Théorème 48. Théorèmes d'isomorphisme

1. *Soit $\varphi: A \to B$ un morphisme d'anneaux.*
   (a) *Le morphisme φ induit un isomorphisme de $A/\operatorname{Ker}(\varphi)$ sur l'anneau $\operatorname{Im}(\varphi)$. En particulier, si φ est surjectif, φ induit un isomorphisme de $A/\operatorname{Ker}(\varphi)$ sur B. De manière générale, l'anneau quotient $A/\operatorname{Ker}(\varphi)$ est toujours isomorphe à un sous-anneau de B.*
   (b) *Supposons φ surjectif. Soit $\mathcal{J}$ un idéal de B. Alors la composition de φ avec le morphisme quotient $B \to B/\mathcal{J}$ induit un isomorphimse de $A/\varphi^{-1}(\mathcal{J})$ sur $B/\mathcal{J}$.*
   (c) *Supposons φ surjectif. Soit $\mathcal{I}$ un idéal de A. Alors la composition de φ avec le morphisme quotient $B \to B/\varphi(\mathcal{I})$ induit un isomorphisme de $A/(\mathcal{I}+\operatorname{Ker}(\varphi))$ sur $B/\varphi(\mathcal{I})$.*
2. *Soit $\mathcal{I}$ un idéal de A. On note $\pi_{\mathcal{I},X}: A[X] \to (A/\mathcal{I})[X]$ l'unique morphisme qui envoie X sur X et qui induit le morphisme $A \to (A/\mathcal{I})[X]$ donné par la composition des flèches naturelle $A \to A/\mathcal{I} \to (A/\mathcal{I})[X]$. Soit $\mathcal{J}$ un idéal de $A[X]$. Alors la composition du morphisme $\pi_{\mathcal{I},X}$ avec le morphisme quotient $(A/\mathcal{I})[X] \to (A/\mathcal{I})[X]/\pi_{\mathcal{I},X}(\mathcal{J})$ induit un isomorphisme de $A[X]/(\mathcal{I}\cdot A[X]+\mathcal{J})$ sur $(A/\mathcal{I})[X]/\pi_{\mathcal{I},X}(\mathcal{J})$.*

