# 代数学入門　2023 年度後期

コスキヴィルタ・ジャンステファン

埼玉大学

## 目次

1 **整数の性質** 5
- 1.1 割り算と余り . . . 5
- 1.2 ユークリッドの互除法 . . . 5
- 1.3 互いに素な整数 . . . 6
- 1.4 素因数分解 . . . 7
- 1.5 合同式 . . . 8
- 1.6 オイラー関数 . . . 9
- 1.7 フェルマーの小定理・ウイルソンの定理 . . . 11

2 **群論** 12
- 2.1 群の定義 . . . 12
- 2.2 準同型 . . . 15
- 2.3 剰余類 . . . 17
- 2.4 正規部分群・剰余群 . . . 18
- 2.5 可解群 . . . 21
- 2.6 シローの定理 . . . 22

3 **可換環** 23
- 3.1 定義 . . . 23
- 3.2 イデアル . . . 25
- 3.3 可換体の準同型定理 . . . 26
- 3.4 素元, 既約元 . . . 28

4 **体論** 31
- 4.1 代数的拡大 . . . 31
- 4.2 代数的閉体 . . . 33
- 4.3 $K$-準同型, $K$-自己同型 . . . 34
- 4.4 代数的閉包 . . . 36
- 4.5 ガロア拡大 . . . 38
- 4.6 ガロア理論の主定理 . . . 39
- 4.7 円分体多項式 . . . 42
- 4.8 ディリクレの弱定理 . . . 44
- 4.9 円分体 . . . 45
- 4.10 ガロアの逆問題 . . . 46

5 **加群** 47
5.1 定義 . . . . . 47
5.2 $A$ 加群の準同型写像 . . . . . 48
5.3 部分加群の和, イデアルと部分加群の積 . . . . . 48
5.4 加群の直積, 加群の直和 . . . . . 49
5.5 自由加群 . . . . . 50
5.6 階数 . . . . . 51
5.7 単項イデアル整域上の加群 . . . . . 52
5.8 線形代数学への応用 . . . . . 54

# 数学記号一覧

| | 記号 | 説明 |
|---|---|---|
| **数論** | $a \equiv b \pmod{n}$ | $n$ を法とし $a$ が $b$ と合同である |
| | $a \mid b$ | $a$ が $b$ を割り切る |
| | $\varphi(n)$ | オイラー関数 |
| | $n\mathbb{Z}$ | $n$ の倍数全体の集合 |
| | $\gcd(a, b)$ | $a$ と $b$ の最大公約数 |
| | $\mathrm{lcm}(a, b)$ | $a$ と $b$ の最小公倍数 |
| **集合論** | $\emptyset$ | 空集合 |
| | $X \setminus Y$ | $X$ から $Y$ を引いた差集合 |
| | $\lvert X \rvert$ | 集合 $X$ の元の個数 |
| | $\mathrm{id}_X$ | 集合 $X$ の恒等写像 |
| | $f \circ g$ | 写像 $f, g$ の合成写像 |
| | $f^{-1}$ | 全単射 $f\colon X \to Y$ の逆写像 |
| | $f^{-1}(A)$ | 写像 $f$ による集合 $A$ の逆像 |
| | $\bigsqcup_{i \in I} X_i$ | 共通部分のない和集合 |
| **線形代数** | $\det(A)$ | 行列 $A$ の行列式 |
| | $\chi_A(X)$ | 行列 $A$ の固有多項式 |
| | $\mu_A(X)$ | 行列 $A$ の最小多項式 |
| | $E_n$ | $n$ 次正方単位行列 |
| | $\mathrm{Span}(u_1, \ldots, u_n)$ | ベクトル $u_1, \ldots, u_n$ の線形結合全体のなす部分空間 |
| | $\mathrm{M}_n(R)$ | 可換環 $R$ の元を成分とする $n$ 次正方行列全体の集合 |
| | $\mathrm{Mat}_{\mathcal{B},\mathcal{C}}(f)$ | 基底 $\mathcal{B}$ と $\mathcal{C}$ に関する線形写像 $f\colon V \to W$ の行列 |
| | $\mathrm{Mat}_{\mathcal{B}}(f)$ | 基底 $\mathcal{B}$ に関する線形変換 $f\colon V \to V$ の行列 |
| | $\mathrm{GL}_n(K)$ | 可換体 $K$ の元を成分とする $n$ 次正則行列全体のなす群 |
| | $C(P)$ | 多項式 $P$ の同伴行列 |
| **群論** | $\langle x \rangle$ | $x$ で生成される巡回部分群 |
| | Ker | 準同型の核 |
| | Im | 準同型の像 |
| | $x^{-1}$ | $x$ の逆元 |
| | $Z(G)$ | 群 $G$ の中心 |
| | $xH$ | 部分群 $H$ による $x$ の左剰余類 |
| | $Hx$ | 部分群 $H$ による $x$ の右剰余類 |
| | $G/H$ | 部分群 $H$ による $G$ の左剰余類全体の集合 (または剰余群) |
| | $H\backslash G$ | 部分群 $H$ による $G$ の右剰余類全体の集合 |
| | $H \triangleleft G$ | $H$ が $G$ の正規部分群であることを意味する記号 |
| | $G \times H$ | $G$ と $H$ の直積 |
| | $\mathrm{Aut}(G)$ | $G$ の自己同型群 |
| | $N_G(H)$ | $G$ における部分群 $H$ の正規化群 |
| | $[G : H]$ | 部分群 $H$ の $G$ における指数 |
| | $\mathfrak{S}_n$ | $n$ 次対称群 |
| | $\mathfrak{A}_n$ | $n$ 次交代群 |

