- 前回主に扱ったこと：可換環とイデアルの定義
- 以下，この講義では特別に断らない限り，可換環を考察する．
- 可換環 R とイデアル $I \subseteq R$ について，商環 R/I を定義する．
- 環準同型写像と環同型写像を定義し，普遍性の例を知る．

記法：R が可換環のとき，$a_1, \cdots, a_n \in R$ について

$$\left\{ \sum_{i=1}^{n} x_i a_i \mid 1 \leq \forall i \leq n, x_i \in R \right\} (= \{a_1, \cdots, a_n \text{ の } R \text{ 線形結合 }\})$$

は R のイデアルである．これを $(a_1, \cdots, a_n)$ と書く．

注意：$(0_R) = \{0_R\}, (1_R) = R, () = \{0_R\}$.

例：$R = \mathbb{Z}$ のとき：

- $(2) = 2\mathbb{Z} = \{$ 偶数 $\}$.
- $a, b \in \mathbb{Z}_{\geq 1}$ が互いに素のとき $(a, b) = \mathbb{Z}$.

定義：整域 R が単項イデアル整域（PID）とは，$\forall I \subseteq R$:イデアル, $\exists a \in R, I = (a)$.

例：

- 有理整数環 $\mathbb{Z}$ は PID.
- 1 変数多項式環 $\mathbb{C}[x]$ は PID だが，2 変数多項式環 $\mathbb{C}[x, y]$ は PID ではない．
- ガウス整数環 $\mathbb{Z}[i] = \{a + b\sqrt{-1} \mid a, b \in \mathbb{Z}\} (\subseteq \mathbb{C})$ は PID である．

注意：可換環 R がネーター環とは，$\forall I \subseteq R$:イデアル, $\exists a_1, \cdots, \exists a_n \in R, I = (a_1, \cdots, a_n)$. 初学者が出合うたいていの可換環はネーター環である．

以下，1 ページと 2 ページでは，R を可換環，$I \subseteq R$ をそのイデアルとする．

命題：$a, b \in R$ について $a \equiv b \pmod{I} :\Leftrightarrow a - b \in I$ とすると，$\equiv$ は R 上の同値関係である．

証明：以下の 3 条件をチェックする：

- $a \equiv a \pmod{I}$.
- $a \equiv b \pmod{I} \Rightarrow b \equiv a \pmod{I}$.
- $a \equiv b \pmod{I}, b \equiv c \pmod{I} \Rightarrow a \equiv c \pmod{I}$.

記法：$a \in R$ について

- $[a] := \{b \in R \mid b \equiv a \pmod{I}\}$（$a$ の同値類．注：本当は $[a]_I$ とでも書かれるもので，$a + I$ とも書かれる）
- $R/I := \{[a] \mid a \in R\}$（同値類の集合）

例：$R=\mathbb{Z}, I=2\mathbb{Z}=(2)$ とすると

- $[0]=[-4]=\cdots=\{$ 偶数 $\}=:$ 偶.
- $[1]=[-101]=\cdots=\{$ 奇数 $\}=:$ 奇.
- $\mathbb{Z}/2\mathbb{Z}=\{$ 偶, 奇 $\}$

例：$R=\mathbb{C}[x], I=(x^2)=\{f(x)x^2 \mid f(x)\in\mathbb{C}[x]\}=\{x^2$ 以上の多項式 $\}$ とすると

$$R/I=\mathbb{C}[x]/(x^2)=\{[ax+b] \mid a,b\in\mathbb{C}\}$$

実際，$g(x)\in\mathbb{C}[x]$ について，$g(x)=x^2Q(x)+Ax+B$ とすると（$Q[x]\in\mathbb{C}[x], A,B\in\mathbb{C}$），$[g(x)]=[Ax+B]$．$Ax+B\equiv A'x+B' \pmod{x^2}$ ならば $A=A', B=B'$ である．

命題：以下は well-defined.