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

$$\varphi: \mathbb{Z}[X] \longrightarrow \mathbb{Z}[i\sqrt{3}]$$ surjectif

$\operatorname{Ker}(\varphi) = \langle X^2+3\rangle$

$\mathbb{Z}[i\sqrt{3}]/2.\mathbb{Z}[i\sqrt{3}]$? 1(c) $A = \mathbb{Z}[X]$

$B = \mathbb{Z}[i\sqrt{3}]$

$\varphi(I) = 2.\mathbb{Z}[i\sqrt{3}]$ $I = 2.\mathbb{Z}[X]$

$\varphi|_{\mathbb{Z}} = \operatorname{Id}_{\mathbb{Z}}$

D'après 1(c) $\mathbb{Z}[i\sqrt{3}]/2.\mathbb{Z}[i\sqrt{3}]$

$$\xrightarrow{\sim} \mathbb{Z}[X]/2.\mathbb{Z}[X]+\operatorname{Ker}(\varphi)$$

$$\xrightarrow{\sim} \mathbb{Z}[X]/\langle 2, X^2+3\rangle$$

Théorème 48. Théorèmes d'isomorphisme

1. *Soit $\varphi\colon A \to B$ un morphisme d'anneaux.*
   (a) *Le morphisme φ induit un isomorphisme de $A/\operatorname{Ker}(\varphi)$ sur l'anneau $\operatorname{Im}(\varphi)$. En particulier, si φ est surjectif, φ induit un isomorphisme de $A/\operatorname{Ker}(\varphi)$ sur B. De manière générale, l'anneau quotient $A/\operatorname{Ker}(\varphi)$ est toujours isomorphe à un sous-anneau de B.*
   (b) *Supposons φ surjectif. Soit $\mathcal{J}$ un idéal de B. Alors la composition de φ avec le morphisme quotient $B \to B/\mathcal{J}$ induit un isomorphimse de $A/\varphi^{-1}(\mathcal{J})$ sur $B/\mathcal{J}$.*
   (c) *Supposons φ surjectif. Soit $\mathcal{I}$ un idéal de A. Alors la composition de φ avec le morphisme quotient $B \to B/\varphi(\mathcal{I})$ induit un isomorphisme de $A/(\mathcal{I}+\operatorname{Ker}(\varphi))$ sur $B/\varphi(\mathcal{I})$.*
2. *Soit $\mathcal{I}$ un idéal de A. On note $\pi_{\mathcal{I},X}\colon A[X] \to (A/\mathcal{I})[X]$ l'unique morphisme qui envoie X sur X et qui induit le morphisme $A \to (A/\mathcal{I})[X]$ donné par la composition des flèches naturelle $A \to A/\mathcal{I} \to (A/\mathcal{I})[X]$. Soit $\mathcal{J}$ un idéal de $A[X]$. Alors la composition du morphisme $\pi_{\mathcal{I},X}$ avec le morphisme quotient $(A/\mathcal{I})[X] \to (A/\mathcal{I})[X]/\pi_{\mathcal{I},X}(\mathcal{J})$ induit un isomorphisme de $A[X]/(\mathcal{I}\cdot A[X]+\mathcal{J})$ sur $(A/\mathcal{I})[X]/\pi_{\mathcal{I},X}(\mathcal{J})$.*

$\mathbb{Z}[X]/\langle 2, X^2+3\rangle$ $\qquad A[X]/\mathcal{I}\cdot A[X]+\mathcal{J}$

On applique 2) avec $A=\mathbb{Z}$ $\quad \mathcal{I}=2\mathbb{Z}$

$\mathcal{J}=(X^2+3)\,\mathbb{Z}[X]$ $\qquad \mathcal{I}\cdot\mathbb{Z}[X]+(X^2+3)\,\mathbb{Z}[X]$

$$= \langle 2, X^2+3\rangle$$

Donc $\mathbb{Z}[X]/(2,X^2+3) \xrightarrow{\sim} \mathbb{Z}/2\mathbb{Z}[X]/\pi_{2\mathbb{Z},X}(\mathcal{J})$

$$\pi_{2\mathbb{Z},X}: \begin{array}{ccc} \mathbb{Z}[X] & \longrightarrow & \mathbb{Z}/2\mathbb{Z}[X] \\ P=\sum_{i=0}^{d} a_i X^i & \longmapsto & \sum_{i=0}^{d} [a_i]_2 X^i \end{array}$$

$a_i \in \mathbb{Z}$

$d \in \mathbb{N}$

$$\pi_{2\mathbb{Z},X}\left((X^2+3)\,\mathbb{Z}[X]\right) = \pi_{2\mathbb{Z},X}(X^2+3)\cdot\mathbb{Z}/2\mathbb{Z}[X]$$
$$=(X^2+[3]_2)\cdot\mathbb{Z}/2\mathbb{Z}[X]$$

$$\pi_{2\mathbb{Z},X} : \begin{array}{ccc} \mathbb{Z}[X] & \longrightarrow & \mathbb{Z}/2\mathbb{Z}[X] \\ P = \sum_{i=0}^{d} a_i X^i & \longmapsto & \sum_{i=0}^{d} [a_i]_2 X^i \end{array}$$

$a_i \in \mathbb{Z}$

$d \in \mathbb{N}$

$$\pi_{2\mathbb{Z},X}\left((X^2+3)\,\mathbb{Z}[X]\right) = \pi_{2\mathbb{Z},X}(X^2+3)\cdot \mathbb{Z}/2\mathbb{Z}[X]$$

$$= (X^2 + [3]_2)\cdot \mathbb{Z}/2\mathbb{Z}[X]$$

Donc $\mathbb{Z}[X]/\langle 2, X^2+3\rangle \simeq \mathbb{Z}/2\mathbb{Z}[X] / \langle X^2 + [1]_2 \rangle$

