- 素イデアルと極大イデアル，素元と既約元の基本的性質を知る．
- PID は UFD であることを示し，整数における素因数分解の一意性を確認する．

定義：可換環 R のイデアル I について，以下のように定義する．

(1) I が素イデアル $\Leftrightarrow R/I$ が整域.
(2) I が極大イデアル $\Leftrightarrow R/I$ が体.

注意：極大イデアルは素イデアル（$\because$ 体は整域だから）．

注意：R が整域または体ならば，定義より $1_R \neq 0_R$ だった．よって，I が素イデアルまたは極大イデアルならば $I \subsetneq R$.

命題：可換環のイデアル $I \subsetneq R$ について，以下の 2 つは同値である．

(1) I は極大イデアル.
(2) イデアル $J \subseteq R$ が，$I \subsetneq J \subseteq R$ ならば，$J = R$.

証明：(2) ならば (1)：$R/I \ni [r]_I \neq 0_{R/I}$ について，$J := (r) + I$ は R のイデアルで，$r \notin I$ より $J = R$. よって $\exists x \in R, \exists i_0 \in I, rx + i_0 = 1_R$. つまり $[r]_I[x]_I = 1_{R/I}$.
(1) ならば (2)：対偶を示す．$I \subsetneq J \subsetneq R$ となるイデアル J について，$r \in J \setminus I$ を取る．$[r]_I \neq 0_{R/I}$ だが，$\forall x \in R, rx \in J$ より，$rx \equiv 1_R \pmod{J}$ となることはない（もしそうなら $1_R = J$ となり $J = R$ となる）．よって $[r]_I \neq 0_{R/I}$ は R/I で逆元を持たない.

注意：選択公理を仮定すると，零環でない可換環 R には少なくとも 1 つ極大イデアルが存在することが示せる（R がネーター環なら，選択公理は不要）．

例：$\mathbb{Z}$ のイデアルは (a) に限るのだった（$a \geq 0$）．以下より，$\mathbb{Z}$ の極大イデアルは，ちょうど (p) である（p は素数）ことが分かる：$(0) = \{0\}, (1) = \mathbb{Z}$ で $a, b \geq 2$ なら $(a) \subsetneq (b) \Leftrightarrow b < a$ かつ $b|a$.

命題：可換環のイデアル $I \subsetneq R$ について，以下の 2 つは同値である．

(1) I は素イデアル.
(2) $\forall a \in R, \forall b \in R, ab \in I \Rightarrow a \in I$ または $b \in I$.

証明：(2) ならば (1)：対偶を示す．R/I が整域でなければ，$\exists a \in R, \exists b \in R, [a]_I \neq 0_{R/I} \neq [b]_I, [ab]_I = 0_{R/I}$. つまり $a \notin I, b \notin I, ab \in I$.
(1) ならば (2)：対偶を示す．上の議論を逆にたどる．

注意：$a, b \in \mathbb{Z}_{\geq 1}$ で p が素数のとき，$p|ab$ ならば $p|a$ または $p|b$.

定義：可換環 R について，$\mathrm{Spec}(R) := \{\mathfrak{p} \subsetneq R \mid \mathfrak{p} \text{ は素イデアル }\}$.

例：$\mathrm{Spec}(\mathbb{Z}) = \{(0), (p) \mid p \text{ は素数 }\}$, $\mathrm{Spec}(\text{体}) = \{(0)\}$.

命題：可換環の環準同型写像 $f : A \to B$ について，$\forall \mathfrak{q} \in \mathrm{Spec}(B), f^{-1}(\mathfrak{q}) \in \mathrm{Spec}(A)$.

証明：合成 $A \xrightarrow{f} B \twoheadrightarrow B/\mathfrak{q}$ を $h : A \to B/\mathfrak{q}$ とすると，$\mathrm{Ker}\, h = f^{-1}(\mathfrak{q})$ である．よって準同型定理より $A/f^{-1}(\mathfrak{q})$ は $B/\mathfrak{q}$ の部分環と同型．$B/\mathfrak{q}$ は整域なので，$A/f^{-1}(\mathfrak{q})$ も整域である．

注意：イデアル $I \subseteq R$ について，

$$V(I) := \{\mathfrak{p} \in \mathrm{Spec}(R) \mid \mathfrak{p} \supseteq I\}$$

とすると，$\mathrm{Spec}(R)$ は $\{V(I) \mid I \subseteq R \text{ はイデアル }\}$ を閉集合系とする位相空間になることが確認できる（ザリスキ－位相）．上の命題は，環準同型 $f : A \to B$ について

$$\mathrm{Spec}(B) \to \mathrm{Spec}(A), \quad \mathfrak{q} \mapsto f^{-1}(\mathfrak{q})$$

が well-defined であることを言っているが，この写像がザリスキー位相に関して連続であることを示すこともできる．

注意：包含環準同型 $\mathbb{Z} \xhookrightarrow{\iota} \mathbb{Q}$ について，$\iota^{-1}((0)) = (0)$ は $\mathbb{Z}$ の極大イデアルでない素イデアル．

定義：整域 R のゼロでない元 $0 \neq a \in R$ が素元とは：$(a) \in \mathrm{Spec}(R)$.

