Exercice 1.7.1

$$\mathbb{Z}[i] = \{a + bi\}_{a,b \in \mathbb{Z}}$$

(b) $\mathbb{Z}[i] \overset{?}{=} \{P(i)\}_{P \in \mathbb{Z}[X]}$

$\vdots$

$= E$

① $\mathbb{Z}[i] \subset E$ est "facile"

En effet soit $z \in \mathbb{Z}[i]$ $z = a + bi$ avec $a, b \in \mathbb{Z}$

Soit $P = a + bX$ alors $z = P(i)$ donc $z \in E$

② $E \subset \mathbb{Z}[i]$?

Méthode élémentaire

Soit $z \in E$. Il existe $d \in \mathbb{N}$, $a_0, \dots, a_d \in \mathbb{Z}$ tels que $z = \sum_{k=0}^{d} a_k \cdot i^k$

Soit $k \in \mathbb{N}$ $i^k = \begin{cases} i & \text{si } k \equiv 1 \ [4] \\ -1 & \text{si } k \equiv 2 \ [4] \\ -i & \text{si } k \equiv 3 \ [4] \\ 1 & \text{si } k \equiv 0 \ [4] \end{cases}$

$$z = \sum_{\substack{k=0 \\ k \equiv 1 \ [4]}}^{d} a_k \cdot \underbrace{i^k}_{i} + \sum_{\substack{k=0 \\ k \equiv 2 \ [4]}}^{d} a_k \cdot \underbrace{i^k}_{-1} + \sum_{\substack{k=0 \\ k \equiv 3 \ [4]}}^{d} a_k \cdot \underbrace{i^k}_{-i} + \sum_{\substack{k=0 \\ k \equiv 0 \ [4]}}^{d} a_k \cdot \underbrace{i^k}_{1}$$

$\in i\mathbb{Z}$ $\in \mathbb{Z}$

Donc $z \in \mathbb{Z}[i]$

Méthode "savante"

1) i annule le polynôme $X^2 + 1 \in \mathbb{Z}[X]$

2) $X^2 + 1$ est un polynôme unitaire

Méthode "savante"

1) i annule le polynôme $X^2+1 \in \mathbb{Z}[X]$
2) X^2+1 est un polynôme unitaire

Soit $z \in E$. Soit $P \in \mathbb{Z}[X]$ tel que $z = P(i)$

Montrons que $z \in \mathbb{Z}[i]$.

Comme X^2+1 est unitaire (ça marchait aussi si le coefficient dominant était inversible) il existe $Q, R \in \mathbb{Z}[X]$ tels que

1) $P = Q \cdot (X^2+1) + R$
2) $\deg(R) < \deg(X^2+1) = 2$

Soit $a, b \in \mathbb{Z}$ tels que $R = a + bX$

On a $P(i) = Q(i) \cdot \underbrace{(i^2+1)}_{=0} + R(i) = a + bi$

donc $z = P(i) \in \mathbb{Z}[i]$

(c) N = "norme"

$$N : \mathbb{Z}[i] \longrightarrow \mathbb{N}$$
$$z \longmapsto z\bar{z} = |z|^2$$

$a, b \in \mathbb{Z}$ $\quad |a+bi|^2 = a^2 + b^2 \in \mathbb{N}$ (car $a^2 \geq 0$, $b^2 \geq 0$)

$\forall z_1, z_2 \in \mathbb{Z}[i] \quad \boxed{N(z_1 z_2) = N(z_1) N(z_2)}$

$\forall z_1, z_2 \in \mathbb{C}, \quad \overline{z_1 z_2} = \overline{z_1} \cdot \overline{z_2}$

(d) Montrons qu'on a $\mathbb{Z}[i]^\times = \{ z \in \mathbb{Z}[i],\ N(z) = 1 \}$ (= : portée plus générale)

puis $= \{1, -1, i, -i\}$ (peut se faire de manière élémentaire)

Montrons qu'on a $\mathbb{Z}[i]^\times \subset \{ z \in \mathbb{Z}[i],\ N(z) = 1 \}$

Soit $z \in \mathbb{Z}[i]^\times$. Il existe $w \in \mathbb{Z}[i]$ tel que $z \times w = 1$