| | | |
|---|---|---|
| | $(a_1 \cdots a_k)$ | 長さ $k$ の巡回置換 |
| | $n_p$ | $p$ シロー部分群の個数 |
| | $\mathbb{Z}/n\mathbb{Z}$ | $n$ を法とする剰余類群 |
| | $(\mathbb{Z}/n\mathbb{Z})^\times$ | 剰余環 $\mathbb{Z}/n\mathbb{Z}$ の乗法群 |
| | $\mathrm{ord}(x)$ | $x$ の位数 |
| **可換環論** | $A[X]$ | $A$ 係数多項式全体のなす環 |
| | $\deg(P)$ | 多項式 $P$ の次数 |
| | $A[X_1, \ldots, X_n]$ | $A$ 係数の多変数多項式間 |
| | $A^\times$ | 可換環 $A$ の乗法群 |
| | $\mathrm{Frac}(A)$ | $A$ の商体 |
| | $A/I$ | イデアル $I$ による $A$ の剰余環 |
| | $\mathrm{char}(A)$ | 可換環 $A$ の標数 |
| | $c(P)$ | 多項式 $P(X)$ の内容 |
| | $P'(X)$ | 多項式 $P(X)$ の微分多項式 |
| **体論** | $L/K$ | 体拡大 $K \subset L$ |
| | $K(\alpha_1, \ldots, \alpha_n)$ | $\alpha_1, \ldots, \alpha_n$ で生成される拡大 |
| | $K[\alpha_1, \ldots, \alpha_n]$ | $\alpha_1, \ldots, \alpha_n$ で生成される $K$ 代数 |
| | $\mathrm{Gal}(L/K)$ | ガロア拡大 $L/K$ のガロア群 |
| | $[L : K]$ | 体拡大 $L/K$ の次数 |
| | $\mu_{\alpha,K}$ | $\alpha$ の $K$ 上の最小多項式 |
| | $\mathrm{Aut}_K(L)$ | 拡大 $L/K$ の $K$-自己同型全体のなす群 |
| | $\overline{\mathbb{Q}}$ | 代数的数全体の集合 |
| | $\overline{K}$ | $K$ の代数的閉包 |
| | $L^H$ | $H$ の固定体 |
| | $\Phi_n(X)$ | $n$ 次円分多項式 |
| | $\mu_n$ | 1 の $n$ 乗根全体の集合 |
| | $\zeta_n$ | $\exp\left(\frac{2i\pi}{n}\right)$ |
| | $F_n$ | 円分体 $\mathbb{Q}(\zeta_n)$ |
| **加群** | $M_1 \oplus M_2$ | 加群 $M_1$, $M_2$ の直和 |
| | $\bigoplus_{i \in I} M_i$ | 加群 $(M_i)_{i \in I}$ の直和 |
| | $\prod_{i \in I} M_i$ | 加群 $(M_i)_{i \in I}$ の直積 |
| | $A^I$ | $\prod_I A$ |
| | $A^{(I)}$ | $\bigoplus_I A$ |
| | $\mathrm{Ann}(x)$ | $x$ の零化イデアル |
| | $M_{\mathrm{tor}}$ | 加群 $M$ のねじれ部分加群 |
| **解析** | $\lim$ | 極限 |

