $\mathbb{R} \oplus \mathbb{R} \to \mathbb{R}$, $(x, y) \mapsto x^2 - dy^2$, donc il est fermé dans $\mathbb{R} \oplus \mathbb{R}$. Il est contenu dans la boule de centre $(0, 0)$ et de rayon 1 (car $-d \geq 1 \Rightarrow -\frac{1}{\sqrt{d}} \leq 1$), donc il est borné dans $\mathbb{R} \oplus \mathbb{R}$. Par conséquent $E(1, -d)$ est compact.
(e) Par (c) on a $\iota(O_K^\times) \subset (\frac{1}{2}\mathbb{Z} \oplus \frac{1}{2}\mathbb{Z}) \cap E(1, -d)$ avec $E(1, -d)$ compact par (f) et $\frac{1}{2}\mathbb{Z} \oplus \frac{1}{2}\mathbb{Z}$ discret (un sous-ensemble D d'un espace topologique X est *discret* si pour tout $x \in D$ il existe un voisinage $\mathcal{V}(x)$ de x dans X tel que $\mathcal{V}(x) \cap D = \{x\}$). L'intersection d'un compact avec un discret étant finie $\iota(O_K^\times)$ est fini, ce qui équivaut à $O_K^\times$ fini par (b).

Remarque. On a le résultat plus précis suivant, laissé en exercice.

Proposition 3.1. *Soit $K = \mathbb{Q}(\sqrt{d})$ avec $d < 0$ entier sans facteur carré. Si $d \neq -3, -1$ alors $O_K^\times = \{\pm 1\}$, si $d = -1$ alors $O_K^\times = \{\pm 1, \pm i\}$, et si $d = -3$ alors $O_K^\times = \{\pm 1, \pm e^{i\pi/3}, \pm e^{i2\pi/3}\}$.*

9. On prend $d = 2$, donc $K = \mathbb{Q}(\sqrt{2})$. Pour tout $n \in \mathbb{Z}$ on pose $u_n = (1 + \sqrt{2})^n \in K$.

(a) Montrer que $u_n \in O_K^\times$ pour tout $n \in \mathbb{Z}$. En déduire que $O_K^\times$ est infini.
(b) Mêmes questions avec $d = 3, 6, 7$ et $u_1 = 2 + \sqrt{3}, 5 + 2\sqrt{6}, 8 + 3\sqrt{7}$ respectivement.

Remarque. $d > 0 \Rightarrow K \subset \mathbb{R}$.
(a) On a $N_{K/\mathbb{Q}}(u_1) = -1$ d'où $u_1 \in O_K^\times$ par **7**, donc $u_1^n \in O_K^\times$ pour tout $n \in \mathbb{Z}$. Comme $u_1 > 1$ on a $u_n \neq u_m$ pour $n \neq m$, donc $O_K^\times$ est infini (et $n \mapsto u_n$ est un morphisme injectif $\mathbb{Z} \hookrightarrow O_K^\times$).
(b) Idem (noter que $2, 3, 6, 7$ sont tous $\equiv 2$ ou $3 \bmod 4\mathbb{Z}$).

10. On prend $d = 5$, donc $K = \mathbb{Q}(\sqrt{5})$. Pour tout $n \in \mathbb{Z}$ on pose $u_n = (\frac{1}{2} + \frac{1}{2}\sqrt{5})^n \in K$.

(a) Montrer que $u_n \in O_K^\times$ pour tout $n \in \mathbb{Z}$. En déduire que $O_K^\times$ est infini.
(b) Mêmes questions avec $d = 13, 17$ et $u_1 = \frac{3}{2} + \frac{1}{2}\sqrt{13}, 4 + \sqrt{17}$ respectivement.

Même chose que **9** (noter que $5, 13, 17$ sont tous $\equiv 1 \bmod 4\mathbb{Z}$).

Remarque. On a le résultat suivant.

Theorem 3.2. *Soit $K = \mathbb{Q}(\sqrt{d})$ avec $d > 0$ entier sans facteur carré. Il existe $u_K \in O_K^\times$ tel que $O_K^\times = \{\pm u_K^n,\ n \in \mathbb{Z}\}$.*

En d'autres termes $O_K^\times$ est un groupe abélien de type fini isomorphe à $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}$ (un isomorphisme est donné par $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z} \to O_K^\times$, $(\varepsilon, n) \mapsto (-1)^\varepsilon u_K^n$).