Prenons la norme $N(z \times w) = N(1) = |1|^2 = 1$

Donc $N(z) \times N(w) = 1$ (d'après (c))

① Montrons que $\mathbb{Z}[i] \subset \{z \in \mathbb{Z}[i],\ N(z)=1\}$

Soit $z \in \mathbb{Z}[i]^\times$ Il existe $w \in \mathbb{Z}[i]$ tel que $z \times w = 1$

Prenons la norme $N(z \times w) = N(1) = |1|^2 = 1$

Donc $N(z) \times N(w) = 1$ (d'après (c))

$\in \mathbb{N}$ $\in \mathbb{N}$

Donc $N(z) = N(w) = 1$

② Montrons $\{z \in \mathbb{Z}[i],\ N(z)=1\} \subset \mathbb{Z}[i]^\times$

Soit $z \in \mathbb{Z}[i]$ tel que $N(z) = 1$

On a $z \times \bar{z} = 1$ Comme $z \in \mathbb{Z}[i]$, on a aussi $\bar{z} \in \mathbb{Z}[i]$

Donc $z \in \mathbb{Z}[i]^\times$ (et on a $z^{-1} = \bar{z}$)

Montrons que $\{z \in \mathbb{Z}[i],\ N(z)=1\} \subset \{1, -1, i, -i\}$?

$\supset$ immédiate

$\{z \in \mathbb{Z}[i],\ N(z)=1\} = \{a+bi\}_{a,b \in \mathbb{Z},\ a^2+b^2=1}$ (*)

L'équation $a^2+b^2=1$ $(a,b) \in \mathbb{Z}^2$ a pour solutions $\{(1,0), (0,1), (-1,0), (0,-1)\} = S$

$a, b \in \mathbb{Z}$ $a^2+b^2=1$ donc $a^2 \leq 1$ (car $b^2 \geq 0$) or $a^2 \in \mathbb{N}$

donc $a^2 \in \{0,1\}$

donc $a \in \{-1, 0, 1\}$

$\{(a,b) \in \mathbb{Z}^2,\ a^2+b^2=1\} \subset S$?

(*) $= \{1+0\cdot i,\ 0+1\cdot i,\ -1+0\cdot i,\ 0+(-1)\cdot i\} = \{1, -1, i, -i\}$

1.7.3 p nombre premier

$$\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \right\}_{\substack{a \in \mathbb{Z} \\ b \in \mathbb{Z} \setminus p\mathbb{Z}}} \subset \mathbb{Q} \neq \mathbb{Z}/p\mathbb{Z}$$

↳ ensemble des entiers qui ne sont pas multiples de p

(a) $\mathbb{Z}_{(p)} \subset \mathbb{Q}$ anneau intègre

sous-anneau

stabilité par $\times$: $a, b, c, d \in \mathbb{Z}$ $p \nmid b$ $p \nmid d$

$$\frac{a}{b} \times \frac{c}{d} = \frac{ac}{bd} \quad \text{et } p \nmid bd \text{ (car } p \text{ premier)}$$

$$\mathbb{Z} \subset \mathbb{Z}_{(p)} \qquad a \in \mathbb{Z} \quad a = \frac{a}{1} \quad p \nmid 1$$

(b)

$$\nu_p : \mathbb{Z}_{(p)} \longrightarrow \mathbb{N} \cup \{+\infty\} \qquad \tilde{\nu}_p(a)$$

$a \neq 0$ $\frac{a}{b}$ $\longmapsto$ le plus grand $n \in \mathbb{N}$ tel que $p^n \mid a$

$a = 0 \longmapsto +\infty$

α

pas entièrement clair a priori : si on a une autre écriture $\alpha = \frac{a'}{b'}$ avec $p \nmid b'$ alors on va obtenir le même résultat

la puissance de p dans la décomposition en facteurs premiers de a

l'unique $n \in \mathbb{N}$ tel que a s'écrive $p^n \cdot a'$ avec $a' \in \mathbb{Z}$ et $p \nmid a'$

$$\tilde{\nu}_p : \mathbb{Z} \longrightarrow \mathbb{N} \cup \{+\infty\}$$

$a \neq 0 \longmapsto$

$0 \longmapsto +\infty$

Question Soit a, a', b, b' tels que $p \nmid b$ $p \nmid b'$ et $\frac{a}{b} = \frac{a'}{b'}$. A-t-on $\tilde{\nu}_p(a) = \tilde{\nu}_p(a')$?