# 1　整数の性質

## 1.1　割り算と余り

自然数, 整数全体の集合をそれぞれ以下のように表す.

$$\mathbb{N} = \{1, 2, 3, \dots\}$$
$$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}.$$

**定理 1.1: (割り算の定理)**　任意の $a, b \in \mathbb{Z}$ $(b > 0)$ に対し,

$$a = bq + r, \quad q \in \mathbb{Z},\ 0 \leq r < b$$

と一意的に書くことができる.

**証明**

- まず, $q, r$ の存在性を示す. $q$ を $\frac{a}{b}$ 以下の最大の整数とする. このとき, $0 \leq \frac{a}{b} - q < 1$ であるので, $0 \leq a - bq < b$ である. ゆえに, $r = a - bq$ とおけば良い.
- $q, r$ の一意性を示す. $a = bq + r = bq' + r'$ を満たす $q, q' \in \mathbb{Z}$, $r, r' \in \{0, \dots, b-1\}$ を考える. このとき, $b(q - q') = r' - r$ である. また, 仮定より $|r - r'| < b$ である. よって, $|b(q - q')| < b$ となり, $|q - q'| < 1$ がいえる. よって, $q = q'$, $r = r'$ が成り立つ.

$a, b$ を整数とする. $b = ac$ となる $c \in \mathbb{Z}$ が存在するとき, $b$ が $a$ の倍数である (または, $a$ が $b$ の約数である) といい, $a \mid b$ と表す. 整数 $a$ に対し, $a$ の倍数全体の集合を $a\mathbb{Z}$ と表す. すなわち,

$$a\mathbb{Z} = \{ak \mid k \in \mathbb{Z}\}.$$

## 1.2　ユークリッドの互除法

$a, b$ を自然数し, $a$ と $b$ の最大公約数を $\gcd(a, b)$ と表す. 以下, 最大公約数を計算するユークリッドの互除法と呼ばれるアルゴリズムを説明する. 有限列 $(a_n)_n$, $(b_n)_n$ を帰納法的に作る. まず,

$$b_0 := b$$
$$a_0 := a$$

とおく. 次に, $n \geq 0$ に対し $a_n$ 及び $b_n$ を作ったとし, $a_{n+1}$ と $b_{n+1}$ を次のように定める. $b_n$ を $a_n$ で割った余りを $a_{n+1}$ とおく. すなわち,

$$b_n = q_n a_n + a_{n+1}, \quad 0 \leq a_{n+1} < a_n$$

である. また, $b_{n+1} := a_n$ と定める. $0 \leq a_{n+1} < a_n$ であるので, 有限回のステップで $a_N = 0$ となる. このとき, 上のアルゴリズムが終了する.

**例 1.2.** $a = 33$, $b = 54$ とする.

$$54 = 1 \times 33 + 21$$
$$33 = 1 \times 21 + 12$$
$$21 = 1 \times 12 + 9$$
$$12 = 1 \times 9 + 3$$
$$9 = 3 \times 3 + 0$$

**定理 1.3**　$a, b$ を自然数とする．以下が成り立つ

(1) $a_0 > a_1 > \cdots > a_{N-1} > a_N = 0$ $(N \geq 1)$ である．

(2) 全ての $n \geq 1$ に対し $\gcd(a_n, b_n) = \gcd(a, b)$ である．

(3) $\gcd(a, b) = a_{N-1}$ である．

(4) $\gcd(a, b) = au + bv$ を満たす整数 $u, v$ が存在する．

**証明**

- (1) は明らかである．
- (2) を示す．$b_n = q_n a_n + a_{n+1}$ と書ける．よって，$d$ が $a_n$ と $a_{n+1}$ の公約数ならば，$d \mid b_n$ である．同様に，$a_{n+1} = b_n - q_n a_n$ であるので，$b_n$ と $a_n$ の任意の公約数は $a_{n+1}$ の約数である．ゆえに，

$$\{a_n \text{ と } b_n \text{ の公約数 }\} = \{a_{n+1} \text{ と } a_n \text{ の公約数 }\}$$

