情報代数学

土谷 昭善 (akiyoshi@is.sci.toho-u.ac.jp)

目 次

1　環の定義

このテキストでは，自然数は 1 以上の整数とする（すなわち，0 は含まない）．また $\mathbb{N}, \mathbb{Z}, \mathbb{Z}_{\geq 0}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ をそれぞれ自然数全体，整数全体，非負整数全体，有理数全体，実数全体，複素数全体の集合とする．

集合とその集合上に定義された演算との組を代数系と呼ぶ．情報数理 C では（アーベル）群と呼ばれる代数系を学習した．簡単に言えば，（アーベル）群は「足し算と引き算ができる集合」のことである．ただし，引き算は「逆元の加法」として定義されるため，群の基本的な演算は実質的には加法の 1 つのみである．

本講義では，この加法に加えて掛け算を備えた集合，すなわち「足し算と引き算と掛け算」ができる集合である**環**を考える．

1.1　群の復習

まず半群，モノイド，群，アーベル群の定義を復習しよう．

定義 1.1.1. G を空ではない集合，$\circ$ を G 上の演算とする．次の 4 つの性質を考える：

(G1)（結合律）任意の a, b, c に対し，$(a \circ b) \circ c = a \circ (b \circ c)$ が成り立つ．

(G2)（単位元の存在）ある元 $e \in G$ が存在して，任意の $a \in G$ に対して $a \circ e = e \circ a = a$ を満たすものが存在する．このとき e を G の $\circ$ に関する**単位元**という．

(G3)（逆元の存在）任意の $a \in G$ に対して，$a \circ h = h \circ a = e$ を満たす $h \in G$ が存在する．このとき，h を a の $\circ$ に関する**逆元**という．また a の逆元を a^{-1} と書く．

(G4)（交換律）任意の $a, b \in G$ に対し $a \circ b = b \circ a$ が成り立つ．

- $(G, \circ)$ が**半群** (semigroup) であるとは (G1) を満たすときをいう．
- $(G, \circ)$ が**モノイド** (monoid) であるとは (G1) と (G2) を満たすときをいう．
- $(G, \circ)$ が**群** (group) であるとは (G1) と (G2) と (G3) を満たすときをいう．
- $(G, \circ)$ が**アーベル群** (abelian group) または**加法群** (additive group) であるとは (G1) と (G2) と (G3) と (G4) を満たすときをいう．

演算が文脈から明らかなときは $(G, \circ)$ を単に G と書いて半群，モノイド，群，アーベル群とみなす．

例えば，$(\mathbb{N}, +)$ は半群であるがモノイドではない．$(\mathbb{Z}_{\geq 0}, +)$ はモノイドであるが群ではない．$(\mathbb{Z}, +)$ は（アーベル）群である．この 3 つの違いはなんであろうか．はじめに説明した通り，（アーベル）群は「足し算」と「引き算」ができる集合である．$\mathbb{N}$ や $\mathbb{Z}_{\geq 0}$ では $3 - 4 = -1$ のように，引き算をすると集合からはみ出る可能性がある．この意味で，$\mathbb{N}$ や $\mathbb{Z}_{\geq 0}$ では引き算ができない．しかし，$\mathbb{Z}$ ではこの問題が解消される．これが $\mathbb{Z}$ だけが群になる理由である．群の定義に戻ると「引き算ができる」というのは条件 (G3) に他ならない．

補足 1.1.2. (1) 群の演算は基本的に「積」または「乗法」と呼ぶ．また $a \circ b$ を単に ab と書くこともある．さらに $n \in \mathbb{Z}$ に対し

$$a^n = \begin{cases} \underbrace{a \circ a \circ \cdots \circ a}_{n \text{ 個}} & (n > 0) \\ e & (n = 0) \\ \underbrace{a^{-1} \circ a^{-1} \circ \cdots \circ a^{-1}}_{-n \text{ 個}} & (n < 0) \end{cases}$$

と表記する．このとき，任意の整数 n, m に対し

$$a^n \circ a^m = a^{n+m}$$
$$a^{nm} = (a^n)^m$$

が成り立つことは簡単に証明できる．ただし，

$$(a \circ b)^n = a^n \circ b^n$$

は一般に成り立たないことに注意する（$a \circ b = b \circ a$ とは限らないから）．

(2) $(G, \circ)$ がアーベル群のとき，演算の記号は $+$ を使うことが多い．この場合，演算は「和」または「加法」と呼ぶ．また単位元は 0 と表し，$a \in G$ に対する逆元は $-a$ と表記する．さらに，演算「$-$」を

$$a - b := a + (-b)$$

と定義することで,「引き算」が定義できる．引き算は (G3) が成り立てば定義できるが,「引き算」というときは基本アーベル群，つまり (G4) まで仮定する．

(3) 「引き算」を定義することのメリットは方程式の移項ができることである．つまり，$(G, +)$ がアーベル群であるとき，任意の $a, b, c \in G$ に対し，$a + c = b$ ならば $a = b - c$ が成り立つ．

単位元に関する重要な性質を復習する．

命題 1.1.3. (1) $(G, \circ)$ を単位元が e であるモノイドとする．このとき，G の単位元は一意的である．

(2) $(G, \circ)$ を群とする．$a, b \in G$ が $a \circ b = e$ を満たすとする．このとき，$b = a^{-1}$ かつ $a = b^{-1}$ である．特に，任意の $a \in G$ に対し，逆元は一意的である．

Proof. (1) $x \in G$ が単位元の条件を満たすとする．このとき，

$$x = x \circ e = e$$

となるので，単位元は一意的である．

(2) $a \circ b = e$ の両辺の左から a^{-1} を掛けると $b = a^{-1}$ が従い，右から b^{-1} を掛けると $a = b^{-1}$ が従う． □

1.2 環の定義

アーベル群は「足し算」と「引き算」ができる集合であった．さらに「掛け算」ができる集合が環である．それでは環の正確な定義を紹介する．

定義 1.2.1. R を空でない集合，$+_R$ と $\cdot_R$ を R 上の演算とする．このとき，$(R, +_R, \cdot_R)$ が**環** (ring) であるとは，以下の条件を満たすときにいう：

(R1) $(R, +_R)$ はアーベル群である．

(R2) $(R, \cdot_R)$ はモノイドである．

(R3) （分配律）任意の $a, b, c \in R$ に対し，

$$a \cdot_R (b +_R c) = (a \cdot_R b) +_R (a \cdot_R c)$$
$$(a +_R b) \cdot_R c = (a \cdot_R c) +_R (b \cdot_R c)$$

が成り立つ．

> 演算が文脈から明らかなときは，$(R, +_R, \cdot_R)$ を単に R と書いて環とみなす．また演算も単に $+$ や $\cdot$ と書く．

例えば，$(\mathbb{Z}, +, \cdot)$ は環である．これを**整数環**という．一方，$(\mathbb{N}, +, \cdot)$ や $(\mathbb{Z}_{\geq 0}, +, \cdot)$ は環ではない．

補足 1.2.2. 環 $(R, +, \cdot)$ に対し，$+$ と $\cdot$ はそれぞれ R の**加法**と**乗法**という．命題 1.1.3 からそれぞれの演算に関する単位元が一意的に存在する．このとき，加法 $+$ に関する単位元を 0_R と表記し，これを R の**零元**という．また乗法 $\cdot$ に関する単位元を 1_R と表記し，これを R の**単位元**という．考えている環が文脈から明らかなときは単に 0 や 1 と表記する．

それではもう少し環の例を見ていく．

例 1.2.3. $R = \{a\}$ とする．このとき，加法 $+$ と乗法 $\cdot$ は

$$a + a = a$$
$$a \cdot a = a$$

と一意的に決まる．すると $(R, +)$ と $(R, \cdot)$ はともに（自明な）アーベル群である．つまり (R1) と (R2) を満たす．さらに，

$$a \cdot (a + a) = a \cdot a = a = a + a = (a \cdot a) + (a \cdot a)$$
$$(a + a) \cdot a = a \cdot a = a = a + a = (a \cdot a) + (a \cdot a)$$

であるので (R3) が満たされる．よって，$(R, +, \cdot)$ は環である．この環を**零環**といい，しばしば 0 と略記する．以降，環 $R \neq 0$ と表記すると R は零環ではない環を意味する．

例 1.2.4. x を変数とする整数係数の（1 変数）多項式全体の集合を $\mathbb{Z}[x]$ とする．つまり，

$$\mathbb{Z}[x] = \left\{ \sum_{i=0}^{d} a_i x^i : d \in \mathbb{Z}_{\geq 0}, a_0, \ldots, a_d \in \mathbb{Z} \right\}$$

である．このとき，通常の多項式の和と積により $\mathbb{Z}[x]$ は環となる．ここで零元は零多項式，単位元は 1 である．これを $\mathbb{Z}$ 上の（1 変数）**多項式環**という．$\mathbb{Z}[x]$ は $\mathbb{Z}$ に並んで重要な環の 1 つである．同様に，$x_1, \ldots, x_n$ を変数とする整数係数の n 変数多項式全体の集合を $\mathbb{Z}[x_1, \ldots, x_n]$ とすると，これも通常の多項式の和と積により環となる．これを $\mathbb{Z}$ 上の n 変数多項式環という．実は $\mathbb{Z}$ だけでなく，一般の可換環 R に対して多項式環を定義することができる．これは後の節で詳しく見る．

例 1.2.5. $R = \mathbb{R} \times \mathbb{R}$ とし，R に加法 $+_R$ と乗法 $\cdot_R$ を

$$(a, b) +_R (c, d) = (a + c, b + d)$$
$$(a, b) \cdot_R (c, d) = (a \cdot c, a \cdot d + b \cdot c)$$

で定義する．ただし，$+$ や $\cdot$ は $\mathbb{R}$ の通常の加法と乗法である．$(R, +_R)$ が $(0, 0)$ を単位元とするアーベル群となることは容易にわかる．つまり，(R1) を満たす．次に $(R, \cdot_R)$ を考える．これが結合律を満たすことの確認は演習問題とする．任意の $(a, b) \in R$ に対し，

$$(a, b) \cdot_R (1, 0) = (a \cdot 1, a \cdot 0 + b \cdot 1) = (a, b)$$
$$(1, 0) \cdot_R (a, b) = (1 \cdot a, 1 \cdot b + 0 \cdot a) = (a, b)$$

であるので，$(R, \cdot_R)$ は $(1, 0)$ を単位元とするモノイドである．最後に分配律を確認する．任意の $(a, b), (c, d), (e, f) \in R$ に対し，

$$\begin{aligned}(a, b) \cdot_R ((c, d) +_R (e, f)) &= (a, b) \cdot_R (c + e, d + f) = (a(c + e), a(d + f) + b(c + e)) \\ &= (ac + ae, (ad + bc) + (af + be)) = (ac, ad + bc) +_R (ae, af + be) \\ &= ((a, b) \cdot_R (c, d)) +_R ((a, b) \cdot_R (e, f))\end{aligned}$$

である．同様に，

$$((a,b)+_R(c,d))\cdot_R(e,f)=((a,b)\cdot_R(e,f))+_R((c,d)\cdot_R(e,f))$$

も示せるので，(R4) を満たす．以上から，$(R,+_R,\cdot_R)$ は零元が $(0,0)$，単位元が $(1,0)$ となる環である．

環の定義では加法に関しては可換性を仮定していたが，乗法に関しては仮定していない．実際，乗法の可換性を満たさない環がある．

定義 1.2.6. R を環とする．R が**可換環** (commutative ring) であるとは，条件

(R4)（交換律）任意の $a,b\in R$ に対し，$ab=ba$ が成り立つ

を満たすときにいう．可換環ではない環を**非可換環** (noncommutative ring) という．

例えば，$\mathbb{Z}$ や $\mathbb{Z}[x]$ は可換環である．非可換環の例を見る．

例 1.2.7. 整数を要素とする 2 次正方行列全体の集合を $M_2(\mathbb{Z})$ とする．つまり，

$$M_2(\mathbb{Z})=\left\{\begin{pmatrix}a & b\\ c & d\end{pmatrix}:a,b,c,d\in\mathbb{Z}\right\}$$

である．このとき，通常の行列の和と積により $M_2(\mathbb{Z})$ は環となる．ここで零元と単位元はそれぞれ

$$\begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix},\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$$

である．これを $\mathbb{Z}$ 上の階数 2 の**行列環**という．このとき，

$$\begin{pmatrix}1 & 1\\ 0 & 0\end{pmatrix}\begin{pmatrix}1 & 0\\ 1 & 0\end{pmatrix}=\begin{pmatrix}2 & 0\\ 0 & 0\end{pmatrix}\neq\begin{pmatrix}1 & 1\\ 1 & 1\end{pmatrix}=\begin{pmatrix}1 & 0\\ 1 & 0\end{pmatrix}\begin{pmatrix}1 & 1\\ 0 & 0\end{pmatrix}$$

より (R4) は満たされない．よって $M_2(\mathbb{Z})$ は非可換環である．同様に，整数を要素とする n 次正方行列全体からなる集合 $M_n(\mathbb{Z})$ も通常の行列の和と積により環となるが，$n\geq 2$ であれば非可換環となる．より一般に環 R の元を要素とする階数 n の行列環 $M_n(R)$ が定義できる．このとき，$M_n(R)$ が可換環となることと $n=1$ かつ R が可換環となることは同値である．

群の直積は自然な演算により再び群になった．環の直積も同様に自然な演算により環になる．R と S を環とする．今，直積 $R\times S$ 上の演算 $+$ と $\cdot$ を以下で定義する．

$$+:(R\times S)\times(R\times S)\to R\times S;((a_1,b_1),(a_2,b_2))\mapsto(a_1+_Ra_2,b_1+_Sb_2),$$
$$\cdot:(R\times S)\times(R\times S)\to R\times S;((a_1,b_1),(a_2,b_2))\mapsto(a_1\cdot_Ra_2,b_1\cdot_Sb_2).$$

命題 1.2.8. $(R\times S,+,\cdot)$ は加法の単位元を $(0_R,0_S)$，乗法の単位元を $(1_R,1_S)$ とする環である．

Proof. 群の直積と同様に各演算が成分ごとに定義されているため従う． □

1.3 環の性質

整数環の性質を思い出す．任意の整数 a に対し，

$$a\cdot 0=0\cdot a=0$$

が成り立つ．つまり，零元との積は常に零元になるという性質である．これは一般の環の場合も成り立つ．

命題 1.3.1. R を環とする．このとき，任意の $a \in R$ に対し，

$$a \cdot 0 = 0 \cdot a = 0$$

である．

Proof. 零元の性質と分配律より

$$a \cdot 0 = a \cdot (0 + 0) = (a \cdot 0) + (a \cdot 0)$$

が成り立つ．両辺に加法に関する逆元 $-(a \cdot 0)$ を加えることで，$a \cdot 0 = 0$ が得られる．同様に，$0 \cdot a = 0$ も示せる． □