(OUI)

$ab' = a'b$

$p \nmid b'$ $p \nmid b$

Fait général

Soit $a, b \in \mathbb{Z} \setminus \{0\}$ $p \nmid b$

$\tilde{\nu}_p(a \times b) = \tilde{\nu}_p(a)$

Conclusion L'application v_p est bien définie et prolonge $\tilde{v}_p$ $\forall x \in \mathbb{Z}$, $v_p(x) = \tilde{v}_p(x)$
$v_p(x)$ vu comme élément de $\mathbb{Z}_{(p)}$

Exemple $p=2$ $v_2\left(\frac{12}{5}\right) = \tilde{v}_2(12) = \tilde{v}_2(2^2 \times 3) = 2$
$12 = 2 \times 3$

$v_2\left(\frac{7}{3}\right) = 0$

$v_2\left(\frac{1}{2}\right) =$ non défini $(= -1)$
$\frac{1}{2} \notin \mathbb{Z}_{(2)}$

$\forall x, y \in \mathbb{Z}_{(p)}$, $v_p(x \times y) = v_p(x) + v_p(y)$

$2 \times \frac{1}{2} = 1$ $v_2(1) = 0$

$v_2(2 \times \frac{1}{2}) = 0 = v_2(2) + v_2\left(\frac{1}{2}\right)$
$= 1$

(b) Démontrer d'abord les relations analogues pour $\tilde{v}_p$
$\forall x, y \in \mathbb{Z}$ $\tilde{v}_p(x \times y) = \tilde{v}_p(x) + \tilde{v}_p(y)$

(c) $x \in \mathbb{Z}_{(p)}^\times$ Soit $y \in \mathbb{Z}_{(p)}$ tel que $x \times y = 1$
donc $v_p(x \times y) = v_p(1) = 0$
donc $v_p(x) + v_p(y) = 0$ donc $v_p(x) = 0$
$\in \mathbb{N}$ $\in \mathbb{N}$

Donc $\mathbb{Z}_{(p)}^\times \subset \{ x \in \mathbb{Z}_{(p)},\ v_p(x) = 0 \}$
L'inclusion réciproque est vraie (à vérifier)
$\mathbb{Z}_{(p)}^\times = \left\{ \frac{a}{b} \right\}$ $a, b \in \mathbb{Z}$ (à montrer)
$p \nmid b$ $p \nmid a$

(d)

$p^n \cdot \mathbb{Z}_{(p)}$ $\quad n \in \mathbb{N}$ $\quad n=0 \quad \mathbb{Z}_{(p)}$

$m, n \in \mathbb{N}$ $\quad m \geq n$ $\quad p^m \cdot \mathbb{Z}_{(p)} \subset p^n \cdot \mathbb{Z}_{(p)}$

$x \in \mathbb{Z}_{(p)}$ tel que $v_p(x) = n$ alors $x \cdot \mathbb{Z}_{(p)} = p^n \cdot \mathbb{Z}_{(p)}$

on verra ça au prochain

I idéal de $\mathbb{Z}_{(p)}$ $\quad n = \min \{ v_p(x),\ x \in I \}$

Alors $I = p^n \cdot \mathbb{Z}_{(p)} = \{ x \in \mathbb{Z}_{(p)},\ v_p(x) \geq n \}$

$\mathbb{Z}_{(p)} \supsetneq p \cdot \mathbb{Z}_{(p)} \supsetneq p^2 \cdot \mathbb{Z}_{(p)} \supsetneq \cdots$

Conclusion $p \cdot \mathbb{Z}_{(p)}$ est un idéal maximal et c'est l'unique idéal maximal de $\mathbb{Z}_{(p)}$

$p \cdot \mathbb{Z}_{(p)}$ est maximal ?

