- 環とイデアルの定義を述べ，$\mathbb{Z}$ のイデアルを決定する．
- 応用として，$113 \cdot 22 + 355 \cdot (-7) = 1$ のように「互いに素な自然数 a, b に対し，うまく整数 x, y を選んで $ax + by = 1$ とできる」という初等整数論の命題を証明する．

定義：環とは，以下の 7 つの公理を満たす 5 つ組 $(R, +, \cdot, 0_R, 1_R)$ のことである．ここで R は集合，$+, \cdot : R \times R \to R$ は写像，$0_R, 1_R \in R$ である．

(1) $\forall a \in R, \forall b \in R, \forall c \in R, (a + b) + c = a + (b + c)$.
(2) $\forall a \in R, \forall b \in R, a + b = b + a$.
(3) $\forall a \in R, 0_R + a = a = a + 0_R$.
(4) $\forall a \in R, \exists b \in R, a + b = 0_R = b + a$.
(5) $\forall a \in R, \forall b \in R, \forall c \in R, (a \cdot b) \cdot c = a \cdot (b \cdot c)$.
(6) $\forall a \in R, 1_R \cdot a = a = a \cdot 1_R$.
(7) $\forall a \in R, \forall b \in R, \forall c \in R, a \cdot (b + c) = a \cdot b + a \cdot c, (a + b) \cdot c = a \cdot c + b \cdot c$.

例：$(\mathbb{Z}, +, \cdot, 0, 1)$ は環である．

例：$\mathrm{M}_n(\mathbb{C}) := \{n \times n \text{ 複素行列 }\}$ について，$(\mathrm{M}_n(\mathbb{C}), +, \cdot, O_n, E_n)$ は環である．

用語：環 $(R, +, \cdot, 0_R, 1_R)$ が以下を満たすとき，可換環という．

(8) $\forall a \in R, \forall b \in R, ab = ba$.

例：$\mathbb{Z}$ は可換環である．$\mathrm{M}_n(\mathbb{C})$ は $n \geq 2$ のとき可換環ではない．

例：$\mathbb{C}[x] := \{ \text{ 複素係数多項式 } \}$ について，$(\mathbb{C}[x], +, \cdot, 0, 1)$ は可換環．

用語：可換環 $(R, +, \cdot, 0_R, 1_R)$ が以下を満たすとき，体という．

(9) $0_R \neq 1_R$ かつ $\forall a \in R, a \neq 0_R \Rightarrow \exists b \in R, ab = 1_R = ba$.

例：$\mathbb{Z}$ は体ではない．$\mathbb{Q}, \mathbb{R}, \mathbb{C}$ は体である．

例：$\mathbb{H} := \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\}$ に

$$i^2 = j^2 = k^2 = -1, \quad ij = k = -ji, \quad jk = i = -kj, \quad ki = j = -ik$$

で「積を入れたもの」を 4 元数環という（しばしば 4 元数体とも呼ばれる）．

- $\mathbb{H}$ は環だが可換環ではない．
- $\mathbb{H}$ は (8) 以外の公理（(1) から (7) および (9)）を満たす（斜体）．

用語：可換環 $(R, +, \cdot, 0_R, 1_R)$ が以下を満たすとき，整域という．

(9') $0_R \neq 1_R$ かつ $\forall a \in R, \forall b \in R, a \neq 0_R, b \neq 0_R \Rightarrow ab \neq 0_R$.

例：$\mathbb{Z}$ は整域である．$\mathrm{M}_2(\mathbb{C})$ において $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}^2 = O_2$ だが，そもそも $\mathrm{M}_2(\mathbb{C})$ は可換環ではない．

命題：$(R, +, \cdot, 0_R, 1_R)$ を環とする．

(A) $x \in R$ が (3) を満たす（つまり $\forall a \in R, x + a = a = a + x$）ならば $x = 0_R$.
(B) $y \in R$ が (6) を満たす（つまり $\forall a \in R, y \cdot a = a = a \cdot y$）ならば $y = 1_R$.

証明：(A) $a = 0_R$ とすると，$x + 0_R = 0_R$．一方 (3) より $x + 0_R = x$ である．(B) も同様.

命題：R を環，$a \in R$ について，$b, b' \in R$ が以下を満たすならば $b = b'$.

$$a + b = 0_R = b + a, \quad a + b' = 0_R = b' + a$$

証明：$(b' + a) + b = b' + (a + b)$ だが，「左辺 $= b$」と「右辺 $= b'$」を導くことができる．

記法：すぐ上の命題より (4) の b は一意的である．これを $-a$ と書く（注意：$-(-a) = a$ である）.

命題：R を環とすると，任意の $a \in R$ について，$(-1_R) \cdot a = -a$ かつ $0_R \cdot a = 0_R$.

