TD1 TANC - Ordres quadratiques imaginaires

Exercice 1. On pose $S = \mathbb{Z}\left[\sqrt{-2}\right]$.

1. S'agit-il d'un ordre maximal ? Quel est son discriminant ?
   Oui, l'ordre maximal de $\mathbb{Q}(\sqrt{-2})$ est $\mathbb{Z}[\sqrt{-2}]$ car $-2 \neq 1 \mod 4$. Pour les mêmes raisons son discriminant est $-2 \times 4 = -8$.
2. Factoriser $\langle 7 \rangle$ en idéaux premiers dans $\mathbb{Z}\left[\sqrt{-2}\right]$.
   7 est un entier impair donc sa factorisation est décrite dans la Proposition 4.11 du cours. On a $\left(\frac{\Delta}{7}\right) = \left(\frac{6}{7}\right) = -1$ donc 7 est inerte, i.e. $\langle 7 \rangle$ est sa propre factorisation en idéaux premiers.
3. Même question avec $\langle 11 \rangle$. Les idéaux intervenant dans la décomposition de $\langle 11 \rangle$ sont-ils principaux ?
   On a $\left(\frac{-8}{11}\right) = \left(\frac{-2\times 4}{11}\right) = \left(\frac{9}{11}\right) = 1$ donc $\langle 11 \rangle = \mathfrak{p}\overline{\mathfrak{p}}$ avec $\mathfrak{p} = \langle 11, \sqrt{-2} - a \rangle$ où a une des racines de $X^2 + 2 \mod 11$ donc $a = 3$ par exemple. On a donc
   $$\langle 11 \rangle = \langle 11, \sqrt{-2} - 3 \rangle \langle 11, \sqrt{-2} + 3 \rangle = \mathfrak{p}\overline{\mathfrak{p}}.$$
   Pour déterminer s'ils sont principaux on peut le faire de deux façons différentes. Puisque $\mathbb{Z}[\sqrt{-2}]$ est principal alors tous les idéaux sont principaux, en particuliers $\mathfrak{p}$ et $\overline{\mathfrak{p}}$. Sinon, on peut remarquer que $N(-3 + \sqrt{-2}) = (-3 + \sqrt{-2})(-3 - \sqrt{-2}) = 11$ donc $11 \in \langle -3 + \sqrt{-2} \rangle$, i.e. $\mathfrak{p} = \langle -3 + \sqrt{-2} \rangle$ et $\overline{\mathfrak{p}} = \langle 3 + \sqrt{-2} \rangle$.
4. On considère désormais $R = \mathbb{Z}[\omega]$ avec $\omega = 2\sqrt{-2}$ le sous-ordre de S de conducteur 2. On considère l'idéal $\mathfrak{a} = \langle 3, 1 + \omega \rangle$ de R.
   (a) Quelle est la norme de $\mathfrak{a}$?
   Pour pouvoir appliquer $N(\langle 3, 1 + \omega \rangle) = nm$ il faut vérifier que le $\mathbb{Z}$-module engendré par les deux générateur est bien l'idéal $\mathfrak{a}$. On a $3 | N(1 + \omega) = 1 + 2 \cdot 4 = 9$ donc c'est bon : $N(\mathfrak{a}) = 3$.
   (b) L'idéal $\mathfrak{a}$ est-il principal ?
   Si $\mathfrak{a}$ était principal alors on aurait $\mathfrak{a} = \langle \alpha \rangle$ pour un certain $\alpha \in R$ donc $N(\mathfrak{a}) = N(\alpha)$. Soit $\alpha = a + b\omega$ avec $a, b \in \mathbb{Z}$ un tel générateur. On a alors $N(\alpha) = a^2 + 8b^2 = 3$ qui n'a pas de solution donc $\mathfrak{a}$ n'est pas principal.
   (c) Montrer que $\mathfrak{a}$ est inversible (on pourra déterminer l'idéal $\mathfrak{a}\overline{\mathfrak{a}}$).

   Méthode 1 : Le conducteur $f = 2$ est premier avec $N(\mathfrak{a}) = 3$ donc $\mathfrak{a}$ est inversible (cf. Proposition 4.9 ou Exercice 7).

