UNIVERSITÉ DE RENNES 1

Théorie algébrique des nombres

Interrogation (corrigé)

Exercice 1

Calculer la différente de l'extension $\mathbb{Q}(\sqrt{-14})/\mathbb{Q}$ et le groupe des classes de $\mathbb{Z}[\sqrt{-14}]$.

Comme $-14 \equiv 2 \not\equiv 1 \pmod 4$, l'anneau des entiers de $\mathbb{Q}(\sqrt{-14})$ est $\mathbb{Z}[\sqrt{-14}]$. Ce anneau étant monogène, engendré par $\sqrt{-14}$, la différente est :

$$\begin{aligned} \mathscr{D}_{\mathbb{Q}(\sqrt{-14})/\mathbb{Q}} &= f'(\sqrt{-14})\mathbb{Z}[\sqrt{-14}] && \text{où } f \text{ est le polynôme minimal de } \sqrt{-14} \\ &= 2\sqrt{-14}\mathbb{Z}[\sqrt{-14}] && \text{car } f(X) = X^2 + 14. \end{aligned}$$

Pour trouver le groupe des classes, on peut utiliser la borne de Minkowski pour trouver dans chaque classe d'idéaux un représentant de petite norme.
Le discriminant étant

$$\operatorname{disc}(\mathbb{Q}(\sqrt{-14})/\mathbb{Q}) = \mathrm{N}_{\mathbb{Q}(\sqrt{-14})/\mathbb{Q}}(2\sqrt{-14}\mathbb{Z}[\sqrt{-14}]) = 56\mathbb{Z},$$

la borne de Minkowski donne que toute classe d'idéaux a un représentant de norme inférieure ou égale à

$$\begin{aligned} &\left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n}\sqrt{56} && \text{avec ici } n = 2 \text{ et } r_2 = 1 \\ &= \frac{4\sqrt{14}}{\pi} \\ &= 4.764... \end{aligned}$$

On cherche donc les idéaux de norme inférieure ou égale à 4.
Le seul idéal de norme 1 est $\mathbb{Z}[\sqrt{-14}])$ tout entier.
Les idéaux de norme 2 sont premiers (car leur norme est un nombre premier) et divisent 2. On a

$$\begin{aligned} \mathbb{Z}[\sqrt{-14}]/2\mathbb{Z}[\sqrt{-14}]) &\simeq \mathbb{F}_2[X]/(X^2+14) \\ &\simeq \mathbb{F}_2[X]/(X)^2, \end{aligned}$$

donc $(2) = (2, \sqrt{-14})^2$. Le seul idéal de norme 2 est donc $(2, \sqrt{-14})$.

On procède de même pour les idéaux de norme 3 :

$$\begin{aligned}\mathbb{Z}[\sqrt{-14}]/3\mathbb{Z}[\sqrt{-14}]) &\simeq \mathbb{F}_3[X]/(X^2+14)\\ &\simeq \mathbb{F}_3[X]/(X-1)(X+1),\end{aligned}$$

donc $(3) = (3, 1-\sqrt{-14})(3, 1+\sqrt{-14})$. On trouve deux idéaux de norme 3 : $(3, 1-\sqrt{-14})$ et $(3, 1+\sqrt{-14})$.

Si $\mathfrak{a}$ est un idéal de norme 4, et si $\mathfrak{p}$ est un diviseur premier de $\mathfrak{a}$, alors $\mathrm{N}(\mathfrak{p})$ est un diviseur premier de 4, donc c'est 2, et $\mathfrak{p} = (2, \sqrt{-14})$. L'idéal $\mathfrak{a}$ est une puissance de $\mathfrak{p}$, avec exposant 2 pour que $\mathrm{N}(\mathfrak{p}) = 4$. On a donc $\mathfrak{a} = (2, \sqrt{-14})^2 = (2)$, qui est trivial dans le groupe des classes.

On trouve quatre représentants possibles : (1) (pour les idéaux principaux), $(2, \sqrt{-14})$, $(3, 1-\sqrt{-14})$ et $(3, 1+\sqrt{-14})$. Notons $1, a, b$ et c les classes correspondantes dans le groupe des classes. On a alors $a^2 = 1$ et $bc = 1$.

Il n'y a pas d'idéal principal de norme 2, 3 ou 6 dans l'anneau $\mathbb{Z}[\sqrt{-14}]$. En effet, s'il y avait un tel idéal principal $(x + y\sqrt{-14})$, alors on aurait $x^2 + 14y^2 \in \{2, 3, 6\}$, donc $y = 0$ et $x^2 \in \{2, 3, 6\}$, ce qui est impossible. On a donc $a \neq 1$, $b \neq 1$ et $c \neq 1$.

