# 第4回 代数系

前回の訂正

$$IJ = \{ \sum ij \mid \begin{matrix} i \in I \\ j \in J \end{matrix} \}$$

$ij$ の形の有限和

eg. $\mathbb{C}[x,y] \supseteq I = (x, y)$

$J = (x, 1+y^2)$

~~$IJ = \{ ij \mid x \mid i,\ y \mid j \}$~~

$IJ = \{ \sum_{\text{有限和}} ij \}$ $xy + x^2 y$

$= xy(1+$

同じことが 群の 交換子 群でもある

$G \geq H, K$

$[H,K] = \{[h,k] = hkh^{-1}k^{-1}$

$| h \in H, k \in K\}$

の生成する 部分群

---

Ex $\mathbb{C}[x,y,z,w]$

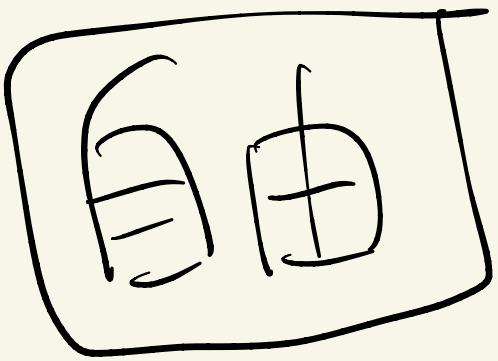
$I = (x,y)$

$J = (z,w)$

$IJ = (xz, xw, yz, yw)$

$\cup$

$xz + yw$



僕は歩く

$(X, \mathcal{O}_X)$
$(Y, \mathcal{O}_Y)$ : 位相sp

w) 直積 $X \times Y$

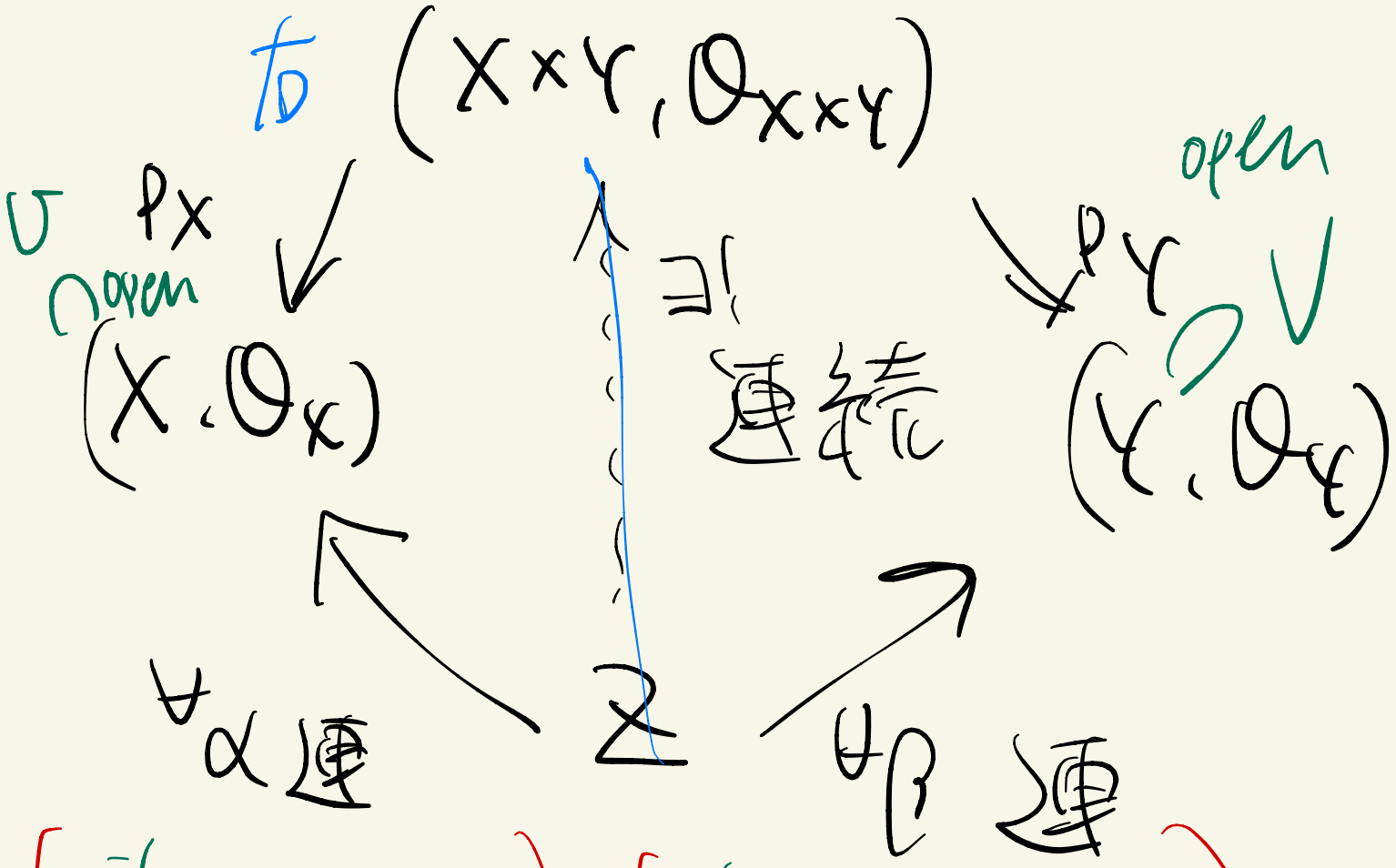
位相を $U \times V$　$U \in \mathcal{O}_X$, $V \in \mathcal{O}_Y$ : open