   Méthode 2 : On a
   $$\mathfrak{a}\overline{\mathfrak{a}} = \langle 9, 3(1+\omega), 3(1-\omega), N(1+\omega) \rangle = \Big\langle 9, \underbrace{6}_{3(1+\omega)+3(1-\omega)}, 3(1-\omega), 9 \Big\rangle = \langle 3, 6, 3(1-\omega), 9 \rangle = \langle 3 \rangle$$
   donc $\mathfrak{a}$ inversible d'inverse $\frac{1}{3}\overline{\mathfrak{a}}$.
   (d) Que peut-on en déduire sur $\mathrm{Cl}(R)$?
   On a donc que $\mathfrak{a}$ est inversible donc a une classe dans le quotient $\mathrm{Cl}(R)$ pourtant il n'est pas principal donc sa classe est non-triviale, i.e. $\mathrm{Cl}(R)$ n'est pas réduit au neutre $[R]$.
5. On considère $\mathfrak{b} = \langle 2, \omega \rangle \subseteq R$.
   (a) Montrer que $\overline{\mathfrak{b}} = \mathfrak{b}$.
   On a $\overline{\omega} = -\omega$.
   (b) Montrer que $\mathfrak{b}^2 = \langle 4, 2\omega \rangle$.
   On a $\mathfrak{b}^2 = \langle 4, 2\omega, \omega^2 \rangle = \langle 4, 2\omega, -8 \rangle = \langle 4, 2\omega \rangle$.
   (c) En déduire que $\mathfrak{b}$ n'est pas inversible.
   On a $4 | N(2\omega) = 4 \cdot 8 = 32$ donc sa norme est $4 \cdot 2 = 8$. Si $\mathfrak{b}$ était inversible on aurait $\mathfrak{b}\overline{\mathfrak{b}} = \mathfrak{b}^2 = N(\mathfrak{b})R = 2R$ qui serait donc de norme $N(2) = 4$.

Exercice 2. On pose $R = \mathbb{Z}\left[\sqrt{-21}\right]$ et $\omega = \sqrt{-21}$. On admet que $\left\{R, \underbrace{\langle 3, \omega\rangle}_{\mathfrak{a}}, \underbrace{\langle 2, 1+\omega\rangle}_{\mathfrak{b}}, \underbrace{\langle 5, 3+\omega\rangle}_{\mathfrak{c}}\right\}$ sont des représentants de toutes les classes de $\mathrm{Cl}(R)$.