次に符号の積を考える．整数環では「マイナス」×「マイナス」=「プラス」,「マイナス」×「プラス」=「マイナス」のような符号の計算が可能だった．一般の環でも同様の計算ができる．

命題 1.3.2. R を環とする．任意の $a, b \in R$ に対し，

(1) $(-a) \cdot b = a \cdot (-b) = -(a \cdot b)$

(2) $(-a) \cdot (-b) = a \cdot b$

が成り立つ．

Proof. (1) まず $(-a) \cdot b = -(a \cdot b)$ を示す．この式を日本語で説明すると「$(-a) \cdot b$ は $a \cdot b$ の加法に関する逆元である」ということである．さらに言い直すと「$(-a) \cdot b$ と $a \cdot b$ の和は 0 である」ということになる．これは

$$((-a) \cdot b) + (a \cdot b) = ((-a) + a) \cdot b = 0 \cdot b = 0$$

より成り立つ．$a \cdot (-b) = -(a \cdot b)$ も同様に示せる．

(2) (1) の結果を用いて次のように示せる：

$$\begin{aligned} a \cdot b &= a \cdot b + 0 \\ &= a \cdot b + (-a) \cdot 0 \\ &= a \cdot b + (-a) \cdot (b + (-b)) \\ &= a \cdot b + (-a \cdot b + (-a) \cdot (-b)) \\ &= (a \cdot b - a \cdot b) + (-a) \cdot (-b) \\ &= 0 + (-a) \cdot (-b) = (-a) \cdot (-b) \end{aligned}$$

□

最後に零環の特徴を紹介する．R が零環のとき，零元と単位元は一致する．つまり，$0 = 1$ となっている．実は $0 = 1$ となるのは零環の場合に限る．

命題 1.3.3. R を環とする．このとき，R が零環であることと，$0 = 1$ であることは同値である．

Proof. $\Rightarrow$ は明らかなので，$\Leftarrow$ を示す．任意の元 $a \in R$ をとる．$0 = 1$ の両辺の左から a をかけると

$$0 = a \cdot 0 = a \cdot 1 = a$$

が成り立つ．これより $R = \{0\}$ となる．よって R は零環である． □

1.4 部分環

群論において，ある群の部分構造として「部分群」を学んだ．環においても，同様に「部分環」を定義する．

$(R,+,\cdot)$ を環とする．R の空でない部分集合 S に対して，写像

$$+|_S : S\times S\to R,\quad (a,b)\mapsto a+b,\qquad \cdot|_S : S\times S\to R,\quad (a,b)\mapsto a\cdot b$$

を定義する．つまり，R の演算を S 上に制限して考える．このとき，$a+b$ や $a\cdot b$ が S に含まれない可能性があるので，$+|_S, \cdot|_S$ が S 上の演算とは限らない．もし $+|_S$ と $\cdot|_S$ が S 上の演算になる，つまり $+|_S : S\times S\to S$ と $\cdot|_S : S\times S\to S$ として定義でき，$(S,+|_S,\cdot|_S)$ が環となり，かつ $1_R\in S$ のとき，S を R の**部分環**（subring）という．自分自身はいつでも部分環である．

まず，部分環 S の零元や単位元，逆元が R から引き継がれることを見る．

補題 1.4.1. R を環とし，$0\neq S$ を R の部分環とする．このとき，

(1) $0_S=0_R$，特に $0_R\in S$ である．

(2) 任意の $a\in S$ に対し，a の R での加法に関する逆元 $-a$ は $-a\in S$ を満たし，これは a の S での加法に関する逆元である．

(3) $1_S=1_R$ である．

Proof. (1) R において

$$0_R+0_S=0_S$$

が成り立つ．0_S の R における加法の逆元を x とすると

$$0_S=0_R+0_S=(x+0_S)+0_S=x+(0_S+0_S)=x+(0_S+_S\,0_S)=x+0_S=0_R$$

となる．特に，$0_R\in S$ である．

(2) a の S の中での逆元を a' とする．このとき，(1) から

$$0_R=a+|_S a'=a+a'$$

である．すると R における加法の逆元の一意性より $-a=a'$ となる．

(3) S の中で，1_S も 1_R も単位元の条件を満たすので，単位元の一意性から $1_S=1_R$ である． □

この補題を使うことで以下の命題が示せる．この命題を部分環の定義と思ってもよい．

命題 1.4.2. $(R,+,\cdot)$ を環とする．部分集合 $\emptyset\neq S\subset R$ が R の部分環である必要十分条件は，次の条件をすべて満たすことである：

(S1) 任意の $a,b\in S$ に対して $a+(-b)\in S$（加法について閉じており，逆元も含む）．

(S2) 任意の $a,b\in S$ に対して $a\cdot b\in S$（乗法について閉じている）．

(S3) $1_R\in S$（単位元を含む）．

Proof. （⇒）$(S,+|_S,\cdot_S)$ を R の部分環とする．このとき，$+|_S$ は S 上の演算であり，補題 1.4.1 の (2) から $-b\in S$ かつ $a+(-b)\in S$ である．よって (S1) が満たされる．また $\cdot|_S$ は S 上の演算なので，(S2) が満たされる．さらに，(S3) は部分環の定義から従う．

（⇐）(S1)，(S2)，(S3) を満たすとする．$+|_S$ の結合律や可換律，$\cdot|_S$ の結合律，そして分配律は元を制限しているだけなので $+$ と $\cdot$ から自動で成り立つ．(S1) より，任意の $a\in S$ に対し，$a+(-a)=0_R\in S$

が成り立ち，さらに $0_R + (-a) = -a \in S$ となる．よって，任意の $a, b \in S$ に対し $a +|_S b \in S$ であり，$+|_S$ は S 上の演算として定義でき，特に $(S, +_S)$ はアーベル群となる．(S2) より，$\cdot|_S$ は S 上の演算として定義でき，(S3) より $1_R \in S$ なので，$(S, \cdot|_S)$ はモノイドである．

以上より，$(S, +|_S, \cdot|_S)$ は環かつ $1_R \in S$ となるので S は R の部分環である． □

以降，S が環 $(R, +, \cdot)$ の部分環のとき，S 上の演算 $+|_S$ と $\cdot|_S$ を単に $+$ と $\cdot$ で書く．

例 1.4.3. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ は明らかに $\mathbb{C}$ の部分環である．より一般に，

$$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$$

はそれぞれ包含関係に対して部分環となる．

例 1.4.4. 偶数全体の集合を $E = \{2x : x \in \mathbb{Z}\}$ と書くと，これは部分環ではない．実際，(S1) と (S2) は成り立つが，$1 \notin E$ なので (S3) を満たさない．

さらに，奇数全体の集合を $O = \{2x + 1 : x \in \mathbb{Z}\}$ と書くと，これも部分環ではない．実際，(S2) と (S3) は成り立つが，$1 + (-1) = 0 \notin O$ なので (S1) を満たさない．

実は $\mathbb{Z}$ は $\mathbb{Z}$ 以外に部分環を持たない．実際，S を $\mathbb{Z}$ の部分環とすると，(S3) より $1 \in S$ であり，(S1) を繰り返し使うと $S = \mathbb{Z}$ がわかる．

例 1.4.5. $\mathbb{C}$ の部分集合 $\mathbb{Z}[\sqrt{-1}]$ を

$$\mathbb{Z}[\sqrt{-1}] = \{a + b\sqrt{-1} : a, b \in \mathbb{Z}\}$$

で定義する．このとき，$\mathbb{Z}[\sqrt{-1}]$ は $\mathbb{C}$ の部分環である．実際，任意の $a+b\sqrt{-1}, c+d\sqrt{-1} \in \mathbb{Z}[\sqrt{-1}] (a, b, c, d \in \mathbb{Z})$ に対し，

$$(a + b\sqrt{-1}) + (-(c + d\sqrt{-1})) = (a - c) + (b - d)\sqrt{-1}$$
$$(a + b\sqrt{-1}) \cdot (c + d\sqrt{-1}) = (ac - bd) + (ad + bc)\sqrt{-1}$$

であり，$a-c, b-d, ac-bd, ad+bc \in \mathbb{Z}$ となるので，(S1) と (S2) が満たされる．また $1 = 1+0\sqrt{-1} \in \mathbb{Z}[\sqrt{-1}]$ なので (S3) も満たされる．よって $\mathbb{Z}[\sqrt{-1}]$ は $\mathbb{C}$ の部分環である．この環 $\mathbb{Z}[\sqrt{-1}]$ を**ガウス整数環**と呼び，その元 $a + b\sqrt{-1}, a, b \in \mathbb{Z}$ を**ガウス整数**という．これは整数の概念を複素数で拡張したものである．

1.5 整域と体

次に環の中でもより良い構造を持つ環を定義する．以降は基本可換環のみを考えていく．整数環 $\mathbb{Z}$ の場合，$ab = 0$ ならいつでも $a = 0$ または $b = 0$ が成り立つ．しかし，一般の環ではこの性質が成り立たない場合がある．つまり，$ab = 0$ であるが，$a = 0$ でも $b = 0$ でもないことが起こり得るのである．

定義 1.5.1. $R \neq 0$ を可換環とする．元 $a \neq 0$ が**零因子** (zero divisor) であるとは，$ax = 0$ を満たす元 $x \in R \setminus \{0\}$ が存在するときにいう．

例 1.5.2. 例 1.2.5 で定義した環 $R = \mathbb{R} \times \mathbb{R}$ を考える．ここで R の演算は

$$(a, b) + (c, d) = (a + c, b + d)$$
$$(a, b) \cdot (c, d) = (a \cdot c, a \cdot d + b \cdot c)$$

で定義される．この環の零元は $(0, 0)$ である．このとき，

$$(0, 1) \cdot (0, 1) = (0 \cdot 0, 0 \cdot 1 +_R 1 \cdot 0) = (0, 0)$$

が成り立つので，$(0, 1)$ は R の零因子であることがわかる．

零因子を持たない環は良い性質を持つことがあるので，そのような環に名前を付けよう．

定義 1.5.3. 可換環 $R \neq 0$ が**整域** (integral domain) であるとは，零因子を持たない，つまり任意の $a, b \in R$ に対し，$ab = 0$ ならば $a = 0$ または $b = 0$ が成り立つときにいう．対偶を考えると，$a \neq 0$ かつ $b \neq 0$ ならばいつでも $ab \neq 0$ となることと同値である．

整数環は整域である．一方，先ほどの例 1.5.2 の R は零因子を持ったので，整域ではない．整域の例をもう 1 つ見る．

例 1.5.4. ガウス整数環 $\mathbb{Z}[\sqrt{-1}]$ は整域である．実際，$x = a + b\sqrt{-1}, y = c + d\sqrt{-1} \in \mathbb{Z}[\sqrt{-1}]$ に対し，$xy = 0$ が成り立つとする．ただし，$a, b, c, d \in \mathbb{Z}$ である．$x = 0$ または $y = 0$ を示す．そのために，$x \neq 0$ としてよい．

$$xy = (ac - bd) + (ad + bc)\sqrt{-1} = 0$$

なので，$ac - bd = 0$ かつ $ad + bc = 0$ が成り立つ．1 つ目の式の両辺に a をかけて，$ad = -bc$ を代入すると

$$a(ac - bd) = a^2c - abd = a^2c + b^2c = c(a^2 + b^2) = 0$$

となる．ここで $x \neq 0$ より $a^2 + b^2 \neq 0$ が成り立つので $c = 0$ が従う．すると $bd = ad = 0$ が成り立つ．$d \neq 0$ ならば $a = b = 0$ となり，これは $x \neq 0$ に矛盾する．よって $d = 0$ である．以上より，$y = 0$ が従うので，$\mathbb{Z}[\sqrt{-1}]$ は整域である．

整域に関する重要な性質を一つ証明する．

命題 1.5.5 (簡約律)**.** R を整域とし $a, b \in R$ と $c \in R \setminus \{0\}$ をとる．このとき，$ac = bc$ ならば $a = b$ が成り立つ．

Proof. $ac = bc$ から移項と分配則により $(a - b)c = 0$ が成り立つ．すると R が整域なので $a - b = 0$ または $c = 0$ が成り立つ．しかし，$c \neq 0$ なので，$a - b = 0$，つまり $a = b$ が従う． □

この命題の性質（簡約律）は「割り算」ができれば直ちに成り立つが，一般に整域では「割り算」を定義することができない．例えば，整数環において，$4 \div 3 \notin \mathbb{Z}$ である．ここから「割り算」の定義について考える.「引き算」の定義を思い出すと，これは加法に関する逆元を足すことで定義されていた．同様に,「割り算」は乗法に関する逆元を掛けることで定義されると考えられるが，環の定義では，乗法に関する逆元の存在を保証していない．実際，零元は乗法に関する逆元を必ず持たない．これは環 $R \neq 0$ と任意の $a \in R$ に対して，

$$0 \cdot a = a \cdot 0 = 0 \neq 1$$

が成り立つからである．そこで「割り算」を定義する際は零元を除いて考える．

定義 1.5.6. $R \neq 0$ を可換環とする．

(1) $a \in R$ に対し，$ab = 1$ を満たす $b \in R$ が存在するとき，a を R の**単元** (unit) または**可逆元** (invertible element) という．このとき，b を a の乗法に関する**逆元**といい，a^{-1} と書く．さらに R の単元全体の集合を $R^\times$ で表す．

(2) 0 以外の全ての元が単元，つまり $R^\times = R \setminus \{0\}$ となる環を**体** (field) という．

補足 1.5.7. R が体であるとき，$a \in R$ と $b \in R \setminus \{0\}$ に対し，

$$a \div b := a \cdot b^{-1}$$

と書くことで，割り算は定義される．つまり，体とは「足し算・引き算・掛け算・割り算」の四則演算が定義される集合ということになる．

有理数全体の集合 $\mathbb{Q}$，実数全体の集合 $\mathbb{R}$，複素数の集合 $\mathbb{C}$ は通常の加法と乗法に関して体となる．これらはそれぞれ**有理数体**，**実数体**，**複素数体**と呼ばれる．

例 1.5.8. 整数環 $\mathbb{Z}$ を考える．このとき，$\mathbb{Z}^\times = \{\pm 1\}$ であるので，$\mathbb{Z}^\times \neq \mathbb{Z} \setminus \{0\}$ となる．よって $\mathbb{Z}$ は体ではない．

さてここまでで，整域と体という 2 つの特別な可換環を考えたが，実はこの 2 つには次のような関係がある．

定理 1.5.9. 体は整域である．

Proof. R を体とする．任意の $a, b \in R$ で $ab = 0$ を満たすものをとる．このとき，$a = 0$ または $b = 0$ となることを示せばよい．$a \neq 0$ と仮定してよい．R は体であるので，$a \in R \setminus \{0\} = R^\times$，つまり，$a$ は単元である．よって，$a^{-1} \in R$ が存在する．$ab = 0$ の両辺に a^{-1} をかけると $b = 0$ が従う．以上より，R が整域であることがわかった． □

