Kit de survie pour travailler avec les anneaux quotients

(du plus vital au plus secondaire)

A anneau, $I \subset A$ idéal

① $\pi : A \longrightarrow A/I$ morphisme quotient est a) surjectif b) de noyau I

Application décrire les idéaux de l'anneau quotient A/I en fonction de ceux de A ; cf proposition 20 du même chapitre ; exercice 2.4

② Croyance populaire "On peut, de manière naturelle, identifier A/I à un sous-ensemble voire à un sous anneau de A"

Une des causes possibles : souvent, on note les éléments du quotient "comme" les éléments de l'anneau de départ

$$\pi : \begin{array}{ccc} A & \longrightarrow & A/I \\ a & \longmapsto & \pi(a) \text{ "}=\text{"} a \end{array}$$

Ex $5 = 2$ dans $\mathbb{Z}/3\mathbb{Z}$ $\quad \mathbb{Z} \longrightarrow \mathbb{Z}/3\mathbb{Z}$, $[5]_3 = [2]_3$, $n \longmapsto [n]_3$

Exemple ~~$x^2 = -1$ n'a pas de solution dans $\mathbb{Z}/5\mathbb{Z}$ car $x^2 \geq 0$ pour tout élément x de $\mathbb{Z}/5\mathbb{Z}$~~

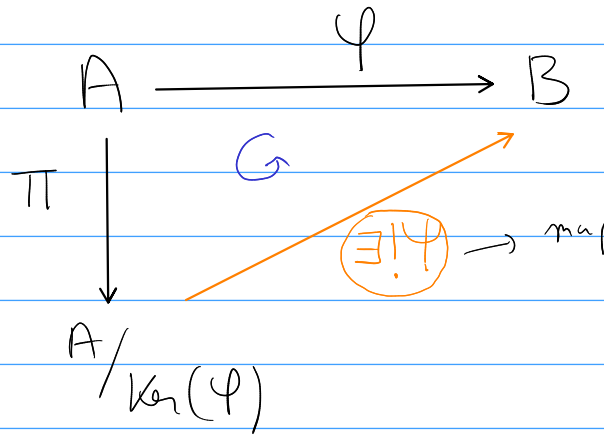
On a $2^2 = -1$ dans $\mathbb{Z}/5\mathbb{Z}$

Vérité En général, A/I n'est isomorphe à aucun sous anneau de A. Même si A/I peut s'identifier à un sous-ENSEMBLE de A, il n'existe pas en général d'identification "naturelle" (et donc la plupart du temps ce genre d'identification n'apporte pas d'information pertinente sur A/I)

③ Théorème de factorisation (version "bon marché")

$\varphi : A \to B$ morphisme d'anneaux

alors "φ se factorise par le morphisme quotient $\pi : A \to A/\ker(\varphi)$"



→ morphisme qui vérifie $\psi \circ \pi = \varphi$

(en particulier $\psi(A/\ker(\varphi)) \subset \varphi(A)$)

En outre $\psi : A/\ker(\varphi) \longrightarrow \varphi(A)$ ← sous anneau de B

est un isomorphisme.

Conséquence Pour montrer que A/I est isomorphe à B, il suffit de construire un morphisme $\varphi : A \to B$ surjectif et de noyau I.

Exemple $\mathbb{Z}[i] \simeq \mathbb{Z}[X]/\langle X^2+1 \rangle$

④ Théorème de factorisation général (propriété universelle des anneaux quotients)

"L'anneau quotient de A par I, c'est un anneau où on a forcé tous les éléments de I à être nuls et c'est le plus petit qui vérifie cette propriété"

$X^2+1 \in \mathbb{R}[X]$ $\quad I \simeq \mathbb{R}[X]/\langle X^2+1 \rangle$

④ Théorème de factorisation général (propriété universelle des anneaux quotients)

« L'anneau quotient de A par I, c'est un anneau où on a forcé tous les éléments de I à être nuls et c'est le plus petit qui vérifie cette propriété »

$X^2+1 \in \mathbb{R}[X]$ $\quad \mathbb{C} \simeq \mathbb{R}[X]/\langle X^2+1\rangle$

$\varphi : A \to B$ tel que $I \subset \ker(\varphi)$ $(\forall a \in I,\ \varphi(a)=0)$