とくに，$\gcd(a_n, b_n) = \gcd(a_{n+1}, a_n) = \gcd(a_{n+1}, b_{n+1})$ である．したがって，$\gcd(a_n, b_n) = \gcd(a_0, b_0) = \gcd(a, b)$ である．
- (3) を示す．$a_N = 0$ とする．このとき，$b_{N-1} = q_{N-1} a_{N-1}$ である．ゆえに，$\gcd(a, b) = \gcd(a_{N-1}, b_{N-1}) = a_{N-1}$ である．
- (4) を示す．帰納法によって，$a_n = au_n + bv_n$ を満たす $u_n, v_n$ が存在することを示す．$n = 0$ のとき，$u_0 = 1$, $v_0 = 0$ とおけば良い．$n = 1$ のとき，$a_1 = b - aq_0$ と書けるので，$u_0 = -q_0$, $v_0 = 1$ とおけば良い．$n \geq 1$ とし，$a_n = au_n + bv_n$ とする．このとき，

$$\begin{aligned} a_{n+1} &= b_n - q_n a_n \\ &= a_{n-1} - q_n a_n \\ &= au_{n-1} + bv_{n-1} - q_n(au_n + bv_n) \\ &= a(u_{n-1} - q_n u_n) + b(v_{n-1} - q_n v_n) \end{aligned}$$

である．よって，全ての $n \geq 1$ に対し，$a_n = au_n + bv_n$ を満たす $u_n, v_n$ が存在する．とくに，$\gcd(a, b) = a_{N-1} = au_{N-1} + bv_{N-1}$ となる．

## 1.3　互いに素な整数

**定義 1.4**　$a, b \in \mathbb{Z}$ が互いに素であるとは，$ax + by = 1$ を満たす $x, y \in \mathbb{Z}$ が存在するときにいう．

**補題 1.5**　$a, b \in \mathbb{Z}$ $(a \neq 0, b \neq 0)$ に対し，

$$a \text{ と } b \text{ が互いに素である} \iff \gcd(a, b) = 1$$

が成り立つ．

**証明**

- 「$\Longrightarrow$」を示す．$ax + by = 1$ を満たす $x, y \in \mathbb{Z}$ を考える．$d \geq 1$ が $a, b$ の公約数ならば，$d$ が $ax + by = 1$ を割り切るので，$d = 1$ となる．
- 「$\Longleftarrow$」を示す．$1 = \gcd(a, b)$ であるとする．ユークリッドの互除法より，$1 = ax + by$ となる $x, y$ が存在する．

**命題 1.6**　$a, b, c$ を 0 でない整数とし, $\gcd(a, b) = 1$ とする. このとき,
(1) $a \mid bc$ ならば $a \mid c$ である.
(2) $a \mid c$ かつ $b \mid c$ ならば, $ab \mid c$ である.

**証明**

- (1) を示す. 仮定より $ax + by = 1$ となる $x, y \in \mathbb{Z}$ が存在する. よって, $c = axc + bcy$ となる. $a \mid bc$ より, $a$ が $axc + bcy$ を割り切る. ゆえに, $a \mid c$ である.
- (2) を示す. $c = ak$ $(k \in \mathbb{Z})$ と書ける. $b \mid c$ であるので, (1) より $b \mid k$ である. ゆえに, $k = br$ $(r \in \mathbb{Z})$ と表すことができる. したがって, $c = ak = abr$ となり, $ab \mid c$ である.

**命題 1.7**　$a, b, c \in \mathbb{Z}$ を 0 でない整数とし, $\gcd(a, b) = 1$ かつ $\gcd(a, c) = 1$ とする. このとき, $\gcd(a, bc) = 1$ である.

**証明**

$ax + by = 1$, $ax' + cy' = 1$ を満たす整数 $x, y, x', y'$ が存在する. ゆえに,

$$1 = (ax + by)(ax' + cy') = a(a'xx' + cxy' + byx') + bcyy'$$

となり, ゆえに $\gcd(a, bc) = 1$ が成り立つ.

**系 1.8**　$\gcd(a, b) = 1$ ならば, 任意の自然数 $r, s$ に対し $\gcd(a^r, b^s) = 1$ である.

**証明**

命題 1.7 を使って帰納法により $\gcd(a^r, b) = 1$ となる. 同じ議論を整数 $a^r$, $b$ に適用させることで $\gcd(a^r, b^s) = 1$ となる.