$\simeq \mathbb{Z}[i\sqrt{3}] / 2\mathbb{Z}[i\sqrt{3}]$

$\mathbb{Z}/2\mathbb{Z}$: corps

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

Exercice 2.7

Idée reçue : ~~Si un élément x d'un anneau intègre A s'écrit $y \times z$ avec y et z dans A, alors x n'est pas irréductible~~

A anneau intègre

$$x \in A \text{ est irréductible} \iff \begin{cases} x \notin A^\times \\ \text{soit } y, z \in A \text{ tels que } x = y \times z \\ \text{alors } y \in A^\times \text{ ou } z \in A^\times \end{cases}$$

p premier

$A = \mathbb{Z}_{(p)}$

$$\mathbb{Z}_{(p)} \setminus \mathbb{Z}_{(p)}^\times = \{ x \in \mathbb{Z}_{(p)},\ v_p(x) \geq 1 \}$$

$$\mathbb{Z}_{(p)}^\times = \{ x \in \mathbb{Z}_{(p)},\ v_p(x) = 0 \}$$

$n \in \mathbb{N}$
$$\{ x \in \mathbb{Z}_{(p)},\ v_p(x) = n \} = \left\{ x \in \mathbb{Z}_{(p)},\ \exists y \in \mathbb{Z}_{(p)}^\times,\ x = p^n \times y \right\}$$
$$= \{ \text{éléments associés à } p^n \}$$

Rappel : Si $x, y \in A$ intègre sont associés, c'est-à-dire il existe $z \in A^\times$ tels que $x = z \times y$ alors x est irréductible ssi y est irréductible

Question : soit $n \in \mathbb{N}$, $n \geq 1$ p^n est-il irréductible dans $\mathbb{Z}_{(p)}$?

$$p^2 = p \times p \quad \text{or } p \notin \mathbb{Z}_{(p)}^\times \text{ car } v_p(p) = 1$$
$p^2 \notin \mathbb{Z}_{(p)}^\times$

donc p^2 n'est pas irréductible

donc $\forall x \in \mathbb{Z}_{(p)},\ v_p(x) = 2 \Rightarrow x$ n'est pas irréductible

$n \geq 2$ $\quad p^n = p \times p^{n-1}$ $\quad$ or $p \notin \mathbb{Z}_{(p)}^\times$

et $p^{n-1} \notin \mathbb{Z}_{(p)}^\times$ car $v_p(p^{n-1}) = n - 1 \geq 1$

donc p^n n'est pas irréductible

Montrons que p est irréductible dans $\mathbb{Z}_{(p)}$

On a $p \notin \mathbb{Z}_{(p)}^{\times}$

Soit $x, y \in \mathbb{Z}_{(p)}$ tels que $p = x \times y$

Montrons que $x \notin \mathbb{Z}_{(p)}^{\times}$ ou $y \notin \mathbb{Z}_{(p)}^{\times}$

$$1 = v_p(p) = \underbrace{v_p(x)}_{\in \mathbb{N}} + \underbrace{v_p(y)}_{\in \mathbb{N}} \quad (*)$$

Supposons $x \in \mathbb{Z}_{(p)}^{\times}$ et montrons que $y \notin \mathbb{Z}_{(p)}^{\times}$

Comme $x \in \mathbb{Z}_{(p)}^{\times}$, on a $v_p(x) = 0$

donc d'après $(*)$ $v_p(y) = 1$ donc $y \notin \mathbb{Z}_{(p)}^{\times}$

Donc p est irréductible.

Exo 2.9

$x^3 = 2 \qquad x \in A$

$\mathbb{R} \to \mathbb{R}$

$A = \mathbb{R}$ $\quad f : x \longmapsto x^3$ est continue, strictement croissante sur $\mathbb{R}$

$\lim_{x \to +\infty} x^3 = +\infty \qquad \lim_{x \to -\infty} x^3 = -\infty$

donc f est bijective et sa bijection réciproque est notée $g : x \longmapsto \sqrt[3]{x}$

