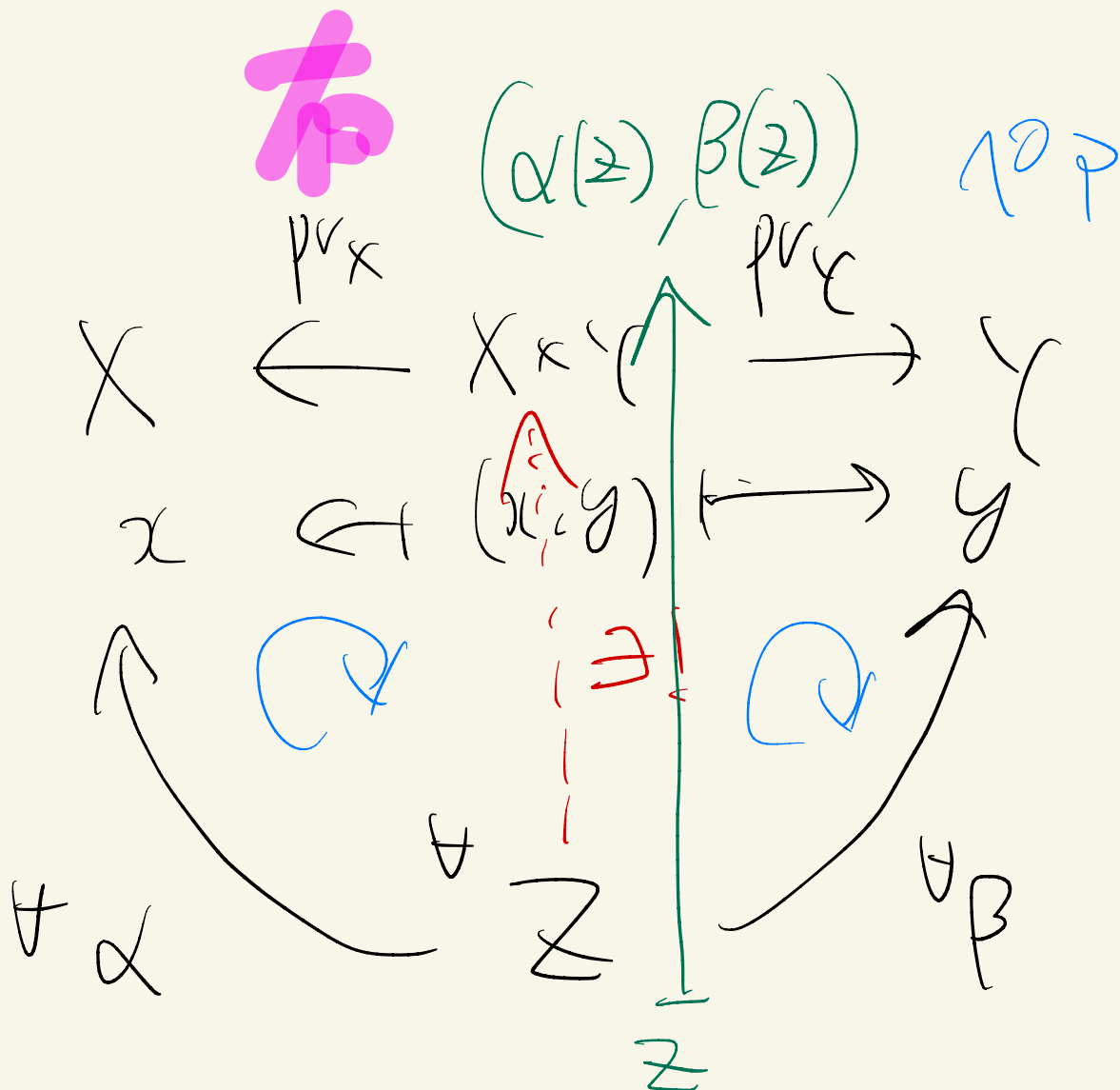