1. Les idéaux $\mathfrak{a}, \mathfrak{b}$ et $\mathfrak{c}$ sont-ils premiers ?
   En vérifiant soigneusement que pour chacun des $\langle n, a+\omega\rangle$ on a $n | N(a+\omega)$ on en déduit qu'ils sont de normes $3, 2$ et 5 qui sont premiers donc les idéaux sont eux-mêmes premiers.
2. Combien R admet-il d'idéaux distincts de norme 2 ? de norme 3 ? de norme 5 ?
   Puisque R est maximal ($-21 = 3 \mod 4$) s'il existe un idéal $\mathfrak{p}$ de norme p on a systématiquement la factorisation $\mathfrak{p}\overline{\mathfrak{p}} = N(\mathfrak{p})R = pR$ donc il y en a au plus 2 : $\mathfrak{p}$ et $\overline{\mathfrak{p}}$. Il faut juste déterminer pour chacun que $\mathfrak{p} \neq \overline{\mathfrak{p}}$. On a $\mathfrak{b}$ de norme 2 et $\overline{\mathfrak{b}} = \langle 2, 1-\omega\rangle = \langle 2, 1-\omega-2\rangle = \mathfrak{b}$. Par ailleurs, $3|\Delta$ donc $\overline{\mathfrak{a}} = \mathfrak{a}$ (cf. Proposition 4.11 et $5 \nmid \Delta$ donc $\overline{\mathfrak{c}} \neq \mathfrak{c}$. Il y a donc 1 idéal de norme 2, 1 de norme 3 et 2 de norme 5.
3. Factoriser $\langle 10, 7+\omega\rangle$.
   Cet idéal est de norme 10 car $10|N(7+\omega) = 70$. Il se factorise donc en idéaux de norme 2 et 5. Il n'y a qu'un seul candidat pour l'idéal de norme 2 et on voit que $10 - (7+\omega) = 3 - \omega = \overline{3+\omega} \in \langle 7, 7+\omega\rangle$ donc il est inclus dans $\overline{\mathfrak{c}}$, i.e.
   $$\langle 10, 7+\omega\rangle = \mathfrak{b}\overline{\mathfrak{c}}$$
   est sa décomposition en idéaux premiers
4. Justifier que pour tout idéal $\mathfrak{d}$ de $R, \mathfrak{d}^4$ est principal.
   $\mathrm{Cl}(R)$ est un groupe d'ordre 4 donc ça vient du théorème de Lagrange.
5. Montrer que $\mathfrak{a}^2 = \langle 3\rangle$ et $\mathfrak{b}^2 = \langle 2\rangle$.
   ça vient du fait que $\overline{\mathfrak{a}} = \mathfrak{a}$ et pareil pour $\mathfrak{b}$. On peut aussi faire les calculs directement :
   $$\mathfrak{a}^2 = \langle 9, 3\omega, \omega^2\rangle = \langle 9, 3\omega, -21\rangle$$
   or le pgcd de 9 et 21 est 3 donc $3 \in \mathfrak{a}^2$.
6. En déduire que $\mathrm{Cl}(R) \simeq (\mathbb{Z}/2\mathbb{Z})^2$.
   C'est un groupe d'ordre 4 donc il est soit isomorphe à $\mathbb{Z}/4\mathbb{Z}$ soit à $(\mathbb{Z}/2\mathbb{Z})^2$. Or $\mathbb{Z}/4\mathbb{Z}$ n'admet qu'un élément d'ordre 2 (la classe de 2).
7. L'idéal $\mathfrak{abc}$ est-il principal ? Même question pour $\mathfrak{c}^{15}$.
   Dans $\mathrm{Cl}(R)$ on a $[\mathfrak{a}][\mathfrak{b}] = [\mathfrak{c}]$ (ça ne peut pas être $[\mathfrak{a}]$ ni $[\mathfrak{b}]$ ni $[R]$) donc $[\mathfrak{abc}] = [\mathfrak{c}^2] = [R]$ donc oui c'est un idéal principal. L'ordre de $[\mathfrak{c}]$ est 2 donc $\mathfrak{c}^{15}$ principal implique $2|15$ mais ce n'est pas le cas donc ce n'est pas un idéal principal.

Exercice 3 (Un premier exemple d'application aux courbes elliptiques)**.**

1. Soit E une courbe elliptique sur un corps fini $\mathbb{F}_q$. On pose a sa trace et π le morphisme de Frobenius de E. On suppose que E est ordinaire et on admet qu'alors $\mathrm{End}_{\overline{k}}(E)$ est isomorphe à un ordre dans un corps quadratique imaginaire $K = \mathbb{Q}(\sqrt{d})$.
   (a) Montrer que $X^2 - aX + q$ est le polynôme minimal de π dans K.
   Puisque π est annulé par le polynôme $\chi = X^2 - aX + q$ c'est un entier algébrique de degré au plus 2. S'il n'est pas de degré 2 il est de degré 1 et c'est donc un entier, i.e. on peut identifier π à une multiplication scalaire de la forme $[n]_E$. Si c'est un entier racine de χ alors, en particulier, χ est à racines réelles et donc son discriminant Δ est positif. Par ailleurs, d'après la borne de Hasse $\Delta = a^2 - 4q \leq 0$. Donc π est un entier si et seulement si $\Delta = a^2 - 4q$ auquel cas on a $a = 0 \mod p$, i.e. E supersingulière.
   (b) Montrer qu'on a toujours
   $$\mathbb{Z}[\pi] \subseteq \mathrm{End}_{\overline{k}}(E) \subseteq \mathscr{O}_K.$$
   On a $\pi \in \mathrm{End}(E)$ donc $\mathbb{Z}[\pi] \in \mathrm{End}(E)$. Par ailleurs, $\mathrm{End}(E)$ est un ordre dans un corps quadratique imaginaire donc est inclus dans l'ordre maximal.
2. On pose $E\colon y^2 = x^3 - x + 2$ sur $\mathbb{F}_5$.
   (a) Montrer que $E = \{(3, \pm 1), [0\colon 1\colon 0]\}$.
   On peut énumérer les point de E on trouve ces trois là.
   (b) Quelle est la trace de E ?
   Sa trace a satisfait $\#E(\mathbb{F}_5) = 5 + 1 - a$ donc $a = 6 - 3 = 3$.
   (c) Montrer que $\chi_\pi = X^2 - 3X + 5$ est le polynôme minimal de π.
   Puisque $3 \neq 0 \mod 5$ notre courbe est ordinaire donc on peut appliquer la question 1).

