1.5.12 (A quelconque)

$$A[[X]]^\times = \left\{ P = \sum_{n=0}^{+\infty} a_n X^n ,\quad a_0 = P(0) \in A^\times \right\}$$

$\subset$ $P = \sum_{n=0}^{+\infty} a_n X^n \in A[[X]]^\times$

$Q = \sum_{n=0}^{+\infty} b_n X^n \in A[[X]]$ tel que $P \times Q = 1$

On $P \times Q = a_0 b_0 + (a_1 b_0 + a_0 b_1) X + (a_2 b_0 + 2 a_1 b_1 + a_0 b_2) X^2 + \cdots$

$= 1$

Par identification, $a_0 b_0 = 1$ donc $a_0 \in A^\times$

$\supset$ Soit $P = \sum_{n=0}^{+\infty} a_n X^n$ tel que $a_0 \in A^\times$

On cherche $Q = \sum_{n=0}^{+\infty} b_n X^n$ $(b_n) \in A^{\mathbb{N}}$ inconnues

tel que $P \times Q = 1$

$/\!/$

$a_0 b_0 + (a_1 b_0 + a_0 b_1) X + (a_2 b_0 + 2 a_1 b_1 + a_0 b_2) X^2 + \cdots$

Par identification

$$\begin{cases} a_0 b_0 = 1 \\ a_1 b_0 + a_0 b_1 = 0 \\ a_2 b_0 + 2 a_1 b_1 + a_0 b_2 = 0 \\ \vdots \\ \text{expression en } a_1, a_2, \dots, a_n \; b_0, b_1, \dots, b_{n-1} + \underset{\in A^\times}{a_0}\, b_n = 0 \end{cases}$$

$\longrightarrow$ a une solution $b_0 \in A$ car $a_0 \in A^\times$ $b_0 = a_0^{-1}$

connu $b_1 = a_0^{-1} \times (-a_1 b_0)$

connu $b_2 = a_0^{-1} \times (-a_2 b_0 - 2 a_1 b_1)$

1.5.13 $\mathbb{K}[[X]]^\times = \{P = \sum_{i=0}^{+\infty} a_i X^i, \quad a_0 \neq 0\}$

$= \{P \in \mathbb{K}[[X]], \nu(P) = 0\}$

$n \in \mathbb{N}$

$\{P \in \mathbb{K}[[X]], \nu(P) = n\}$

$= \{P \in \mathbb{K}[[X]], \exists Q \in \mathbb{K}[[X]]^\times, P = X^n \times Q\}$

$\supset$ $P = X^n \times Q$ $\quad \nu(P) = \nu(X^n) + \nu(Q)$

$Q \in \mathbb{K}[[X]]^\times$ $\quad = n + 0$

$\subset$ $\nu(P) = n$ $\quad P = \sum_{i=n}^{+\infty} a_i X^i = X^n \cdot \underbrace{(\overset{\in \mathbb{K}^\times}{a_n} + a_{n+1} X + a_{n+2} X^2 + \dots)}_{Q \in \mathbb{K}[[X]]^\times}$

$a_n \neq 0$

I idéal non nul de $\mathbb{K}[[X]]$

$n := \min_{P \in I} \nu(P)$

Alors $\quad I = X^n \cdot \mathbb{K}[[X]] = \{P \in \mathbb{K}[[X]], \nu(P) \geq n\}$

(à terminer en s'inspirant du cas de $\mathbb{Z}_{(p)}$)

Exercice 2.6

1. $\mathbb{Z}[i\sqrt{3}]$ est un sous-anneau de $\mathbb{C}$ (or $\mathbb{C}$ est intègre)

$$\mathbb{Z}[i\sqrt{3}] \overset{\text{(définition)}}{:=} \{P(i\sqrt{3}),\ P\in\mathbb{Z}[X]\}$$