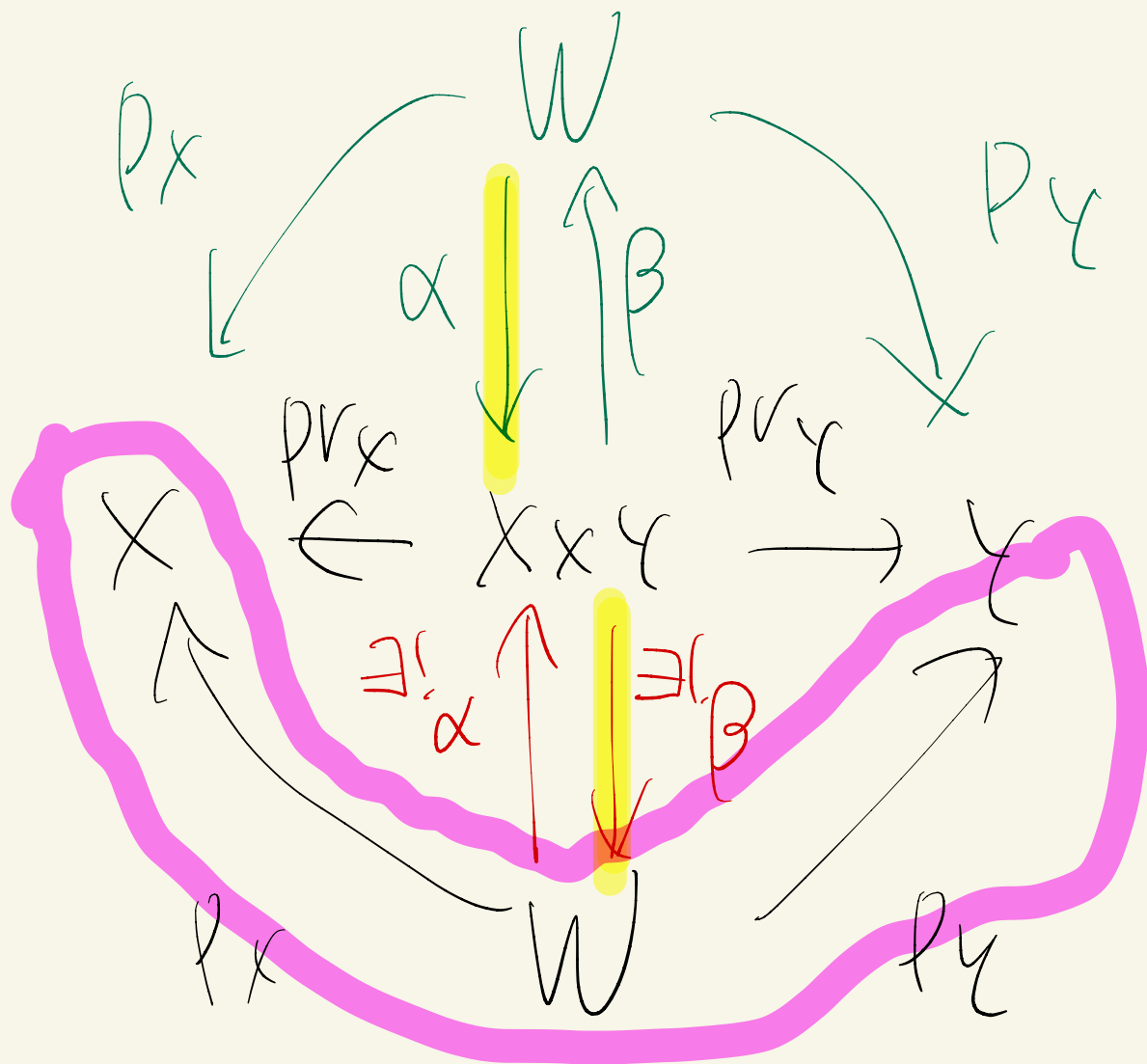