"とする" (うy)

---

$\subseteq$　　$\supseteq$

$\frac{2}{3}$




$\left(p_X^{-1}(U) = U\times Y\right) \cap \left(p_Y^{-1}(V) = X\times V\right)$

同じ普遍性をもつ $\Leftarrow U\cap V$

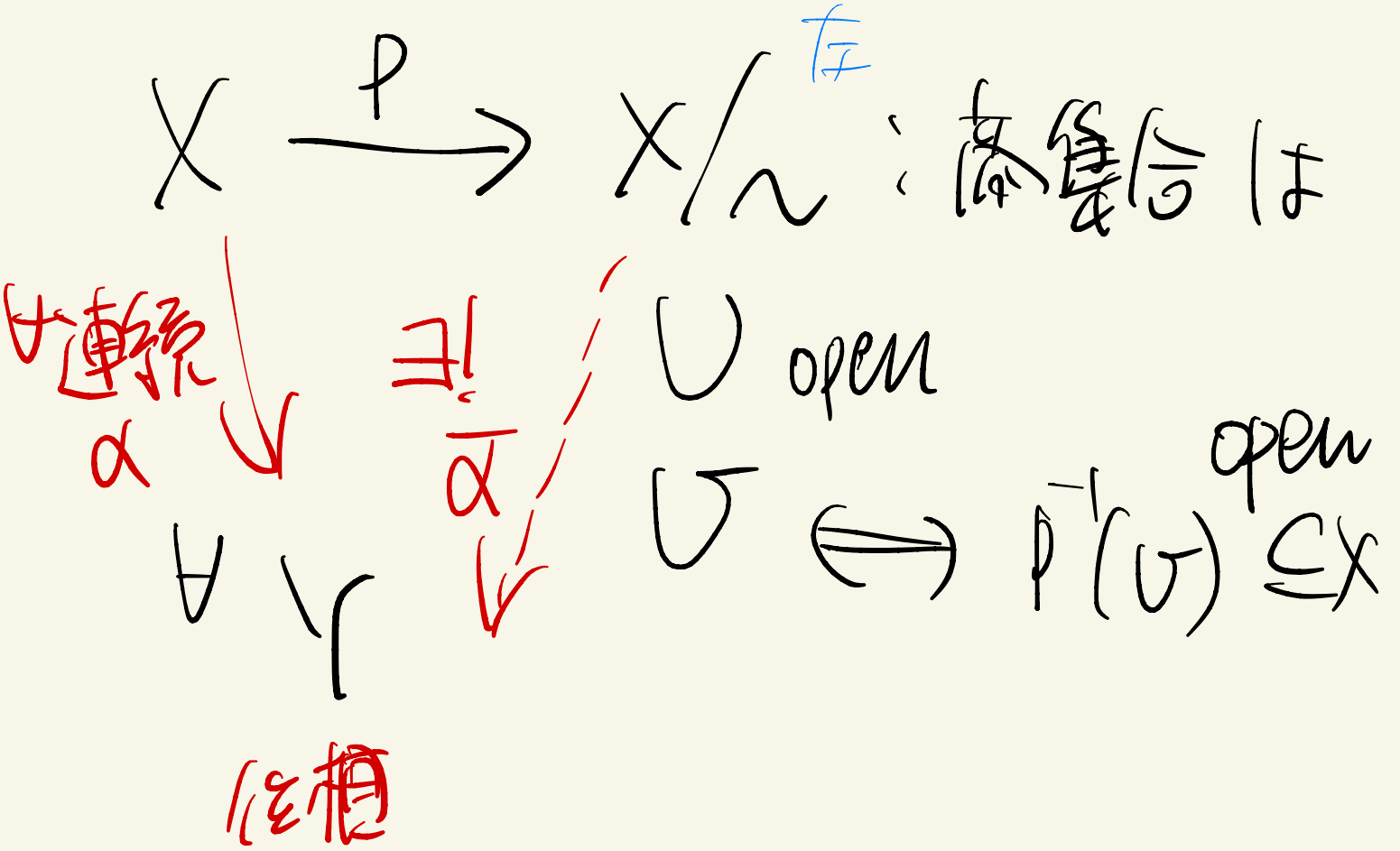
積位相は $p_X, p_Y$ が
連続になる最弱の位相

仮に積位相の def を忘れたとする

# 商位相

商位相は $p$ が連続になる最強の位相

$X$ : set　$\sim$ : equiv rel




s.t. $x \sim x' \text{ in } X \Rightarrow \alpha(x) = \alpha(x')$

という普遍性をもっている。

# 環は終わり

右剰のみ

Recall

$I \subseteq R$ が素 ideal $\overset{\text{def}}{\iff}$ $R/I$ が整域