$\varphi_1 : A \to B_1$ tels que $I \subset \ker(\varphi_1)$
$\varphi_2 : A \to B_2$ $\quad I \subset \ker(\varphi_2)$

$\varphi_1 < \varphi_2$ (SSI) il existe

$$\begin{array}{ccc} A & \xrightarrow{\varphi_2} & B_2 \\ {\scriptstyle\varphi_1}\downarrow & \nearrow_{\psi} & \\ B_1 & & \end{array}$$

tel que $\psi \circ \varphi_1 = \varphi_2$

$$\begin{array}{ccc} A & \xrightarrow{\varphi} & B \\ {\scriptstyle\pi}\downarrow & & \\ A/I & & \end{array}$$

$\pi < \varphi$

Alors φ se factorise par π ssi « B est un anneau dans lequel I devient nul »

ssi $\boxed{\ker(\varphi) \supset I}$

$\ker(\pi) = I$ (dans ce cas la factorisation est unique)

$$\mathrm{Hom}\left(A/I, B\right) = \left\{ \varphi \in \mathrm{Hom}(A,B),\ \ker(\varphi) \supset I \right\}$$

⚠ ça ne « marche pas » par $\mathrm{Hom}\left(B, A/I\right)$

Exemple $n, m \in \mathbb{N}$ $\quad \mathrm{Hom}\left(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}\right)$?

⑤ Théorèmes d'isomorphismes « compliqués » (théorème 48)

$\mathbb{Z}[i]$
p nombre premier

p inéquitable dans $\mathbb{Z}[i]$?

$2 = (1+i)(1-i)$
$\notin \mathbb{Z}[i]^\times$ $\quad \notin \mathbb{Z}[i]^\times$

(6) Théorèmes d'isomorphismes "compliqués" (théorème 48)

$\mathbb{Z}[i]$

p nombre premier

p irréductible dans $\mathbb{Z}[i]$?

$2 = (1+i)(1-i)$, $(1+i) \notin \mathbb{Z}[i]^\times$, $(1-i) \notin \mathbb{Z}[i]^\times$

p irréductible dans $\mathbb{Z}[i]$ $\Leftrightarrow$ $p \cdot \mathbb{Z}[i]$ est un idéal premier

$\mathbb{Z}[i] \simeq \mathbb{Z}[X]/\langle X^2+1 \rangle$

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

$(\mathbb{Z}/p\mathbb{Z})$: corps

$\Leftrightarrow$ $\mathbb{Z}[i]/p\mathbb{Z}[i]$ est intègre

$\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$

$n \longmapsto [n]_p$

(5) I idéal de A

I est premier $\Leftrightarrow$ A/I est intègre

I est maximal $\Leftrightarrow$ A/I est un corps

Ex $\langle X, Y \rangle$ est un idéal maximal de $\mathbb{C}[X,Y]$

Exemple $\mathbb{Z}[i] \simeq \mathbb{Z}[X]/\langle X^2+1 \rangle$

$$\varphi : \mathbb{Z}[X] \longrightarrow \mathbb{C}, \quad P(X) \longmapsto P(i)$$

l'unique morphisme d'anneau de $\mathbb{Z}[X]$ vers $\mathbb{C}$ qui envoie X sur i

$\mathrm{Im}(\varphi) = \mathbb{Z}[i]$ (déjà vu)

$\ker(\varphi) = \{ P \in \mathbb{Z}[X],\ P(i) = 0 \}$

$= \langle X^2+1 \rangle = (X^2+1) \cdot \mathbb{Z}[X]$?

$X^2+1 \in \ker(\varphi)$ donc $\langle X^2+1 \rangle \subset \ker(\varphi)$

Soit $P \in \ker(\varphi)$. Comme X^2+1 a son coefficient dominant inversible, il existe $Q, R \in \mathbb{Z}[X]$ tels que $\begin{cases} P = (X^2+1)Q + R \\ \deg(R) < \deg(X^2+1) = 2 \end{cases}$

Soit $P \in \ker(\varphi)$. Comme X^2+1 a son coefficient dominant inversible, il existe $Q, R \in \mathbb{Z}[X]$ tels que $\begin{cases} P = (X^2+1)Q + R \\ \deg(R) < \deg(X^2+1) = 2 \end{cases}$

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

$0 = P(i) = (i^2+1)\cdot Q(i) + R(i)$

donc $0 = a + bi$

donc $a = b = 0$ donc $R = 0$ donc $P = (X^2+1)Q$

donc $P \in (X^2+1)\mathbb{Z}[X]$

donc $\ker(\varphi) = (X^2+1)\mathbb{Z}[X]$

D'après le théorème d'isomorphisme $\mathbb{Z}[i]$ est isomorphe à

$$\mathbb{Z}[X] / (X^2+1)\mathbb{Z}[X]$$

$n, m \in \mathbb{Z}$ $\quad \mathrm{Hom}\left(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}\right)$?