第3回 代数系

普遍性 "全体から見た特徴付け"

直積 $X, Y : \text{set}$ あり





$$\exists \alpha \neq \beta \circ \alpha = id_W$$

$$\alpha \circ \beta = id_{X \times W} \quad \text{bln check}$$

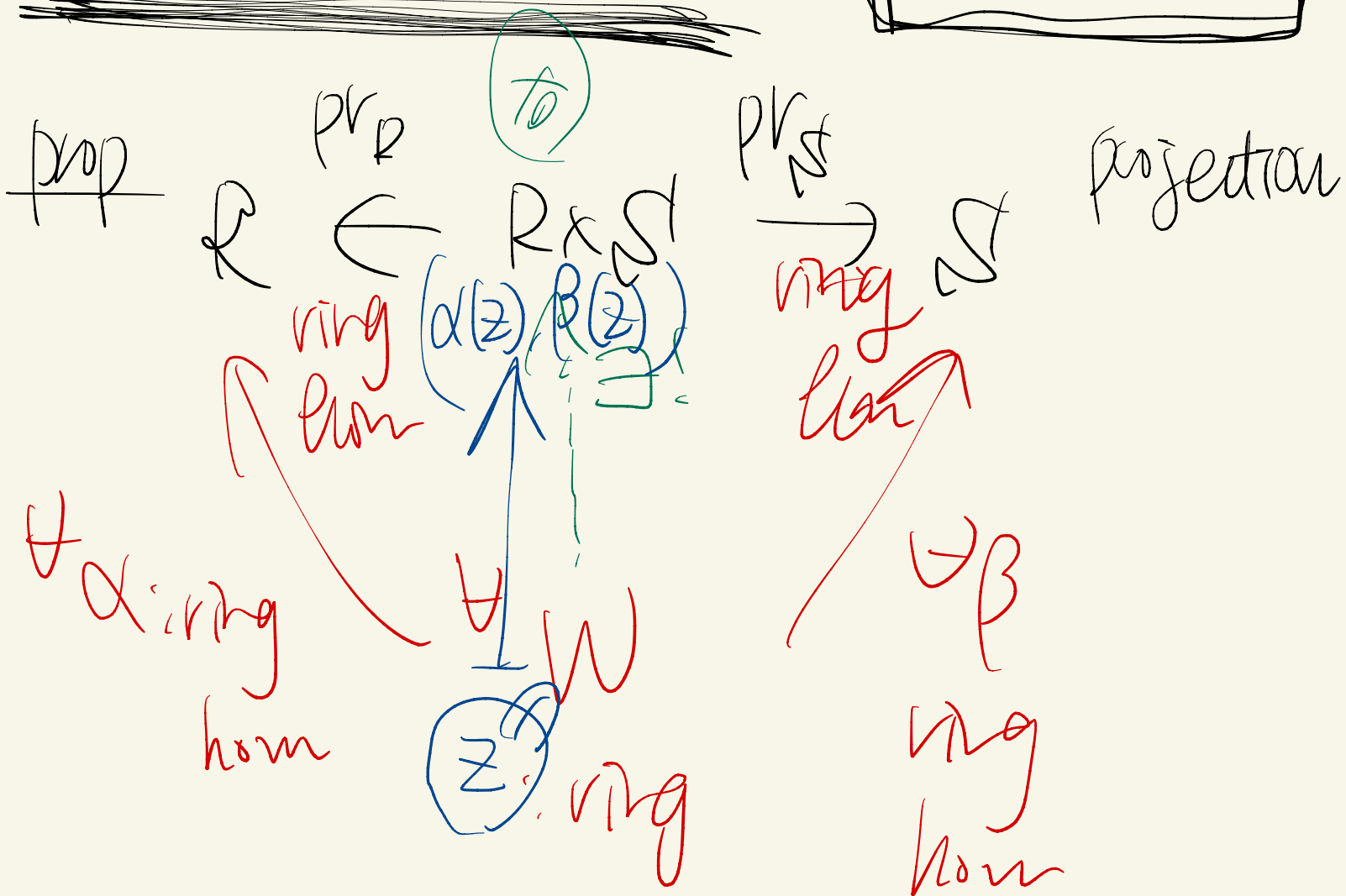
$$Z'' \in Z_0$$

R, S : 可換環

中国剰余定理
(CRT)

$R \times S$: 直積環

環の公理



$\exists! (\alpha(z), \beta(z))$

ring hom $\mathbb{Z} \rightarrow R \times S = \mathbb{Z} \rightarrow R \times S$

≡ 同型定理 商 (左) / 集合, 環

≠ 商集合の普遍性 =

$X: \text{set} \quad \sim: \text{equiv} \text{ rel}$

$\hookrightarrow X/\sim: \text{商集合}$

$x \mapsto [x] = \underbrace{C_x}_{\text{左}} = \{y \in X \mid y \sim x\}$
 $X \xrightarrow{p} X/\sim$