Comme $a^2 = 1$, l'ordre du groupe des classes est pair. Comme il y a au plus 4 éléments, cet ordre est 2 ou 4. Si le groupe avait deux éléments, on aurait $a = b = c$, et $ab = a^2 = 1$. Or $(2, \sqrt{-14})(3, 1-\sqrt{-14})$ est de norme 6 donc n'est pas principal, donc $ab \neq 1$ est le groupe des classes a 4 éléments.

Le groupe des classes est donc isomorphe à $\mathbb{Z}/4\mathbb{Z}$ ou à $(\mathbb{Z}/2\mathbb{Z})^2$. Si c'était le second, on aurait $b^2 = 1 = bc$ donc $b = c$, ou $b \neq c$ puisqu'il y a 4 éléments.

Le groupe des classes est donc isomorphe à $\mathbb{Z}/4\mathbb{Z}$. L'unique élément d'ordre 2 est a et les deux éléments d'ordre 4 sont b et c.

On peut vérifier ce résultat en comptant les formes quadratiques positives réduites de discriminant -56, i.e. les $Ax^2 + Bxy + Cy^2$ avec $A, B, C \in \mathbb{Z}$, $B^2 - 4AC = -56$ (discriminant), $A > 0$ (forme positive), $|B| \leqslant A \leqslant C$ avec $B \geqslant 0$ si $|B| = A$ ou $A = C$ (forme réduite). On a alors $56 = 4AC - B^2 \geqslant 3A^2$ donc $A \in \{1, 2, 3, 4\}$. De plus, comme $B^2 = 4AC - 56$, l'entier B est forcément pair.

- Si $A = 1$ alors $B = 0$ et $C = 14$.
- Si $A = 2$ alors $B = 0$ et $C = 7$, ou $B = 2$ et aucun entier C ne convient.
- Si $A = 3$ alors $B = 0$ et aucun C ne convient, ou $B = \pm 2$ et $C = 5$.
- Si $A = 4$ alors $B = 0$ et aucun C ne convient, ou $B = \pm 2$ et aucun C ne convient, ou $B = 4$ et aucun C ne convient.

On trouve donc 4 formes positives réduites : $x^2 + 14y^2$, $2x^2 + 7y^2$, $3x^2 - 2xy + 5y^2$ et $3x^2 + 2xy + 5y^2$, ce qui confirme l'ordre du groupe des classes.

Exercice 2

Dans l'anneau $A = \mathbb{Z}[\sqrt{-5}]$, on a $(2) = (2, 1 + \sqrt{-5})^2$, et l'idéal $\mathfrak{p} = (2, 1 + \sqrt{-5})$ n'est pas principal. En revanche, l'anneau localisé $A_\mathfrak{p}$ est principal. Trouver un générateur de $\mathfrak{p}$ dans $A_\mathfrak{p}$. (Indication : on a $14 = (3 - \sqrt{-5})(3 + \sqrt{-5})$; compter les facteurs $\mathfrak{p}$ de chaque côté).

L'anneau $A_\mathfrak{p}$ est de valuation discrète, et son idéal maximal $\mathfrak{p}$ est engendré par n'importe quel élément x de valuation $v_\mathfrak{p}(x) = 1$.

On a ici $(2) = \mathfrak{p}^2$ donc $v_\mathfrak{p}(2) = 2$. Comme 7 et 2 sont premiers entre eux (par exemple, on a $7 - 3 \cdot 2 = 1$), $\mathfrak{p}$ ne peux pas diviser (7) (sinon il diviserait (1)), donc $v_\mathfrak{p}(7) = 0$ et $v_\mathfrak{p}(14) = 2$.

On a donc $v_\mathfrak{p}(3 - \sqrt{-5}) + v_\mathfrak{p}(3 + \sqrt{-5}) = 2$.

Comme $\overline{\mathfrak{p}} = \mathfrak{p}$ (par exemple parce que $\mathfrak{p}$ est l'unique idéal premier au-dessus de (2)), on a

$$v_\mathfrak{p}(3 - \sqrt{-5}) = v_{\overline{\mathfrak{p}}}(3 + \sqrt{-5}) = v_\mathfrak{p}(3 + \sqrt{-5}),$$

donc

$$v_\mathfrak{p}(3 - \sqrt{-5}) = v_\mathfrak{p}(3 + \sqrt{-5}) = 1.$$

L'élément $3 + \sqrt{-5}$ est donc un générateur de l'idéal $\mathfrak{p}$ dans le localisé $A_\mathfrak{p}$.

Le choix de 14 dans cet exercice est complètement arbitraire : n'importe quel entier de la forme $x^2 + 5y^2$ qui soit multiple de 2 mais pas de 4 convient aussi. Poar exemple, avec $6 = 1^2 + 5 \cdot 1^2$, on trouve $1 \pm \sqrt{-5}$ comme générateurs de l'idéal.