満たす $\overset{\text{def}}{\iff}$ $R/I$ が体

$\iff$ $I \subsetneq J \subseteq R$

iff $\Rightarrow J = R$

($\iff$) 対偶

$R/I \ni [a] \neq 0$, $[b] \neq 0$ $\quad [ab] = 0$

($\Rightarrow$) $\exists a \notin I, \exists b \notin I \Rightarrow ab \in I$

Ex $R=\mathbb{Z}$

$p$: 素数 $\quad p \mid ab \Rightarrow p \mid a$ or $p \mid b$

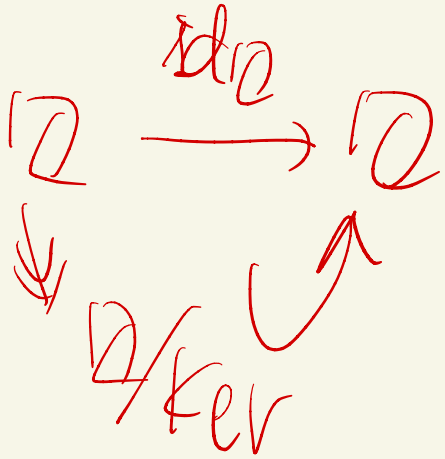
$a, b \in \mathbb{Z}_{\geq 1}$

($x \mid y \iff x$ が $y$ を割り切る)