例：$R = \mathbb{Z}$ のとき，a が素元 $\Leftrightarrow a = \pm p$（ここで p は素数）．

例：$\mathbb{Z}[x]$ で $a = 2, x$ はともに素元だが，$\mathbb{Q}[x]$ で $a = 2$ は $(2) = (1) = \mathbb{Q}[x]$ より素元ではない（$a = x$ は素元である）．

例：ガウス整数環 $\mathbb{Z}[i](= \{a + bi \mid a, b \in \mathbb{Z}\})$ において，2 は素元でない．実際，$2 = (1 + i)(1 - i)$ だが $1 \pm i \notin (2)$ が分かる．

定義：群とは，以下の 3 つの公理を満たす 3 つ組 $(G, \cdot, e)$ のことである．

(1) $\forall a \in G, \forall b \in G, \forall c \in G, (ab)c = a(bc)$.
(2) $\forall a \in G, ea = a = ae$.
(3) $\forall a \in G, \exists b \in G, ab = e = ba$

注意：$e' \in G$ が，$\forall a \in G, e'a = a = ae'$ ならば $e = e'$（環のときと同様）．(3) の b も一意的で，a^{-1} と書く．

記法：さらに (4) を満たすとき，アーベル群、可換群、加群などと呼ぶ（このとき，$\cdot$ を $+$ で，e を 0 または 0_G と書くことが多い）．

(4) $\forall a \in G, \forall b \in G, ab = ba$.

定義：可換環 R について，$(R^\times, \cdot, 1_R)$ は可換群になる（R の乗法群と言う）．ここで

$$R^\times := \{a \in R \mid \exists b \in R, ab = 1_R = ba\}.$$

例:$\mathbb{Z}^\times = \{\pm 1\}$, 体$^\times$ = 体 $\setminus \{0\}$, $\{0\}^\times = \{0\}$, $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$, $(\mathbb{Z}/12\mathbb{Z})^\times = \{[1]_{12\mathbb{Z}}, [5]_{12\mathbb{Z}}, [7]_{12\mathbb{Z}}, [11]_{12\mathbb{Z}}\}$.

記法：可換環 R の元 $a, b \in R$ について，$a|b \Leftrightarrow \exists c \in R, b = ac$（これは $(b) \subseteq (a)$ とも同値）.

定義：可換環 R の元 $a, b \in R$ について，a と b が同伴である（この講義では $a \approx b$ と書く）とは：
$c \in R^\times$, $b = ac$.

命題：$\approx$ は R 上の同値関係である．さらに R が整域ならば，以下はすべて同値：

(A) $a \approx b$.
(B) $a|b$ かつ $b|a$.
(C) $(a) = (b)$.

証明：容易.

注意：整域 R の零でない元 a が素元 $\Leftrightarrow (a) \in \mathrm{Spec}(R)$ だった．よって素元 a は $a \notin R^\times$ が分かる（$a \in R^\times$ と $(a) = R$ は同値）.

定義：整域 R の元 a が既約元とは

(1) $a \neq 0_R, a \notin R^\times$
(2) $\forall b \in R, \forall c \in R, a = bc \Rightarrow b \in R^\times$ または $c \in R^\times$.

命題：整域 R の素元 a は既約元である.

証明：(1) は OK．(2) を示すため，$a = bc$ とする．$bc \in (a)$ より，$b \in (a)$ または $c \in (a)$．$b \in (a)$ なら $\exists r \in R, b = ar$．つまり $a = arc$ となって $1 = rc$．つまり $c \in R^\times$．$c \in (a)$ の場合も同様.

例：$\mathbb{C}$ の部分環 $\mathbb{Z}[\sqrt{-5}](= \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\})$ において，$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ で，$2, 3, 1 \pm \sqrt{-5}$ のどれも既約元だが素元でないことが確認できる.