4. Irréductibles

11. Soit $\alpha \in O_K$. Montrer que $N_{K/\mathbb{Q}}(\alpha)$ irréductible dans $\mathbb{Z} \Rightarrow \alpha$ irréductible dans O_K.

Remarque. La réciproque est fausse, voir **12.**(b),(d).
Soit $\alpha \in O_K$ réductible c'est-à-dire $\alpha = \beta\gamma$ avec $\beta, \gamma \in O_K$ et $\beta, \gamma \notin O_K^\times$. Alors $N_{K/\mathbb{Q}}(\alpha) = N_{K/\mathbb{Q}}(\beta)N_{K/\mathbb{Q}}(\gamma)$ par **6**, avec $N_{K/\mathbb{Q}}(\beta), N_{K/\mathbb{Q}}(\gamma) \in \mathbb{Z}$ et $N_{K/\mathbb{Q}}(\beta), N_{K/\mathbb{Q}}(\gamma) \notin \mathbb{Z}^\times$ par **7**. Donc $N_{K/\mathbb{Q}}(\alpha)$ est réductible dans $\mathbb{Z}$.

12. On prend $d = -5$, donc $K = \mathbb{Q}(\sqrt{-5})$.

(a) Montrer que $a^2 + 5b^2 \neq 2$ et $a^2 + 5b^2 \neq 3$ pour tous $a, b \in \mathbb{Z}$.
(b) Montrer que $2, 3, 1 + \sqrt{-5}, 1 - \sqrt{-5}$ sont des éléments irréductibles de O_K.
(c) Montrer que O_K n'est pas factoriel.
(d) Mêmes questions avec $d = 10$ et $2, 3, 4 + \sqrt{10}, 4 - \sqrt{10}$.

(a) Soient $a, b \in \mathbb{Z}$. On a $a^2 + 5b^2 = 2 \Rightarrow a^2 \equiv 2 \bmod 5\mathbb{Z}$. La classe de 2 n'étant pas un carré dans $\mathbb{Z}/5\mathbb{Z}$ (les carrés dans $\mathbb{Z}/5\mathbb{Z}$ sont les classes de $0, 1$ et 4) on en déduit que $a^2 + 5b^2 \neq 2$. De même la classe de 3 n'est pas un carré dans $\mathbb{Z}/5\mathbb{Z}$. (Autre preuve : si $b = 0$ on a $a^2 \neq 2, 3$ et si $b \neq 0$ alors $a^2 + 5b^2 \geq 5$.)
(b) Soient $\alpha, \beta \in O_K$ tels que $2 = \alpha\beta$. On a $4 = N_{K/\mathbb{Q}}(2) = N_{K/\mathbb{Q}}(\alpha)N_{K/\mathbb{Q}}(\beta)$ par **6**, d'où $N_{K/\mathbb{Q}}(\alpha) = 1, 2$, ou 4 (car $d < 0 \Rightarrow N_{K/\mathbb{Q}}(\xi) \geq 0$ pour tout $\xi \in K$). D'après **5** on a $O_K = \mathbb{Z}[\sqrt{-5}]$ puisque $-5 \equiv 3 \bmod 4\mathbb{Z}$, donc $\alpha = a + b\sqrt{-5}$ avec $a, b \in \mathbb{Z}$. D'après (a) $N_{K/\mathbb{Q}}(\alpha) = a^2 + 5b^2 \neq 2$, donc soit $N_{K/\mathbb{Q}}(\alpha) = 1$ ce qui équivaut à $\alpha \in O_K^\times$ par **7**, soit $N_{K/\mathbb{Q}}(\alpha) = 4$ ce qui équivaut à $N_{K/\mathbb{Q}}(\beta) = 1$, i.e. $\beta \in O_K^\times$. Donc 2 est irréductible dans O_K. Les autres cas se traitent de façon similaire en utilisant $N_{K/\mathbb{Q}}(3) = 9$ et $N_{K/\mathbb{Q}}(1 + \sqrt{-5}) = N_{K/\mathbb{Q}}(1 - \sqrt{-5}) = 6$.
(c) On a $6 = 2.3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ et $2, 3, 1 + \sqrt{-5}, 1 - \sqrt{-5}$ sont irréductibles dans O_K d'après (b). Donc 6 admet deux décompositions différentes en produit d'irréductibles dans O_K, donc O_K n'est pas factoriel.
(d) On a $10 \equiv 2 \bmod 4\mathbb{Z}$ d'où $O_K = \mathbb{Z}[\sqrt{10}]$, $a^2 - 10b^2 \neq 2, 3$ pour tous $a, b \in \mathbb{Z}$ puisque ni 2 ni 3 ne sont des carrés dans $\mathbb{Z}/10\mathbb{Z}$ (les carrés dans $\mathbb{Z}/10\mathbb{Z}$ sont $0, 1, 4, 5, 6$ et 9), et $N_{K/\mathbb{Q}}(2) = 4$, $N_{K/\mathbb{Q}}(3) = 9$, $N_{K/\mathbb{Q}}(4 - \sqrt{10}) = N_{K/\mathbb{Q}}(4 + \sqrt{10}) = 6$. La même preuve qu'en (b) montre que $2, 3, 4 + \sqrt{10}$ et $4 - \sqrt{10}$ sont irréductibles dans O_K, et O_K n'est pas factoriel puisque $6 = 2.3 = (4 + \sqrt{10})(4 - \sqrt{10})$.