- $+_{R/I}: R/I\times R/I\to R/I, ([a],[b])\mapsto[a+b]$.
- $\times_{R/I}: R/I\times R/I\to R/I, ([a],[b])\mapsto[ab]$.

証明：$a,b,c,d\in R$ について，$a\equiv c \pmod I, b\equiv d \pmod I$ ならば $a+b\equiv c+d \pmod I, ab\equiv cd \pmod I$ を示せばよい．

$\underline{a+b\equiv c+d \pmod I \text{ であること}}$：$(a+b)-(c+d)=(a-c)+(b-d)\in I$.

$\underline{ab\equiv cd \pmod I \text{ であること}}$：$ab-cd=(a-c)b+c(b-d)\in I$.

命題：$(R/I, +_{R/I}, \times_{R/I}, [0_R], [1_R])$ は可換環の公理を満たす．

証明：全部はやらないが，例えば加法の結合法則を示すには

$$\forall a\in R, \forall b\in R, \forall c\in R, ([a]+[b])+[c]=[a]+([b]+[c])$$

を言えばよい．左辺 $=[a+b]+[c]=[(a+b)+c]$ であり，右辺 $=[a]+[b+c]=[a+(b+c)]$ だが，R 中で $(a+b)+c=a+(b+c)$ なので，左辺 $=$ 右辺である．他も同様.

記法：$(R/I, +_{R/I}, \times_{R/I}, [0_R], [1_R])$ を R の I による商環と言い，単に R/I と書く．

注意：$\mathbb{C}[x]/(x^2)$ において，$\varepsilon:=[x]\in\mathbb{C}[x]/(x^2)$ とすると，$\varepsilon^2=[x^2]=[0]$ である（べき零元）．つまり $\varepsilon(\neq[0])$ は「無限小」の一例と思うことができる．

定義：可換環 $(R,+_R,\times_R,0_R,1_R)$ と $(S,+_S,\times_S,0_S,1_S)$ について，写像 $f:R\to S$ が環準同型写像とは，f が以下の 3 条件を満たすこと．

(1) $\forall a\in R, \forall b\in R, f(a+_R b)=f(a)+_S f(b)$.
(2) $\forall a\in R, \forall b\in R, f(a\times_R b)=f(a)\times_S f(b)$.
(3) $f(1_R)=1_S$.

注意：$f(0_R) = 0_S$.

証明：$0_R = 0_R + 0_R$ と (1) より，$f(0_R) = f(0_R) + f(0_R)$．両辺に $-f(0_R)$ を加える．

命題：任意の可換環 R について，恒等写像 $\mathrm{id}_R : R \to R$ は環準同型写像（明らか）．

命題：環準同型写像 $R \xrightarrow{f} S \xrightarrow{g} T$ について，合成 $g \circ f : R \to T$ は環準同型写像（容易）．

注意：上の 2 つの命題は，以下のように表現される：「可換環の集まり **CRing** は，環準同型写像を射とする圏をなす」

命題：可換環 R とイデアル $I \subseteq R$ について，写像 $\pi : R \to R/I, a \mapsto [a]$ は環準同型写像．

証明：R/I の構成の際に示している．

命題：1 点集合 $\{*\}$ は，ただ 1 通りの可換環の構造をもつ（零環）が，零環は以下の性質をもつ：

「任意の可換環 R について，ただ 1 つの環準同型写像 $f : R \to \{*\}$ が存在する」

注意：このような「全体における立ち位置」による特徴付けを普遍性と言う（正確な議論はしない．気になる人は「表現可能関手の表現（米田の補題）」をキーワードに調べてみるとよい）．

注意：「」を以下のように略記することがある：$\forall R \in \mathbf{CRing}, \exists! f : R \to \{*\} \in \mathbf{CRing}$.

