- 前回主に扱ったこと：商環と環準同型写像.
- 商環の普遍性を確認し，環準同型定理を導く（それぞれ集合版にも触れる).
- イデアルが互いに素であることを定義し，中国剰余定理を導く.
- 応用として「2 で割った余りと 3 で割った余りから 6 で割った余りが分かる」といった常識的事実（105 減算）や，大きな整数正方行列の行列式の計算方法（モジュラー算法）を見る.

普遍性の例：集合 X と Y について，直積集合 $X \times Y$ は次の性質を持つ（ここで $\mathrm{pr}_X : X \times Y \to X, (x, y) \mapsto x$ と $\mathrm{pr}_Y : X \times Y \to X, (x, y) \mapsto y$ は射影である）:

「任意の集合 Z と任意の写像 $\alpha : Z \to X, \beta : Z \to Y$ について，$\alpha = \mathrm{pr}_X \circ f, \beta = \mathrm{pr}_Y \circ f$ となるただ 1 つの写像 $f : Z \to X \times Y$ が存在する」

$$\begin{tikzcd}
 & Z \arrow[d, dotted, "f"] \arrow[ddl, "\alpha"'] \arrow[ddr, "\beta"] & \\
 & X \times Y \arrow[dl, "\mathrm{pr}_X"] \arrow[dr, "\mathrm{pr}_Y"'] & \\
X & & Y
\end{tikzcd}$$

証明：$f : Z \to X \times Y, z \mapsto (\alpha(z), \beta(z))$ がそのような写像であることが確認できる.

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，直積集合 $R \times S$ は可換環の構造 $(R \times S, +_{R\times S}, \times_{R\times S}, (0_R, 0_S), (1_R, 1_S))$ を持つことが確認できる．これを R と S の直積環と言って，単に $R \times S$ と書く．ここで，環演算は成分ごとに以下のように定義している.

$$\begin{aligned}
+_{R\times S} &: (R \times S) \times (R \times S) \to (R \times S), \quad ((r, s), (r', s')) \mapsto (r +_R r', s +_S s'), \\
\times_{R\times S} &: (R \times S) \times (R \times S) \to (R \times S), \quad ((r, s), (r', s')) \mapsto (r \times_R r', s \times_S s').
\end{aligned}$$

注意：集合 X, Y の直積 $X \times Y$ の普遍性に現れる「集合」と「写像」を「可換環」と「環準同型写像」に変えると，直積環 $R \times S$ の（**CRing** における）普遍性になっている.

命題（商集合の普遍性）：集合 X とその上の同値関係 $\sim$ による商集合 $X/\sim$ は次の性質を持つ（ここで $p : X \to X/\sim, x \mapsto C_x := \{y \in X \mid y \sim x\}$ は自然な全射）:

「任意の集合 Z と任意の写像 $\alpha : X \to Z$ について，

$$\forall x_1 \in X, \forall x_2 \in X, x_1 \sim x_2 \Rightarrow \alpha(x_1) = \alpha(x_2)$$

ならば，$\alpha = f \circ p$ となるただ 1 つの写像 $f : X/\sim \to Z$ が存在する」

$$\begin{tikzcd}
X \arrow[r, "p"] \arrow[dr, "\alpha"'] & X/\sim \arrow[d, dotted, "f"] \\
 & Z.
\end{tikzcd}$$

証明：$\alpha = f \circ p$ とすると，$\forall x \in X, \alpha(x) = f(C_x)$ でなければならないので，f は存在するとただ 1 つ．よって $f(C_x) = \alpha(x)$ によって $f : X/\sim \to Z$ が well-defined であることを言えばよい．つまり $\forall x \in X, \forall x' \in X, C_x = C_{x'} \Rightarrow \alpha(x) = \alpha(x')$ を言う．定義によって $C_x = C_{x'} \Leftrightarrow x \sim x'$.

系（集合での準同型定理）：集合 A, B と写像 $h : A \to B$ について，A 上の同値関係 $\sim_h$ を

$$a_1 \sim_h a_2 \Leftrightarrow h(a_1) = h(a_2)$$

と定めると，単射 $\overline{h} : A/\sim_h \to B$ は全単射 $\overline{h} : A/\sim_h \to \operatorname{Im} h$ を誘導する．

証明：$\overline{h} : A/\sim_h \to B$ は単射である（実際 $a, b \in A$ について，$\overline{h}(C_a) = \overline{h}(C_b)$ は $h(a) = h(b)$ と同値で，定義よりこれは $a \sim_h b (\Leftrightarrow C_a = C_b)$ と同値）．よって $\overline{h} : A/\sim_h \to \operatorname{Im} h$ は全単射である．

命題（商環の普遍性）：可換環 R とそのイデアル I による商環 R/I は以下の普遍性を持つ：

「任意の可換環 Z と任意の環準同型写像 $\alpha : R \to Z$ について，

$$\forall r \in R, \forall r' \in R, r \equiv r' \pmod{I} \Rightarrow \alpha(r) = \alpha(r')$$