13. On prend $d = -5$, donc $K = \mathbb{Q}(\sqrt{-5})$.

(a) Soit $\alpha \in O_K$. Montrer que $\alpha \mid 3$ et $\alpha \mid (1 + \sqrt{-5}) \Rightarrow \alpha \in O_K^\times$ (utiliser **12**(b)).
(b) Montrer que $\big(3O_K + (1 + \sqrt{-5})O_K\big) \cap \mathbb{Z} = 3\mathbb{Z}$.
(c) En déduire que le Lemme de Bézout est faux dans O_K.

(a) D'après **12**(b) les éléments 3 et $1 + \sqrt{-5}$ sont irréductibles dans O_K, donc $\alpha \mid 3 \Rightarrow \frac{\alpha}{3}$ ou $\alpha \in O_K^\times$ et $\alpha \mid (1 + \sqrt{-5}) \Rightarrow \frac{\alpha}{1+\sqrt{-5}}$ ou $\alpha \in O_K^\times$. On en déduit le résultat.
(b) On a $3\mathbb{Z} \subset \mathbb{Z}$ et $3\mathbb{Z} \subset 3O_K \subset 3O_K + (1 + \sqrt{-5})O_K$ d'où $3\mathbb{Z} \subseteq (3O_K + (1 + \sqrt{-5})O_K) \cap \mathbb{Z}$. Comme $-5 \equiv 3 \bmod 4\mathbb{Z}$ on a $O_K = \mathbb{Z}[\sqrt{-5}]$ par **5**, donc tout élément de l'idéal $(3O_K + (1+\sqrt{-5})O_K)$ s'écrit comme $3(a+b\sqrt{-5}) + (1+\sqrt{-5})(a'+b'\sqrt{-5})$ avec $a, b, a', b' \in \mathbb{Z}$. On a $3(a+b\sqrt{-5}) + (1+\sqrt{-5})(a'+b'\sqrt{-5}) = (3a+a'-5b') + (3b+a'+b')\sqrt{-5} \in \mathbb{Z} \Leftrightarrow 3b+a'+b' = 0$, ce qui implique $3a + a' - 5b' = 3a + a' + b' - 6b' = 3a - 3b - 6b' \in 3\mathbb{Z}$. Donc $(3O_K + (1 + \sqrt{-5})O_K) \cap \mathbb{Z} \subseteq 3\mathbb{Z}$.
(c) Les éléments 3 et $1 + \sqrt{-5}$ sont premiers entre eux d'après (a), et d'après (b) on a $(3O_K + (1 + \sqrt{-5})O_K) \cap \mathbb{Z} = 3\mathbb{Z}$ ce qui par **2** implique $3O_K + (1 + \sqrt{-5})O_K \neq O_K$.