(d) Montrer que

$$\mathbb{Z}[\pi] = \mathbb{Z}[X]/\langle \chi_\pi \rangle \simeq \mathbb{Z}\left[\frac{1+\sqrt{-11}}{2}\right].$$

Le discriminant de χ_π est $\Delta = (-3)^2 - 4 \times 5 = -11$. Ainsi $\mathbb{Z}[\pi] = \mathbb{Z}[X]/\langle X^2 - aX + q \rangle$ est un ordre de discriminant -11 dans $\mathbb{Q}(\sqrt{\Delta}) = \mathbb{Q}(\sqrt{-11})$. Par ailleurs, par unicité de l'ordre associé à un discriminant on en déduit que $\mathbb{Z}[\pi] = \mathbb{Z}\left[\frac{1+\sqrt{-11}}{2}\right]$ puisque le discriminant de ce dernier est -11.

On peut aussi le voir directement de la façon suivante : le polynôme minimal de $\omega = \frac{1+\sqrt{-11}}{2}$ est $\chi = X^2 - X + 3$. Or $\chi_\pi(X+1) = (X+1)^2 - 3(X+1) + 5 = X^2 - X + 3 = \chi$ donc $\pi - 1$ et ω ont le même polynôme minimal, i.e. $\pi - 1 = \omega$ ou $\pi - 1 = \overline{\omega}$. On a alors

$$\mathbb{Z}[\pi] = \mathbb{Z}[\pi - 1] = \mathbb{Z}[\omega].$$

(e) En déduire que $\mathrm{End}_{\overline{\mathbb{F}_5}}(E) \simeq \mathbb{Z}\left[\frac{1+\sqrt{-11}}{2}\right]$.
Ceci provient des inclusions de la question 1.b) puisque $\mathbb{Z}[\omega]$ est l'ordre maximal.

Exercice 4. Soit $R = \mathbb{Z}[\omega]$ un ordre quadratique imaginaire et $\alpha = a + b\omega \in R$. On considère $\chi = X^2 - tX + n \in \mathbb{Z}[X]$ le polynôme minimal de ω. On pose $N(\alpha) = \overline{\alpha}\alpha$ et $\widetilde{N}(\alpha R) = \#R/\alpha R$. On veut montrer que

$$N(\alpha) = \widetilde{N}(\alpha R).$$

1. On identifie R à $\mathbb{Z}^2$ grâce à sa $\mathbb{Z}$-base $\mathscr{B} = (1, \omega)$. Montrer que $M = \begin{pmatrix} a & -nb \\ b & a + bt \end{pmatrix}$ est une matrice de présentation de $\alpha R \subseteq R$.
Le module αR est engendré par $\alpha \cdot 1, \alpha \cdot \omega$ et, dans la base $\mathscr{B}$ on a

$$\alpha = a + b\omega \text{ et } \alpha\omega = -nb + (a + bt)\omega$$

d'où l'expression de la matrice M qu'on cherche.

2. Montrer que $\#R/\alpha R = |\det M|$ (on pourra penser aux formes de Smith ou au théorème de la base adaptée).
On considère $S = PMQ = \begin{pmatrix} d_1 & 0 \\ 0 & d_2 \end{pmatrix}$ une forme de Smith de M avec P et Q inversibles donc de déterminant ± 1 et $d_1 | d_2$ des entiers positifs. Puisque $\alpha R = M\mathbb{Z}^2 = \mathrm{im}\, M \underset{{}^{-1}P}{\simeq} \mathrm{im}\, S$ on a

$$R/\alpha R \simeq \mathbb{Z}^2/\mathrm{im}\, M \simeq \mathbb{Z}^2/\mathrm{im}\, S \simeq \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z}.$$

Donc $\widetilde{N}(\alpha) = d_1 d_2$. Enfin, puisque $\det S = d_1 d_2 = \pm \det M = |\det M|$ on a donc bien le résultat annoncé.