$\forall \alpha \searrow \forall \beta \nearrow$
 $\exists! \frac{\alpha}{\beta} = f$

商集合 $\in$ factor する

$x_1 \sim x_2$
 $\Downarrow$
 $\alpha(x_1) = \alpha(x_2)$

$$x \sim x' \Rightarrow \alpha(x) = \alpha(x') \quad \text{(\u53cd\u5b9a)}$$

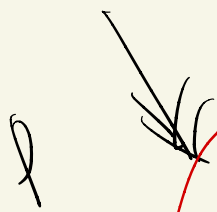
$\Updownarrow$ def $a \neq b \Rightarrow a \notin b$

$$C_x = C_{x'}$$

$$C_x = \{y \in X \mid y \sim x\}$$

Cor

$$A \xrightarrow{a} B$$



$$A / \sim_a$$

$\exists!$ は単射
 $\underline{a}$

$$\Rightarrow C_a, C_b$$

$$a \sim_a a' \Leftrightarrow a(a) = a(a') \quad (\neq \text{equiv set } \{= \neq\})$$

$$\begin{matrix} & a \\ & \searrow \\ a & A \xrightarrow{h} B & h(a) \end{matrix}$$

$$\begin{matrix} & \nearrow \\ p & \cancel{A/\sim} \cup \exists! & \nearrow \\ & h \end{matrix}$$

Ca

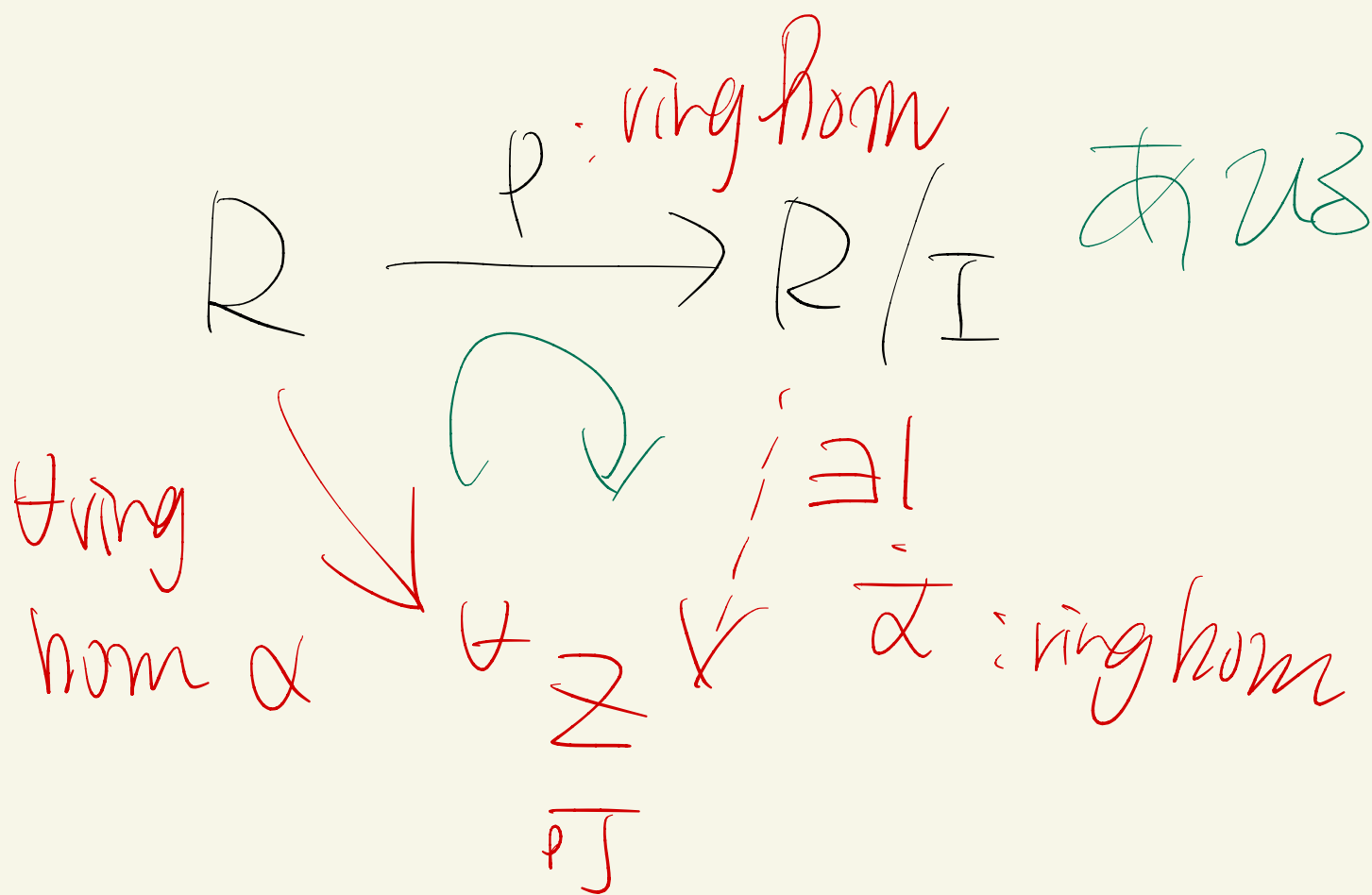
$$\begin{matrix} & \sim \\ & \xrightarrow{\quad} \\ a & A/\sim & \text{Int}h \\ & h & \text{bij} \end{matrix}$$