5. Anneaux euclidiens

14. On prend $d = -1$, donc $K = \mathbb{Q}(\sqrt{-1}) = \mathbb{Q}(i)$. Soient $\alpha, \beta \in O_K$ avec $\beta \neq 0$ et $x, y \in \mathbb{Q}$ tels que $\frac{\alpha}{\beta} = x + iy \in K$.

(a) Montrer qu'il existe $a, b \in \mathbb{Z}$ tels que $|x - a| \leq \frac{1}{2}$ et $|y - b| \leq \frac{1}{2}$.
(b) Montrer que $|\frac{\alpha}{\beta} - (a + ib)| \leq \frac{1}{\sqrt{2}}$.
(c) Soient $\delta = a + ib$ et $\rho = \alpha - \delta\beta$. Montrer que $N_{K/\mathbb{Q}}(\rho) < N_{K/\mathbb{Q}}(\beta)$.
(d) En déduire que O_K est euclidien.

Remarque. Pour tout $z = x + iy \in \mathbb{Q}(i)$ on a $N_{\mathbb{Q}(i)/\mathbb{Q}}(z) = x^2 + y^2 = |z|^2$.
(a) On a $\mathbb{Q} \oplus \mathbb{Q} \subset \mathbb{R} \oplus \mathbb{R}$ et $\mathbb{R} \oplus \mathbb{R} = \bigcup_{(a,b)\in\mathbb{Z}\oplus\mathbb{Z}} \{(x, y) \in \mathbb{R} \oplus \mathbb{R}$ tels que $|x - a| \leq \frac{1}{2}$ et $|y - b| \leq \frac{1}{2}\}$.

(b) On a $|\frac{\alpha}{\beta} - (a+ib)| = |(x-a)+i(y-b)| = \sqrt{(x-a)^2+(y-b)^2} \leq \sqrt{\frac{1}{4}+\frac{1}{4}} = \frac{1}{\sqrt{2}}$ par (a).
(c) On a $\rho = \beta(\frac{\alpha}{\beta} - (a+ib))$ et par (c) on obtient $N_{K/\mathbb{Q}}(\rho) = N_{K/\mathbb{Q}}(\beta)N_{K/\mathbb{Q}}(\frac{\alpha}{\beta} - (a+ib)) = N_{K/\mathbb{Q}}(\beta)|\frac{\alpha}{\beta} - (a+ib)|^2 \leq \frac{1}{2}N_{K/\mathbb{Q}}(\beta) < N_{K/\mathbb{Q}}(\beta)$.
(d) On a $\alpha = \beta\delta + \rho$ avec $\delta, \rho \in O_K$ et $N_{K/\mathbb{Q}}(\rho) < N_{K/\mathbb{Q}}(\beta)$. Donc O_K muni de l'application $N_{K/\mathbb{Q}} : O_K \to \mathbb{N}$ est euclidien.

15. On prend $d = 2$, donc $K = \mathbb{Q}(\sqrt{2})$. Montrer que O_K est euclidien.

Soient $\alpha, \beta \in O_K$ avec $\beta \neq 0$. Soient $x, y \in \mathbb{Q}$ tels que $\frac{\alpha}{\beta} = x + iy \in K$. Soient $a, b \in \mathbb{Z}$ tels que $|x-a| \leq \frac{1}{2}$ et $|y-b| \leq \frac{1}{2}$. Enfin, soient $\delta = a + ib, \rho = \alpha - \delta\beta \in O_K$. Alors on a $\alpha = \beta\delta + \rho$ et $|N_{K/\mathbb{Q}}(\rho)| = |N_{K/\mathbb{Q}}(\beta)N_{K/\mathbb{Q}}(\frac{\alpha}{\beta} - (a+ib))| = |N_{K/\mathbb{Q}}|\,|(x-a)^2 - 2(y-b)^2| \leq |N_{K/\mathbb{Q}}|(|x-a|^2 + 2|y-b|^2) \leq |N_{K/\mathbb{Q}}|(\frac{1}{4} + 2\frac{1}{4}) = \frac{3}{4}|N_{K/\mathbb{Q}}| < |N_{K/\mathbb{Q}}|$. Donc O_K muni de l'application $|N_{K/\mathbb{Q}}| : O_K \to \mathbb{N}$ est euclidien.