## 1.4　素因数分解

**定義 1.9**　自然数 $p \geq 2$ が素数であるとは, $1, p$ 以外の正の約数を持たないことをいう.

**定理 1.10: (素因数分解)**　2 以上の任意の整数 $a$ に対し,

$$a = p_1^{k_i} \dots p_r^{k_r}$$

となる相異なる素数 $p_1, \dots, p_r$ と自然数 $k_1, \dots, k_r$ が存在する. さらに順序を除いてこの表し方が一意的である.

**証明**

- 素因数分解の存在性を $a$ に関する帰納法によって示す. $a = 2$ のとき明らかである. $a > 2$ とする. $a$ が素数ならば, $r = 1$, $p_1 = a$, $k_1 = 1$ とおけば良い. $a$ が素数でない場合は, $a = bc$ (但し $2 \leq b, c < a$) と表すことができる. 帰納法の仮定より, $b$ 及び $c$ が素因数分解を持つ. $a = bc$ より $a$ も素因数分解を持つ. 以上より, 素因数分解の存在性が示せた.

- 順序を除いた素因数分解の一意性を示す．$a$ に関する帰納法によって証明する．$a = 2$ のとき明らかである．$a \geq 2$ とし，

$$a = p_1^{k_1} \dots p_r^{k_r} = q_1^{m_1} \dots q_s^{m_s} \qquad (p_i \text{ は相異なる}, q_j \text{ は相異なる})$$

を満たす素数 $p_1, \dots, p_r, q_1, \dots, q_s$ 及び自然数 $k_1, \dots, k_r, m_1, \dots, m_s$ を考える．$p_1$ が $a$ の約数であるので，$p_1 \mid q_j$ となる $j \in \{1, \dots, s\}$ が存在する．$q_1, \dots, q_s$ の添え字を付け直して，$j = 1$ として良い．$q_1$ が素数より，$p_1 = q_j$ となる．したがって，

$$p_1^{k_1 - 1} \dots p_r^{k_r} = q_1^{m_1 - 1} \dots q_s^{m_s}$$

となる．帰納法の仮定より $r = s$ であり，また $p_1, \dots, p_r$ と $q_1, \dots, q_r$ が順序を除いて一致する．

## 1.5　合同式

$n$ を自然数とする．

**定義 1.11**　2 つの整数 $a, b \in \mathbb{Z}$ が $n$ を法として合同であるとは，$a - b$ が $n$ の倍数であるときにいい，

$$a \equiv b \pmod{n}$$

と表す．

合同関係は $\mathbb{Z}$ 上の同値関係である．つまり，以下の 3 つ条件を満たす．

- 反射率：$a \equiv a \pmod{n}$
- 対称律：$a \equiv b \pmod{n} \iff b \equiv a \pmod{n}$
- 推移律：$a \equiv b \pmod{n}$ かつ $b \equiv c \pmod{n}$ ならば $a \equiv c \pmod{n}$.

反射率，対称律は明らかである．推移律のみ確認する．$a \equiv b \pmod{n}$ かつ $b \equiv c \pmod{n}$　のとき，$b - a = rn$ かつ $c - b = sn$ となる $r, s \in \mathbb{Z}$ が存在する．ゆえに，

$$c - a = (c - b) + (b - a) = rn + sn = (r + s)n$$

となり，$a \equiv c \pmod{n}$ である．$k \in \mathbb{Z}$ の同値類を $\overline{k}$ とおく．すなわち

$$\begin{aligned} \overline{k} &= \{m \in \mathbb{Z} \mid m \equiv k \pmod{n}\} \\ &= \{k + rn \mid r \in \mathbb{Z}\}. \end{aligned}$$

同値類 $\overline{k}$ を $k + n\mathbb{Z}$ とも表す．また，同値類全体の集合を $\mathbb{Z}/n\mathbb{Z}$ と書く．

**命題 1.12**　以下が成り立つ．

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}$$

さらに，$\overline{0}, \dots, \overline{n-1}$ は相異なる元である．とくに，$\mathbb{Z}/n\mathbb{Z}$ はちょうど $n$ 個の元から構成されている．