$A = \mathbb{Z}$ $I = n\mathbb{Z}$ $B = \mathbb{Z}/m\mathbb{Z}$

$$\mathrm{Hom}\left(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}\right) = \left\{ \varphi \in \mathrm{Hom}(\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) \;\middle|\; \ker(\varphi) \supset n\mathbb{Z} \right\} (*)$$

$$\mathrm{Hom}(\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) = \{*\} = \left\{ \varphi_m : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z},\ x \mapsto [x]_m \right\}$$

$$\ker(\varphi_m) = m\mathbb{Z}$$

$$\text{Donc } \mathrm{Hom}\left(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}\right) = \begin{cases} \{\varphi_m\} & \text{si } m\mathbb{Z} \supset n\mathbb{Z} \quad (\Leftrightarrow m \mid n) \\ \emptyset & \text{si } m\mathbb{Z} \not\supset n\mathbb{Z} \end{cases}$$

En particulier $\mathrm{Hom}\left(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}\right) = \left\{ \mathrm{Id}_{\mathbb{Z}/n\mathbb{Z}} \right\}$

$\langle X, Y \rangle = X \cdot \mathbb{C}[X,Y] + Y \cdot \mathbb{C}[X,Y]$

est un idéal maximal de $\mathbb{C}[X,Y]$?

Montrons $\mathbb{C}[X,Y] / \langle X, Y \rangle \simeq \mathbb{C}$

(Si c'est vrai, comme $\mathbb{C}$ est un corps, cela montre que $\langle X, Y \rangle$ est un idéal maximal)

(?) $\varphi : \mathbb{C}[X,Y] \longrightarrow \mathbb{C}$ surjectif de noyau $\langle X, Y \rangle$

$P \longmapsto P(0,0)$

(Retour sur la démonstration du théorème 4.6 – existence de l'anneau quotient)

A, I $\quad x R_I y \iff x - y \in I$

$\pi : A \longrightarrow B = A/R_I$ $\quad$ (π est surjective)

$x \longmapsto \overline{x}$

$x, y \in A \quad \overline{x} + \overline{y} := \overline{x+y}$ bien défini ?

Soit $\alpha, \beta \in B$ On veut définir $\alpha + \beta$

On choisit $x \in A$ tel que $\alpha = \overline{x}$ (un tel x n'est pas unique en général)

$y \in A$ " $\beta = \overline{y}$

$\alpha + \beta \overset{?}{:=} \overline{x+y}$ Problème ça dépend peut être du choix de x et y

À montrer Si $x', y' \in A$ sont d'autres éléments tels que $\overline{x'} = \alpha$ et $\overline{y'} = \beta$ alors $\overline{x'+y'} = \overline{x+y}$

En effet on a $\overline{x'} = \alpha = \overline{x}$ donc $\overline{x'} = \overline{x}$

donc $x' R_I x$

donc $x' - x \in I$

De même, on a $y' - y \in I$

On veut montrer $\overline{x'+y'} = \overline{x+y}$ ce qui équivaut à $(x'+y') R_I (x+y)$ ce qui équivaut à $(x'+y') - (x+y) \in I$ (?)

$(x'+y') - (x+y) = \underbrace{(x'-x)}_{\in I} + \underbrace{(y'-y)}_{\in I}$

donc $\in I$ car I est un sous groupe de $(A,+)$

Sous les mêmes hypothèses ($\overline{x} = \overline{x'}$ et $\overline{y} = \overline{y'}$) il faut montrer $\overline{xy} = \overline{x'y'}$ i.e $xy - x'y' \in I$ (?)

$xy - x'y' = xy - x'y + x'y - x'y' = y(x-x') + x'(y-y')$

$x-x' \in I$, $y-y' \in I$