$P = Q.(X^2+3)+R$, $P(i\sqrt{3}) = R(i\sqrt{3})$; $Q, R \in \mathbb{Z}[X]$, $\deg(R)\leq 1$ donc $R = a+bX$, $a,b\in\mathbb{Z}$; $P = a+bX$

$$\overset{\text{(propriété)}}{=} \{a+ib\sqrt{3},\ a,b\in\mathbb{Z}\}$$

$$\mathbb{Z}[i\sqrt{3}] \overset{?}{\simeq} \mathbb{Z}[X]/\langle X^2+3\rangle$$

? $\varphi : \mathbb{Z}[X]\to\mathbb{Z}[i\sqrt{3}]$ surjectif de noyau $(X^2+3)\mathbb{Z}[X]$

On prend $\varphi : \begin{array}{rcl}\mathbb{Z}[X] & \to & \mathbb{Z}[i\sqrt{3}] \\ P & \mapsto & P(i\sqrt{3})\end{array}$ surjectif par définition !!

Montrons que $\mathrm{Ker}(\varphi) = (X^2+3)\mathbb{Z}[X]$

$\supset$ $X^2+3 \in \mathrm{Ker}(\varphi)$ $\quad (X^2+3)(i\sqrt{3}) = (i\sqrt{3})^2+3 = 0$

donc $\underbrace{(X^2+3).\mathbb{Z}[X]}_{\text{idéal engendré par } X^2+3} \subset \underbrace{\mathrm{Ker}(\varphi)}_{\text{idéal}}$

$\subset$ Soit $P\in\mathrm{Ker}(\varphi)$ c'est-à-dire $P(i\sqrt{3}) = 0$

X^2+3 a un coefficient dominant inversible dans $\mathbb{Z}$

Soit $P = (X^2+3)Q+R$ la division euclidienne dans $\mathbb{Q}[X]$

$Q, R\in\mathbb{Q}[X]$ de P par X^2+3 dans $\mathbb{Z}[X]$

$Q, R\in\mathbb{Z}[X]$ $\quad \deg(R)\leq 1 = \deg(X^2+3)-1$

$$P(i\sqrt{3}) = 0.Q(i\sqrt{3}) + R(i\sqrt{3})$$

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

$0 = P(i\sqrt{3}) = R(i\sqrt{3}) = a+ib\sqrt{3}$

Donc en prenant les parties réelles et imaginaires

$a = 0$
$b\sqrt{3} = 0$ donc $b = 0$ $\quad$ donc $R = 0$ et $P = (X^2+3)Q \in (X^2+3)\mathbb{Z}[X]$

$X+1 = (2X+2)\times\frac{1}{2}$ $\quad P = (X^2+3)Q \quad Q\in\mathbb{Q}[X]$

2.6 2)

$$N : \begin{array}{rcl} \mathbb{Z}[i\sqrt{3}] & \longrightarrow & \mathbb{N} \\ z & \longmapsto & |z|^2 = z\bar{z} \end{array}$$

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

$$= \{ a + ib\sqrt{3} ,\ \begin{array}{l} a, b \in \mathbb{Z} \\ a^2+3b^2 = 1 \end{array} \} = \{1, -1\}$$

$\{ a^2+3b^2 = 1 \quad (a,b) \in \mathbb{Z}^2 \} = \{ (1,0), (-1,0) \}$

si $|b| \geq 1$ $\quad a^2+3b^2 \geq 3$ $\quad$ donc $b = 0$

3) $\quad a^2+3b^2 = 2 \quad (a,b) \in \mathbb{Z}^2$

si $|b| \geq 1$ $\quad a^2+3b^2 \geq 3 > 2$ $\quad$ donc $b=0$ $\quad$ donc $a^2 = 2$

($2 \notin \mathbb{Z}[i\sqrt{3}]^\times$ car $N(2) = 2^2 \neq 1$)

2 n'est pas irréductible ssi il existe $z_1, z_2 \in \mathbb{Z}[i\sqrt{3}]$

$2 = 1 \times 2 = (-1) \times (-2)$ $\quad$ telle que $2 = z_1 \times z_2$

et $z_1, z_2 \notin \mathbb{Z}[i\sqrt{3}]^\times$

si c'est vrai $\quad 4 = N(2) = \underset{\mathbb{N}}{N(z_1)} \times \underset{\mathbb{N}}{N(z_2)}$ $\quad$ or $N(z_1) \neq 1$, $N(z_2) \neq 1$

donc $\quad N(z_1) = N(z_2) = 2$

or d'après la question 2) $\{ z \in \mathbb{Z}[i\sqrt{3}] ,\ N(z) = 2 \} = \emptyset$