ならば，$\alpha = \overline{\alpha} \circ \pi$ となるただ 1 つの環準同型写像 $\overline{\alpha} : R/I \to Z$ が存在する」

$$\begin{tikzcd} R \arrow[r, "\pi"] \arrow[dr, "\alpha"'] & R/I \arrow[d, dotted, "\bar{\alpha}"] \\ & Z. \end{tikzcd}$$

証明：（集合論的）写像 $\overline{\alpha} : R/I \to Z$ で $\alpha = \overline{\alpha} \circ \pi$ となるものがただ 1 つ存在するので（すぐ前にやった），$\overline{\alpha}$ が環準同型であることを言えばよいが，$\forall x \in R, \overline{\alpha}([x]) = \alpha(x)$ から容易に確認できる．

定義：可換環 $(R, +.\cdot, 0_R, 1_R)$ の部分集合 $S \subseteq R$ が以下の条件を満たすとき，$(S, +|_{S \times S}, \cdot|_{S \times S}, 0_R, 1_R)$ は可換環になる．このとき S を R の部分環と言う．

(1) $1_R \in S$.
(2) $\forall s \in S, \forall t \in S, s \pm t \in S, st \in S$.

例：$\mathbb{Z} \subseteq \mathbb{Q}$ は $\mathbb{Q}$ の部分環．一方 $2\mathbb{Z} \subseteq \mathbb{Z}$ は，(1) が成り立たないため，この講義では $\mathbb{Z}$ の部分環ではない（$\mathbb{Z}$ のイデアルにはなっている）．

命題：可換環の環準同型写像 $f : R \to R'$ について

(1) $\operatorname{Im} f$ は R' の部分環.
(2) $f^{-1}(0_{R'})(= \{x \in R \mid f(x) = 0_{R'}\})$ は R のイデアル.

証明：容易.

記法：$f^{-1}(0_{R'})$ を f の核と呼び，$\operatorname{Ker} f$ と書く．

定理（環準同型定理）：可換環の環準同型写像 $f : R \to R'$ について，単射環準同型写像 $\overline{f} : R/\operatorname{Ker} f \to R'$ は，（すぐ下の命題によって）環同型 $\overline{f} : R/\operatorname{Ker} f \xrightarrow{\sim} \operatorname{Im} f$ を誘導する．

証明：$x, x' \in R$ について，以下を確認すればよい：$x \sim_f x' \Leftrightarrow x \equiv x' \pmod{\operatorname{Ker} f}$.

$(\Rightarrow)$：$f(x) = f(x')$ ならば $f(x - x') = 0_{R'}$．よって $x - x' \in \operatorname{Ker} f$.

$(\Leftarrow)$：上を逆にたどればよい．

命題：可換環の環準同型写像 $f : R \to S$ について，以下の 2 条件は同値である．

(A) f は環同型写像

(B) f は（集合論的）全単射

証明：(A)$\Rightarrow$(B) は明らか．(A)$\Leftarrow$(B) を言うには，f の（集合論的）逆写像 $g : S \to R$ が環準同型であることを示せる．例えば $\forall a \in S, \forall b \in S, g(a + b) = g(a) + g(b)$ を示そう．

今，f は全単射なので $\exists! A \in R, a = f(A)$ かつ $\exists! B \in R, b = f(B)$．$f$ は準同型なので $f(A) + f(B) = f(A + B)$ なので，$g(f(A) + f(B)) = g(f(A + B)) = A + B$．よって，左辺 $= A + B$．一方，$g(a) + g(b) = g(f(A)) + g(f(B)) = A + B$ なので，右辺 $= A + B$ でもある．

系（中国剰余定理の簡易版）：可換環 R とそのイデアル I, J について，環準同型

$$f : R \to (R/I) \times (R/J), \quad r \mapsto ([r]_I, [r]_J)$$

は，単射環準同型 $\overline{f} : R/(I \cap J) \to (R/I) \times (R/J)$ を誘導する．

証明：$\operatorname{Ker} f = I \cap J$ を示せばよいが，f の定義より明らか．

例：$R = \mathbb{Z}, I = 2\mathbb{Z}, J = 3\mathbb{Z}$ とすると，$I \cap J = 6\mathbb{Z}$ で，

$$\mathbb{Z}/6\mathbb{Z} \to (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z}), \quad [r]_{6\mathbb{Z}} \mapsto ([r]_{2\mathbb{Z}}, [r]_{3\mathbb{Z}})$$

が単射環準同型と言っている．この例では，もちろん環同型でもある．

イデアルの演算：R を可換環，I, J をそのイデアルとする．以下は R のイデアルである（容易）．

(1) $I + J := \{i + j \mid i \in I, j \in J\}$（和．有限個のイデアルの和も同様）．

(2) $I \cap J$（共通部分）．

(3) $IJ := \bigcup_{n \geq 0} \{\sum_{k=1}^{n} i_k j_k \mid i_k \in I, j_k \in J\}$（積．有限個のイデアルの積も同様）．