Def $R$: 可換環

$$\mathrm{Spec}(R) = \{ \mathfrak{p} \subsetneq R \mid \mathfrak{p}: \text{素 ideal} \}$$

Ex $\mathbb{Z}/(0) \xrightarrow{\sim} \mathbb{Z}$




Ex $R \supsetneq I \neq (0)$

$\exists x \neq 0$

$\exists y \quad xy = 1 \in I$

$\therefore I = R$

prop $f$ : ring hom

$A \longrightarrow B$ ⇒ $f^{-1}(\mathfrak{q}) \subsetneq A$

$\cup$ $\cup$ 素

$f^{-1}(\mathfrak{q})$ $\mathfrak{q}$ も素ideal

素idealのring homによる

引き戻しは素ideal

(!)

$A \xrightarrow{f} B \xrightarrow{\pi} B/\mathfrak{q}$ : 合成 $h$

$B/\mathfrak{q}$ 整域

$\ker h = f^{-1}(\mathfrak{q})$

$= \{a \in A \mid f(a) \in \mathfrak{q}\}$

~~$A/\ker h$~~

$A/f^{-1}(\mathfrak{q})$

整域の部分環は整域

別証

$f^{-1}(\mathfrak{q}) \ni xy \Rightarrow f^{-1}(\mathfrak{q}) \ni x,\ f^{-1}(\mathfrak{q}) \ni y$

を示す.

def より $f(xy) \in \mathfrak{q}$

$\|$ ring hom

$f(x)f(y)$

$\mathfrak{q}$: 素ideal より $f(x) \in \mathfrak{q}$ or $f(y) \in \mathfrak{q}$

$\therefore x \in f^{-1}(\mathfrak{q})$ or $y \in f^{-1}(\mathfrak{q})$

( $f^{-1}(\mathfrak{q}) \neq A$ を示す　　$f(1_A)$

$f^{-1}(\mathfrak{q}) = A \Leftrightarrow 1_A \in f^{-1}(\mathfrak{q}) \Rightarrow \mathfrak{q} \ni 1_B$ : 矛盾 )

$R$ に対し $\mathrm{Spec}(R) = \{\text{素ideal}\}$

可換環　　集合

実は $\mathrm{Spec}(R)$ は位相空間になる

by

$I \subseteq R$ : ideal

$V(I) = \{\mathfrak{p} \supseteq I\}$ を閉集合系とする

---

$A \xrightarrow{f} B$ : ring hom

$\mathrm{Spec}(B) \to \mathrm{Spec}(A)$ は実は連続になる

$\mathfrak{q} \mapsto f^{-1}(\mathfrak{q})$

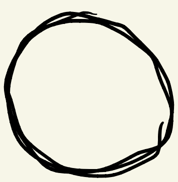
このことは現代数学が到達した
空間概念の1つの形

空間 X 〜〜 その上の関数 (環)

Map(X, ℝ)