整数環は整域だが体ではなかった．つまり，この定理の逆は一般には成り立たない．しかし，集合が有限集合であれば逆が成り立つ．

定理 1.5.10. R を整域とする．このとき，R が有限集合であれば，R は体である．

Proof. 零元でない任意の元 $a \in R$ をとる．今，写像 $f : R \to R$ を $f(x) = ax$ で定義する．この写像が単射であることを示す．任意の $x, y \in R$ で $f(x) = f(y)$ となるものをとる．すると $ax = ay$ となる．$a \neq 0$ であるので簡約律から $x = y$ が従う．よって f は単射である．すると R が有限集合であるので，f が全単射となることがわかる（補足 1.5.11 参照）．よって $f(x) = ax = 1$ を満たす元 $x \in R$ が存在する．つまり，a は単元である．よって $R^\times = R \setminus \{0\}$ が従うので，R は体である． □

補足 1.5.11. 証明では次の事実を使っている．有限集合 A, B と写像 $f : A \to B$ に対し，次は同値：

(1) f は全単射である．

(2) f は単射かつ $|A| \geq |B|$ である．

(3) f は全射かつ $|A| \leq |B|$ である．

$\mathbb{Z}$ は $\mathbb{Q}$ の部分環であった．このとき，$\mathbb{Q}$ は体であるが，$\mathbb{Z}$ は体ではない．つまり，一般に体の部分環は体ではない．しかし，これは整域の場合，その性質は部分環に引き継がれる．

命題 1.5.12. 整域の任意の部分環は整域である．

Proof. R を整域とし，S を R の部分環とする．任意の零元ではない $0 \neq x, y \in S$ をとる．R は整域なので $xy \neq 0$ が従う．R と S の零元は一致するので，これは S の中でも成り立つ．よって S は零因子を持たない，すなわち整域である． □

したがって，先ほど，ガウス整数環 $\mathbb{Z}[\sqrt{-1}]$ が整域であることを定義に則って示したが，$\mathbb{C}$ の部分環であることからこれは直ちに従う．

1.6　多項式環

例 1.2.4 では整数係数の多項式環を考えたが，より一般に係数としてある可換環の元を考えることができる．可換環 R に対して，x を変数とする R **係数の多項式**とは，ある非負整数 $d \in \mathbb{Z}_{\geq 0}$ と元 $a_0, a_1, \ldots, a_d \in R$ を用いて

$$\sum_{i=0}^{d} a_i x^i = a_0 + a_1 x + \cdots + a_d x^d$$

と表されるものをいう．R 係数多項式全体の集合を $R[x]$ で表す．また $R[x]$ に加法 $+$ と乗法 $\cdot$ を以下で定義する：2 つの多項式 $\sum_{i=0}^{d} a_i x^i, \sum_{i=0}^{e} b_i x^i \in R[x]$ に対し，

$$\left(\sum_{i=0}^{d} a_i x^i\right) + \left(\sum_{i=0}^{e} b_i x^i\right) = \sum_{i=0}^{\max\{d,e\}} (a_i + b_i) x^i,$$

$$\left(\sum_{i=0}^{d} a_i x^i\right) \cdot \left(\sum_{i=0}^{e} b_i x^i\right) = \sum_{k=0}^{d+e} \left(\sum_{i+j=k} a_i b_j\right) x^k,$$

ただし，定義されていない a_i, b_i は 0 とする．

命題 1.6.1. 上記の演算により $R[x]$ は零元を 0_R，単位元を 1_R とする可換環となる．$R[x]$ を R **上の (1 変数) 多項式環**という．

Proof. 演習問題とする． □

通常の場合と同様に多項式の次数を定義する．

定義 1.6.2. 0 でない多項式 $f = \sum_{i=0}^{d} a_i x^i \in R[x]$ に対し，$a_i \neq 0$ となる最大の整数 i を f の**次数**といい，$\deg(f)$ で表す．また便宜上 $\deg(0) = -\infty$ とする．すると定義から $\deg(f) \geq 0 \iff f \neq 0$ となる．

多項式環の重要な性質としてもとの R が整域であれば，その多項式環も整域になることである．

定理 1.6.3. R を整域とする．

(1) $f, g \in R[x]$ に対し，$\deg(fg) = \deg(f) + \deg(g)$ である．

(2) $R[x]$ は整域である．

Proof. (1) $f = 0$ または $g = 0$ ならば両辺はともに $-\infty$ となるので主張が成り立つ．$f \neq 0$ かつ $g \neq 0$ を仮定し，$n = \deg(f), m = \deg(g)$ とする．$f = \sum_{i=0}^{n} a_i x^i, g = \sum_{i=0}^{m} b_i x^i$ と表すと，$a_n, b_m \neq 0$ である．すると

$$fg = (a_n b_m) x^{n+m} + (n + m - 1 \text{ 次以下の多項式})$$

であり，R は整域であるので，$a_n b_m \neq 0$ が成り立つ．よって $\deg(fg) = n + m = \deg(f) + \deg(g)$ が従う．

(2) 0 でない 2 つの多項式 $f, g \in R[x]$ をとる．このとき，$fg \neq 0$ が言えれば主張が従う．$\deg(f), \deg(g) \geq 0$ と (1) より

$$\deg(fg) = \deg(f) + \deg(g) \geq 0 + 0 = 0.$$

よって $fg \neq 0$ となる．

□

多変数の多項式環も 1 変数の場合と同様に定義できる．$x_1, \ldots, x_n$ を変数とする可換環 R 上の n 変数多項式環を $R[x_1, \ldots, x_n]$ とする．一方で $R[x_1, \ldots, x_n]$ は次のように定義することができる．まず 1 変数多項式環 $R[x_1]$ を考える．そしてこの可換環 $R[x_1]$ 上の 1 変数多項式環 $(R[x_1])[x_2]$ を考える．すると $R[x_1, x_2]$ の演算（和と積）の結果は $(R[x_1])[x_2]$ の演算の結果と一致している．実際，$R[x_1, x_2]$ の演算は x_1 と x_2 を同時に考え，$(R[x_1])[x_2]$ の演算は x_2 をまず考え，続いて x_1 を考えるが，結果として得られる多項式や演算が一致するため，$R[x_1, x_2] = (R[x_1])[x_2]$ と同一視してよい．これを続けることで $R[x_1, \ldots, x_n]$ は

$$R[x_1, \ldots, x_n] = (R[x_1, \ldots, x_{n-1}])(x_n)$$

として定義することができる．この定義の利点は帰納法が使いやすいところである．実際，定理 1.6.3 から次の系が得られる．

系 1.6.4. R を整域とする．このとき，$R[x_1, \ldots, x_n]$ は整域である．

2　イデアルと剰余環

群論では，正規部分群によって定義される商集合に群構造が入り，それを剰余群と呼んでいた．環の場合も同様に，ある種の部分構造を用いて「商集合」に環構造を入れることを考える．しかし，環の場合，部分環を用いて商集合に群構造を入れることは一般にはできない．そこで，部分環とは異なる，もう 1 つの環の部分構造であるイデアルを導入する．イデアルは，剰余環を定義するために必要な条件を満たしており，群における正規部分群のような役割を果たす．この節では，まずイデアルの定義と基本的な性質を学び，それを用いて剰余環を構成する方法について説明する．

2.1　イデアル

それではイデアルを定義する．

定義 2.1.1. R を可換環とする．部分集合 $I \subset R$ が R の**イデアル** (ideal) であるとは，次を満たすときをいう．

(1) $0 \in I$.

(2) $x, y \in I$ ならば $x + y \in I$.

(3) $x \in I$ かつ $a \in R$ ならば $ax \in I$.

まず「自明」なイデアルを考える．

例 2.1.2. $R \neq 0$ を可換環とする．このとき，$\{0\}$ は R のイデアルである．実際,

(1) $0 \in \{0\}$.

(2) $0 + 0 = 0 \in \{0\}$.

(3) 任意の $a \in R$ に対し，$a \cdot 0 = 0 \in \{0\}$.

から従う．一方，R 自身も明らかに R のイデアルである．この $\{0\}$ と R を R の自明なイデアルといい，それ以外のイデアルを**真のイデアル** (proper ideal) という．つまり，真のイデアルとは $\{0\} \subsetneq I \subsetneq R$ を満たすイデアル I のことである．

命題 2.1.3. R を可換環，I を R のイデアルとする．このとき，次は同値である．

(1) $I = R$,

(2) I は単元を含む,

(3) $1 \in I$.

Proof. (1)⇒(2) は明らかである．

(2)⇒(3)：$a \in I$ を R の単元とすると，$ab = 1$ となる $b \in R$ が存在するが，$a \in I$ から $ab = 1 \in I$ である．

(3)⇒(1)：$I \subset R$ は明らかである．任意の $a \in R$ をとると，$1 \in I$ から $a = 1 \cdot a \in I$ であるので，$R \subset I$ が成り立つ．よって $I = R$ である．　□

それではイデアルの具体例を見ていく．整数環で考えると，イデアルというのは「倍数」の集合である．

例 2.1.4. 整数 n に対し，$n\mathbb{Z} := \{nx : x \in \mathbb{Z}\}$ とする．このとき，$n\mathbb{Z}$ は $\mathbb{Z}$ のイデアルである．実際，

(1) $0 = n \cdot 0 \in n\mathbb{Z}$ である．

(2) 任意の $x, y \in n\mathbb{Z}$ をとると，ある整数 x', y' を使って $x = nx', y = ny'$ と書ける．すると $x + y = nx' + ny' = n(x' + y')$ であり，$x' + y'$ は整数なので $x + y \in n\mathbb{Z}$ が従う．

(3) 任意の $x = nx' \in n\mathbb{Z}$ と $a \in \mathbb{Z}$ をとる．すると $ax = a(nx') = n(ax')$ であり，ax' は整数なので $ax \in n\mathbb{Z}$ である．

逆に，$\mathbb{Z}$ のどんなイデアル I もある整数 n を用いて $I = n\mathbb{Z}$ と書ける．これは後で証明するが，この性質が非常に重要になってくる．

例 2.1.4 のイデアルの構成を拡張する．

定義 2.1.5. R を可換環とし，$n_1, \ldots, n_s$ を R の元とする．このとき，

$$\langle n_1, \ldots, n_s \rangle = \left\{ \sum_{i=1}^{s} a_i n_i \ : \ a_1, \ldots, a_s \in R \right\}$$

とおく．

例えば，例 2.1.4 の $n\mathbb{Z}$ は $\langle n \rangle$ である．実はこのように構成した集合 $\langle n_1, \ldots, n_s \rangle$ はいつでもイデアルになる．

命題 2.1.6. R を可換環とし，$n_1, \ldots, n_s \in R$ とすると，$\langle n_1, \ldots, n_s \rangle$ は $n_1, \ldots, n_s$ を含む R の最小のイデアルである．$\langle n_1, \ldots, n_s \rangle$ を $n_1, \ldots, n_s \in R$ **により生成されるイデアル**という．

Proof. $I = \langle n_1, \ldots, n_s \rangle$ とする．まず $0 = \sum_{i=1}^{s} 0 \cdot n_i$ だから，$0 \in I$ である．次に $x = \sum_{i=1}^{s} a_i n_i, y = \sum_{i=1}^{s} b_i n_i \in I$ と仮定し，$c \in R$ とする．このとき

$$x + y = \sum_{i=1}^{s} (a_i + b_i) n_i \in I,$$
$$cx = \sum_{i=1}^{s} (ca_i) n_i \in I$$

より，I はイデアルである．

次に最小性を示す．$n_1, \ldots, n_s$ を含む R の勝手なイデアルを J とする．このとき，$I \subset J$ を言えばよい．任意の $x = \sum_{i=1}^{s} a_i n_i \in I$ をとる．各 i に対し，仮定より $n_i \in J$ である．また J はイデアルなので $a_i n_i \in J$ である．再び J はイデアルなので，$x = \sum_{i=1}^{s} a_i n_i \in J$ が従い，$I \subset J$ が成り立つ． □

例 2.1.7. イデアル $\langle n_1, \ldots, n_s \rangle$ は，多変数の多項式環，例えば $\mathbb{R}[x, y, z]$ とその多項式の連立方程式を考えるとうまく解釈できる．$f_1 = xy + z^2 - 2, f_2 = x^2 - yz, f_3 = xz - y^2$ のとき，イデアル $\langle f_1, f_2, f_3 \rangle$ は

$$h_1 f_1 + h_2 f_2 + h_3 f_3 = h_1(xy + z^2 - 2) + h_2(x^2 - yz) + h_3(xz - y^2)$$

と表すことのできる多項式全体の集合である．ここで，$h_1, h_2, h_3 \in \mathbb{R}[x, y, z]$ である．今，連立方程式 $f_1 = f_2 = f_3 = 0$ を考える．これらの方程式から，代数演算を用いて別の方程式を導くことができる．たとえば，最初の方程式と $h_1 = x + y + z \in \mathbb{R}[x, y, z]$ の積をとる，2 番目の方程式と $h_2 = 2xz + z^3 \in \mathbb{R}[x, y, z]$ の積をとる．さらに 3 番目の方程式と $h_3 = x^2 - z^2 \in \mathbb{R}[x, y, z]$ の積をとる．このようにして作った式の和をとると，

$$h_1 f_1 + h_2 f_2 + h_3 f_3 = (x + y + z)(xy + z^2 - 2) + (2xz + z^3)(x^2 - yz) + (x^2 - z^2)(xz - y^2) = 0$$

が成り立つ．この方程式の左辺は，まさにイデアル $\langle f_1, f_2, f_3 \rangle$ の要素になっていることに注意する．したがって，連立方程式 $f_1 = f_2 = f_3 = 0$ の解は，$\langle f_1, f_2, f_3 \rangle$ のどの多項式 $f \in \langle f_1, f_2, f_3 \rangle$ に対しても，方程

式 $f=0$ の解となる．つまり，$\langle f_1,f_2,f_3\rangle$ は連立方程式 $f_1=f_2=f_3=0$ から「帰結された多項式（方程式）」全体からなる集合と考えることができる．

この講義で考えるイデアルは基本 $\langle n_1,\dots,n_s\rangle$ の形で書けるものである．このようなイデアルは有限生成なイデアルと呼ばれる．

定義 2.1.8. R を可換環とする．イデアル I が**有限生成** (finitely generated) であるとは，$I=\langle n_1,\dots,n_s\rangle$ となる $n_1,\dots,n_s\in R$ が存在するときをいい，$n_1,\dots,n_s$ を I の**生成系** (system of generators) という．さらに，イデアル I が 1 つの元で生成される，つまり $I=\langle n\rangle$ と表せるとき，I は**単項イデアル** (principal ideal) という．このとき，I を nR と書くこともある．

補足 2.1.9. 自明なイデアルは単項イデアルである．実際，$\{0\}=\langle 0\rangle$ であり，$R=\langle 1\rangle$ である．