6. Ramification

On fixe un nombre premier *impair* $p \in \mathbb{Z}$.

16. Montrer que l'inclusion $\mathbb{Z}[\sqrt{d}\,] \hookrightarrow O_K$ induit un isomorphisme d'anneaux unitaires

$$\mathbb{Z}[\sqrt{d}\,]/p\mathbb{Z}[\sqrt{d}\,] \xrightarrow{\sim} O_K/pO_K.$$

Si $d \equiv 2$ ou $3 \bmod 4\mathbb{Z}$ alors $O_K = \mathbb{Z}[\sqrt{d}]$ d'après **5** d'où $pO_K = p\mathbb{Z}[\sqrt{d}]$ et donc $O_K/pO_K = \mathbb{Z}[\sqrt{d}]/p\mathbb{Z}[\sqrt{d}]$.
Supposons $d \equiv 1 \bmod 4\mathbb{Z}$ donc $O_K = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$. Soit $\varphi : \mathbb{Z}[\sqrt{d}] \hookrightarrow O_K \to O_K/pO_K$ le morphisme d'anneaux unitaires obtenu en composant l'inclusion de $\mathbb{Z}[\sqrt{d}]$ dans O_K avec le morphisme de projection $O_K \to O_K/pO_K$. On a $\operatorname{Ker}\varphi = \mathbb{Z}[\sqrt{d}] \cap p\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$. On a $p\mathbb{Z}[\sqrt{d}] \subset \mathbb{Z}[\sqrt{d}]$, et $\mathbb{Z}[\sqrt{d}] \subset \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ d'où $p\mathbb{Z}[\sqrt{d}] \subset p\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$, par conséquent $p\mathbb{Z}[\sqrt{d}] \subseteq \operatorname{Ker}\varphi$.
Soient $a, b, a', b' \in \mathbb{Z}$; on a $a + b\sqrt{d} = pa' + pb'\frac{1+\sqrt{d}}{2} \Leftrightarrow 2a + 2b\sqrt{d} = p(2a' + b') + pb'\sqrt{d} \Leftrightarrow 2a = p(2a' + b')$ et $2b = pb'$.
Si $b' = 0$ on a $a + b\sqrt{d} = pa' \Leftrightarrow (a, b) = (pa', 0)$; si $2a' + b' = 0$ on a $a + b\sqrt{d} = -pa'\sqrt{d} \Leftrightarrow (a, b) = (0, -pa'^!)$; si $b'(2a' + b') \neq 0$ on a $2a = p(2a' + b')$ et $2b = pb' \Rightarrow p \mid a$ et $p \mid b$ puisque p est impair. On en déduit que $\operatorname{Ker}\varphi \subseteq p\mathbb{Z}[\sqrt{d}]$. Donc $\operatorname{Ker}\varphi = p\mathbb{Z}[\sqrt{d}]$.
Comme p est impair il est premier à 2 et par le lemme de Bezout ($\mathbb{Z}$ principal) il existe $r, s \in \mathbb{Z}$ tels que $2r + ps = 1$. On a $(r + r\sqrt{d}) + ps\frac{1+\sqrt{d}}{2} = (2r + ps)\frac{1+\sqrt{d}}{2} = \frac{1+\sqrt{d}}{2}$, donc $\frac{1+\sqrt{d}}{2} \in \mathbb{Z}[\sqrt{d}] + p\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$, ce qui équivaut à $\mathbb{Z}[\frac{1+\sqrt{d}}{2}] \subseteq \mathbb{Z}[\sqrt{d}] + p\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$. Comme $\mathbb{Z}[\sqrt{d}] + p\mathbb{Z}[\frac{1+\sqrt{d}}{2}] \subseteq \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ on en déduit $\mathbb{Z}[\sqrt{d}] + p\mathbb{Z}[\frac{1+\sqrt{d}}{2}] = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$, ce qui signifie que φ est surjective.