証明：$0_R = 0_R + 0_R$ より，$0_R \cdot a = 0_R \cdot a + 0_R \cdot a$．両辺に $-(0_R \cdot a)$ を加えると $0_R = 0_R \cdot a$ を導くことができる．$(-1_R) \cdot a = -a$ を言うには，$a + (-1_R) \cdot a = 0_R$ を言えばよいが

$$a + (-1_R) \cdot a = 1_R \cdot a + (-1_R) \cdot a = (1_R + (-1_R)) \cdot a = 0_R \cdot a = 0_R.$$

系：R を環とすると，$(-1_R) \cdot (-1_R) = 1_R$.

証明：すぐ上の命題より，左辺 $= -(-1_R) = 1_R$.

注意：以下，このような常識的な変形は断りなく用いる．例えば，$ab = 1_R = ba$ となる b を a^{-1} とか $\frac{1}{a}$ と書く，などである．a^{-1} の一意性や，$(a^{-1})^{-1} = a$ についても同様である．

命題：有限整域は体である．

証明：R が整域のとき，$R \ni a \neq 0_R$ について，写像

$$f_a : R \to R, x \mapsto ax$$

は単射である（実際，$ax = ax'$ ならば $a(x - x') = 0_R$ だが，R は整域なので $x - x' = 0$．よって $x = x'$ である）.

一般に有限集合 X について，単射 $g : X \to X$ は全射でもあることに注意すると，R が有限集合であれば f_a は全射である．つまり $\exists b \in R, f_a(b) = 1_R$.

注意：「有限斜体は体」であることも知られている（Wedderburn の定理）.

定義：可換環 R の部分集合 $I \subseteq R$ がイデアルとは，以下の 3 条件をみたすことである．

(I1) $I \neq \emptyset$.
(I2) $\forall x \in I, \forall y \in I, x + y \in I$.
(I3) $\forall a \in R, \forall x \in I, ax \in I$.

例：$R = \mathbb{Z}$ において，$I = 2\mathbb{Z} = \{2x \mid x \in \mathbb{Z}\}(=\{\text{ 偶数 }\})$ は R のイデアル．一方，$I' = \{\text{ 奇数 }\}$ は R のイデアルではない．

注意：イデアルの定義で，(I1),(I2),(I3) を (I1'),(I2),(I3) に変えても同じ．

(I1') $0_R \in I$

証明：(I1),(I2),(I3)⇒ (I1') を言えばよい：$i_0 \in I \neq \emptyset$ を取る．このとき $0_R \cdot i = 0_R \in I$.

例：$I = \{0\}$ および $I = R$ は R のイデアル．

注意：イデアル $I \subseteq R$ について，$I = R \Leftrightarrow 1_R \in I$.

証明：$\Rightarrow$ は明らか．$\Leftarrow$ を言うには，$I \supseteq R$ を言えばよい：任意の $a \in R$ について，$a \cdot 1_R = a \in I$.

定理：$\mathbb{Z}$ のイデアル I について，$\exists! d \geq 0, I = d\mathbb{Z}(= \{dx \mid x \in \mathbb{Z}\} = \{d \text{ の倍数 }\})$.

証明：d の一意性は明らかである．$I = \{0\}$ ならば $d = 0$ なので，$I \supsetneq \{0\}$ とする．

> 主張：$\Sigma = \{i \in I \mid i > 0\}$ とすると $\Sigma \neq \emptyset$.
> 実際 $0 \neq i_0 \in I$ が取れるが，$(-1)i_0 \in I$ でもあるのだった（主張の証明終わり）．

$d = \min \Sigma$ について $I = d\mathbb{Z}$ が分かる．実際 $d \in I$ なので $d\mathbb{Z} \subseteq I$ である．逆に，$i \in I$ を d で「割り算」すると

$$\exists q \in \mathbb{Z}, \exists r \in \mathbb{Z}, 0 \leq r < d, i = dq + r$$

となる商 q と余り q が取れるが，$r = i - dq \in I$ なので，d の最小性より $r = 0$.

応用：$a, b \in \mathbb{Z}_{\geq 1}$ が互いに素なとき

$$\exists x \in \mathbb{Z}, \exists y \in \mathbb{Z}, ax + by = 1.$$

証明：$I := \{ax + by \mid x, y \in \mathbb{Z}\}(\supsetneq \{0\})$ は $\mathbb{Z}$ のイデアルであることが確認できる．上記定理より $\exists! d \geq 1, I = d\mathbb{Z}$ である．d は $a, b \in I$ を割り切るので，$d = 1$ でなければならない．よって $1 \in I$.

例：$113 \cdot 22 + 355 \cdot (-7) = 1$.