3. Conclure.
On remarque que $N(\alpha) = (a + b\omega)(a + b\overline{\omega}) = a^2 + ba\overline{\omega} + ab\omega + b^2\omega\overline{\omega} = a^2 + abt + nb^2 = \det M = \widetilde{N}(\alpha)$.

Exercice 5 (Décomposition des premiers impairs)**.** Soit $K = \mathbb{Q}(\sqrt{d})$ un corps quadratique imaginaire, $\mathscr{O}_K = \mathbb{Z}[\omega_K] = \mathbb{Z}[X]/\langle \chi \rangle$ son ordre maximal de discriminant Δ_K et $R = \mathbb{Z}[X]/\langle \chi_\omega \rangle$ un ordre quelconque de discriminant Δ. On considère un nombre premier impair p.

1. Montrer que $R/\langle p \rangle \simeq \mathbb{F}_p[X]/\langle \chi_\omega \rangle$.
On a

$$R/\langle p \rangle \simeq \mathbb{Z}[X]/\langle \chi_\omega, p \rangle \simeq (\mathbb{Z}/p\mathbb{Z})[X]/\langle \chi_\omega \rangle \simeq \mathbb{F}_p[X]/\langle \chi_\omega \rangle.$$

2. Montrer que si Δ n'est pas un carré modulo p alors $\langle p \rangle$ est premier dans R.
Puisque $\mathbb{F}_p$ est de caractéristique $p \neq 2$, $\overline{\chi_\omega} \in \mathbb{F}_p[X]$ a une racine dans $\mathbb{F}_p$ si et seulement si son discriminant est un carré. Donc si son discriminant n'est pas un carré alors le quotient est une extension de degré 2 de $\mathbb{F}_p$, i.e. isomorphe à $\mathbb{F}_{p^2}$. En particulier, c'est un corps donc le quotient est intègre et donc $\langle p \rangle$ premier (même maximal) dans R.

3. On suppose que $p | \Delta$ et on pose $\mathfrak{p} = \langle p, \sqrt{\Delta_K} \rangle$.
(a) Montrer que $\mathfrak{p}^2 = \langle p \rangle$.
On a $\mathfrak{p}^2 = \langle p^2, p\sqrt{\Delta_K}, \Delta_K \rangle$ puisque $p | \Delta_K = 4d$ ou d et $p \neq 2$ alors $p | d$. Mais d est sans facteurs carrés [1] donc $\mathrm{pgcd}(p^2, \Delta_K) = p \in \mathfrak{p}^2$ et donc $\mathfrak{p}^2 = \langle p \rangle$.

1. C'est ici qu'on se sert de l'hypothèse $\mathscr{O}_K$ maximal. Si l'ordre n'était pas maximal alors son discriminant serait de la forme $4f^2d$ ou f^2d et il se pourrait donc que $p^2 | \Delta$ (si $p | f$).

(b) Justifier que $\chi \mod p$ possède une unique racine a. Montrer qu'alors $\mathfrak{p} = \langle p, \omega_K - a\rangle$.
Puisque $\Delta = 0 \in \mathbb{F}_p, \overline{\chi_\omega}$ admet une racine double $a \in \mathbb{F}_p$ donc $\chi_\omega(X) = (X-a)^2 + pQ \in \mathbb{Z}[X]$ et donc $(\omega - a)^2 = -pQ(\omega)$. En passant à la norme on a $p^2 | N(\omega - a)^2$ donc $p | N(\omega - a)$, i.e. $\langle p, \omega - a\rangle$ est bien un idéal de norme p. Par unicité de la décomposition en idéaux premier et la question 3.a) on a $\mathfrak{p} = \langle \omega - a\rangle$.

4. On suppose que $\Delta \mod p$ est un carré non nul.

(a) Montrer que χ possède deux racines distinctes a_1 et a_2 modulo p.
Puisque Δ est un carré non nul,χ_ω a deux racines distinctes modulo p.

(b) Montrer que les idéaux $\mathfrak{p}_i = \langle p, \omega - a_i\rangle$ définissent des idéaux premiers inversibles de R.
On écrit $\chi_\omega = X^2 - tX + n$ avec $t = \mathrm{Tr}(\omega) = \omega +$ et $n = N(\omega)$. On a $N(\omega - a_i) = a_i^2 - ta_i + n = \chi_\omega(a_i) = 0 \mod p$ donc $p | N(\omega - a_i)$ donc ce sont des idéaux p donc inversibles puisque p premier avec $\Delta = f^2 \Delta_K$ donc premier avec f, le conducteur de R.