(4) $(I : J) := \{r \in R \mid \forall j \in J, rj \in I\}$（商）．

(5) $\sqrt{I} := \{r \in R \mid \exists n \geq 0, r^n \in I\}$（根基）．

例：$R = \mathbb{Z}$ で，$a, b \geq 1$ について $I = (a)(= a\mathbb{Z}), J = (b)$ のとき

$$(a) + (b) = (\gcd(a, b)), \quad (a) \cap (b) = (\operatorname{lcm}(a, b)), \quad (a)(b) = (ab).$$

定義：可換環 R のイデアル I, J が互いに素とは：$I + J = R$.

注意：$I + J = R$ は以下と同値：$\exists i \in I, \exists j \in J, i + j = 1_R$.

定理：可換環 R の互いに素なイデアル I, J について

(1) $IJ = I \cap J$.
(2) $R/IJ \to (R/I) \times (R/J), [r]_{IJ} \mapsto ([r]_I, [r]_J)$ は環同型写像.

証明：(1) $IJ \subseteq I \cap J$ は明らかなので，$IJ \supseteq I \cap J$ を示す：仮定より $\exists i_0 \in I, \exists j_0 \in J, i_0 + j_0 = 1_R$. よって $x \in I \cap J$ について，$x = xi_0 + xj_0 \in I \cap J$.

(2) (1) と中国剰余定理の簡易版より，写像の全射性を言えばよい：$([a]_I, [b]_I) \in (R/I) \times (R/J)$ について，$y = bi_0 + aj_0$ とすると，$[y]_I = [a]_I, [y]_J = [b]_J$ である.

定理（中国剰余定理, CRT）：可換環 R のイデアル $I_1, \cdots, I_n$ が，任意の $1 \leq i \neq j \leq n$ について $I_i + I_j = R$ ならば,

(1) $I_1 \cdots I_n = I_1 \cap \cdots \cap I_n$.
(2) $R/I_1 \cdots I_n \to (R/I_1) \times \cdots \times (R/I_n), [r]_{I_1 \cdots I_n} \mapsto ([r]_{I_1}, \cdots, [r]_{I_n})$ は環同型写像.

証明：n についての帰納法（$n = 1$ は明らかで，$n = 2$ はすぐ前でやった).

(1) $i = 1, \cdots, n-1$ について $x_i \in I_i, y_i \in I_n$ を $x_1 + y_1 = 1_R, \cdots, x_{n-1} + y_{n-1} \in 1_R$ と取る.

$$1_R - x_1 \cdots x_{n-1} = (x_1 + y_1) \cdots (x_{n-1} + y_{n-1}) - x_1 \cdots x_{n-1} \in I_n$$

なので，$J := I_1 \cdots I_{n-1} (= I_1 \cap \cdots \cap I_{n-1})$ とすると，$J + I_n = R$. よって $JI_n = J \cap I_n$.

(2) $R/JI_{n-1} \xrightarrow{\sim} (R/J) \times (R/I_n)$ から従う.

例（105 減算）：$R = \mathbb{Z}, I_1 = 3\mathbb{Z}, I_2 = 5\mathbb{Z}, I_3 = 7\mathbb{Z}$ とすると

$$\mathbb{Z}/105\mathbb{Z} \xrightarrow{\sim} (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z}) \times (\mathbb{Z}/7\mathbb{Z}), \quad [r]_{105\mathbb{Z}} \mapsto ([r]_{3\mathbb{Z}}, [r]_{5\mathbb{Z}}, [r]_{7\mathbb{Z}}).$$

これは整数 n の 3,5,7 の余りを知ることと，n の 105 の余りを知ることが同値であると言っている.

注意：$R = \mathbb{Z}[x], I = (2), J = (x)$ とすると，$I + J = (2, x) \subsetneq \mathbb{Z}[x]$ なので（つまり $f(x), g(x) \in \mathbb{Z}[x]$ をうまく選んで $1 = 2f(x) + xg(x)$ とは出来ない)，I と J は $\mathbb{Z}[x]$ のイデアルとしては互いに素ではない（「$\mathbb{Q}[x]$ のイデアルとしては」互いに素である).

注意：$A = (a_{ij})_{1 \leq i,j \leq n} \in \mathrm{M}_n(\mathbb{Z})$ について

$$|\det A| \leq \prod_{j=1}^{n} \sqrt{a_{1j}^2 + \cdots + a_{nj}^2}$$

なので，十分たくさんの素数 p について，$\mathbb{Z}/p\mathbb{Z}$ で $\det A$ を計算すると，CRT から $\det A \in \mathbb{Z}$ を復元できる．$\mathbb{Z}/p\mathbb{Z}$ は体なので（次回示す)，ガウス消去法を行列式の計算に用いることができる.