UNIVERSITÉ DE RENNES 1

**Théorie algébrique des nombres 1**

*Corrigé de l'interrogation*

# Exercice 1

Montrer que tout anneau principal est un anneau de Dedekind.

## Méthode 1 : en revenant à la définition

Par définition, un anneau de Dedekind est un anneau intègre, noethérien, de dimension 1, intégralement clos.

Par définition, un anneau principal est intègre.

Dans un anneau principal, tous les idéaux sont principaux, donc de type fini, donc tout anneau principal est noethérien.

Soit $A$ un anneau principal.

Montrons que la dimension de Krull de $A$ est 1. Comme $A$ est intègre, l'idéal 0 est premier, donc cela revient à montrer que tout idéal premier non nul est maximal. Soit $(p)$ un idéal premier non nul (principal puisque $A$ est principal), et soit $(a)$ un idéal (principal) contenant $(p)$. Comme $p \in (a)$, il existerait un $b \in A$ tel que $ab = p$. Or $(p)$ est premier, donc $a \in (p)$ ou $b \in (p)$. Si $a \in (p)$, on aurait $(p) = (a)$. Si $b \in (p)$, alors il existerait un $c \in A$ tel que $b = pc$, donc $pac = p$, donc $ac = 1$ puisque $A$ est intègre et $p \neq 0$, donc $(a) = A$. L'idéal $(p)$ est donc bien maximal.

Montrons que l'anneau $A$ est intégralement clos. Soient $x \in \operatorname{Frac} A$, et un polynôme unitaire $P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in A[X]$ tels que $P(x) = 0$. Soient $u, v \in A$, $v \neq 0$, tels que $x = \frac{u}{v}$. L'idéal $(u, v)$ est un idéal principal $(w)$, et quitte à diviser $u$ et $v$ par $w$, on peut supposer $w = 1$. Comme $P(x) = 0$, on a $u^n = -a_{n-1}u^{n-1}v - \cdots - a_0v^n \in (v)$. Si $(v) \neq A$, il existerait un idéal premier $\mathfrak{p}$ tel que $(v) \subseteq \mathfrak{p}$, donc on aurait $u^n \in \mathfrak{p}$, donc $u \in \mathfrak{p}$, donc $A = (u, v) \subseteq \mathfrak{p}$ : contradiction. Donc $v \in A^\times$, donc $x \in A$. Donc l'anneau $A$ est intégralement clos.

Donc tout anneau principal est un anneau de Dedekind.

## Méthode 2 : par les idéaux fractionnaires inversibles

Rappelons que si $A$ est un anneau intègre, alors $A$ est un anneau de Dedekind si et seulement si tous ses idéaux fractionnaires non nuls sont inversibles (cf. Atiyah & MacDonald, théorème 9.8).

Soit $A$ un anneau principal. Par définition, $A$ est intègre. Les idéaux fractionnaires de $A$ sont de la forme $Ax$ avec $x \in \operatorname{Frac} A$. Si $x \neq 0$, alors l'idéal fractionnaire $Ax$ est clairement inversible, d'inverse $A\frac{1}{x}$. Donc $A$ est un anneau de Dedekind.

## Exercice 2

Calculer le groupe des classes de l'anneau des entiers de $\mathbb{Q}(\sqrt{-17})$.

Posons $K = \mathbb{Q}(\sqrt{-17})$. C'est un corps quadratique imaginaire. Comme $-17 \not\equiv 1 \pmod 4$, l'anneau des entiers de $K$ est $\mathscr{O}_K = \mathbb{Z}[\sqrt{-17}]$, qui est monogène. Le polynôme minimal de $\sqrt{-17}$ est $X^2 + 17$. La différente de l'extension $K/\mathbb{Q}$ est donc l'idéal $2\sqrt{-17}\mathscr{O}_K$, et le discriminant est l'idéal $\mathrm{N}_{K/\mathbb{Q}}(2\sqrt{-17})\mathbb{Z} = 2^2 \cdot 17\,\mathbb{Z}$.

La borne de Minkowski donne que tout élément du groupe des classes a un représentant entier de norme au plus

$$\begin{aligned} \left(\frac{4}{\pi}\right)^1 \frac{2!}{2^2} \left(2^2 \cdot 17\right)^{1/2} &= \frac{4}{\pi}\sqrt{17} \\ &= 5.2497... \end{aligned}$$

On cherche donc quels sont les idéaux (entiers) de $\mathscr{O}_K$ de norme au plus 5.