Soit $x \in \mathbb{R}$ $\qquad x^3 = 2 \iff x = \sqrt[3]{2}$

$A = \mathbb{Q}$

$\mathbb{Q} \subset \mathbb{R}$

$$v_2 : \mathbb{Q} \longrightarrow \mathbb{Z} \cup \{+\infty\}$$
$$0 \longmapsto +\infty$$
$$\frac{x}{y} \longmapsto v_2(x) - v_2(y) \qquad y, x \in \mathbb{Z},\ y \neq 0$$

$$\forall x, y \in \mathbb{Q},\quad v_2(xy) = v_2(x) + v_2(y)$$

Soit $x \in \mathbb{Q}$ tel que $x^3 = 2$

Alors $v_2(x^3) = v_2(2) = 1$

$$v_2(x^3) = 3\underbrace{v_2(x)}_{\in \mathbb{Z} \cup \{+\infty\}}$$

donc 3 divise 1

contradiction

$A = \mathbb{C}$ $\quad x \in \mathbb{C}$ $\qquad x^3 = 2 \iff x \in \{\sqrt[3]{2}, j\sqrt[3]{2}, j^2\sqrt[3]{2}\}$

où $j \in \mathbb{C}$ qui vérifie $j^3 = 1$, $j \neq 1$

$$j = \frac{-1 + i\sqrt{3}}{2}$$

$$A = \mathbb{Q}[X] / \langle X^3 - 2 \rangle$$

$$\pi : \mathbb{Q}[X] \longrightarrow \mathbb{Q}[X] / \langle X^3 - 2 \rangle$$

$$X \longmapsto \alpha = \pi(X)$$

$\mathrm{Ker}(\pi) = \langle X^3 - 2 \rangle$ donc $\pi(X^3 - 2) = 0$

$$\pi(X^3-2) = \pi(X)^3 - \pi(2) = \alpha^3 - 2$$

A est-il un corps ?

A est un corps $\iff \langle X^3 - 2 \rangle$ est un idéal maximal

$\iff X^3 - 2$ est irréductible dans $\mathbb{Q}[X]$

$X^3 - 2$ et $\deg(X^3 - 2) = 3$ n'a pas de racine dans $\mathbb{Q}$ OK

donc $X^3 - 2$ est irréductible dans $\mathbb{Q}[X]$

⚠

$P = (X^2 + 1)^2$ $\forall x \in \mathbb{Q}, \ P(x) > 0$

$$= \underbrace{(X^2 + 1)}_{\notin \mathbb{Q}[X]^\times = \mathbb{Q}^\times} \times \underbrace{(X^2 + 1)}_{\notin \mathbb{Q}[X]^\times = \mathbb{Q}^\times}$$

Montrons que $X^3 - 2$ est irréductible dans $\mathbb{Q}[X]$

$X^3 - 2 \in \mathbb{Q}[X]^\times = \mathbb{Q}^\times$

Montrons que X^3-2 est irréductible dans $\mathbb{Q}[X]$

$X^3-2 \in \mathbb{Q}[X]^\times = \mathbb{Q}^\times$

Soit $P, Q \in \mathbb{Q}[X]$ tels que $X^3-2 = P \times Q$

Montrons que $Q \in \mathbb{Q}[X]^\times$ ou $P \in \mathbb{Q}[X]^\times$

Supposons que $P \notin \mathbb{Q}[X]^\times$ Montrons que $Q \in \mathbb{Q}[X]^\times$

$3 = \deg(P \times Q) = \underbrace{\deg(P)}_{\in \mathbb{N}} + \underbrace{\deg(Q)}_{\in \mathbb{N}}$ donc $\deg(P) \leq 3$

On $P \notin \mathbb{Q}[X]^\times$ et $P \neq 0$ donc $\deg(P) \geq 1$

Donc $\deg(P) \in \{1, 2, 3\}$

$\boxed{\text{Si } \deg(P) = 3}$, on a $\deg(Q) = 0$ donc $\boxed{Q \in \mathbb{Q}[X] = \mathbb{Q}^\times}$

Si $\deg(P) = 1$ P s'écrit $\alpha X + \beta$ avec $\alpha, \beta \in \mathbb{Q}$ $\alpha \neq 0$

$X^3-2 = P \times Q$ et $P\left(-\frac{\beta}{\alpha}\right) = 0$ $\underbrace{-\frac{\beta}{\alpha}}_{\in \mathbb{Q}}$ est racine de X^3-2 X

Si $\deg(P) = 2$ alors $\deg(Q) = 1$ le même raisonnement aboutit à une contradiction

Donc $A = \mathbb{Q}[X] / \langle X^3 - 2 \rangle$ est un corps

<u>Question</u> Y a-t-il dans A d'autres éléments x que $\pi(X) = \alpha$ qui vérifient $x^3 = 2$?