R : 可

$\cup$

I : ideal

$\leadsto R/I$: 商環



if $r \equiv r' \pmod{I} \Rightarrow \alpha(z) = \alpha(z')$
in $\mathbb{Z}$

$$\overline{\alpha}([\alpha] + [\gamma])$$

$$\stackrel{||}{=} \overline{\alpha}([\alpha]) + \overline{\alpha}([\gamma])?$$

$$\overline{\alpha}([1_R]) = 1_Z?$$

def $\stackrel{||}{=} \overline{\alpha}(1_R) \stackrel{||}{=} \alpha(\text{blank Prim})$
 $\text{temp} \leq$

部分環 $S \subseteq R$: 部分集合

$\left\{ \begin{array}{l} \text{和と積が閉じている} \\ 1_R \in S \end{array} \right.$

Remark $\hookrightarrow \nexists S \hookrightarrow R$: 包含は
ring hom ("check $\neq =$ ")

Ex $2\mathbb{Q} \subseteq \overset{\text{ideal}}{\mathbb{Q}}$ は部分環でない
 ~~$\mathbb{Q}$~~
 $1_{\mathbb{Q}}$

環の準同型定理

Thm

$$\begin{array}{ccc} x, x' \in R & \xrightarrow{f} & R' \\ & \searrow p & \nearrow \exists! \\ & R/\ker f & \text{単射} \end{array} \quad \text{ring hom}$$

① $x \underset{f}{\sim} x' \Leftrightarrow x \equiv x' \pmod{\ker f}$

$f(x) = f(x')$

を check すると

写像としての単射がある。
(by 集合の準同型定理)

(準同型) ② $f^{-1}(0_{R'}) = \ker f \subseteq R$: ideal

③ $\text{Im } f \subseteq R'$ (部分環)

環の同型定理

Thm

$$\begin{array}{ccc}
 R & \xrightarrow{f} & R \text{ : ring hom} \\
 \downarrow \varphi & \nearrow \exists! \bar{f} & \\
 R/\ker f & & \text{ring hom}
 \end{array}$$

Can $\bar{f} : R/\ker f \xrightarrow{\sim} \text{Im } f$

ring hom + inj + surj

(ring isom)

$\alpha: X \rightarrow Y$ 写像は X と Y について条件

Ex $\alpha: \mathbb{R} \rightarrow \mathbb{R}$

$$x \mapsto x^2$$

~~α'~~ $\alpha': \mathbb{R} \rightarrow \mathbb{R}_{\geq 0}$

$$x \mapsto x^2$$

$$\gamma: A \rightarrow B$$



$$A \times B \supseteq P$$

st...