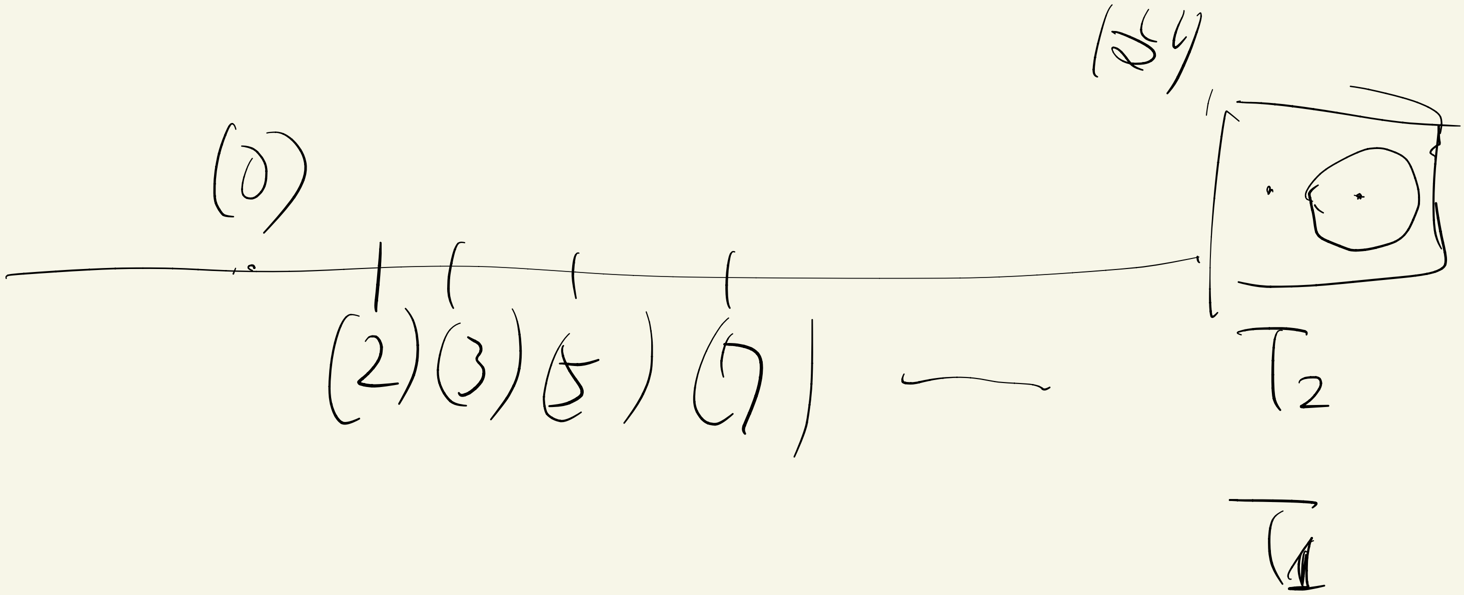
Spec(A) ←―― A

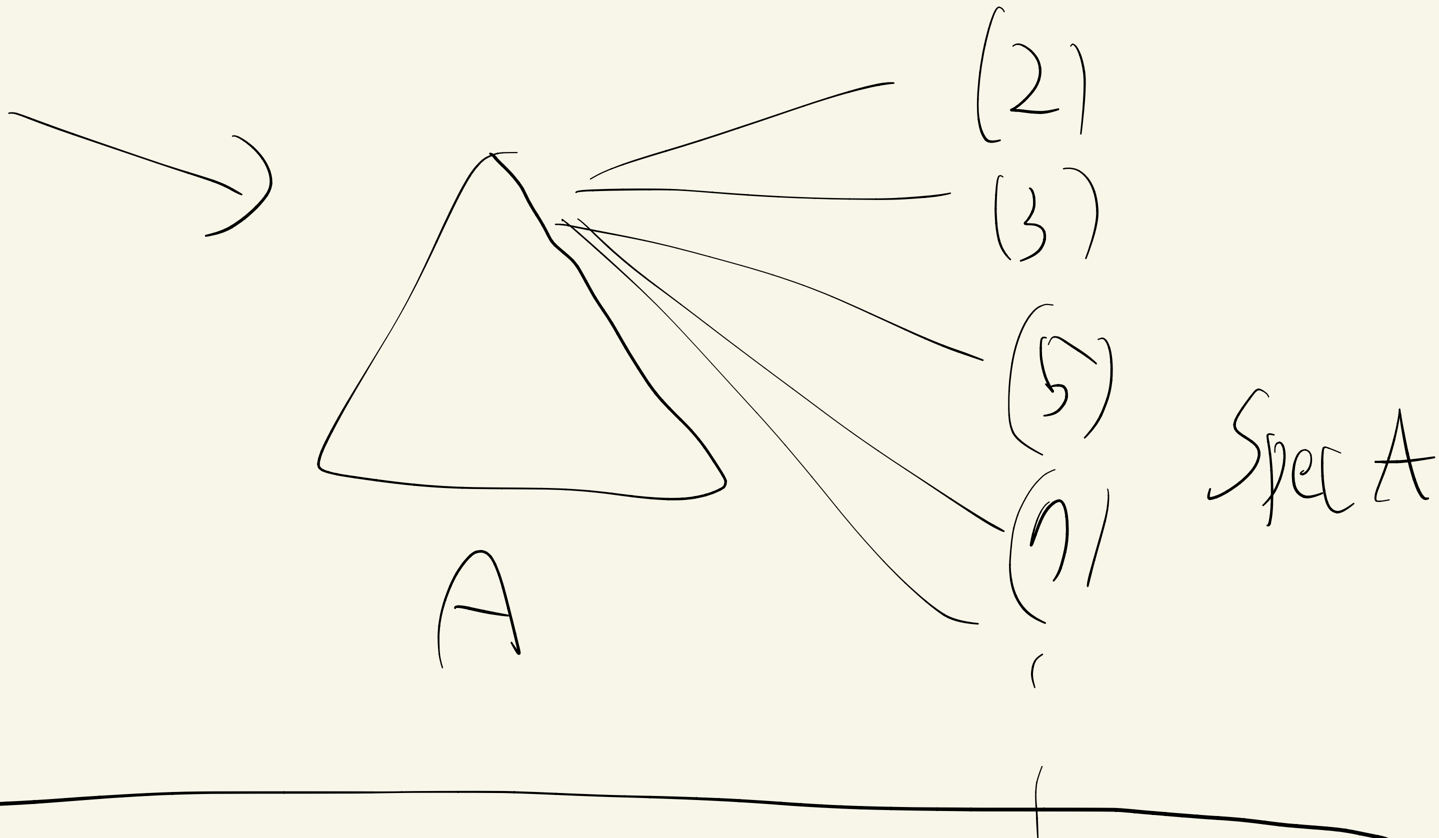
S

Ex  ← この上の連続関数は最大値をもつ

ℝ

スキーム　Grothendieck



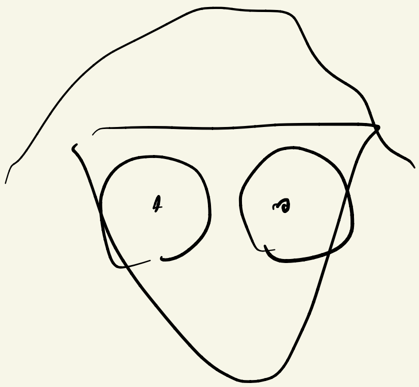