17. Montrer que le morphisme $\mathbb{Z}[X] \to \mathbb{Z}[\sqrt{d}]$, $P(X) \mapsto P(\sqrt{d})$ induit un isomorphisme d'anneaux unitaires

$$\big(\mathbb{Z}/p\mathbb{Z}\big)[X]\Big/(X^2 - \bar{d}\,) \xrightarrow{\sim} O_K/pO_K$$

où $\bar{d} = d + p\mathbb{Z}$ est la classe de d modulo $p\mathbb{Z}$.

Le morphisme $\psi : \mathbb{Z}[X] \to \mathbb{Z}[\sqrt{d}]$, $P(X) \mapsto P(\sqrt{d})$ est surjectif. Son noyau est l'intersection de $\mathbb{Z}[X]$ avec le noyau du morphisme $\mathbb{Q}[X] \to \mathbb{Q}[\sqrt{d}]$, $P(X) \mapsto P(\sqrt{d})$, lequel est $(X^2 - d)\mathbb{Q}[X]$ puisque $X^2 - d$ est irréductible dans $\mathbb{Q}[X]$ (d sans facteur carré). Donc $\operatorname{Ker}\psi = (X^2 - d)\mathbb{Z}[X]$ et ψ induit un isomorphisme d'anneaux unitaires $\mathbb{Z}[X]/(X^2 - d) \xrightarrow{\sim} \mathbb{Z}[\sqrt{d}]$. On en déduit un isomorphisme $\big(\mathbb{Z}[X]/(X^2 - d)\big)/p\big(\mathbb{Z}[X]/(X^2 - d)\big) \xrightarrow{\sim} \mathbb{Z}[\sqrt{d}]/p\mathbb{Z}[\sqrt{d}]$. L'isomorphisme $\mathbb{Z}[X]/p\mathbb{Z}[X] \simeq (\mathbb{Z}/p\mathbb{Z})[X]$ induit un isomorphisme $\big(\mathbb{Z}[X]/(X^2 - d)\big)/p\big(\mathbb{Z}[X]/(X^2 - d)\big) \simeq (\mathbb{Z}/p\mathbb{Z})[X]/(X^2 - \bar{d}\,)$ et d'après **16** on a un isomorphisme $\mathbb{Z}[\sqrt{d}]/p\mathbb{Z}[\sqrt{d}] \simeq O_K/pO_K$. En composant on obtient un isomorphisme $(\mathbb{Z}/p\mathbb{Z})[X]/(X^2 - \bar{d}\,) \simeq O_K/pO_K$.

Definition 6.1. L'entier d est un *carré modulo* n si le polynôme $X^2 - \bar{d} \in \big(\mathbb{Z}/n\mathbb{Z}\big)[X]$ a une racine dans $\mathbb{Z}/n\mathbb{Z}$, c'est-à-dire s'il existe $r \in \mathbb{Z}$ tel que $d \equiv r^2 \bmod n\mathbb{Z}$.

18. Montrer que

$$\begin{aligned} d \in p\mathbb{Z} &\Rightarrow O_K/pO_K \text{ n'est pas intègre} \\ d \notin p\mathbb{Z} \text{ et } d \text{ carré modulo } p &\Rightarrow O_K/pO_K \simeq \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z} \\ d \text{ non carré modulo } p &\Rightarrow O_K/pO_K \text{ est un corps.} \end{aligned}$$

Si $d \in p\mathbb{Z}$ alors $O_K/pO_K \simeq (\mathbb{Z}/p\mathbb{Z})[X]/(X^2)$ d'après **17**. En notant $\bar{X} = X + X^2\mathbb{Z}[X]$ on a $\bar{X} \neq 0$ et $\bar{X}^2 = 0$, donc O_K n'est pas intègre.
Si $d \notin p\mathbb{Z}$ et $d \equiv r^2 \bmod p\mathbb{Z}$ alors $X^2 - \bar{d} = X^2 - \bar{r}^2 = (X-\bar{r})(X+\bar{r})$ dans $(\mathbb{Z}/p\mathbb{Z})[X]$ qui est principal puisque $\mathbb{Z}/p\mathbb{Z}$ est un corps. De plus $\bar{r} \neq -\bar{r}$ puisque $p \neq 2$, donc $X-\bar{r}$ et $X+\bar{r}$ sont premiers entre eux dans $(\mathbb{Z}/p\mathbb{Z})[X]$ (irréductibles distincts). Par **17** et le théorème chinois on obtient $O_K/pO_K \simeq (\mathbb{Z}/p\mathbb{Z})[X]/(X-\bar{r})(X+\bar{r}) \simeq (\mathbb{Z}/p\mathbb{Z})[X]/(X-\bar{r}) \oplus (\mathbb{Z}/p\mathbb{Z})[X]/(X+\bar{r}) \simeq \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$.
Si d n'est pas un carré modulo p alors $X^2 - \bar{d}$ est irréductible et donc $(X^2 - \bar{d})$ est maximal dans $(\mathbb{Z}/p\mathbb{Z})[X]$. Par **17** on a $O_K/pO_K \simeq (\mathbb{Z}/p\mathbb{Z})[X]/(X^2 - \bar{d})$ qui est un corps puisque $(X^2 - \bar{d})$ est maximal.