$\mathbb{Z}$ のイデアルは全て単項イデアルとなることを見よう．

定理 2.1.10. 整数環 $\mathbb{Z}$ の任意のイデアルは単項イデアルである．

Proof. I を $\mathbb{Z}$ の任意のイデアルとする．$I\neq\{0\}$ と仮定してよい．集合 $N=\{|a|:a\in I\setminus\{0\}\}$ を考えると，N は空ではない $\mathbb{N}$ の部分集合である．このとき，N は最小値 d_0 を持つ．そこで $|a|=d_0$ を満たす $a\in I\setminus\{0\}$ をとる．$I=\langle a\rangle$ となることを示す．$a\in I$ とイデアルの性質より $\langle a\rangle\subset I$ が従う．そこで，$x\in I\setminus\langle a\rangle$ が存在したと仮定する．$a\neq 0$ であるので，$q,r\in R$ を用いて $x=aq+r$ と書くことができる．ただし，$0\leq r<|a|$ である．もし $r=0$ ならば，$x=aq\in\langle a\rangle$ なので仮定に矛盾する．よって $0<r<|a|=d_0$ である．しかし，$0\neq r=x-aq\in I$ から，これは d_0 の最小性に矛盾する．以上より，$I=\langle a\rangle$ が従い，I は単項イデアルである． □

補足 2.1.11. 情報代数 C では，任意の $a,b\in\mathbb{Z}$ に対して，$\langle a,b\rangle=\langle d\rangle$ を満たす $d\in\mathbb{Z}$ が存在することを示した．この定理はその一般化である．

それでは単項イデアルでないイデアルの例を見る．

例 2.1.12. 1 変数多項式環 $\mathbb{Z}[x]$ とそのイデアル $I=\langle 2,x\rangle$ を考えよう．このとき， I が単項イデアルでないことを示す．I が単項イデアルであると仮定する．このとき，ある $0\neq f\in\mathbb{Z}[x]$ を用いて，$I=\langle f\rangle$ と書ける．すると $2,x\in I$ より，$g,h\in\mathbb{Z}[x]$ を用いて，$2=fg,x=fh$ と書ける．よって f,g は定数，つまり $f,g\in\mathbb{Z}$ でないといけない．$0\neq f=a\in\mathbb{Z}$ とすると，$\dfrac{x}{a}=h\in\mathbb{Z}[x]$ なので，$a=\pm 1$ である．よって a は I の単元となり，$I=\mathbb{Z}[x]$ が従う．しかし，$1\notin I$ からこれは矛盾．以上より，I は単項イデアルではない有限生成イデアルである．

有限生成ではないイデアルの例を見る．

例 2.1.13 (概略)**.** 無限変数多項式環 $\mathbb{Z}[x_1,x_2,\dots]$ を考える．これは項が無限個あったり，項の中の変数が無限個あるというのではなく，各項で使っていい変数が無限個あるということである．すると通常の多項式の和と積により $\mathbb{Z}[x_1,x_2,\dots]$ は可換環となる．今，全ての変数 $x_1,x_2,\dots$ を含む最小のイデアル $I=\langle x_1,x_2,\dots\rangle$ を考える（そのようなものが取れることは認める）．もし I が有限生成であれば有限個の多項式 $f_1,\dots,f_s\in\mathbb{Z}[x_1,x_2,\dots]$ を用いて $I=\langle f_1,\dots,f_s\rangle$ とできる．$f_1,\dots,f_s$ に現れる変数の中で添え字が最大のものを x_k とする．すると

$$I=\langle f_1,\dots,f_s\rangle\subset\langle x_1,\dots,x_k\rangle\subset I$$

となるので，$I=\langle x_1,\dots,x_k\rangle$ である．$x_{k+1}\in I$ から，$g_1,\dots,g_k\in\mathbb{Z}[x_1,x_2,\dots]$ を用いて $x_{k+1}=g_1x_1+\cdots+g_kx_k$ と書ける．今，$x_1=\cdots=x_k=0,x_{k+1}=1$ をこの式に代入すると，$1\neq 0$ となり矛盾．よって I は有限生成ではないイデアルである．

環の性質を見るために，その環に含まれるイデアル全体を考えることがある．例えば，環が体であるかどうかは含まれるイデアルを見ることで判定できる．

命題 2.1.14. $R \neq 0$ を可換環とする．このとき，R が体であることと，R が真のイデアルを持たないことは同値である．

Proof. （⇒）R が体であるとし，I を $\{0\}$ でない R のイデアルとする．このとき，$0 \neq x \in I$ がとれるが，R は体であるため，$x^{-1} \in R$ が存在する．するとイデアルの性質から $x \cdot x^{-1} = 1 \in I$ である．これは $I = R$ を意味するので，R は真のイデアルを持たない．

（⇐） R が体でないとする．するとある元 $0 \neq x \in R$ は乗法に関する逆元を持たない．$I = \langle x \rangle \neq \{0\}$ とするとイデアル I は 1 を含まない．実際，1 を含めば $ax = 1$ を満たす $a \in R$ が存在することとなり，この場合 a は x の乗法に関する逆元となってしまうからである．よって $I \neq R$ となるので，I は真のイデアルとなる． □

最後に複数のイデアルから新たにイデアルを作る方法を見る．

定理 2.1.15. R を可換環とし，I, J を R のイデアルとする．このとき，集合 $I \cap J, I + J, IJ$ はそれぞれ R のイデアルである．ただし，

$$I + J := \{x + y : x \in I, y \in J\},$$
$$IJ := \left\{ \sum_{i=1}^{n} x_i y_i : n \in \mathbb{N}, x_i \in I, y_i \in J (i = 1, 2, \ldots, n) \right\}$$

である．

Proof. $I + J$ が R のイデアルとなることを見る．まず I, J はイデアルなので，$0 \in I, J$ である．よって $0 = 0 + 0 \in I + J$ が成り立つ．次に任意の $a, b \in I + J$ をとる．このとき，$x_1, x_2 \in I$ と $y_1, y_2 \in J$ を使って $a = x_1 + y_1, b = x_2 + y_2$ と書くことができる．すると

$$a + b = (x_1 + y_1) + (x_2 + y_2) = (x_1 + x_2) + (y_1 + y_2)$$

が成り立つ．I, J はイデアルなので，$x_1 + x_2 \in I, y_1 + y_2 \in J$ が従い，$a + b \in I + J$ がわかる．最後に任意の $a \in I + J$ と $c \in R$ をとる．このとき，$x \in I, y \in J$ を使って $a = x + y$ と書ける．すると

$$ca = c(x + y) = cx + cy$$

が成り立つ．I, J はイデアルなので，$cx \in I, cy \in J$ が従い，$ca \in I + J$ がわかる．以上より，$I + J$ は R のイデアルである．

$I \cap J$ と IJ が R のイデアルとなることの証明は演習問題とする． □

補足 2.1.16. 一般に

$$IJ \neq \{xy : x \in I, y \in J\}$$

である．実際，$R = \mathbb{Z}[x], I = \langle 2, x \rangle, J = \langle 3, x \rangle$ とすると，

$$2 \cdot 3 + x \cdot x = 6 + x^2 \in IJ$$

であるが，$6 + x^2 = fg$ となる $f \in I, g \in J$ が存在しない．よって

$$IJ \supsetneq \{fg : f \in I, g \in J\}$$

である．

2.2 剰余環

情報数理 C で学習した剰余類 $\mathbb{Z}/m\mathbb{Z}$ を思い出す．m を自然数とする．2 つの整数 $x, y \in \mathbb{Z}$ に対して，二項関係 $\equiv_m$ を

$$x \equiv_m y \overset{\text{def}}{\iff} x - y \in m\mathbb{Z}$$

で定義すると，これは同値関係となる．整数 a に対し，a の $\equiv_m$ に関する同値類，つまり $x \equiv_m a$ を満たす整数全体の集合を $a + m\mathbb{Z}$ で表し，法 m に関する a の**剰余類**という．つまり，

$$a + m\mathbb{Z} := \{x \in \mathbb{Z} : x \equiv_m a\} \subset \mathbb{Z}$$

である．ここで $0 + m\mathbb{Z}$ は $m\mathbb{Z}$ のことである．文脈から m が明らかな場合は，$\overline{a}$ と書くことが多い．つまり，$\overline{a} = a + m\mathbb{Z}$ である．また剰余類全体の集合を $\mathbb{Z}/m\mathbb{Z}$ と書く．つまり，

$$\mathbb{Z}/m\mathbb{Z} = \{\overline{a} : a \in \mathbb{Z}\}$$

である．このとき，

$$\mathbb{Z}/m\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}$$

である．特に，$|\mathbb{Z}/m\mathbb{Z}| = m$ である．この剰余類 $\mathbb{Z}/m\mathbb{Z}$ は「余りの世界」であった．また m を 2 以上の自然数とし，$\mathbb{Z}/m\mathbb{Z}$ 上の演算 $+$ を

$$\begin{array}{rccc} +: & \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} & \longrightarrow & \mathbb{Z}/m\mathbb{Z} \\ & \cup & & \cup \\ & (\overline{a}, \overline{b}) & \longmapsto & \overline{a} + \overline{b} := \overline{a +_{\mathbb{Z}} b} \end{array}$$

で定義する．ただし $+_{\mathbb{Z}}$ は $\mathbb{Z}$ 上の加法である（以降は単に $+$ と書く）．するとこの演算は well-defined であり，$(\mathbb{Z}/m\mathbb{Z}, +)$ はアーベル群となる．今回はさらに環の構造を入れる．今，$\mathbb{Z}/m\mathbb{Z}$ 上の演算 $\cdot$ を

$$\begin{array}{rccc} \cdot: & \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} & \longrightarrow & \mathbb{Z}/m\mathbb{Z} \\ & \cup & & \cup \\ & (\overline{a}, \overline{b}) & \longmapsto & \overline{a} \cdot \overline{b} := \overline{a \cdot_{\mathbb{Z}} b} \end{array}$$

で定義する．ただし $\cdot_{\mathbb{Z}}$ は $\mathbb{Z}$ 上の乗法である（以降は単に $\cdot$ と書く）．するとこの演算は well-defined であり，$(\mathbb{Z}/m\mathbb{Z}, +, \cdot)$ は可換環となる．

群では $\mathbb{Z}/m\mathbb{Z}$ を一般化し，群 G を正規部分群 N で「割った」剰余群 G/N が定義された．$\mathbb{Z}/m\mathbb{Z}$ は $\mathbb{Z}$ がもとの群で，$m\mathbb{Z}$ がその正規部分群である．環の場合も同様に剰余環というものに一般化できる．この場合，正規部分群の代わりにイデアルを用いる．R を可換環，I を R のイデアルとする．R 上の二項関係 $\sim_I$ を

$$x \sim_I y \overset{\text{def}}{\iff} x - y \in I$$

で定義する．

命題 2.2.1. $\sim_I$ は R 上の同値関係である．

Proof. （反射律）任意の $x \in R$ に対し $x - x = 0 \in I$ なので，$x \sim_I x$ である．

（対称律）任意の $x, y \in R$ で $x \sim_I y$ となるものをとる．このとき，$x - y \in I$ なので，

$$y - x = -(x - y) = (-1)(x - y) \in I$$

が従い，$y \sim_I x$ が成り立つ．

（推移律）任意の $x, y, z \in R$ で $x \sim_I y, y \sim_I z$ となるものとる．このとき，$x - y, y - z \in I$ なので，

$$x - z = (x - y) + (y - z) \in I$$

が従い，$x \sim_I z$ が成り立つ．

以上より $\sim_I$ は同値関係である． □

R の $\sim_I$ に関する商集合を $R/\sim_I$ の代わりに R/I と書く．また $x \in R$ に対し，x の $\sim_I$ に関する同値類を $x+I$ または $\overline{x}$ で表す．つまり，$x+I=\overline{x}=\{y \in R : x \sim_I y\}$ であり，

$$R/I = \{x+I : x \in R\}$$

である．今，R/I 上に加法と乗法を

$$(x+I)+(y+I) := (x +_R y)+I,$$
$$(x+I)\cdot(y+I) := (x \cdot_R y)+I$$

で定義する．ここで $+_R, \cdot_R$ は R の加法と乗法である．以降は単に $+$ と $\cdot$ で書く．

命題 2.2.2. R/I 上の演算 $+$ と $\cdot$ はともに well-defined であり，この演算により R/I は零元 $0+I$，単位元を $1+I$ とする可換環となる．

Proof. (well-defined 性) $x+I=x'+I, y+I=y'+I$ となる任意の R/I の元をとる．これは $x-x', y-y' \in I$ を意味する．$+$ に関して示したいことは $(x+y)+I=(x'+y')+I$ である．これは $(x+y)-(x'+y') \in I$ を示せばよいが，$(x+y)-(x'+y')=(x-x')+(y-y')$ と I がイデアルであることから従う．よって $+$ は well-defined である．同様に $\cdot$ に関して示したいことは $(xy)+I=(x'y')+I$ である．これは $xy-x'y' \in I$ を示せばよいが，$xy-x'y'=x(y-y')+y'(x-x')$ と I がイデアルであることから従う．よって $\cdot$ は well-defined である．

$(R/I, +, \cdot)$ が可換環であることの証明は演習問題とする． □

R/I は，R の元を「I の違いを無視して」見たときの世界を表している．特に，$x, y \in R$ が $x-y \in I$ を満たすなら，x と y は「R/I の中で同じもの」として扱う．このようにして得られる R/I の元が剰余類であり，それらをもとにした環構造が剰余環である．例えば，$R=\mathbb{Q}[x], I=\langle x^2+1\rangle$ とすると，R/I は「$x^2+1=0$ が成り立つと仮定した世界」での可換環である．つまり，この環の中では，x^3 は $x^3=(x^2+1)x-x$ なので，$-x$ と思うことができる（実際は，$\overline{x^3}=\overline{-x}$）．

2.3 素イデアルと極大イデアル

イデアルと剰余環は密接な関係をもち，互いにその構造を反映し合っている．つまり，イデアルの性質を調べれば剰余環の構造がわかり，逆に，剰余環を調べることでイデアルの性質も明らかになる．本節では，この関係性を「剰余環が整域あるいは体になるのはどのようなときか」を通して見ていく．そのために素イデアルという概念を導入する．

定義 2.3.1. R を可換環とし，$I \subsetneq R$ を R のイデアルとする．I が**素イデアル** (prime ideal) であるとは，任意の $a, b \in R$ に対し，$ab \in I$ ならば $a \in I$ または $b \in I$ が成り立つときにいう．対偶を考えると，$a \notin I$ かつ $b \notin I$ ならばいつでも $ab \notin I$ となることと同値である．