$a \in A$ $\quad a = \alpha \times (\alpha^{-1} a)$

$\alpha \in A^\times$

4) $m \in \mathbb{Z} \setminus \{0\}$

$m\mathbb{Z}$ est premier $\iff$ $|m|$ est un nombre premier

$\iff$ m est irréductible

$$\boxed{\text{« premier } \iff \text{ irréductible »}}$$ (vrai dans $\mathbb{Z}$, dans $\mathbb{Z}[i]$)

en général « premier $\Rightarrow$ irréductible »

Dans $\mathbb{Z}[i\sqrt{3}]$ « irréductible $\Rightarrow$ premier » est FAUSSE

notion arithmétique — notion algébrique

2 est irréductible mais $2.\mathbb{Z}[i\sqrt{3}]$ n'est pas premier

<u>Méthode élémentaire</u> $\quad 4 = (1+i\sqrt{3})(1-i\sqrt{3})$

$4 = 2\times 2 \in 2.\mathbb{Z}[i\sqrt{3}]$

Si $2\mathbb{Z}[i\sqrt{3}]$ est premier, alors $1+i\sqrt{3}$ ou $1-i\sqrt{3} \in 2\mathbb{Z}[i\sqrt{3}]$

Il existe $z \in \mathbb{Z}[i\sqrt{3}]$ tel que

$1+i\sqrt{3} = 2.z$ impossible !

ou $1-i\sqrt{3} = 2.z$ (soit de manière élémentaire, soit en utilisant la norme)

<u>Méthode basée sur un théorème d'isomorphisme</u>

$$\mathbb{Z}[i\sqrt{3}] \simeq \mathbb{Z}[X]/\langle X^2+3\rangle$$

$$\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}, \quad m \mapsto [m]_2$$

$$\mathbb{Z}[i\sqrt{3}]/2\mathbb{Z}[i\sqrt{3}] \simeq \mathbb{Z}[X]/\langle 2, X^2+3\rangle$$

donc non intègre

$$\simeq (\mathbb{Z}/2\mathbb{Z})[X]/\langle X^2+[3]_2\rangle$$

$$\simeq \underbrace{(\mathbb{Z}/2\mathbb{Z})}_{\text{corps}}[X]/\langle \underbrace{X^2+[1]_2}_{\text{polynôme non irréductible}}\rangle$$ donc non intègre

$$X^2+[1]_2 = (X+[1]_2)^2$$

1.4.7

$$\varphi : \mathbb{Z} \longrightarrow \mathbb{Q}, \quad n \longmapsto n$$ morphisme d'anneaux ($\mathbb{Z}$ est un sous anneau de $\mathbb{Q}$)

$\mathbb{Z}$ est un idéal de $\mathbb{Z}$

$\varphi(\mathbb{Z}) = \mathbb{Z}$

$\mathbb{Z}$ n'est pas un idéal de $\mathbb{Q}$

argument élaboré : $\mathbb{Q}$ est un corps donc ses seuls idéaux sont $\{0\}$ et $\mathbb{Q}$

$\{0\} \neq \mathbb{Z}$, $\mathbb{Q} \neq \mathbb{Z}$

argument élémentaire : $1 \in \mathbb{Z}$, $\frac{1}{2} \in \mathbb{Q}$, $1 \times \frac{1}{2} \notin \mathbb{Z}$

donc $\mathbb{Z}$ n'est pas un idéal de $\mathbb{Q}$

Propriété générale Soit A un anneau et $B \subset A$ un sous-ensemble.

$1_A \in B$ est un sous-anneau de A et un idéal de A $\Longleftrightarrow$ $B = A$

Contre-exemple général pour 1.4.7

Soit A un anneau, $B \subset A$ un sous anneau tel que $B \neq A$

$$\varphi : B \longrightarrow A, \quad b \longmapsto b$$

1) B est un idéal de B
2) φ est un morphisme d'anneaux
3) $\varphi(B) = B$ n'est pas un idéal de A