Ex $\beta: \{-1, 0, 1\} \rightarrow \{-1, 0, 1\}$

~~β'~~ $x \mapsto x$

$$\beta': \{-1, 0, 1\} \rightarrow \{-1, 0, 1\}$$

$$x \mapsto x^3$$

中国剩余定理

↑
中国剩余定理

Jordan

$$\begin{array}{ccc} R & \xrightarrow{f} & R' : \text{ring hom} \\ \downarrow \times & \nearrow \exists! & \\ \mathfrak{p} & R/\ker f & \text{ring hom} \end{array}$$

$$\begin{array}{ccc} R \supseteq I, J & R \xrightarrow{\alpha} & (R/I) \times (R/J) \\ \downarrow \times & \nearrow & \\ & R/I \cap J & \text{ring hom} \end{array}$$

$\ker \alpha = I \cap J$

Ideal $\alpha \equiv$ 理想

e.g. $R = \mathbb{Q} \supseteq \begin{matrix} I = 2\mathbb{Q} \\ J = 3\mathbb{Q} \end{matrix}$

$$I + J = \{ 2x + 3y \mid x \in \mathbb{Q}, y \in \mathbb{Q} \} \\ = \mathbb{Q}$$

$$I \cap J = 6\mathbb{Q}$$

$$IJ = \{ 2x \cdot 3y \mid x, y \in \mathbb{Q} \} = 6\mathbb{Q}$$

$$\text{rad}(\underbrace{108}_{2^2 3^3}) = 2 \cdot 3 = 6$$

$$I + J \quad \text{不一定} \quad I \cup J$$

$$\textcircled{1} (a) + (b) = (d) \quad \textcircled{2} \exists \neq \text{ID}$$

$$d \mid a, b$$

$$\text{---} \exists x \exists y \quad ax + by = d$$

$$\text{if } d' \mid a \text{ and } d' \mid b \Rightarrow d' \mid d$$

$\therefore d$: 最大公因数

def $R \supseteq I, J$ ^{ideal} 互素 $\iff$

$$\Leftrightarrow R = I + J$$

def

$\iff$
互素

$$\Leftrightarrow \exists r_0 \in I \exists s_0 \in J. \quad r_0 + s_0 = 1_R$$

$\boxed{\text{CPT}}$ $\mathbb{R} \supseteq I, J$ s.t. $I \cap J = \mathbb{R}$

$$\Rightarrow \overline{I \cap J} = \overline{I} \cap \overline{J}$$

$$\mathcal{Q} \subseteq \{ \mathcal{M} \in \mathcal{P} \mid \exists j \in I \}$$

$$\mathbb{N} : 1 = \sum_{i_0 \in I} f_{i_0} \quad \exists i_0 \in I \exists f_{i_0} \in J$$

$$x \in I \cap J, \quad x = \frac{x|_I}{I} \otimes \frac{x|_J}{J}$$

Con $R/IJ \cong R/I \times R/J$: ring isom

① $R \rightarrow R/I \times R/J$ (if $I+J=R$)

$p \searrow$
 $R / \frac{IJ}{\cancel{IJ}} (y)_{IJ} \xrightarrow{\quad} \text{bl' isom } \frac{\cong}{\circ} (f=c)$
 $\Leftrightarrow \text{bz'}$