(c) Montrer que $\mathfrak{p}_1\mathfrak{p}_2 \subseteq \langle p\rangle$.
On a

$$\mathfrak{p}_1\mathfrak{p}_2 = \left\langle p^2, p(\omega - a_1), p(\omega - a_2), (\omega - a_1)(\omega - a_2)\right\rangle = \left\langle p^2, p(\omega - a_1), p(\omega - a_2), pQ(\omega)\right\rangle \subseteq \langle p\rangle$$

avec $Q \in \mathbb{Z}[X]$ tel que $\chi_\omega(X) = (X - a_1)(X - a_2) + pQ(\omega)$.

(d) En déduire que $\mathfrak{p}_1\mathfrak{p}_2 = \langle p\rangle$.
On a $N(\mathfrak{p}_1\mathfrak{p}_2) = N(\mathfrak{p}_1)N(\mathfrak{p}_2) = p^2 = N(p)$ car les idéaux sont inversibles. On a donc une inclusion d'idéaux de même norme, c'est donc une égalité.

On aurait aussi pu invoquer le fait que $\mathfrak{p}_1\overline{\mathfrak{p}_1} = \langle p\rangle$ par inversibilité et en déduire que $\mathfrak{p}_2 = \overline{\mathfrak{p}_1}$ (ou le montrer directement) par unicité de la décomposition en idéaux premiers des idéaux inversibles.

(e) Montrer que $R/\langle p\rangle \simeq \mathbb{F}_p \times \mathbb{F}_p$ en déduire que $\mathfrak{p}_2 \neq \mathfrak{p}_1$ (on pourra remarquer que $\mathbb{F}_p \times \mathbb{F}_p$ ne contient pas d'élément nilpotent).
Soit par le théorème des restes on a

$$R/\langle p\rangle \simeq \mathbb{F}_p[X]/\langle \chi_\omega\rangle = \mathbb{F}_p[X]/\langle (X - a_1)(X - a_2)\rangle \simeq \mathbb{F}_p[X]/\langle X - a_1\rangle \times \mathbb{F}_p[X]/\langle X - a_2\rangle \simeq \mathbb{F}_p \times \mathbb{F}_p.$$

Toutes mes excuses, l'indication que je donne porte à confusion. Je voulais que vous disiez que $R/\langle p\rangle \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ ou $\simeq \mathbb{Z}/p^2\mathbb{Z}$ et en déduire que, puisqu'il n'y a pas de nilpotent alors on est dans le premier cas. Cependant, cette dichotomie s'obtient par le théorème de classification des groupes finis et il peut y avoir deux autres possibilités pour un anneau à p^2 éléments : $\mathbb{F}_{p^2}$ (exclus car notre quotient n'est pas intègre) et un autre anneau plus exotique [2] (mais exclus quand même car il contient des nilpotents). Bien entendu ce raisonnement est bien trop compliqué pour cette question. Je propose tout de même de montrer qu'il n'y a pas de nilpotent dans le quotient.

On prend $v = a\overline{X} + b \in \mathbb{F}_p[X]/\langle \chi_\omega\rangle$ avec $\overline{X}$ la classe de X dans le quotient un nilpotent tel que $(a\overline{X} + b)^n = 0$ avec $n \geq 2$. On a nécessairement $a \neq 0$ car sinon $v \in \mathbb{F}_p$ qui n'a pas de nilpotent. On a donc $\chi_\omega | (aX + b)^n$ ce qui signifie que $\frac{-b}{a} \in \mathbb{F}_p$ est une racine multiple de χ_ω ce qui est absurde d'après l'hypothèse $\Delta \neq 0 \in \mathbb{F}_p$.

J'ai fait l'effort de distinguer le cas maximal et le cas quelconque pour une excellente raison : le résultat de la question 3 est faux dans le cas quelconque.

Exercice 6 (Décomposition de 2)**.** Soit $\mathcal{O}_K = \mathbb{Z}[\omega]$ l'ordre maximal d'un corps quadratique imaginaire $\mathbb{Q}(\sqrt{d})$.