$\overline{\{(0)\}} = \mathrm{Spec}(\mathbb{Z})$ が[illegible]

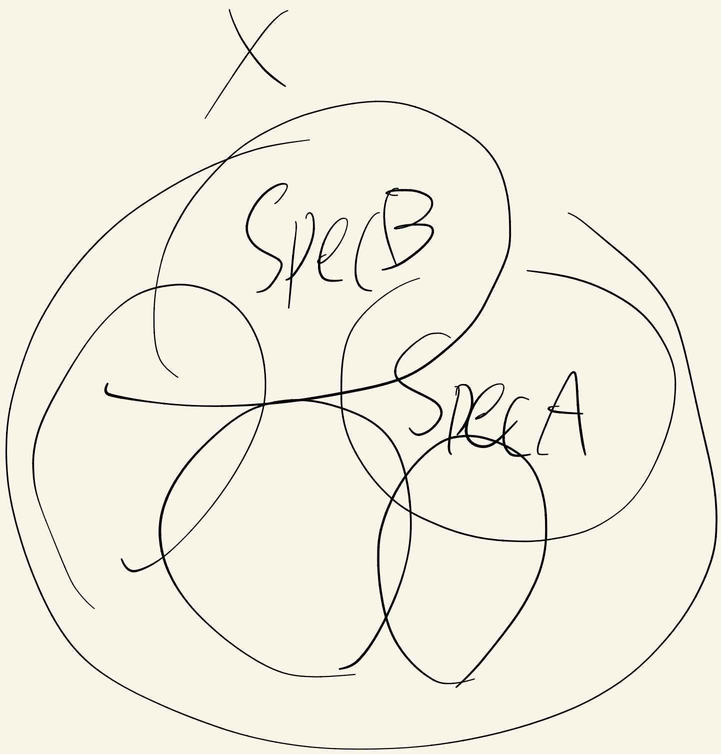
$\because$ $(0) \in C \Rightarrow C = \mathrm{Spec}(\mathbb{Z})$

