$\varphi : A \xrightarrow{\sim} B$ iso — A intègre $\Leftrightarrow$ B intègre

I idéal de A, I premier $\Leftrightarrow$ A/I est intègre

2.11

① $\mathbb{Z}[i]/p\cdot\mathbb{Z}[i] \xrightarrow{\sim} (\mathbb{Z}/p\mathbb{Z})[X] / \langle X^2 + [1]_p \rangle$

cf exemple 2.6

$\mathbb{Z}[i\sqrt{3}]/2\mathbb{Z}[i\sqrt{3}] \to \mathbb{Z}/2\mathbb{Z}[X]/\langle X^2+[3]_2\rangle$ ($\mathbb{Z}/p\mathbb{Z}$ est un corps)

$p\cdot\mathbb{Z}[i]$ est premier

$\Leftrightarrow$ $(X^2+[1]_p)\cdot \mathbb{Z}/p\mathbb{Z}[X]$ est un idéal premier de $\mathbb{Z}/p\mathbb{Z}[X]$

$\Leftrightarrow$ $\Pi := X^2 + [1]_p$ est un polynôme irréductible de $\mathbb{Z}/p\mathbb{Z}[X]$

$\deg(\Pi) = 2$

$\Leftrightarrow$ Π n'a pas de racine dans $\mathbb{Z}/p\mathbb{Z}[X]$ — CRUCIAL

$\Leftrightarrow$ -1 n'est pas un carré modulo p

$(\forall a \in \mathbb{Z}/p\mathbb{Z},\ a^2 + [1]_p \neq [0]_p)$

② $\mathbb{Z}[i]^\times = \{z \in \mathbb{Z}[i],\ N(z) = 1\}$ (cf. 2.6 $\mathbb{Z}[i\sqrt{3}]^\times = \{z \in \mathbb{Z}[i\sqrt{3}],\ N(z)=1\}$)

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

$\supset$: $N(z) = 1 = z\cdot\bar{z}$, $z \in \mathbb{Z}[i]$, $\bar{z} \in \mathbb{Z}[i]$ donc $z \in \mathbb{Z}[i]^\times$

③ $z_2 = z_1 z_3$, $z_3 \in \mathbb{Z}[i]$

$N(z_2) = N(z_1)N(z_3)$

ou $N(z_2) = N(z_1)$

donc (si $N(z_2) \neq 0$, i.e. $z_2 \neq 0$) $N(z_3) = 1$ donc $z_3 \in \mathbb{Z}[i]^\times$ donc z_1 et z_2 sont associés

④ $z \in \mathbb{Z}[i]$

$z \notin \mathbb{Z}[i]^\times$ car $N(z) = 1$

$N(z) = p$ premier ($p \neq 1$!)

Soit $z_1, z_2 \in \mathbb{Z}[i]$ tels que $z = z_1 \times z_2$

Montrons que $z_1 \in \mathbb{Z}[i]^\times$ ou $z_2 \in \mathbb{Z}[i]^\times$

$N(z) = N(z_1)N(z_2)$ donc

p premier, $N(z_1), N(z_2) \in \mathbb{N}$

$N(z_1) = p$ et $N(z_2) = 1$ donc $z_2 \in \mathbb{Z}[i]^\times$

ou

$N(z_1) = 1$ et $N(z_2) = p$ donc $z_1 \in \mathbb{Z}[i]^\times$

⑤ $p = a^2 + b^2$, $a, b \in \mathbb{Z}$

$[0]_p = [a]_p^2 + [b]_p^2$

$[0]_p = \alpha^2 + \beta^2$

$\alpha := [a]_p$

$\beta := [b]_p$

$\beta = [0]_p$?

⑤ $p = a^2 + b^2$ $a, b \in \mathbb{Z}$

$[0]_p = [a]_p^2 + [b]_p^2$

$[0]_p = \alpha^2 + \beta^2$ $\beta \neq [0]_p$

$[0]_p = \left(\frac{\alpha}{\beta}\right)^2 + [1]_p$

on "divise" par β

$\alpha := [a]_p$

$\beta := [b]_p$

donc $\beta \in (\mathbb{Z}/p\mathbb{Z})^\times$ (p premier)

$\beta = [0]_p$?

Si $\beta = [0]_p$ alors $[a]_p^2 = [0]_p$ donc $[a]_p = [0]_p$

↳ p est premier

$[a]_p = [0]_p$ $p \mid a$ $a = pa'$

$[b]_p = [0]_p$ $p \mid b$ $b = pb'$

$p = p^2(a'^2 + b'^2)$

donc $1 = p(a'^2 + b'^2)$ donc $p \mid 1$ ✗

donc $\mathbb{Z}/p\mathbb{Z}$ est intègre

$[2]_4^2 = [0]_4$ mais $[2]_4 \neq [0]_4$

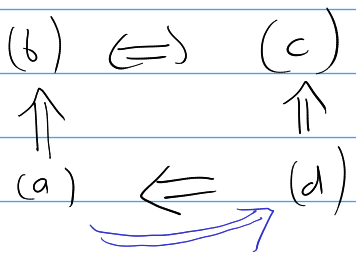
$p = a^2 + b^2 = (a + ib)(a - ib)$

si $a + ib \notin \mathbb{Z}[i]^\times$ $N(a+ib) = p \neq 1$

ou (exclusif) $a - ib \notin \mathbb{Z}[i]^\times$ $N(a-ib) = p \neq 1$

donc p est non irréductible

⑥



(a) ⇒ (d)