1. On suppose que $2 | \Delta_K$. On pose $\mathfrak{p} = \left\langle 2, 1 + \sqrt{d}\right\rangle$ si d impair et $\mathfrak{p} = \left\langle 2, \sqrt{d}\right\rangle$ sinon.

(a) Montrer que $\mathfrak{p}^2 = \langle 2\rangle$.
Si d est pair sans facteur carré alors $\mathrm{pgcd}(4, d) = 2$ donc

$$\mathfrak{p}^2 = \left\langle 4, 2\sqrt{d}, d\right\rangle = \langle 2\rangle.$$

Sinon, d est impair et puisque $2 | \Delta$ c'est que $d = 3 \mod 4$

$$\mathfrak{p}^2 = \left\langle 2, 1 + \sqrt{d}\right\rangle^2 = \left\langle 4, 2 + 2\sqrt{d}, 1 + d + 2\sqrt{d}\right\rangle = \left\langle 4, 2 + 2\sqrt{d}, d - 1\right\rangle$$

on a donc $d - 1 = 2 \mod 4$ donc $\mathrm{pgcd}(4, d - 1) = 2$ et la conclusion est la même.

2. Cet autre anneau est isomorphe à $S/\mathfrak{p}^2$ avec S un ordre quadratique et $\mathfrak{p}$ un idéal de norme p qui divise le discriminant de S. Prendre par exemple S l'ordre maximal de $\mathbb{Q}(\sqrt{-p})$.

(b) **Une curiosité arithmétique** (question facultative). Si je vous demande quel est votre anneau commutatif unitaire à 4 éléments préféré je suis à peu près certain que vous me répondrez que c'est l'un des 3 anneaux non-isomorphes suivants : $\mathbb{Z}/4\mathbb{Z}, (\mathbb{Z}/2\mathbb{Z})^2$ ou $\mathbb{F}_4$. On considère $A = \mathscr{O}_K/\langle 2\rangle$. Montrer que A est de caractéristique 2 et qu'il admet un nilpotent. En déduire que A n'est isomorphe à aucun des 3 anneaux [3] à 4 éléments cités précédemment.
L'anneau A est de caractéristique 2 car ce n'est pas l'anneau nul et $2 = 0 \in A$ (donc $A \not\simeq \mathbb{Z}/4\mathbb{Z}$). Si on pose $u = \sqrt{d}$ ou $u = 1 + \sqrt{d}$ suivant la parité de d on a alors $u \neq 0 \in A$ et $u^2 \in \mathfrak{p}^2 = \langle 2\rangle$ donc $u^2 = 0 \in A$, i.e. u nilpotent donc $A \not\simeq \mathbb{F}_4$ qui est un corps et $A \not\simeq (\mathbb{Z}/2\mathbb{Z})^2$ qui n'est pas intègre mais ne possède aucun nilpotent.

2. On suppose que $2 \nmid \Delta_K$.
   (a) Justifier qu'on a alors $d = 1 \mod 4$ et que $\mathscr{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$. On pose $\omega = \frac{1+\sqrt{d}}{2}$.
   Dans tous les autres cas $\Delta = 4d$ donc $2|\Delta$.
   (b) On suppose que $d = 1 \mod 8$. Montrer que $\mathfrak{p} = \langle 2, 1+\omega\rangle$ vérifie $\mathfrak{p}\overline{\mathfrak{p}} = \langle 2\rangle$. Justifier que $\mathfrak{p} \neq \overline{\mathfrak{p}}$ (on pourra justifier que $R/\langle 2\rangle$ n'a pas de nilpotent).
   On a
$$\begin{aligned}\mathfrak{p}\overline{\mathfrak{p}} &= \langle 4, 2(1+\omega), 2(1+\overline{\omega}), N(1+\omega)\rangle \\ &= \left\langle 4, 2(1+\omega) + 2(1+\overline{\omega}) - 4, 2(1+\overline{\omega}), 2 + \frac{1-d}{4}\right\rangle \\ &= \left\langle 4, 2\cdot \underbrace{(\omega+\overline{\omega})}_{1}, 2(1+\overline{\omega}), 2\left(1 + \frac{1-d}{8}\right)\right\rangle \\ &= \langle 2\rangle\end{aligned}$$
   On a $\overline{\mathfrak{p}} = \langle 2, 1+\overline{\omega}\rangle = \langle 2, 1+1-\omega\rangle = \langle 2, \omega\rangle$. On a alors $\mathfrak{p} = \overline{\mathfrak{p}}$ si et seulement si $\omega \in \mathfrak{p}$ ce qui impliquerait que $\omega + 1 - \omega = 1 \in \mathfrak{p}$, i.e. $R = \mathfrak{p}$ ce qui est absurde puisqu'il est de norme 2.
   (c) On suppose que $d = 5 \mod 8$. Montrer qu'alors $\langle 2\rangle$ est un idéal premier.
   Puisque $\chi = X^2 - X + \frac{1-d}{4}$ est le polynôme minimal de ω et $\frac{1-d}{4} = 1 \mod 2$ on a
$$R/\langle 2\rangle \simeq \mathbb{F}_2[X]/\langle \chi\rangle = \mathbb{F}_2[X]/\left\langle X^2 + X + 1\right\rangle$$
   mais le polynôme $X^2 + X + 1$ est irréductible sur $\mathbb{F}_2$ donc $R/\langle 2\rangle \simeq \mathbb{F}_4$, i.e. $\langle 2\rangle$ est premier.