<u>Indication</u> Montrer que A est isomorphe à un sous-corps de $\mathbb{R}$

$x^3 - 2 = 0 \qquad x \in \mathbb{Z}/n\mathbb{Z}$

Si n est explicitement donné $\quad n = 25$

$$\mathbb{Z}/25\mathbb{Z} = \{[0]_{25}, [1]_{25}, \dots, [24]_{25}\}$$
$$= \{[m]_{25}, \ 0 \leq m \leq 24\}$$

On prend chaque élément dans $\mathbb{Z}/25\mathbb{Z}$ et on regarde s'il vérifie l'équation

$x = [3]_{25} \qquad x^3 = [3]_{25}^3 = [3^3]_{25} = [27]_{25}$
$= [2]_{25}$ ok

$x = [4]_{25} \qquad x^3 \neq [2]_{25}$

$\mathbb{Z}/5\mathbb{Z}$ on applique la méthode ci-dessus $\quad S = \{[3]_5\}$

$\mathbb{Z}/10\mathbb{Z} \qquad 10 = 2 \times 5$
pgcd$(2,5) = 1$

$m \in \mathbb{Z}$

$[m]_{10}^3 = [2]_{10}$

$\mathbb{Z}/35\mathbb{Z}$

$\iff 10 \mid m^3 - 2$

$\iff \begin{cases} 2 \mid m^3 - 2 \\ 5 \mid m^3 - 2 \end{cases} \iff \begin{cases} [m]_2^3 = [2]_2 \\ [m]_5^3 = [2]_5 \end{cases}$

$\mathbb{Z}/7d\mathbb{Z} \qquad d \in \mathbb{N}$

$$\pi: \begin{array}{rcl} \mathbb{Z}/25\mathbb{Z} & \to & \mathbb{Z}/5\mathbb{Z} \\ [m]_{25} & \mapsto & [m]_5 \end{array}$$

$m \in \mathbb{Z}$

Si $x \in \mathbb{Z}/25\mathbb{Z}$ vérifie $x^3 = [2]_{25}$

alors $\pi(x)^3 = [2]_5$

donc $\pi(x) \in \{[3]_5\}$

Idée $\left\{ x \in \mathbb{Z}/25\mathbb{Z} \ , \ \begin{array}{c} \pi(x) = [3]_5 \\ \text{et} \\ x^3 = [2]_{25} \end{array} \right\}$

$$\pi : \mathbb{Z}/25\mathbb{Z} \to \mathbb{Z}/5\mathbb{Z}$$
$$[n]_{25} \longmapsto [n]_5$$
$n \in \mathbb{Z}$

Si $x \in \mathbb{Z}/25\mathbb{Z}$ vérifie $x^3 = [2]_{25}$

alors $\pi(x)^3 = [2]_5$

donc $\pi(x) \in \{[3]_5\}$

Idée $\{x \in \mathbb{Z}/25\mathbb{Z} \;,\; \pi(x) = [3]_5 \text{ et } x^3 = [2]_{25}\}$

$$\pi(x) = [3]_5 = \pi([3]_{25})$$

$x = [n]_{25}$ $\qquad n = 3 + 5k \qquad k \in \mathbb{Z}$

$n \in \mathbb{Z}$

$x^3 = [2]_{25} \Leftrightarrow 25 \mid (3+5k)^3 = 3^3 + 3.3^2.5k + \underbrace{3.3.(5k)^2 + (5k)^3}_{\text{multiple de } 25}$

$\Updownarrow$

$25 \mid 3^3 + 3.3^2.5k$

équation linéaire en k