例 2.3.2. 整数環 $\mathbb{Z}$ とイデアル $2\mathbb{Z}$ を考える．ここで $2\mathbb{Z} \subsetneq \mathbb{Z}$ に注意する．もし a と b がともに奇数ならば，ab も奇数である．つまり $a, b \notin 2\mathbb{Z}$ ならば $ab \notin 2\mathbb{Z}$ が成り立つので，$2\mathbb{Z}$ は素イデアルである．またイデアル $\{0\}$ を考えると，$\mathbb{Z}$ は整域なので，$ab=0$ であれば $a=0$ または $b=0$ が成り立つので $\{0\}$ は素イデアルである．一方，イデアル $6\mathbb{Z}$ を考えると，$2\cdot 3=6 \in 6\mathbb{Z}$ であるが，$2, 3 \notin 6\mathbb{Z}$ であるので，$6\mathbb{Z}$ は素イデアルではない．あとで見るが 2 以上の自然数 n に対し，$n\mathbb{Z}$ が素イデアルである必要十分条件は n が素数になることである．したがって，素イデアルは素数の概念を一般の環に拡張するためのものである．

素イデアルの定義を見ると，整域の定義に似ていることに気づくであろう．実際，剰余環を考えると素イデアルは整域に対応している．

定理 2.3.3. R を可換環，$I \subsetneq R$ を R のイデアルとする．このとき，I が素イデアルであることと R/I が整域であることは同値である．

Proof. （⇒）I が素イデアルであると仮定する．$ab + I = 0 + I$ となる任意の $a + I, b + I \in R/I$ をとる．これは $ab - 0 = ab \in I$ を意味する．I は素イデアルであるので，$a \in I$ または $b \in I$ が成り立つ．そこで $a \in I$ としてもよい．すると $a + I = 0 + I$ が成り立ち R/I が整域であることが従う．

（⇐）I が素イデアルでないと仮定する．すると $ab \in I$ であるが，$a \in I$ でも $b \in I$ でもない元 $a, b \in R$ が存在する．これは，$ab + I = 0 + I$ であるが，$a + I = 0 + I$ でも $b + I = 0 + I$ でもないことを意味する．したがって R/I が整域でないことがわかる． □

次に極大イデアルの概念を導入する．

定義 2.3.4. R を可換環とし，$I \subsetneq R$ を R のイデアルとする．I が**極大イデアル** (maximal ideal) であるとは，I を真に含むイデアルが R だけのときにいう．つまり，J が $I \subsetneq J \subset R$ を満たすイデアルならば $J = R$ である．

例 2.3.5. 整数環 $\mathbb{Z}$ とイデアル $2\mathbb{Z}$ を考える．$2\mathbb{Z} \subsetneq J \subset \mathbb{Z}$ を満たすイデアル J をとると，$2k + 1 \in J$ を満たす整数 k が存在する．すると $(2k + 1) + (-2k) = 1 \in J$ となるので，$J = R$ が従う．よって $2\mathbb{Z}$ は極大イデアルである．一方，$\{0\}$ や $6\mathbb{Z}$ は $\{0\} \subsetneq 6\mathbb{Z} \subsetneq 2\mathbb{Z} \subsetneq \mathbb{Z}$ となるイデアルの列が存在するので，極大イデアルではない．

ここまでで

- 極大イデアルかつ素イデアルの例（$2\mathbb{Z}$），
- 極大イデアルではないが素イデアルである例（$\{0\}$），
- 極大イデアルでも素イデアルでもない例（$6\mathbb{Z}$）

が存在したが，極大イデアルであるが素イデアルではない例は存在するのであろうか．実は極大イデアルであればいつでも素イデアルである．

定理 2.3.6. R を可換環とし，$I \subsetneq R$ を R のイデアルとする．このとき，I が極大イデアルであれば，I は素イデアルである．

Proof. $ab \in I$ を満たす任意の $a, b \in R$ をとる．$a \notin I$ のとき，$J = \langle a \rangle + I$ とおくと J は I と a の両方を含むイデアルなので，$I \subsetneq J$ である．ここで，I は極大イデアルであったので，$J = R$ でなくてはいけない．すると $1 \in R = J = \langle a \rangle + I$ より，ある $x \in R$ と $y \in I$ を使って $1 = ax + y$ と書ける．両辺に b を掛けると $b = abx + by$ となるが，$ab, y \in I$ より $b \in I$ が従う．よって I は素イデアルである． □

極大イデアルも素イデアルと同様で剰余環を使って判定できる．

定理 2.3.7. R を可換環，$I \subsetneq R$ を R のイデアルとする．このとき，I が極大イデアルであることと，R/I が体であることは同値である．

Proof. （⇒）I を極大イデアルとする．$a + I \neq 0 + I$ を満たす任意の $a + I \in R/I$ をとる．すると $a \notin I$ なので，定理 2.3.6 の証明から，ある $x \in R$ と $y \in I$ を使って $1 = ax + y$ と書ける．すると

$$1 + I = (ax + y) + I = (a + I)(x + I) + (y + I) = (a + I)(x + I) + (0 + I) = (a + I)(x + I)$$

となるので，$a + I$ は単元である．つまり，$(R/I)^\times = (R/I) \setminus \{0 + I\}$ であるので R/I は体である．

（⇐）$I \subsetneq J$ となるイデアル J をとる．このとき，$x \in J \setminus I$ が存在する．$x \notin I$ より $x+I \neq 0+I$ である．R/I は体であるので，$(x+I)(y+I) = (1+I)$ となる $y+I \in R/I$ が存在する．このとき，$1+I = xy+I$ なので，$1-xy \in I \subset J$ である．また $x \in J$ より $(1-xy)+xy = 1 \in J$ となるので $J = R$．したがって I は極大イデアルである． □

このように剰余環の性質を調べるには，イデアルの性質を見ればいいことがわかる．この関係性を元に，$\mathbb{Z}/n\mathbb{Z}$ がいつ整域や体になるかを考える．

定理 2.3.8. n を 2 以上の自然数とする．このとき以下は同値である．

(1) n は素数である．

(2) $\mathbb{Z}/n\mathbb{Z}$ は体である．

(3) $\mathbb{Z}/n\mathbb{Z}$ は整域である．

この定理の証明のために，$n\mathbb{Z}$ がいつ素イデアルや極大イデアルになるかを考える．

補題 2.3.9. n を 2 以上の自然数とする．

(1) n が素数であれば $n\mathbb{Z}$ は極大イデアル，特に素イデアルである．

(2) n が合成数であれば，$n\mathbb{Z}$ は素イデアルではない．特に，極大イデアルではない．

Proof. (1) $n\mathbb{Z} \subsetneq \mathbb{Z}$ に注意する．$n\mathbb{Z} \subsetneq J \subset \mathbb{Z}$ となるイデアル J を考える．このとき $x \in J \setminus n\mathbb{Z}$ が存在する．n は素数なので $\gcd(x,n) = 1$，よってある整数 a, b を使って $1 = ax + bn$ と書ける．$x, n \in J$ より $1 = ax + bn \in J$ である．よって $J = \mathbb{Z}$ なので $n\mathbb{Z}$ は極大イデアルである．

(2) 仮定より 2 以上の整数 a, b を使って $n = ab$ と書ける．このとき，$ab \in n\mathbb{Z}$ であるが，$a \in n\mathbb{Z}$ でも $b \in n\mathbb{Z}$ でもないので，$n\mathbb{Z}$ は素イデアルではない． □

それでは定理 2.3.8 を証明する．

定理 2.3.8 の証明. ((1)⇒(2)) n を素数とすると，補題 2.3.9 の (1) より $n\mathbb{Z}$ は極大イデアルである．よって定理 2.3.7 より $\mathbb{Z}/n\mathbb{Z}$ は体である．

((2)⇒(3)) これは定理 1.5.9 である．

((3)⇒(1)) 対偶を考える．n を合成数とする．このとき，補題 2.3.9 の (2) から $n\mathbb{Z}$ は素イデアルではない．よって定理 2.3.3 から $\mathbb{Z}/n\mathbb{Z}$ は整域ではない．

以上より，(1)〜(3) は同値である． □

3　準同型写像と準同型定理

環の理論において，環同士を比較する際には，単なる集合の対応ではなく，環の構造（加法・乗法）を保つ写像に注目する必要がある．群論において，2 つの群を群として比較するために群準同型写像を導入したように，環でもその構造を保つ写像として環準同型写像を定義する．特に環構造が完全に一致する場合を表す環同型写像の概念を導入し，群のときと同様に準同型定理を証明する．

3.1　準同型写像

それではまず，環準同型写像を定義する．

定義 3.1.1. R, S を可換環とする．写像 $f : R \to S$ が（環）**準同型写像** (homomorphism) であるとは，以下の 3 つの条件を満たすときにいう．

(1) 任意の $x, y \in R$ に対し，$f(x +_R y) = f(x) +_S f(y)$.

(2) 任意の $x, y \in R$ に対し，$f(x \cdot_R y) = f(x) \cdot_S f(y)$.

(3) $f(1_R) = 1_S$.

準同型写像の定義の (1) は $(R, +_R, 0_R)$ と $(S, +_S, 0_S)$ をアーベル群として見れば，f が群準同型写像になることに他ならない．したがって，次の性質が成り立つ．

命題 3.1.2. R, S を可換環とし，$f : R \to S$ を環準同型写像とする．

(1) $f(0_R) = 0_S$.

(2) 任意の $x \in R$ に対し，$f(-x) = -f(x)$.

Proof. 情報数理 C の 5.1 節を参照. □

一方で，定義の (2) を考えると以下が示せる．

命題 3.1.3. R, S を可換環とし，$f : R \to S$ を環準同型写像とする．もし $x \in R$ が R の単元であれば，$f(x)$ は S の単元である．

Proof. x が R の単元とすると，$x \cdot_R y = 1_R$ を満たす $y \in R$ が存在する．すると，f が準同型写像であるので，

$$1_S = f(1_R) = f(x \cdot_R y) = f(x) \cdot_S f(y)$$

が成り立つので，$f(x)$ は S の単元である． □

それでは準同型写像の例を見ていこう．

例 3.1.4. (1) 整数環 $\mathbb{Z}$ から剰余環 $\mathbb{Z}/n\mathbb{Z}$ の写像 $\varphi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ を $\varphi(a) = \overline{a}$ で定めると，φ は環準同型写像である．実際，任意の $a, b \in \mathbb{Z}$ に対して，

$$\varphi(a + b) = \overline{a + b} = \overline{a} + \overline{b} = \varphi(a) + \varphi(b),$$
$$\varphi(ab) = \overline{ab} = \overline{a} \cdot \overline{b} = \varphi(a) \cdot \varphi(b)$$

である．また $\varphi(1) = \overline{1}$ より，準同型写像の条件を満たす.

より一般に，可換環 R とそのイデアル I に対し，写像 $\varphi : R \to R/I$ を $x \mapsto \overline{x}$ で定めると，φ は環準同型写像となる．これを**自然な（全射）準同型写像**という．

(2) $\mathbb{Q}[x]$ から $\mathbb{Q}$ への写像 $\varphi : \mathbb{Q}[x] \to \mathbb{Q}$ を $f \mapsto f(1)$（多項式に 1 を代入）で定義すると，φ は環準同型写像である（確かめよ）．より，一般に，可換環 R と元 $a \in R$ に対し，写像 $\varphi : R[x] \to R$ を $f \mapsto f(a)$（多項式に a を代入）で定義すると，φ は環準同型写像である．これを**代入写像**という．

(3) 単位元を保たない例として，$\mathbb{Z} \to \mathbb{Z}$ に $f(a) = 2a$ と定めた写像は加法と乗法の条件は満たすが，$f(1) = 2 \neq 1$ なので環準同型写像ではない．補足として，$\mathbb{Z}$ をアーベル群として見れば，f は群準同型写像である．

群準同型写像のときと同様に，像と核を定義する．

定義 3.1.5. R, S を可換環とし，$f : R \to S$ を環準同型写像とする．元 $x \in R$ に対し，$f(x)$ を x の f に関する**像**という．また集合

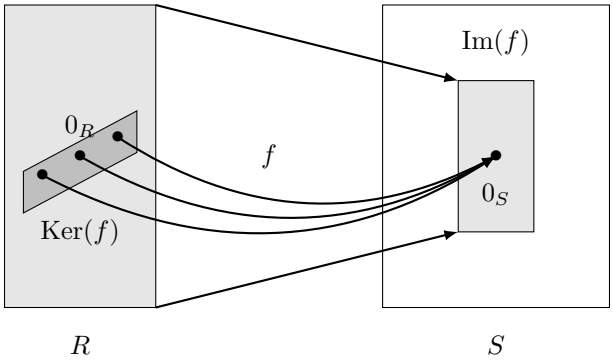
$$\mathrm{Im}(f) := \{f(x) : x \in R\} \subset S$$

を f の**像** (image) という．一方，集合

$$\mathrm{Ker}(f) := \{x \in R : f(x) = 0_R\} \subset R$$

を f の**核** (kernel) という．

下図のように，$\mathrm{Ker}(f)$ とは加法の単位元 1 点に圧縮される集合のことである．



したがって，f を群 $(R, +_R)$ から $(S, +_S)$ への群準同型写像と思えば，$\mathrm{Ker}(f)$ は集合として一致している（$\mathrm{Im}(f)$ は明らかに群でも環でも一致している）．

群のときは $\mathrm{Im}(f)$ も $\mathrm{Ker}(f)$ も群構造を持っていたが，環の場合は少し役割が異なる．

命題 3.1.6. R, S を可換環とし，$f : R \to S$ を環準同型写像とする．

(1) $\mathrm{Im}(f)$ は S の部分環である．

(2) $\mathrm{Ker}(f)$ は R のイデアルである．

Proof. (1) 任意の $x, y \in \mathrm{Im}(f)$ をとる．このとき，ある $x', y' \in R$ を使って $x = f(x'), y = f(y')$ と書ける．すると f が準同型写像であることから $-x = -f(x') = f(-x')$ かつ

$$x +_S (-y) = f(x') +_S f(-y') = f(x' +_R (-y')),$$
$$x \cdot_S y = f(x') \cdot_S f(y') = f(x' \cdot_R y')$$

が得られ，$x' +_R (-y)', x' \cdot_R y' \in R$ なので，$x +_S (-y), x \cdot_S y \in \mathrm{Im}(f)$ が従う．また $f(1_R) = 1_S \in \mathrm{Im}(f)$ である．以上より，$\mathrm{Im}(f)$ は S の部分環である．

(2) $f(0_R) = 0_S$ より $0_R \in \mathrm{Ker}(f)$ である．任意の $x, y \in \mathrm{Ker}(f)$ と $a \in R$ をとる．このとき，$f(x) = f(y) = 0_S$ である．f が準同型写像であることから

$$f(x +_R y) = f(x) +_S f(y) = 0_S +_S 0_S = 0_S,$$
$$f(a \cdot_R x) = f(a) \cdot_S f(x) = f(a) \cdot_S 0_S = 0_S$$

が得られるので，$x +_R y, a \cdot_R x \in \mathrm{Ker}(f)$ が従う．以上より，$\mathrm{Ker}(f)$ は R のイデアルである． □

また群のときと同様で，$\mathrm{Ker}(f)$ から f の単射性がわかる．

命題 3.1.7. R, S を可換環とする．環準同型写像 $f : R \to S$ が単射である必要十分条件は $\mathrm{Ker}(f) = \{0_R\}$ である．