→ ① Tout idéal de $\mathbb{Z}_{(p)}$ est de la forme $p^n \cdot \mathbb{Z}_{(p)}$ $\quad n \in \mathbb{N}$

"facile" ② $n \in \mathbb{N}$ $\quad p^n \mathbb{Z}_{(p)} \subset p \mathbb{Z}_{(p)}$ $\quad (n \geq 1)$ $\quad p^n = p \cdot p^{n-1} \in p \cdot \mathbb{Z}_{(p)}$ donc $p^n \cdot \mathbb{Z}_{(p)} \subset p \cdot \mathbb{Z}_{(p)}$

"facile" ③ $p \mathbb{Z}_{(p)} \subsetneq \mathbb{Z}_{(p)}$ $\quad x \notin$ contient des éléments de valuation 0

$v_p(x) \geq 1$ $\quad$ par exemple $v_p(1) = 0$

$\mathrm{Hom}_{\text{anneaux}}(\mathbb{Q}, \mathbb{Q}) \overset{?}{=} \{ \mathrm{Id}_{\mathbb{Q}} \}$

$\supset$ claire

$\varphi : x \mapsto -x$

$\varphi(x \times y) = -(x \times y)$

$\varphi(x) \times \varphi(y) = (-x) \times (-y) = x \times y$

$\varphi(1) = -1 \neq 1$

Soit $\varphi \in \mathrm{Hom}(\mathbb{Q}, \mathbb{Q})$ $\quad \varphi(0)=0$

$a, b \in \mathbb{Q}$, $b \neq 0$ $\quad \varphi\left(\frac{a}{b}\right) = \varphi\left(a \times \frac{1}{b}\right) = \varphi(a) \times \varphi\left(\frac{1}{b}\right)$

$\varphi(a) = a$

En effet

($a \in \mathbb{N}$) $\quad a = \underbrace{1+1+1+1+\cdots+1}_{a \text{ fois}}$

$\varphi(a) = \underbrace{\varphi(1)+\varphi(1)+\cdots+\varphi(1)}_{a \text{ fois}}$ $\quad \varphi(1)=1$

$= \underbrace{1+1+\cdots+1}_{a \text{ fois}}$

$= a$

$a \in \mathbb{Z} \setminus \mathbb{N}$ $\quad \varphi(a) = -\varphi(-a)$ (φ est un morphisme de groupes)

$= -(-a) = a$

Méthode plus "savante" $\quad \mathbb{Z} \xhookrightarrow{\iota} \mathbb{Q}$, $n \longmapsto n$ $\quad \iota$ morphisme d'anneaux

$$\mathbb{Z} \xhookrightarrow{\iota} \mathbb{Q} \xrightarrow{\varphi} \mathbb{Q}$$

$\psi = \varphi \circ \iota \in \mathrm{Hom}_{\text{anneaux}}(\mathbb{Z}, \mathbb{Q})$

$\| \ (\text{Cons})$

$\{ n \in \mathbb{Z} \longmapsto n \cdot 1_{\mathbb{Q}} = n \}$

$n \in \mathbb{Z}$ $\quad n = \psi(n) = \varphi(\iota(n)) = \varphi(n)$ donc $\varphi(n)=n$

$\varphi : \mathbb{Q} \longrightarrow \mathbb{Q}$

On a vu $\forall a \in \mathbb{Z}, \ \varphi(a) = 0$

$b \in \mathbb{Z} \setminus \{0\}$ $\quad \varphi\left(\frac{1}{b}\right) = ?$

$b \times \frac{1}{b} = 1$ donc $\varphi\left(b \times \frac{1}{b}\right) = \varphi(1) = 1$

donc $\varphi(b) \times \varphi\left(\frac{1}{b}\right) = 1$

donc $b \times \varphi\left(\frac{1}{b}\right) = 1$

donc $\varphi\left(\frac{1}{b}\right) = \frac{1}{b}$

$a \in \mathbb{Z}$
$b \in \mathbb{Z} \setminus \{0\}$ $\quad \varphi\left(\frac{a}{b}\right) = \varphi\left(a \times \frac{1}{b}\right) = \varphi(a) \times \varphi\left(\frac{1}{b}\right)$

$= a \times \frac{1}{b}$

$= \frac{a}{b}$

Conclusion $\forall x \in \mathbb{Q}, \ \varphi(x) = x$

Indication (1.4.7) $\quad \iota : \mathbb{Z} \longrightarrow \mathbb{Q}$, $n \longmapsto n$

$\{\text{idéaux de } \mathbb{Q}\} = \{\{0\}, \mathbb{Q}\}$