閉 " $V(I) = \{\mathfrak{p} \supseteq I\}$

# 可換環 = 空間

ピカソの絵






スキーム

ページランク = 固有値1の
固有ベクトル

# 素因数分解の一意性 (右)

解 $(G, \cdot, e)$ 群

abelian group

Abel Noetherian

noetherian

Def $R$: 可 $\leadsto R^\times = U(R) = \{a \in R \mid \exists b \in R,\ ab = 1\}$

Unit

1の約数

Ex $\mathbb{Z}^\times = \{\pm 1\}$

記法 $a, b \in R$

$a \mid b \overset{\text{def}}{\iff} \exists c \in R,\ b = ac$

$\iff (b) \subseteq (a)$ iff

(!) $\Rightarrow$ $b \in (a) \therefore (b) \subseteq (a)$

$\Leftarrow$ $b \in (b) \subseteq (a)$ //

Ex $a \nmid b,\ b \nmid c \Rightarrow a \nmid c$

$b = ap,\ c = bq$

$c = apq$

$p, q \in R^{\times}$

$pq \in R^{\times}$

prop $R^\times$ は可換群

① $a, b \in R^\times$ (i.e. $\exists c\ ac=1$, $\exists d\ bd=1$)

$ab \in R^\times$ ? ($abcd=1$)

素元 $\Vert$ $p \mid ab \Rightarrow p \mid a$ or $p \mid b$ $\Vert$

既約元 $a=bc \Rightarrow b \in R^\times$ or $c \in R^\times$

i.e. $a \sim c$ or $a \sim b$

素元 $\Rightarrow$ 既約元

Prop

$R$ : 整域 $a \neq 0$

$ab = ac \Rightarrow b = c$

$a(b-c) = 0$

$\Rightarrow b-c=0 \Rightarrow b=c$

Def (UFD)

Ex $6 = 2\cdot 3 = (-2)(-3)$

$(p_1) \ni p_1 \cdot 1 = q_1 \cdots q_s$

$\Rightarrow \exists i,\ q_i \in (p_1)$ $\quad q_1 = p_1 c$ 存在 $c \in R^\times$

$1 = c^{-1} q_2 \cdots q_s \Rightarrow q_2 \sim q_s \in R^\times$

$(p_1) \ni p_1 \times \cdots \times p_r = q_1 \times \cdots \times q_s$

$\exists i \quad q_i \in (p_1)$

$p_2 p_3 \cdots p_r = (d q_2) q_3 \cdots q_s$

あとは帰納法の仮定

---

$d q_2$ は素元

∵ $(d q_2) = (q_2)$

$\left( \begin{array}{l} c d = 1 \\ c d q_2 = q_2 \end{array} \right)$

$\left( \begin{array}{l} (d q_2) \subseteq (q_2) \\ q_2 \in (d q_2) \text{ は } d^{-1}(d q_2) = q_2 \text{ から従う} \end{array} \right)$

例 $R$ : PID

素元 $\Leftarrow$ 既約元

∵ $a$ : irr

$\{0\} \subsetneq (a) \subsetneq R$

$\subseteq (b) \subsetneq$

$(a)$ が極大を示す ($\Rightarrow$ $(a)$ は素 ideal)

$a \in (a) \subseteq (b)$ をとる

i.e. $\exists c \in R \quad a = bc$

$a$ : irr $\Rightarrow$ $\underline{b \in R^\times}$ or $\underline{c \in R^\times}$