Exercice 7. Soit $\mathfrak{a}$ un idéal d'un ordre quadratique R de norme première à f, le conducteur de R dans $\mathscr{O}_K$. On veut montrer que $\mathfrak{a}$ est inversible. On pose
$$\begin{aligned} m_f : \quad R/\mathfrak{a} &\longrightarrow R/\mathfrak{a} \\ a &\longmapsto af. \end{aligned}$$

1. Montrer que m_f est un isomorphisme de groupes (on pourra considérer une relation de Bézout entre f et $N(\mathfrak{a})$).
   Soit $a \in \ker m_f$ alors $af = 0$ donc l'ordre de a divise f mais par le théorème de Lagrange l'ordre de a divise aussi $\#R/\mathfrak{a} = N(\mathfrak{a})$ donc l'ordre de a divise le pgcd de f et $N(\mathfrak{a})$ qui est 1. Donc $a = 0$. Le morphisme m_f définit donc un morphisme de groupe injectif entre groupes de même cardinal. C'est donc un isomorphisme.
2. En déduire que $\mathfrak{a} + fR = R$.
   Puisque m_f est surjective alors $\overline{1} \in \operatorname{im} m_f$, i.e. $\exists a \in R/af + \mathfrak{a} = 1 + \mathfrak{a}$. On a donc
$$R = afR + \mathfrak{a} \subseteq fR + \mathfrak{a} \subseteq R$$
   d'où $fR + \mathfrak{a} = R$.
3. Soit $\beta \in K$ tel que $\beta\mathfrak{a} \subseteq \mathfrak{a}$, i.e. $\beta \in R_{\mathfrak{a}}$.
   (a) Justifier que $\beta \in \mathscr{O}_K$.
   $\beta \in R_{\mathfrak{a}} \subseteq \mathscr{O}_K$.
   (b) Montrer que $\beta R \subseteq R$.
   On a
$$\beta R = \beta(fR + \mathfrak{a}) = f\underbrace{\beta R}_{\subseteq \mathscr{O}_K} + \underbrace{\beta\mathfrak{a}}_{\subseteq \mathfrak{a}} \subseteq f\mathscr{O}_K + \mathfrak{a} \subseteq R + \mathfrak{a} = R$$
   car $f\mathscr{O}_K \subseteq R$ (théorème de Lagrange appliqué à $\mathscr{O}_K/R$ de cardinal f, voir la preuve de la Proposition 4.5).
   (c) En déduire que $\mathfrak{a}$ est inversible.
   On a donc $R \subseteq R_{\mathfrak{a}} \subseteq R$ donc $R = R_{\mathfrak{a}}$ et, d'après la Proposition 4.7, $\mathfrak{a}$ est inversible dans $R_{\mathfrak{a}} = R$.

3. Avec A la liste est complète ! Tout anneau commutatif unitaire à 4 éléments est isomorphe à $\mathbb{Z}/4\mathbb{Z}, (\mathbb{Z}/2\mathbb{Z})^2, \mathbb{F}_4$ ou à A.