注意：上記命題は以下のように表現される：「圏 **CRing** において，零環（ふつう $\{0\}$ と書く）は終対象である」

証明：ただ 1 つの写像 $f : R \to \{*\}, a \mapsto *$ が環準同型であることがチェックできる．

命題：可換環 $\mathbb{Z}$ は次の性質をもつ：

「任意の可換環 R について，ただ 1 つの環準同型写像 $\mathbb{Z} \to R$ が存在する」

証明：環準同型 $f : \mathbb{Z} \to R$ は，$f(1) = 1_R$ なので，$n \geq 1$ について

$$f(n) = f(\underbrace{1 + \cdots + 1}_{n}) = \underbrace{f(1) + \cdots + f(1)}_{n} = \underbrace{1_R + \cdots + 1_R}_{n}$$

でなければならない．また $0 = n + (-n)$ より $f(0) = f(n) + f(-n)$．$f(0) = 0_R$ だったので，$f(-n) = -(\underbrace{f(1) + \cdots + f(1)}_{n})$ でもなければならない．

つまり f は存在したとすると，ただ 1 つである．逆に，上のように定義した f は環準同型になっていることがチェックできる（単に面倒）．

注意：上記命題は以下のように表現される：「圏 **CRing** において，有理整数環 $\mathbb{Z}$ は始対象である」

定義：可換環の環準同型写像 $f : R \to S$ が環同型写像であるとは：

$$\exists g : S \to R : \text{環準同型写像}, f \circ g = \mathrm{id}_S, g \circ f = \mathrm{id}_R.$$

注意：このとき g も環同型写像である（当たり前）.

記法：可換環 R, S について，環同型写像 $f : R \to S$ が存在するとき，R と S は環同型と言って，$R \cong S$ と書く．環準同型写像 f についても同型であることを強調するときは，$f : R \xrightarrow{\sim} S$ のように書くことがある.

命題：環同型は「同値関係」である（ただし，「すべての可換環の集まり」は集合ではない）．つまり，可換環 R, S, T について以下が成り立つ（容易）.

(1) $R \cong R$.
(2) $R \cong S \Rightarrow S \cong R$.
(3) $R \cong S, S \cong T \Rightarrow R \cong T$.

命題：可換環 X が次の性質をもつとき，$X \cong \{0\}$（環同型）.

「任意の可換環 R について，ただ 1 つの環準同型写像 $f : R \to X$ が存在する」

証明：仮定より，ただ 1 つの環準同型 $\alpha : \{0\} \to X$ が存在する（$R = \{0\}$ とした）．一方，$\{0\}$ も同じ普遍性を満たすので，環準同型 $\beta : X \to \{0\}$ が存在する（もちろんただ 1 つ）.

今，合成 $X \xrightarrow{\beta} \{0\} \xrightarrow{\alpha} X$ は環準同型だが，もちろん $\mathrm{id}_X : X \to X$ も環準同型である．普遍性における「ただ 1 つの」から $\alpha \circ \beta = \mathrm{id}_X$ でなければならない．同様に $\beta \circ \alpha = \mathrm{id}_{\{0\}}$ も分かる.

注意：以下は「ベーシック圏論」の序文からの引用である.

▌　この証明は，環の特殊性をほとんど使っておらず，実際はより高次の一般性に依拠している.

例：可換環 X が次の性質をもつとき，$X \cong \mathbb{Z}$（環同型）.

「任意の可換環 R について，ただ 1 つの環準同型写像 $f : X \to R$ が存在する」

証明：同様（単に矢印の向きを逆にすればよい）.

例：任意の集合 R について，1 点集合 $\{*\}$ へのただ 1 つの写像 $R \to \{*\}$ が存在する.

例：任意の集合 R について，空集合 $\emptyset$ からただ 1 つの写像 $\emptyset \to R$ が存在する.

注意：これらは集合の圏 **Set** における普遍性の例であり，$\{*\}$ や $\emptyset$ を全単射（**Set** における同型射と同じ）を除いて決定する.