$\Downarrow \qquad\qquad \Downarrow$

$(b) = R \qquad (a) = (b)$

**Thm** PID ⇒ UFD が目標

これが言えると

- $\mathbb{Z}$ は PID
- $\mathrm{Spec}(\mathbb{Z}) = \{(0), (p) \mid p \text{ は素数}\}$
- $\mathbb{Z}^\times = \{\pm 1\}$

F: $\mathbb{Z}$ 普通の素因数分解の一意性

が出る

**Lem** R: PID, ideal の ACC 成立

(5) $I_1 \subseteq I_2 \subseteq$ ———

$J = \bigcup_{n \geq 1} I_n$ はRのideal $= \overset{\exists}{(j)}$

$\left( \sum_{n \geq 1} I_n \text{ はいつでも ideal} \right)$

$IJ \quad I+J \neq I \cup J$

↑ (i) $x, y \in J$

i.e. $\exists m_1,\ x \in I_{m_1}$,

$\exists m_2,\ y \in I_{m_2}$

$m = \max\{m_1, m_2\}$, $x, y \in I_m$

$\therefore x + y \in I_m \subseteq J$

$J \ni g$ i.e. $\exists N$, $I_N \ni g$

$$J = \bigcup_{n \geq 1} I_n$$

このとき $I_N \supseteq J$

より $I_N = I_{N+1} = \cdots = J$ //

---

<u>prop</u> $R$ : PID $\ni a$ : ~~単元~~, ~~0~~

$\exists b \in R$ : irr s.t. $b \mid a$

(:) $a$ : irr $\Rightarrow$ done $(b = a)$

o.w. $a = a'a''$ $a', a'' \in R^\times$

どちらかが irr $\Rightarrow$ done

o.w. $a' = a'''a''''$ どちらかが irr $\Rightarrow$ done

そうでなければ…… とくり返す

$a = a' a''$ $\quad a' = a''' a''''$

$a''', a'''' \notin R^\times$

$(a) \subsetneq (a') \subsetneq (a'') \subseteq \cdots$

これ無限にくり返すことはない。//

Ex $12347891 = \underline{a}b$

$cd$

<u>Thm</u> PID ⇒ UFD (既約元⇔素元)

(証) $a \in R$ : $\cancel{0}$, $\cancel{R^\times}$

$\parallel$

$a_1 \sim a_r$ : 既約元の積を言う。

とにかく $a = {}^\exists a_1 c$ $\quad \exists a_1$ : irr

$c \in R^\times$ そうでない $c = {}^\exists a_2 d$ $\quad \exists a_2$ : irr

~~$c \in R^\times$ なら~~ $(a) \subsetneq (a_1) \subsetneq (a_2) \subsetneq \cdots$

そうさが続くかぎり　できない

それはないので このprocessは有限回で止まって $a = a_1 \sim a_r u$ $\exists u \in R^\times$ となる.

---

<u>Thm</u> $R$ : UFD $\Rightarrow$ $R[x]$ もUFD

(Gauss)

$\left(\mathbb{Z}[x_1, \dots, x_{n-1}]\right)[x_n]$

$\mathbin{/\!/}$

(ex) $\mathbb{Z}[x_1 \sim x_n]$ もUFD

$\mathbb{Q}[x_1 \sim x_n]$

(∵ $\mathbb{Z}, \mathbb{Q}$ : PID)

# アインシュタイン既約判定法

整域 $R \to$ 商体 $K = \mathrm{Frac}(R)$

$= \mathbb{Q}(R)$

$\mathbb{Q} \to \overline{\mathbb{Q}} = \mathrm{Frac}(\mathbb{Q})$

$= \mathbb{Q}(\mathbb{Q})$

も体である。

---

宿題 Def. 準同型, CRT, UFD

PID

---

$AB = E_n \Rightarrow BA = E_n$

$n \times n$