Proof. 情報数理 C の 5.1 節を参照. □

最後に $\mathrm{Ker}(f)$ の例を見る．

例 3.1.8. (1) 環準同型写像 $\varphi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}; a \mapsto \overline{a}$ に対し，

$$\mathrm{Ker}(\varphi) = \{a \in \mathbb{Z} : f(a) = \overline{a} = \overline{0}\} = \{a \in \mathbb{Z} : a - 0 = a \in n\mathbb{Z}\} = n\mathbb{Z}$$

である．一般に，自然な全射 $\varphi : R \to R/I, a \mapsto \overline{a}$ に対し，$\mathrm{Ker}(\varphi) = I$ である．

(2) 環準同型写像 $\varphi : \mathbb{Q}[x] \to \mathbb{Q}; f \mapsto f(1)$ に対し，

$$\mathrm{Ker}(\varphi) = \{f(x) \in \mathbb{Q}[x] : f(1) = 0\}$$

である．これは，$x = 1$ を代入して 0 になる多項式全体の集合であり，明らかに $x - 1$ を因数にもつ多項式の集合と一致する．したがって，

$$\mathrm{Ker}(\varphi) = \langle x - 1 \rangle = \{(x - 1)g(x) : g(x) \in \mathbb{Q}[x]\}$$

である．このように，代入写像の核は対応する代入点を根にもつ多項式の生成するイデアルとなる．

3.2 同型写像

群のときと同様に,「同型」を定義する．これは 2 つの環が「環として同じ」という意味である．

定義 3.2.1. R, S を可換環とする．写像 $f : R \to S$ が**同型写像** (isomorphism) であるとは f が全単射な環準同型写像のときにいう．R と S の間に同型写像が存在するとき，R と S は**同型** (isomorphic) であるといい，$R \cong S$ と書く．

補足 3.2.2. 群のときと同様で，$f : R \to S$ が同型写像のとき，$f^{-1} : S \to R$ も同型写像である．

さて，同型は「環として同じ」という意味なので，同型な環は同じ代数的性質を持つ．実際，次が成り立つ．

命題 3.2.3. R と S を同型な可換環とし，$f : R \to S$ を同型写像とする．

(1) R は整域である $\iff S$ は整域である．

(2) R は体である $\iff$ S は体である．

(3) $f(R^\times) = S^\times$．

Proof. 補足 3.2.2 より (1), (2) は $\Rightarrow$ のみ示せば十分．

(1) $x \cdot_S y = 0_S$ を満たす任意の $x, y \in S$ をとる．f は全射なので，$f(x') = x, f(y') = y$ を満たす $x', y' \in R$ が存在する．すると

$$f(x' \cdot_R y') = f(x') \cdot_S f(y') = x \cdot_S y = 0_S = f(0_R)$$

が成り立つ．このとき，f は単射であるので $x' \cdot_R y' = 0_R$ が従う．よって R は整域であるので，$x' = 0_R$ または $y' = 0_R$ が成り立つ．そこで，$x' = 0_R$ としてよい．すると，

$$x = f(x') = f(0_R) = 0_S$$

となるので，S は整域となる．

(2) $0_S \neq x \in S$ を任意に取る．f は全射なので，$f(x') = x$ を満たす $x' \in R$ が存在する．もし $x' = 0_R$ なら $x = f(x') = f(0_R) = 0_S$ となり矛盾．よって $x' \neq 0_R$ となる．このとき，R は体であるので，x' は R の単元である．すると命題 3.1.3 から $f(x') = x$ は S の単元となり，S が体になることがわかる．

(3) 命題 3.1.3 から $f(R^\times) \subset S^\times$ であることが従う．逆の包含関係を示すために，任意の $x \in S^\times$ をとる．このとき，$x \cdot_S y = 1_S$ を満たす $y \in S$ が存在する．また f が全射であるので，$f(x') = x, f(y') = y$ を満たす $x', y' \in R$ が存在する．すると

$$f(1_R) = 1_S = x \cdot_S y = f(x') \cdot_S f(y') = f(x' \cdot_R y')$$

が成り立つ．よって f が単射であるので $1_R = x' \cdot_R y'$ が成り立ち，$x' \in R^\times$ となる．これから $x = f(x') \in f(R^\times)$ となるので，$S^\times \subset f(R^\times)$ が得られる．以上より，$f(R^\times) = S^\times$ である． □

この命題の (2) の証明では f の単射性を使っていない．実は単射性は体の性質に含まれている．

命題 3.2.4. R を体，$0 \neq S$ を可換環，$f : R \to S$ を環準同型写像とする．このとき，f は単射である．

Proof. 体は自明なイデアルしか持たないので，$\mathrm{Ker}(f) = \{0_R\}$ または $\mathrm{Ker}(f) = R$ である．一方，$S \neq 0$ より $1_S \neq 0_S$ である．すると，$1_S = f(1_R)$ から $1_R \notin \mathrm{Ker}(f)$ が成り立つので，$\mathrm{Ker}(f) \neq R$，よって $\mathrm{Ker}(f) = \{0_R\}$ が従い，f が単射であることがわかる． □

同型と非同型の環の例を見ていこう．

例 3.2.5. (1) 実数体 $\mathbb{R}$ と複素数体 $\mathbb{C}$ を比べてみよう．同型写像 $f : \mathbb{C} \to \mathbb{R}$ が存在すると仮定しよう．$r = f(\sqrt{-1})$ とおくと，

$$r^2 = f(\sqrt{-1})^2 = f(-1) = -1$$

である．しかし，$r^2 = -1$ を満たす実数 r は存在しないので矛盾である．よって $\mathbb{C}$ と $\mathbb{R}$ の間には同型写像は存在しない．よって $\mathbb{C}$ と $\mathbb{R}$ は同型ではない．

(2) 次の行列の集合を考える．

$$D = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} : a, b \in \mathbb{R} \right\} \subset M_2(\mathbb{R}).$$

このとき，D は $M_2(\mathbb{R})$ の可換な部分環である（$M_2(\mathbb{R})$ 自身は非可換である）．今，写像 $\phi : \mathbb{C} \to D$ を

$$a + b\sqrt{-1} \mapsto \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

で定義する．ただし，$a, b \in \mathbb{R}$ である．すると，ϕ は同型写像である（確かめよ）．したがって，$\mathbb{C} \cong D$ が従う．

3.3 準同型定理

群で学習した準同型定理はそのまま環の準同型定理に拡張できる．

定理 3.3.1 (環の準同型定理)**.** R, S を可換環とする．任意の環準同型写像 $\phi : R \to S$ に対し，

$$\overline{\phi} : R/\mathrm{Ker}(\phi) \to \mathrm{Im}(\phi);\ a + \mathrm{Ker}(\phi) \mapsto \phi(a)$$

は well-defined な同型写像である．つまり，$R/\mathrm{Ker}(\phi) \cong \mathrm{Im}(\phi)$ である．特に，ϕ が全射の場合，$R/\mathrm{Ker}(\phi) \cong S$ が成り立つ．

Proof. 群の準同型定理の証明から，示すべきことは $\overline{\phi}$ が環準同型写像であること，特に，乗法に関する性質 (2) と乗法の単位元の性質 (3) だけである．任意の $x + \mathrm{Ker}(\phi), y + \mathrm{Ker}(\phi) \in R/\mathrm{Ker}(\phi)$ に対し，

$$\overline{\phi}((x + \mathrm{Ker}(\phi))(y + \mathrm{Ker}(\phi))) = \overline{\phi}(xy + \mathrm{Ker}(\phi)) = \phi(xy) = \phi(x)\phi(y) = \overline{\phi}(x + \mathrm{Ker}(\phi))\overline{\phi}(y + \mathrm{Ker}(\phi))$$

である．また

$$\overline{\phi}(1_R + \mathrm{Ker}(\phi)) = \phi(1_R) = 1_S$$

であるので，証明が完了した． □

準同型写像の使用例を紹介する．

例 3.3.2. $\mathbb{C}$ と $\mathbb{R}[x]/\langle x^2 + 1\rangle$ が同型であることを見る．まず，写像 $\phi : \mathbb{R}[x] \to \mathbb{C}$ を $f(x) \mapsto f(\sqrt{-1})$ で定義する．これは代入写像（を制限したもの）なので準同型写像である．また ϕ は全射である．実際，任意の $a + b\sqrt{-1} \in \mathbb{C}$（$a, b \in \mathbb{R}$）に対し，$f(x) = a + bx \in \mathbb{R}[x]$ とすると，$\phi(f(x)) = f(\sqrt{-1}) = a + b\sqrt{-1}$ であることから従う．さらに $\mathrm{Ker}(\phi) = \langle x^2 + 1\rangle$ である．実際，$\mathrm{Ker}(\phi)$ は $\sqrt{-1}$（と $-\sqrt{-1}$）を根に持つ $\mathbb{R}[x]$ の多項式全体の集合であることから従う．すると，準同型定理から

$$\mathbb{R}[x]/\langle x^2 + 1\rangle = \mathbb{R}[x]/\mathrm{Ker}(\phi) \cong \mathbb{C}$$

がわかる．

3.4 中国式剰余定理

群に関する中国式剰余定理を思い出そう．

定理 3.4.1 (中国式剰余定理 (群版))**.** m, n を互いに素な自然数とする．このとき,「群として」

$$\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

である．

「群として」と書いているのは，群では加法のみ考えていたので，乗法に関して同じ構造を持つかわからないからである．しかし，これは「環として」同型であると拡張できる．ここでは，中国式剰余定理をより一般の形で証明する．まずは「互いに素」という概念をイデアルに導入する．

定義 3.4.2. R を可換環とする．R のイデアル I, J が $I + J = R$ を満たすとき，I, J は**互いに素**であるという．

m, n が互いに素な自然数であれば，$m\mathbb{Z}$ と $n\mathbb{Z}$ は互いに素である．実際，m, n は互いに素なので，$am + bn = 1$ を満たす整数 $a, b \in \mathbb{Z}$ が存在する．したがって，$1 \in m\mathbb{Z} + n\mathbb{Z}$ がわかり，$m\mathbb{Z} + n\mathbb{Z} = \mathbb{Z}$ が従う．これを用いて中国式剰余定理を一般化する．

定理 3.4.3 (中国式剰余定理 (一般))**.** R を可換環とし，I, J を互いに素な R のイデアルとする．このとき，

$$R/IJ \cong R/I \times R/J$$

である．

この定理の証明のために次の補題を証明する．

補題 3.4.4. R を可換環とし，I, J を互いに素な R のイデアルとする．このとき，$IJ = I \cap J$ である．

Proof. $I \cap J = (I \cap J)R = (I \cap J)(I + J) \subset IJ \subset I \cap J$ から従う． □

定理 3.4.3 の証明. 補題 3.4.4 から $R/IJ = R/(I \cap J)$ である．今，写像 $f : R/(I \cap J) \to R/I \times R/J$ を

$$x + (I \cap J) \mapsto (x + I, x + J)$$

で定義する．これは well-defined な準同型写像である．実際，$x + (I \cap J) = y + (I \cap J)$ となる，$x, y \in R$ をとる．このとき，$x - y \in I \cap J$ である．したがって，$x + I = y + I$ かつ $x + J = y + J$ が成り立つ．よって $f(x + (I \cap J)) = (x + I, x + J) = (y + I, y + J) = f(y + (I \cap J))$ なので，f は well-defined である．また f が準同型写像であることは容易に示せる．

したがって，f が全単射であれば定理の主張が成り立つ．$x + (I \cap J) \neq y + (I \cap J)$ となる，$x, y \in R$ をとる．このとき，$x - y \notin I \cap J$ である．すると，$x - y \notin I$ または $x - y \notin J$ が成り立つ．つまり，$x + I \neq y + I$ または $x + J \neq y + J$ が成り立つので，

$$f(x + (I \cap J)) = (x + I, x + J) \neq (y + I, y + J) = f(y + (I \cap J))$$

である．よって，f は単射である．一方，任意の $(r + I, s + J) \in R/I \times R/J$ をとる．$I + J = R$ から $a + b = 1 \in R$ となる $a \in I$ と $b \in J$ が存在する．このとき，$x = rb + sa$ とすると，$x - r = rb + sa - r = r(1 - a) + sa - r = (s - r)a \in I$ から $r + I = x + I$ である．同様に，$s + J = x + J$ がわかる．したがって，

$$f(x + (I \cap J)) = (x + I, x + J) = (r + I, s + J)$$

であるので，f は全射である．

以上より，f は同型写像であるので，定理の証明が完了した． □

系 3.4.5 (中国式剰余定理（環論版）)**.** m, n を互いに素な自然数とする．このとき,「環として」

$$\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

である．

4　素因数分解と環の構造

情報数理 C では，次の 3 つの基本的な事実を学習した：

(1) 整数に対して「余りを考慮した割り算」が常に可能（剰余の定理）.

(2) 任意の $a_1, \dots, a_n \in \mathbb{Z}$ が生成するイデアルは，ある 1 つの整数によって生成される（単項イデアル性）.

(3) 任意の整数 n は素数の積に一意的に分解できる（素因数分解の一意性）.

これらの事実の間には密接な関係がある．実際，(1) の性質から (2) が導かれ，(2) が成り立つことで (3) も証明できる.

実は，これらの性質は整数環 $\mathbb{Z}$ に特有のものではなく，より一般の可換環でも類似の構造が存在する．たとえば，多項式環 $\mathbb{R}[x]$ においても，剰余の定理，単項イデアル性，および因数分解の一意性が成り立つことが知られている.

この節では，整数や多項式のように「余りを考慮した割り算」が可能な可換環を抽象的に定式化し，それらに共通する因数分解の構造を統一的に理解することを目指す.

4.1　ユークリッド整域

まず考える概念は「剰余の定理」，つまり「余りを考慮した割り算」を整域に導入することである．このような割り算の仕組みが備わっている整域をユークリッド整域という.

定義 4.1.1. 整域 R と関数 $\delta : R \setminus \{0\} \to \mathbb{Z}_{\geq 0}$ が以下の条件を満たすとき，組 (R, δ)（または単に R）を**ユークリッド整域**といい，関数 δ を**ユークリッド関数**という：元 $a \in R$ と元 $0 \neq b \in R$ に対し，元 $q, r \in R$ で条件

(1) $a = bq + r$,

(2) $r = 0$ または $\delta(r) < \delta(b)$

を満たすものが存在する.

例 4.1.2. $R = \mathbb{Z}$ とし $\delta(x) = |x|$ と定義すれば，δ の条件は剰余の定理に他ならない．よってこの関数のもと，$\mathbb{Z}$ はユークリッド整域である.

それでは体上の多項式環（例えば $\mathbb{R}[x]$）がユークリッド整域となることを見ていく．これは多項式環に対して剰余の定理が成り立つことを示せばよい.

定理 4.1.3. R を体とする．このとき，多項式 $f \in R[x]$ と多項式 $0 \neq g \in R[x]$ に対し，多項式 $q, r \in R[x]$ で条件

(1) $f = gq + r$,

(2) $\deg(r) < \deg(g)$

を満たすものが一意的に存在する.