L'idéal de norme 1 est $\mathscr{O}_K = (1)$ lui-même, et il est principal.

Les idéaux de norme 2 divisent (2), donc correspondent à des idéaux de l'anneau $\mathscr{O}_K/(2) \simeq \mathbb{F}_2[X]/(X+1)^2$. Il n'y a donc qu'un seul idéal de norme 2 : $\left(2, 1+\sqrt{-17}\right)$, et que l'on a $(2) = \left(2, 1+\sqrt{-17}\right)^2$.

Les idéaux de norme 3 correspondent à des idéaux $\mathscr{O}_K/(3) \simeq \mathbb{F}_3[X]/(X-1)(X+1)$. On trouve donc qu'il y a deux idéaux distincts de norme 3 : $\left(3, 1+\sqrt{-17}\right)$ et $\left(3, 1-\sqrt{-17}\right)$, dont le produit est (3).

Les idéaux de norme 5 correspondent à des idéaux de $\mathscr{O}_K/(5) \simeq \mathbb{F}_5/(X^2-3)$, qui est un corps puisque 3 n'est pas un carré modulo 5. Il n'y a donc pas d'idéal de norme 5 (et (5) est premier).

Les idéaux de norme 4 sont des diviseurs de $(4) = \left(3, 1+\sqrt{-17}\right)^4$, donc le seul idéal de norme 4 est $\left(2, 1+\sqrt{-17}\right)^2 = (2)$, qui est principal.

Notons $1, a, b, c$ les images respectives de (1), $\left(2, 1+\sqrt{-17}\right)$, $\left(3, 1+\sqrt{-17}\right)$ et $\left(3, 1-\sqrt{-17}\right)$ dans le groupe des classes. On a alors $a^2 = 1$ et $bc = 1$, et le groupe des classes est $H(K) = \{1, a, b, c\}$ (certains de ces éléments pouvant être égaux). Le groupe des classes a donc au plus 4 éléments.

Comme l'équation diophantienne $x^2 + 17y^2 = 2$ n'a pas de solution, il n'y a pas d'idéal principal de norme 2, donc $a \neq 1$. De même, $x^2 + 17y^2 = 3$ n'a pas de solution donc $b \neq 1$ et $c \neq 1$.

Comme $a$ est d'ordre 2, le groupe $H(K)$ est d'ordre 2 ou 4. S'il était d'ordre 2, on aurait $a = b = c$ (car ces éléments sont différents de 1), donc $b^2 = 1$. L'idéal $\left(3, 1+\sqrt{-17}\right)^2$ serait donc un idéal principal de norme 9. Or l'équation diophantienne $x^2 + 17y^2 = 9$ a pour solutions $(x, y) = (\pm 3, 0)$, donc l'unique idéal principal de norme 9 est (3), donc on aurait $\left(3, 1+\sqrt{-17}\right)^2 = (3)$, ce qui contredit l'unicité de la factorisation.

Donc $H(K)$ est d'ordre 4, donc il est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2$ ou à $\mathbb{Z}/4\mathbb{Z}$. Dans le premier cas, on aurait aussi $b^2 = 1$, et on a montré que c'est impossible. Donc $H(K) \simeq \mathbb{Z}/4\mathbb{Z}$, les classes $1$, $a$, $b$, $c$ sont distinctes, et $b$ et $c$ sont des générateurs.

On a montré au passage que $b^2 = c^2 = a$, qui peut aussi se déduire en factorisant l'idéal $\left(1 + \sqrt{-17}\right)$. On a $\mathscr{O}_K/\left(1 + \sqrt{-17}\right) \simeq \mathbb{Z}[X]/\left(X^2 + 17, X + 1\right) \simeq \mathbb{Z}/18\mathbb{Z}$, donc

$$\left(1 + \sqrt{-17}\right) = \left(2, 1 + \sqrt{-17}\right)\left(3, 1 + \sqrt{-17}\right)^2,$$

donc $ab^2 = 1$, donc $b^2 = a$ puisque $a^2 = 1$.