19. On suppose que O_K est factoriel. Montrer que

$$\begin{aligned} d \in p\mathbb{Z} &\Rightarrow p = \pi^2 \text{ avec } \pi \in O_K \text{ irréductible} \\ d \notin p\mathbb{Z} \text{ et } d \text{ carré modulo } p &\Rightarrow p = \pi_1\pi_2 \text{ avec } \pi_1 \neq \pi_2 \in O_K \text{ irréductibles} \\ d \text{ non carré modulo } p &\Rightarrow p \text{ est irréductible dans } O_K. \end{aligned}$$

On a $N_{K/\mathbb{Q}}(p) = p^2 \notin \mathbb{Z}^\times$ donc par **7** $p \notin O_K^\times$. Soient $m \geq 1$, $n_j \geq 1$, et $\pi_j \in O_K$ irréductibles deux à deux distincts tels que $p = \pi_1^{n_1} \dots \pi_m^{n_m}$. Le théorème chinois donne $O_K/pO_K \simeq O_K/\pi_1^{n_1}O_K \oplus \dots \oplus O_K/\pi_m^{n_m}O_K$, donc O_K/pO_K est intègre ssi $n_j = 1$ pour tout $1 \leq j \leq m$ auquel cas c'est un corps ssi $m = 1$. On en déduit le résultat par **19**.

20. On suppose $p \equiv 1 \bmod 4\mathbb{Z}$.

(a) Montrer que -1 est un carré modulo p.
(b) Montrer qu'il existe $a, b \in \mathbb{Z}$ tels que $p = a^2 + b^2$.

(a) Soit x un générateur du groupe multiplicatif cyclique $(\mathbb{Z}/p\mathbb{Z})^\times$ d'ordre $p-1$. Comme p est impair on a $\frac{p-1}{2} \in \mathbb{Z}$, d'où $\operatorname{ord}\left(x^{\frac{p-1}{2}}\right) = 2$ et par conséquent $x^{\frac{p-1}{2}} = -1$. Comme 4 divise $p-1$ on a $\frac{p-1}{4} \in \mathbb{Z}$, d'où $\left(x^{\frac{p-1}{4}}\right)^2 = -1$.
(b) Soit $K = \mathbb{Q}(\sqrt{-1}) = \mathbb{Q}(i)$. Par **5** $O_K = \mathbb{Z}[i]$ et d'après **14** c'est un anneau euclidien donc factoriel. Comme -1 est un carré carré modulo p par (a), on a d'après **19** $p = \pi_1\pi_2$ avec $\pi_1 \neq \pi_2 \in O_K$ irréductibles. La norme $N_{K/\mathbb{Q}}$ est positive et l'on a $N_{K/\mathbb{Q}}(p) = p^2 = N_{K/\mathbb{Q}}(\pi_1)N_{K/\mathbb{Q}}(\pi_2)$ avec $N_{K/\mathbb{Q}}(\pi_j) \neq 1$ (sinon π_j serait une unité par **7**), donc $N_{K/\mathbb{Q}}(\pi_1) = N_{K/\mathbb{Q}}(\pi_2) = p$ puisque p est premier. Soient $a, b \in \mathbb{Z}$ tels que $\pi_1 = a + ib$; alors $N_{K/\mathbb{Q}}(a+ib) = a^2 + b^2 = p$.