$$([a]_I, [b]_J) \in (R/I) \times (R/J)$$

$$1 = i_0 + j_0 \quad \exists i_0 \in I \quad \exists j_0 \in J$$

$$y = bi_0 + aj_0 \quad \forall a, b \in R$$

$$(A) \quad [y]_I = [a]_I \quad \text{in } R/I$$

$$(B) \quad [y]_J = [b]_J \quad \text{in } R/J$$

(C) of (A) $y = bi_0 + a(1-i_0)$

$$\therefore y - a = (b-a)i_0 \in I$$

(D) of (B) 同様

Ex $\mathbb{Z}/60 \cong \mathbb{Z}/20 \times \mathbb{Z}/30$

$$[r]_{60} \mapsto ([r]_{20}, [r]_{30})$$

eg. $[2]_{60} \mapsto ([0]_{20}, [2]_{30})$

$[5]_{60} \mapsto ([1]_{20}, [2]_{30})$

Thm (CRT) $R: \text{JD}$ $I_1, \dots, I_n: \text{ideal}$

$$I_i + I_j = R \quad (\leq i < j \leq n)$$

① $I_1 \cdots I_n = I_1 \cap \cdots \cap I_n$

② $R/I_1 \cdots I_n \cong (R/I_1) \times \cdots \times (R/I_n)$

$$[r]_{I_1 \cdots I_n} \mapsto ([r]_{I_1}, \dots, [r]_{I_n})$$

① n は正の整数 $n \leq 2: OK$

$$J := I_1 \cap \dots \cap I_{n-1} = I_1 \cap \dots \cap I_{n-1} : OK$$

$$\begin{aligned} \wedge \quad x_1 + y_1 &= 1 \quad \left(\begin{array}{l} \exists x_1 \in I_1, \exists y_1 \in I_n \\ \vdots \\ \exists x_{n-1} \in I_{n-1}, \exists y_{n-1} \in I_n \end{array} \right) \\ x_{n-1} + y_{n-1} &= 1 \end{aligned}$$

J と I_n は互いに素な素イデアル

$$1 - \underbrace{x_1 - \dots - x_{n-1}}_{\wedge} \in J \text{ と } \pi \text{ する}$$

$$I_1 \cap \dots \cap I_{n-1} = J$$

$$(x_1 + y_1) - \dots - (x_{n-1} + y_{n-1}) = x_1 - \dots - x_{n-1}$$

$$2^{n-1} \square = I_n \text{ の } 2^{n-1} \square \notin I_n$$

$$\therefore I_n J = I_n \cap J = I_n \cap (I_1 \cap \dots \cap I_{n-1})$$

$$\begin{aligned} I_n I_1 \dots I_{n-1} &= I_1 \cap \dots \cap I_n \\ \parallel \\ I_1 \dots I_n \end{aligned} //$$

$$\textcircled{2} R/JI_n \cong (R/J) \times R/I_n$$

$$R/J \cong R/I_1 \times \dots \times R/I_{n-1} //$$

~~Ex~~ 105 = 減算

Rem $R = \mathbb{Q}(x) \supset I = (2)$
 $\supset J = (x)$

係数の偶数
偶数

定数に注意

~~Q(x)~~ じゃダメ
 $I + J \nsubseteq R$ じゃ check して子。

応用例 (modular 演算)

$$A = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ \vdots & & & & \\ 0 & \dots & 0 \end{pmatrix}$$

中間式

は“うしろ”

大抵は行列, 整数成分

① $\det$ を知りたい (4) 3 (5) ~~体~~

①
②

③ $\mathbb{Q}/p_i\mathbb{Z}$ で計算

④ $\det A$ を

Gauss 消去法

計算可能

この $\mathbb{Z}$ 大抵は整数

② 素数 $p_1 \sim p_r$ を $\mathbb{Z}$ に与える

素 ideal

Recall 体 $\Rightarrow$ 整域

$\mathbb{Q}$ $\mathbb{Q}$

$$0 \neq 1$$

极大

$\downarrow$

素

Recall $R/I = \text{零环} \Leftrightarrow I = R$

Ex $\mathbb{Q} \not\subset \mathbb{Q} \subset \mathbb{Q}$
 $\mathbb{Q} \not\subset \mathbb{Q} \subset \mathbb{Q}$

① $\boxed{\Leftrightarrow} [r]_I \neq 0_{R/I} \Leftrightarrow r \notin I$

$$J = (r) + I \not\subset I \quad \therefore J = R$$

$$1 = r^3 x + 2^3 \Rightarrow [r]_I [x]_I = 1_{R/I} \text{ in } R/I$$

$$(\Rightarrow) \exists I \subseteq J \subseteq R$$

$$\Rightarrow R/I \text{ 域}$$

$$\textcircled{1} r \in J \setminus I$$

$$(r)_I \neq 0 \text{ in } R/I$$

$$\forall x \in R \quad rx \in J \neq 1$$

$$\underline{rx \equiv 1 \pmod{J} \text{ 不成立}}$$



$$\left(\exists x \in R \quad 1 - rx \in J \Rightarrow 1 \in J \right)$$

矛盾

Ex $\phi \in \mathbb{Q} : \neq \text{ideal}$

$\phi \neq (0) \Rightarrow \phi : \text{极大}$

① 有限整域は体

$$|\mathbb{Q}/a\mathbb{Q}| = a$$

$\mathbb{R}[x]$ は一般の PID と同様

e.g. $\mathbb{C}[x]$

$\forall A \neq \text{素環} \exists \text{极大 ideal}$
assuming 整环 (整)

② 同

次回 素因数分解の
一意性