定義：整域 R が一意分解整域（UFD）とは：

$$\forall a \in R, a \neq 0_R, a \notin R^\times \Rightarrow \exists r \geq 1, \exists p_1, \cdots, \exists p_r \in R : \text{素元 s.t. } a = p_1 \cdots p_r.$$

定理：R を UFD, $0 \neq a \in R \setminus R^\times$ が,

$$a = p_1 \cdots p_r = q_1 \cdots q_s$$

のとき（ここで $r, s \geq 1$ で $p_1, \cdots, p_r, q_1, \cdots, q_s$ は素元），$r = s$ であり，さらに $q_1, \cdots, q_s$ を並び替えて $1 \leq \forall i \leq r, p_i \approx q_i$ とできる.

証明：$r \leq s$ としてよく，r についての帰納法で示す．

$r = 1$ のとき：$p_1 = q_1 \cdots q_s$ だが，$\exists i, p_1 | q_i$．並び替えて $i = 1$ としてよい．$\exists c \in R^\times, q_1 = p_1 c$ だが，q_1 は既約元でもあるので $c \in R^\times$．つまり $p_1 \approx q_1$．今，$1 = c^{-1} q_2 \cdots q_s$ となるので $s = 1$ でなければならない．

$r \geq 2$ のとき：$p_1 \cdots p_r = q_1 \cdots q_s$ で，上と同様に $\exists d \in R^\times, q_1 = p_1 d$ とできる．すると $p_2 \cdots p_r = d q_2 \cdots q_s$ なので，帰納法の仮定から $r - 1 = s - 1$ かつ $q_2, \cdots, q_s$ を並び替えて $q_2 \approx d p_2$ かつ $3 \leq \forall i \leq r, q_i \approx p_i$ とできる（$d \in R^\times$ より $(dq_2) = (q_2)$ なので dq_2 も素元である）．

命題：PID R において，$a \in R$ が素元であることと，既約元であることは同値である．

証明：既約元が素元であることを言えばよいので，a を既約元とする．$(0) = \{0\} \subsetneq (a) \subsetneq R = (1)$ を注意する．今 $(a) \subseteq (b)$（つまり $\exists c \in R, a = bc$）とする．$b \in R^\times$ ならば $(b) = R$ で，$c \in R^\times$ ならば $(a) = (b)$ となるので，(a) は極大イデアル（特に $(a) \in \operatorname{Spec} R$）．

補題：PID R において，イデアルの昇鎖律（ACC）が成り立つ：$I_1 \subseteq I_2 \subseteq \cdots$ が R のイデアルならば，$\exists N \geq 1, I_N = I_{N+1} = \cdots$．

証明：$J := \bigcup_{i \geq 1} I_i$ が R のイデアルであることは簡単に確認できる．$J = (j)$ とできるが，N を $I_N \ni j$ と取ると，$J = I_N = I_{N+1} = \cdots$ が分かる（実際，$I_N \supseteq J$ である）．

注意：上の議論と全く同様に，ネーター環において ACC が成り立つ（普通はこれをネーター環の定義にする）．

命題：PID R の元 a が，$a \neq 0_R, a \notin R^\times$ ならば，$\exists b \in R$：既約元, $b | a$.

証明：a が既約元なら OK（$b = a$ とする）．そうでないとき $\exists a_1 \notin R^\times, \exists a_2 \notin R^\times, a = a_1 a_2$ とできるが，どちらかが既約元なら OK．そうでなければ $\exists a_3 \notin R^\times, \exists a_4 \notin R^\times, a_1 = a_3 a_4$ と繰り返す．この過程で既約元が現れなければ $(a) \subsetneq (a_1) \subsetneq \cdots$ となって，ACC に反する．

定理：PID は UFD.

証明：PID R と $a \in R$ が $a \neq 0, a \notin R^\times$ が，既約元の積 $a = a_1 \cdots a_r$ になることを示せばよい．上の命題より $\exists a_1$：既約元, $a_1 \mid a$（そこで $a = a_1 c$ とする）．$c \notin R^\times$ なら，$\exists a_2 \in R$：既約元, $a_2 \mid c$（そこで $c = a_2 d$ とする）．この操作が終わらないと $(a) \subsetneq (c) \subsetneq (d) \subsetneq \cdots$ となって，ACC に反する．よって $\exists a_1$：既約元 , $\cdots$, $\exists a_r$：既約元, $\exists u \in R^\times$, $a = a_1 \cdots a_r u$ となる．

注意：$\operatorname{Spec}(\mathbb{Z}) = \{(0), (p) \mid p \text{ は素数 }\}$ と $\mathbb{Z}^\times = \{\pm 1\}$ より，整数における「素因数分解の一意性」が示された．

定理：R が UFD ならば，R 係数 1 変数多項式環 $R[X]$ も UFD.

注意：ここでは証明を行わないが，これによって $\mathbb{Z}[x_1, \cdots, x_n]$ や $k[x_1, \cdots, x_n]$ における素因数分解の一意性も分かる（ここで k は体）．