p non irréductible

$p = z_1 z_2$ $N(z_1) \neq 1$ $N(z_2) \neq 1$

$p^2 = N(z_1) N(z_2)$ $\in \mathbb{N}$ $\in \mathbb{N}$

donc $N(z_1) = N(z_2) = p$

donc ($z_1 = a + ib$ $a, b \in \mathbb{Z}$) $p = a^2 + b^2$

$z \in \mathbb{Z}[i]$ $N(z) = z\bar{z} = |z|^2$

(P) : propriété de l'énoncé

(P') : Soit $z \in \mathbb{Z}[i]$ irréductible et $a, b \in \mathbb{Z}[i]$ tels que z divise ab.

Alors $z \mid a$ (ou) $z \mid b$

Dans $\mathbb{Z}[i\sqrt{3}]$ (P) et (P') sont fausses.

$2 \cdot 2 = (1 + i\sqrt{3})(1 - i\sqrt{3})$

2 est irréductible dans $\mathbb{Z}[i\sqrt{3}]$

$1 + i\sqrt{3}$, $1 - i\sqrt{3}$ sont irréductibles $\mathbb{Z}[i\sqrt{3}]$ (même démo que pour 2)

$2(1 + i\sqrt{3})$ divise 4 ?

$N(z) \neq 1$ $\in \mathbb{N}$ $\in \mathbb{N}$ donc $\begin{cases} z = a+ib \\ p = a^2+b^2 \end{cases}$ $a, b \in \mathbb{Z}$

$z \in \mathbb{Z}[i]$ $N(z) = z\bar{z} = |z|^2$ (p) : propriété de l'énoncé

(p') : Soit $z \in \mathbb{Z}[i]$ irréductible et $a, b \in \mathbb{Z}[i]$ tels que z divise ab.
Alors $z \mid a$ ou $z \mid b$

Dans $\mathbb{Z}[i\sqrt{3}]$ (p) et (p') sont fausses.

$2 \cdot 2 = (1+i\sqrt{3})(1-i\sqrt{3})$ (*)

2 est irréductible dans $\mathbb{Z}[i\sqrt{3}]$

$1+i\sqrt{3}$, $1-i\sqrt{3}$ sont irréductibles $\mathbb{Z}[i\sqrt{3}]$ (on démontre que pour 2)

$2(1+i\sqrt{3})$ divise 4 ?

$\Leftrightarrow$ $(1+i\sqrt{3})$ divise 2 ?

$2 = (1+i\sqrt{3})z$ $z \in \mathbb{Z}[i\sqrt{3}]$

$N(2) = N(1+i\sqrt{3})N(z)$

donc $4 = 4\,N(z)$

donc $N(z) = 1$

donc $z \in \mathbb{Z}[i\sqrt{3}]^\times = \{1, -1\}$

donc $2 = 1+i\sqrt{3}$ ou $2 = -1-i\sqrt{3}$ ✗

2 irréductible, $2 \mid 4$

$(1+i\sqrt{3})$ irréductible, $(1+i\sqrt{3}) \mid 4$ cf (*)

2 et $1+i\sqrt{3}$ ne sont pas associés (cf à droite)

OR $2(1+i\sqrt{3})$ ne divise pas 4

Donc (p) ne vaut pas dans $\mathbb{Z}[i\sqrt{3}]$

(3.3)

$$X^4+1 = X^4+2X^2+1-2X^2$$
$$= (X^2+1)^2 - 2X^2$$
$$= (X^2-\sqrt{2}X+1)(X^2+\sqrt{2}X+1)$$

Q_0 R_0 irréductibles dans $\mathbb{R}[X]$

$X^4+1 = Q_1 R_1$ $Q_1, R_1 \in \mathbb{Q}[X]$

$\deg(Q_1) = \deg(R_1) = 2$

On peut supposer Q_1 et R_1 unitaires

$Q_1 R_1 = Q_0 R_0$

Q_0 est irréductible

$Q_0 \mid Q_1 R_1$

donc (lemme d'Euclide dans $\mathbb{R}[X]$) $Q_0 \mid Q_1$ ou $Q_0 \mid R_1$ (dans $\mathbb{R}[X]$)

$\deg(Q_0) = \deg(Q_1) = 2$
Si $Q_0 \mid Q_1$
Q_0, Q_1 unitaires

donc $Q_0 = Q_1$ ou $\sqrt{2} \notin \mathbb{Q}$ ✗