Proof. $g = b_0 + b_1 x + \cdots + b_d x^d \in R[x]$ とする．ただし，$b_d \neq 0$ である．R は体であるので，b_d は単元である．つまり，b_d^{-1} が存在する.

（存在）$f = 0$ の場合は $r = q = 0$ とすればよいことに注意する（$\deg(0) = -\infty$ であった）．$\deg(g) = d = 0$ の場合は $q = b_0^{-1} g$ と $r = 0$ とすれば条件を満たす．$d \geq 1$ かつ $f \neq 0$ の場合を $e = \deg(f)$ に関する帰納法で証明する.

(i) $e < d$ の場合は $q = 0$ と $r = g$ とすれば条件を満たす．特に，$e = 0$ のときに成り立つ．
(ii) $e - 1$ まで正しいと仮定する．(i) より $e \geq d$ としてよい．今，$f = a_0 + a_1 x + \cdots + a_e x^e$ と表し，

$$h = f - a_e b_d^{-1} g x^{e-d}$$

とおく．このとき，右辺では x^e の項が消えるので，$\deg(h) \leq e - 1$ である．よって帰納法の仮定から

$$h = q_0 g + r_0, \deg(r_0) < \deg(g)$$

を満たす $q, r \in R[x]$ が存在する．このとき，

$$f = h + a_e b_d^{-1} g x^{e-d} = (q_0 + a_e b_d^{-1} x^{e-d}) g + r_0$$

であり，$\deg(r_0) < \deg(g)$ であったので，$q_0 + a_e b_d^{-1} x^{e-d}, r_0 \in R[x]$ は f に関して (1) と (2) の条件を満たす．よって e のときも成り立つことがわかった．

（一意性）多項式の組 (q, r) と (q', r') が f に関して条件 (1) と (2) を満たすとする．つまり，

$$f = gq + r, \deg(r) < \deg(g),$$
$$f = gq' + r', \deg(r') < \deg(g)$$

が成り立つとする．このとき，

$$(q - q')g = r' - r$$

となる．$q - q' \neq 0$ と仮定すると，

$$\deg(g) \leq \deg(g) + \deg(q - q') = \deg(g(q - q')) = \deg(r' - r) \leq \max(\deg(r), \deg(r'))$$

を得る．これは $\deg(r), \deg(r') < \deg(g)$ に矛盾する．よって $q - q' = 0$，つまり $q = q'$ となり，$r = r'$ も成り立つ．したがって，一意性が示された． □

系 4.1.4. R を体とし，関数 $\delta : R[x] \setminus \{0\} \to \mathbb{Z}_{\geq 0}$ を $\delta(f) = \deg(f)$ で定義する．このとき，$(R[x], \delta)$ はユークリッド整域である．

4.2 単項イデアル整域

次に全てのイデアルが単項イデアルとなる環を考えていこう．

定義 4.2.1. R を整域とする．R の任意のイデアルが単項イデアル，つまり，任意のイデアル $I \subset R$ に対し，ある元 $a \in R$ が存在して $I = \langle a \rangle = \{ax : x \in R\}$ と書けるとき，R を**単項イデアル整域**（Principal Ideal Domain, PID）という．

例えば，$\mathbb{Z}$ は単項イデアル整域である．実は，ユークリッド整域はいつでも単項イデアル整域である．

定理 4.2.2. ユークリッド整域は単項イデアル整域である．

Proof. (R, δ) を任意のユークリッド整域とし，I を R の任意のイデアルとする．もし $I = \{0\}$ なら $I = \langle 0 \rangle$ なので単項イデアルである．よって $I \neq \{0\}$ と仮定してよい．このとき，元 $a \in I \setminus \{0\}$ がとれることに注意する．すると $\emptyset \neq \delta(I \setminus \{0\}) \subset \mathbb{Z}_{\geq 0}$ であるので，$\delta(I \setminus \{0\})$ は最小値 d_0 を持つ．そこで $\delta(a) = d_0$ を満たす $a \in I \setminus \{0\}$ をとる．

$I = \langle a \rangle$ となることを示す．$a \in I$ とイデアルの性質より $\langle a \rangle \subset I$ が従う．そこで，$x \in I \setminus \langle a \rangle$ が存在したと仮定する．$a \neq 0$ であり，(R, δ) がユークリッド整域であるので，$q, r \in R$ を用いて $x = aq + r$ と書くこ

とができる．ただし，$r=0$ または $\delta(r)<\delta(a)$ である．もし $r=0$ ならば，$x=aq\in\langle a\rangle$ なので仮定に矛盾する．よって $r\neq 0$ かつ $\delta(r)<\delta(a)=d_0$ である．しかし，$0\neq r=x-aq\in I$ より，これは d_0 の最小性に矛盾する．以上より，$I=\langle a\rangle$ が従い，R は単項イデアル整域である． □

体 R に対し，$R[x]$ がユークリッド環となることから次の系が得られる．

系 4.2.3. R を体とする．このとき，$R[x]$ は単項イデアル整域である．

4.3 一意分解環

次に素因数分解を整域に導入する．まず素数の概念を拡張しよう．

定義 4.3.1. R を整域とする．

- $a,b\in R$ に対し，a は b を**割り切る**とは，$c\in R$ を用いて $b=ac$ と表せるときにいい，$a|b$ と表す．
- $a,b\in R$ が**同伴**であるとは，単元 $c\in R^\times$ を用いて $b=ac$ と書けるときにいい，$a\sim b$ と表す．
- $0\neq a\in R$ が**素元** (prime element) であるとは，イデアル $\langle a\rangle$ が素イデアルとなるときにいう．
- $0\neq a\in R$ が**既約元**であるとは，$a=bc$ ならば，b または c が単元となるときにいう．

次の命題を示しておく．

命題 4.3.2. R を整域とし，$0\neq a\in R$ をとる．

(1) a が素元であれば，a は既約元である．

(2) a が単元であれば，a は素元ではない．

Proof. (1) $a=bc$ と書けたとする．このとき，$bc\in\langle a\rangle$ であり，$\langle a\rangle$ は素イデアルであるので，b または c は $\langle a\rangle$ の元である．$b\in\langle a\rangle$ としよう．すると $x\in R$ を用いて $b=ax$ と書ける．よって

$$a=bc=axc$$

となる．R は整域なので，簡約律から $xc=1$ となる．これは c が単元であることを意味するので，a は既約元である．

(2) a が単元なら，a^{-1} が存在して，$1=a\cdot a^{-1}\in\langle a\rangle$ であり，$\langle a\rangle=R$ となるので，$\langle a\rangle$ は素イデアルではない．よって a は素元ではない． □

ここで既約元であるが素元ではない例を見ていこう．

例 4.3.3. $\mathbb{Z}[\sqrt{-5}]:=\{a+b\sqrt{-5}:a,b\in\mathbb{Z}\}$ を考える．これはガウス整数環と同様で $\mathbb{C}$ の部分環である．$\mathbb{Z}[\sqrt{-5}]$ において，2 が既約元であるが素元でないことを見る．素元でないことは，

$$6=(1+\sqrt{-5})(1-\sqrt{-5})\in\langle 2\rangle$$

かつ $1\pm\sqrt{-5}\notin\langle 2\rangle$ であることからわかる．2 が既約元であることを見ていこう．

$$2=(a+b\sqrt{-5})(c+d\sqrt{-5})$$

と書けたとし，$(a+b\sqrt{-5})(c+d\sqrt{-5})$ がともに単元でないと仮定する．両辺の共役をとると

$$2=(a-b\sqrt{-5})(c-d\sqrt{-5})$$

が得られるので，2 式の両辺をそれぞれ掛けると，

$$4=(a^2+5b^2)(c^2+5d^2)$$

となる．$a^2+5b^2=1$ であれば，$(a+b\sqrt{-5})(a-b\sqrt{-5})=a^2+5b^2=1$ となるため $a+b\sqrt{-5}$ が単元でないことに矛盾する．よって，$a^2+5b^2\neq 1$ である．同様に，$c^2+5d^2\neq 1$ となる．すると $a^2+5b^2=c^2+5d^2=2$ でないといけない．しかし，これを満たす $a,b,c,d\in\mathbb{Z}$ は存在しない．よって 2 は既約元となる．

それでは素因数分解の概念を環に拡張しよう．

定義 4.3.4. R を整域とする．0 でも単元でもない任意の R の元が，有限個の素元の積で表される（**素元分解**を持つ）とき，R を**一意分解整域** (Unique Factorization Domain, UFD) という．

まず一意分解整域において，素元分解は一意的な表示を持つことを示そう．

定理 4.3.5. R を一意分解整域とし，a を 0 でも単元でもない $a\in R$ をとる． このとき，a の素元分解は順番と同伴の差を除いて一意的である．つまり，素元 $p_1,\dots,p_s,q_1,\dots,q_t\in R$ を用いて

$$a=p_1\cdots p_s=q_1\cdots q_t$$

と表せたとき，$s=t$ であり，$p_1,\dots,p_s$ の順番を入れ替えると任意の $1\leq i\leq s$ に対して $p_i\sim q_i$ となる．

Proof. s に関する帰納法で示す．$s=1$ のとき，$a=p_1=q_1\cdots q_t$ である．p_1 は素元なので，既約元である．したがって，$t\geq 2$ ならば，q_1 または $q_2\cdots q_t$ は単元となる．すると，q_1 は素元であるので，$q_2\cdots q_t$ が単元となる．よってある $u\in R^\times$ を用いて $1=u(q_2\cdots q_t)=(uq_2\cdots q_{t-1})q_t$ と書けるが，q_t が単元となり矛盾する．したがって $t=1$ であり，特に，$p_1=q_1$ から $p_1\sim q_1$ である．

そこで $s\geq 2$ と仮定し，$s-1$ まで正しいとする．p_s は素元なので，$q_1\cdots q_t\in\langle p_s\rangle$ から $q_j\in\langle p_s\rangle$ となる j が存在する（演習問題）．$j=t$ としてよい．するとある元 $u\in R$ を用いて $q_t=up_s$ と表せる．q_t は既約元であるので，u または p_s が単元となるが，p_s が素元であるので，u が単元となる．よって $p_s\sim q_t$ である．また

$$p_1\cdots p_{s-1}p_s=q_1\cdots q_{t-1}up_s$$

であり，R が整域かつ $p_s\neq 0$ から簡約律により

$$p_1\cdots p_{s-1}=q_1\cdots q_{t-1}u=q_1\cdots q_{t-2}(uq_{t-1})$$

が得られる．ここで $\langle q_{t-1}\rangle=\langle uq_{t-1}\rangle$ である．実際，$\langle uq_{t-1}\rangle\subset\langle q_{t-1}\rangle$ は明らかであり，任意の $aq_{t-1}\in\langle q_{t-1}\rangle$ に対し，$aq_{t-1}=(au^{-1})(uq_{t-1})\in\langle uq_{t-1}\rangle$ である．よって，uq_{t-1} は素元である．すると，帰納法の仮定により，$s-1=t-1$，つまり $s=t$ であり，$p_1,\dots,p_{s-1}$ の順番を入れ替えると，$1\leq i\leq s-2$ に対して，$p_i\sim q_i$ かつ $p_{s-1}\sim uq_{t-1}\sim q_{t-1}$ となる．これに $p_s\sim q_t$ を追加することで，定理の主張が示された． □

実は単項イデアル整域であればいつでも一意分解整域である．

定理 4.3.6. 単項イデアル整域は一意分解整域である．

この証明のための準備をする．

補題 4.3.7. R を単項イデアル整域とする．このとき，$a \in R$ が素元であることと，a が既約元であることは同値である．

Proof. a が既約元のときに，素元となることを示せばよい．そのために，$\langle a \rangle$ が極大イデアルとなることを示す．$\langle a \rangle \subset I \subsetneq R$ となるイデアル I をとる．R は単項イデアル整域であるので，単元ではない元 $d \in R$ を用いて $I = \langle d \rangle$ と書ける．すると $a \in I$ なので，$u \in R$ を用いて $a = ud$ と書ける．このとき，a は既約元であるので，u または d は単元であるが，d は単元でないので u が単元となる．よって $d = au^{-1}$ と書ける．今，任意の $x \in I$ をとると，ある $y \in R$ を用いて $x = dy$ と書ける．このとき，

$$x = dy = (au^{-1})y = a(u^{-1}y) \in \langle a \rangle$$

であるので $\langle a \rangle = I$ が成り立つ．よって $\langle a \rangle$ は極大イデアルである．特に素イデアルとなるので，a は素元である． □

補題 4.3.8. R を単項イデアル整域とし，R のイデアルの無限昇鎖列

$$I_1 \subset I_2 \subset I_3 \subset$$

を考える．このとき，ある整数 n が存在して

$$I_n = I_{n+1} = I_{n+2} = \cdots$$

となる．つまり，R のイデアルの無限昇鎖列は必ず停止する．

Proof. $I = \bigcup_{k=1}^{\infty} I_k$ とおく．このとき，I は R のイデアルである（演習問題）．R は単項イデアル整域であるので，ある元 d を用いて $I = \langle d \rangle$ と書ける．このとき，$d \in I$ なので，ある整数 n で $d \in I_n$ となるものが存在する．よって

$$I = \langle d \rangle \subset I_n \subset I_{n+1} \subset I_{n+2} \subset \cdots \subset I$$

より，

$$I_n = I_{n+1} = I_{n+2} = \cdots$$

が従う． □

それでは定理 4.3.6 を証明しよう．

定理 4.3.6 の証明. R を単項イデアル整域とし，$a \in R$ を 0 でも単元でもない元とする．補題 4.3.7 より a が有限個の既約元の積で表せることを示せばよい．a が有限個の既約元の積で表せないと仮定する．すると，a は既約元ではないので，$a = bc$ で b も c も単元とならないものが存在する．このとき，$b, c \neq a$ である．すると

$$\langle a \rangle \subsetneq \langle b \rangle, \langle c \rangle$$

が成り立つ．もし b と c がともに既約元の積で表せると，a が既約元の積で表せないことに矛盾する．そこで $a_1 = b$ が既約元の積で表せないとする．すると同様の議論により，既約元の積で表せない元 a_2 が存在して

$$\langle a \rangle \subsetneq \langle a_1 \rangle \subsetneq \langle a_2 \rangle$$

が成り立つ．これを繰り返すと R のイデアルの真の無限昇鎖列

$$\langle a \rangle \subsetneq \langle a_1 \rangle \subsetneq \langle a_2 \rangle \subsetneq \langle a_3 \rangle \subsetneq$$

