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 ?
2. Factoriser $\langle 7 \rangle$ en idéaux premiers dans $\mathbb{Z}\left[\sqrt{-2}\right]$.
3. Même question avec $\langle 11 \rangle$. Les idéaux intervenant dans la décomposition de $\langle 11 \rangle$ sont-ils principaux ?
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 $\mathfrak{a}$?
   (b) L'idéal $\mathfrak{a}$ est-il principal ?
   (c) Montrer que $\mathfrak{a}$ est inversible (on pourra déterminer l'idéal $\mathfrak{a}\overline{\mathfrak{a}}$).
   (d) Que peut-on en déduire sur $\mathrm{Cl}(R)$?
5. On considère $\mathfrak{b} = \langle 2, \omega \rangle \subseteq R$.
   (a) Montrer que $\overline{\mathfrak{b}} = \mathfrak{b}$.
   (b) Montrer que $\mathfrak{b}^2 = \langle 4, 2\omega \rangle$.
   (c) En déduire que $\mathfrak{b}$ n'est pas inversible.

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 ?
2. Combien R admet-il d'idéaux distincts de norme 2 ? de norme 3 ? de norme 5 ?
3. Factoriser $\langle 10, 7+\omega \rangle$.
4. Justifier que pour tout idéal $\mathfrak{d}$ de R, $\mathfrak{d}^4$ est principal.
5. Montrer que $\mathfrak{a}^2 = \langle 3 \rangle$ et $\mathfrak{b}^2 = \langle 2 \rangle$.
6. En déduire que $\mathrm{Cl}(R) \simeq (\mathbb{Z}/2\mathbb{Z})^2$.
7. L'idéal $\mathfrak{abc}$ est-il principal ? Même question pour $\mathfrak{c}^{15}$.

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.
   (b) Montrer qu'on a toujours
   $$\mathbb{Z}[\pi] \subseteq \mathrm{End}_{\overline{k}}(E) \subseteq \mathscr{O}_K.$$
2. On pose $E\colon y^2 = x^3 - x + 2$ sur $\mathbb{F}_5$.
   (a) Montrer que $E = \{(3, \pm 1), [0\colon 1\colon 0]\}$.
   (b) Quelle est la trace de E ?
   (c) Montrer que $\chi_\pi = X^2 - 3X + 5$ est le polynôme minimal de π.
   (d) Montrer que
   $$\mathbb{Z}[\pi] = \mathbb{Z}[X]/\langle \chi_\pi \rangle \simeq \mathbb{Z}\left[\frac{1+\sqrt{-11}}{2}\right].$$
   (e) En déduire que $\mathrm{End}_{\overline{\mathbb{F}_5}}(E) \simeq \mathbb{Z}\left[\frac{1+\sqrt{-11}}{2}\right]$.

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 $\alpha R \subseteq R$.
2. Montrer que $\#R/\alpha R = |\det M|$ (on pourra penser aux formes de Smith ou au théorème de la base adaptée).
3. Conclure.

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 $R/\langle p\rangle \simeq \mathbb{F}_p[X]/\langle\chi_\omega\rangle$.
2. Montrer que si Δ n'est pas un carré modulo p alors $\langle p\rangle$ est premier dans R.
3. On suppose que $p|\Delta$ et on pose $\mathfrak{p} = \langle p, \sqrt{\Delta_K}\rangle$.
   (a) Montrer que $\mathfrak{p}^2 = \langle p\rangle$.
   (b) Justifier que $\chi \mod p$ possède une unique racine a. Montrer qu'alors $\mathfrak{p} = \langle p, \omega_K - a\rangle$.
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.
   (b) Montrer que les idéaux $\mathfrak{p}_i = \langle p, \omega - a_i\rangle$ définissent des idéaux premiers inversibles de R.
   (c) Montrer que $\mathfrak{p}_1\mathfrak{p}_2 \subseteq \langle p\rangle$.
   (d) En déduire que $\mathfrak{p}_1\mathfrak{p}_2 = \langle p\rangle$.
   (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).

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 $\mathscr{O}_K = \mathbb{Z}[\omega]$ 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 $\mathfrak{p}^2 = \langle 2\rangle$.
   (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 [1] à 4 éléments cités précédemment.
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 $\omega = \frac{1+\sqrt{d}}{2}$.
   (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).
   (c) On suppose que $d = 5 \mod 8$. Montrer qu'alors $\langle 2\rangle$ est un idéal 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

$$\begin{array}{rccc} m_f : & R/\mathfrak{a} & \longrightarrow & R/\mathfrak{a} \\ & a & \longmapsto & af. \end{array}$$

1. Montrer que m_f est un isomorphisme de groupes (on pourra considérer une relation de Bézout entre f et $N(\mathfrak{a})$).
2. En déduire que $\mathfrak{a} + fR = R$.
3. Soit $\beta \in K$ tel que $\beta\mathfrak{a} \subseteq \mathfrak{a}$, i.e. $\beta \in R_{\mathfrak{a}}$.
   (a) Justifier que $\beta \in \mathscr{O}_K$.
   (b) Montrer que $\beta R \subseteq R$.
   (c) En déduire que $\mathfrak{a}$ est inversible.

1. 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.