が得られるが，補題 4.3.8 に矛盾する．よって a が有限個の既約元の積で表せることがわかり，R が一意分解整域であることが従う． □

系 4.3.9. R を体とする．このとき，$R[x]$ は一意分解整域である．

したがって，$\mathbb{R}[x]$ は一意分解整域であるので，因数分解の一意性がわかる．最後に，かなり非自明な一意分解整域の例を見る．

定理 4.3.10. ガウス整数環 $\mathbb{Z}[\sqrt{-1}]$ は一意分解整域である．

この証明のために，$\mathbb{Z}[\sqrt{-1}]$ がユークリッド整域となることを示す．そのためには，ユークリッド関数を定義する必要がある．関数 $N : \mathbb{Z}[\sqrt{-1}] \to \mathbb{Z}_{\geq 0}$ を $N(a+b\sqrt{-1}) = a^2+b^2$ で定義する．これを $\mathbb{Z}[\sqrt{-1}]$ の**ノルム**という．定義から $x \in \mathbb{Z}[\sqrt{-1}]$ に対し，$N(x) = x\overline{x} = |x|^2$ である．ここで，$\overline{x}$ は x の複素共役である．この N がユークリッド関数の条件を満たしていればよい．

補題 4.3.11. $x, y \in \mathbb{Z}[\sqrt{-1}]$（$y \neq 0$）に対し，

$$x = yq + r \text{ かつ } N(r) < N(y)$$

を満たす $q, r \in \mathbb{Z}[\sqrt{-1}]$ が存在する．

Proof. $\dfrac{x}{y}$ を実数化したとき $\alpha+\beta\sqrt{-1}$ となったとする．ここで，$\alpha, \beta \in \mathbb{R}$ である．また $|\alpha - a|, |\beta - b| \leq \dfrac{1}{2}$ となる整数 $a, b \in \mathbb{Z}$ をとり，$q = a + b\sqrt{-1}$ とおく．このとき，$q \in \mathbb{Z}[\sqrt{-1}]$ であり，さらに

$$\left|\frac{x}{y} - q\right|^2 = (\alpha - a)^2 + (\beta - b)^2 \leq \frac{1}{4} + \frac{1}{4} < 1$$

である．$r = x - yq$ とおくと，$r \in \mathbb{Z}[\sqrt{-1}]$ かつ $x = yq + r$ である．すると，

$$N(r) = |r|^2 = |x - yq|^2 = |y|^2 \cdot \left|\frac{x}{y} - y\right|^2 < |y|^2 = N(y)$$

である．よって補題の主張が成り立つことがわかった． □

したがって，この補題により，$(\mathbb{Z}[\sqrt{-1}], N)$ がユークリット整域となることがわかるので，定理 4.3.10 が従う．

4.4 一意分解整域上の多項式環

系 4.3.9 のおかげで，$\mathbb{R}[x]$ が一意分解整域であることがわかったが，$\mathbb{R}[x, y]$ の場合はどうであろうか．他にも $\mathbb{Z}[x]$ の場合はどうであろうか．$\mathbb{R}[x]$ や $\mathbb{Z}$ は体ではないため，系 4.3.9 が使えない．しかし実は次の定理からこれらが一意分解整域であることがわかる．

定理 4.4.1. R が一意分解整域ならば，$R[x]$ も一意分解整域である．

よって，$\mathbb{R}[x]$ および $\mathbb{Z}$ はそれぞれ一意分解整域であったので，$\mathbb{R}[x, y] = (\mathbb{R}[x])[y]$ と $\mathbb{Z}[x]$ も一意分解整域となることがわかる．この定理の証明には少し準備が必要である．まず，整域 R は一般には体ではないが，R から体を作ることができる．例えば，$\mathbb{Z}$ は体ではないが，$\mathbb{Z}$ から $\mathbb{Q}$ を同値関係を使って構成していたことを思い出そう（情報数理 B11 回目）．それを一般の整域で行う．

R を整域とし，$R^* = R \setminus \{0\}$ とする．直積集合 $R \times R^*$ 上の二項関係 $\sim$ を以下で定義する．

$$(p_1, q_1) \sim (p_2, q_2) \overset{\text{def}}{\Leftrightarrow} p_1 \cdot q_2 = p_2 \cdot q_1$$

この $\sim$ は同値関係である．各 $(p,q) \in R \times R^*$ に対し，同値類 $[(p,q)]_\sim$ を $\dfrac{p}{q}$ と表記し，その商集合を K と表す．つまり，

$$K := \left\{ \frac{p}{q} : p, q \in R, q \neq 0 \right\}$$

である．今，集合 K 上に演算 $+_K$ と $\cdot_K$ を次で定義する：

$$\frac{p_1}{q_1} +_K \frac{p_2}{q_2} = \frac{p_1 q_2 + p_2 q_1}{q_1 q_2}$$
$$\frac{p_1}{q_1} \cdot_K \frac{p_2}{q_2} = \frac{p_1 p_2}{q_1 q_2}$$

この演算は well-defined であり，以降は単に $+$ と $\cdot$ で書く．

命題 4.4.2. $(K, +, \cdot)$ は体である．また R の各元 $a \in R$ を $\dfrac{a}{1} \in K$ と同一視することで，R は K の部分環として見なせる．

Proof. 証明略. □

整域 R に対し，上記の体 K を $K(R)$ で表し，R の**商体**という．複雑に書いたが，結局，商体とは整域の元を使って分数を作り，その分数を集めたものである．こうすることで，整域の中では乗法の逆元を持たない元に無理やり逆元を作ることができる．つまり，足りない乗法の逆元を加えた集合が商体である．

ここからは一意分解整域のみを考える．

定義 4.4.3. R を一意分解整域とし，$a_1, \ldots, a_n \in R$ の少なくとも 1 個は 0 でないとする．

(1) $d \in R$ は，各 i に対し，$d | a_i$ を満たすとき，$a_1, \ldots, a_n$ の**公約元**という．

(2) $a_1, \ldots, a_n$ の公約元 $g \in R$ は，任意の $a_1, \ldots, a_n$ の公約元 d に対し，$d | g$ を満たすとき，$a_1, \ldots, a_n$ の**最大公約元**といい，$\gcd(a_1, \ldots, a_n)$ で表す．

(3) $\gcd(a_1, \ldots, a_n) = 1$ のとき，$a_1, \ldots, a_n$ は**互いに素**という．

まずは最大公約元がいつでも存在し，それが同伴の差を除いて一意的であることを示そう．

命題 4.4.4. R を一意分解整域とし，$a_1, \ldots, a_n \in R$ の少なくとも 1 個は 0 でないとする．このとき， $\gcd(a_1, \ldots, a_n)$ は同伴の差を除いて一意的に存在する．

Proof. $a_1, \ldots, a_m \neq 0, a_{m+1} = \cdots = a_n = 0$ としてよい．R は一意分解整域なので，各 $1 \leq i \leq m$ に対し，

$$a_i = u_i \prod_{j=1}^{k} p_j^{r_{ij}}$$

と表すことができる．ただし，$u_i \in R^\times$ で $p_1, \ldots, p_k$ は $a_1 \ldots, a_m$ の素元分解に現れる全ての素元である．a_i が単元の場合は単に $a_i = u_i$ である．今，

$$g := \prod_{j=1}^{k} p_j^{\min(r_{1j}, \ldots, r_{mj})}$$

とすると，任意の i に対し，$g | a_i$ である．また，$b \in R$ が $a_1, \ldots, a_n$ の任意の公約元とする．このとき，

$$b = v \prod_{j=1}^{k} p_j^{s_j}$$

と書ける．ただし，$v \in R^\times$ である．すると，任意の i に対し，$b|a_i$ より

$$s_j \leq \min(r_{1j}, \ldots, r_{mj})$$

が各 j に対して成り立つ．よって $b|g$ である．これは $\gcd(a_1, \ldots, a_n) = g$ を意味するので，存在が言えた．

最後に一意性を示す．g, g' をともに，$a_1, \ldots, a_n$ の最大公約元とする．すると g の最大公約元の性質から $g'|g$ が成り立つ．したがって，ある $a \in R$ を用いて $g = ag'$ と書ける．同様に，$g'|g$ も成り立つのである $b \in R$ を用いて $g' = bg$ と書ける．すると，

$$g = ag' = abg$$

であるので，$g \neq 0$ かつ R が整域であることから，簡約律により $ab = 1$，つまり a は単元であるので，$g \sim g'$ が従う．よって最大公約元の一意性が言えた． □

系 4.4.5. $a_1, \ldots, a_n$ が互いに素であることと，$\gcd(a_1, \ldots, a_n)$ が単元であることは同値である．

それでは多項式環の話に入っていこう．

定義 4.4.6. R を一意分解整域とする．多項式 $f = a_0 + a_1 x + \cdots + a_n x^n \in R[x]$ が**原始的**であるとは，$\gcd(a_0, \ldots, a_n) = 1$ となるときにいう．

原始的多項式について次の命題を証明する．

命題 4.4.7 (ガウスの補題)**.** R を一意分解整域，$K = K(R)$，$f = a_0 + a_1 x + \cdots + a_n x^n, g = b_0 + b_1 x + \cdots + b_m x^m \in R[x]$ とする．

(1) f, g が原始的なら fg も原始的である．

(2) f が原始的であり，多項式環 $K[x]$ において $f|g$ ならば，$R[x]$ においても $f|g$ である．

Proof. (1) fg が原始的でないなら，fg の係数の最大公約元は単元ではない，つまり R の素元 p を選んで fg の全ての係数を割ることができる（命題 4.4.4 の証明参照）．一方，f は原始的であるので，$a_0, \ldots, a_n$ の中で p で割り切れないものが存在する．そのうち添え字が最小なものを r とする．同様に，$b_0, \ldots, b_m$ の中で p で割り切れないもののうち添え字が最小なものを s とする．今，fg の $r + s$ 次の係数を考えると

$$a_0 b_{r+s} + \cdots + a_{r-1} b_{s+1} + a_r b_s + a_{r+1} b_{s-1} + \cdots + a_{r+s} b_0$$

である．ただし，定義されていない a_i, b_j は 0 とする．このとき，r, s の定義から $a_r b_s$ を除いて，全ての項は p で割り切れる．しかし，p は素元であるので $a_r b_s$ は p で割り切れない．したがって，この係数は p で割り切れなくなり矛盾する．よって fg は原始的である．

(2) $g \neq 0$ としてよい．仮定から

$$h = \frac{p_0}{q_0} + \frac{p_0}{q_1} x + \cdots + \frac{p_\ell}{q_\ell} x^\ell \in K[x], p_i, q_j \in R, q_j \neq 0$$

を用いて $g = fh$ と書ける．この h が $R[x]$ の多項式として見なせることがわかればよい．$c = q_1 \cdots q_\ell$ とすると，ch は $R[x]$ の多項式として見なせることができる．この ch の係数の最大公約元を d とする．このとき，$ch = dt$ となる $t \in R[x]$ がとれ，t は原始的である．(1) から ft は原始的であるので，$cg = cfh = dft$ から d は dft の係数の最大公約元であり，c が dft の係数の公約元であることがわかる．すると，$c|d$ が得られるので，$h = \dfrac{d}{c} t \in R[x]$ が従う． □

それでは定理 4.4.1 を示す．

定理 4.4.1 の証明. 定数ではない原始的多項式 $f \in R[x]$ が $R[x]$ において素元分解を持つことを示せば十分である．実際，原始的でない多項式は原始的多項式に素元がかけられているだけである．

$K = K(R)$ とすると，系 4.3.9 より $K[x]$ は一意分解整域である．すると f は $K[x]$ の多項式として素元分解

$$f = h_1 \cdots h_n, h_i \in K[x]$$

を持つ．各 i に対し，c_i を h_i の係数の分母の積とし，$c_i h_i \in R[x]$ の係数の最大公約元を d_i とすれば，原始的多項式 $f_i \in R[x]$ を選んで，$c_i h_i = d_i f_i$ となるようにできる．したがって

$$f \cdot \prod_{i=1}^{n} c_i = \prod_{i=1}^{n} d_i \cdot \prod_{i=1}^{n} f_i$$

である．f_i は全て原始的であるので，ガウスの補題 (1) から $\prod_{i=1}^{n} f_i$ も原始的であり，$d := \prod_{i=1}^{n} d_i$ が $\prod_{i=1}^{n} d_i \cdot \prod_{i=1}^{n} f_i$ の係数の最大公約元となる．一方，f は原始的であるから，$c := \prod_{i=1}^{n} c_i$ は $f \cdot \prod_{i=1}^{n} c_i$ の係数の最大公約元である．すると，c, d は R の元として同伴であるので，単元 $u \in R^\times$ を用いて $d = uc$ と書ける．したがって，$fc = uc \prod_{i=1}^{n} f_i$ となるが，$R[x]$ は整域なので，簡約律から $f = u \prod_{i=1}^{n} f_i$ が得られる．したがって，各 f_i が $R[x]$ において素元であれば f は $R[x]$ において素元分解を持つことになり証明が終了する．f_i と h_i は $K[x]$ において同伴であるので，$K[x]$ のイデアルとして等式 $f_i K[x] = h_i K[x]$ を得る．よって h_i が $K[x]$ の素元であることから f_i も $K[x]$ の素元である．今，$I = f_i R[x]$ とし，$ab \in I$ を満たす $a, b \in R[x]$ をとる．このとき，$R[x]$（および $K[x]$）において $f_i | ab$ であるが，$(I \subset) f_i K[x]$ が素イデアルであるので，$K[x]$ において $f_i | a$ または $f_i | b$ が成り立つ．$f_i | a$ としよう．するとガウスの補題 (2) より $R[x]$ においても $f_i | a$ である．したがって I が素イデアルであることがわかったので，f_i は $R[x]$ において素元である． □

4.5 環の階層構造

ここまでの議論から，次のような整域の階層関係が成り立つことがわかった：

$$\text{ユークリッド整域} \Rightarrow \text{単項イデアル整域} \Rightarrow \text{一意分解整域（} \Rightarrow \text{整域）}$$

このような階層構造を理解する上で重要なのは,「逆が成り立つかどうか」を検討することである．すなわち，2 つの概念の間に真の包含関係があるのか，それとも同値であるのかを見極めるためには，次のような「反例」を探すことが鍵となる：

(1) 一意分解整域ではない整域,

(2) 単項イデアル整域ではない一意分解整域,

(3) ユークリッド整域ではない単項イデアル整域.

このうち，(1) の例としては $\mathbb{Z}[\sqrt{-5}]$ がよく知られており，(2) の例には $\mathbb{Z}[x]$ や $\mathbb{R}[x, y]$ が挙げられる．いずれも実際に多項式やイデアルを扱ってみることで，これらの環が該当することを確認できる．

しかし，(3) のように「ユークリッド整域ではない単項イデアル整域」の例を見つけることは非常に困難である．実際，そのような例として最も有名なのが，次の複素数体 $\mathbb{C}$ の部分環である：

$$R = \mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right] := \left\{a + b\frac{1+\sqrt{-19}}{2} : a, b \in \mathbb{Z}\right\}$$

この環 R は単項イデアル整域であるが，ユークリッド整域ではないことが知られている．ただし，その証明は代数的整数論やイデアル類群の理論を要し，本講義の範囲を超えるため，ここでは紹介のみにとどめる．

このように，反例の存在を通じて構造の違いを把握することは，可換環論の理解を深めるうえで非常に有用である．