**証明**

$k \in \mathbb{Z}$ とし，$k$ を $n$ で割った余りを $r$ と書く．このとき $k \equiv r \pmod{n}$ であるので，$\overline{k} = \overline{r}$ が成り立つ．よって，$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}$ となる．次に，$\overline{0}, \dots, \overline{n-1}$ が相異なることを示す．$0 \leq k, k' \leq n - 1$ で，$\overline{k} = \overline{k'}$ とする．このとき，$0 \leq |k - k'| \leq n - 1$ かつ $k - k'$ は $n$ の倍数である．したがって，$k = k'$ が成り立つ．

次に, $\mathbb{Z}/n\mathbb{Z}$ 上の足し算と掛け算を定義する. $k, k' \in \mathbb{Z}$ に対し,

$$\overline{k} + \overline{k}' := \overline{k+k'}$$
$$\overline{k} \times \overline{k}' := \overline{kk'}$$

と定義する. 上記の演算は代表元の取り方によらないことに注意する. つまり, $k_1 \equiv k_2 \pmod{n}$ かつ $k_1' \equiv k_2' \pmod{n}$ ならば, $k_1 + k_1' \equiv k_2 + k_2' \pmod{n}$ かつ $k_1 k_1' \equiv k_2 k_2' \pmod{n}$ である. 実際, $k_2 = k_1 + rn$, $k_2' = k_1' + r'n$ とおくと

$$(k_2 + k_2') - (k_1 + k_1') = (r + r')n$$
$$(k_2 k_2') - (k_1 k_1') = k_2(k_2' - k_1') + k_1'(k_2 - k_1) = (k_2 r' + k_1' r)n$$

と表せる. ゆえに, $\mathbb{Z}/n\mathbb{Z}$ の演算は well-defined である.

**定義 1.13** $\overline{k} \in \mathbb{Z}/n\mathbb{Z}$ とする. $\overline{k}$ が可逆元であるとは, $\overline{k} \times \overline{k'} = \overline{1}$ となる $k' \in \mathbb{Z}$ が存在することをいう.

**命題 1.14** $k \in \mathbb{Z}$ とする.

$$\overline{k} \quad \text{が可逆元である} \iff \quad \gcd(k, n) = 1.$$

**証明**

$\overline{k}$ が可逆元のとき, $\overline{k} \times \overline{k'} = \overline{1}$ となる $k'$ が存在する. よって $\overline{kk'} = \overline{1}$ であり, $kk' = 1 + nr$ $(r \in \mathbb{Z})$ と表せる. よって, $kk' - nr = 1$ となり, $k, n$ が互いに素である. 逆に, $\gcd(k, n) = 1$ のとき, $uk + nv = 1$ となる $u, v \in \mathbb{Z}$ が存在する. よって, $\overline{uk} = \overline{u}\,\overline{k} = \overline{1}$ である. したがって, $\overline{k}$ が可逆元である.

$x \in \mathbb{Z}/n\mathbb{Z}$ を可逆元とする. このとき, $xy = \overline{1}$ を満たす元 $y \in \mathbb{Z}/n\mathbb{Z}$ は一意的である. なぜならば, $xy = xy' = \overline{1}$ とすると,

$$y = y\overline{1} = y(xy') = (xy)y' = \overline{1}y' = y'$$

となる. $y$ を $x^{-1}$ とおき, $x$ の逆元という. $xx^{-1} = 1$ より, $x^{-1}$ も可逆元であり, さらに $(x^{-1})^{-1} = x$ である. また, $x, y$ が可逆元ならば, $(xy)(y^{-1}x^{-1}) = \overline{1}$ より $xy$ も可逆元であり, $(xy)^{-1} = y^{-1}x^{-1}$ が成り立つ. $\mathbb{Z}/n\mathbb{Z}$ の可逆元全体の集合を $(\mathbb{Z}/n\mathbb{Z})^\times$ とおく. すなわち,

$$(\mathbb{Z}/n\mathbb{Z})^\times = \left\{\overline{k} \in \mathbb{Z}/n\mathbb{Z} \mid \gcd(k, n) = 1\right\}$$

である. $x \in (\mathbb{Z}/n\mathbb{Z})^\times$ のとき, 以下の写像は全単射である.

$$\mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}\ , \quad y \mapsto xy$$
$$(\mathbb{Z}/n\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/n\mathbb{Z})^\times , \quad y \mapsto xy.$$

実際, 写像 $y \mapsto x^{-1}y$ は上の写像の逆写像である.

## 1.6 オイラー関数

自然数 $n$ に対し,

$$\varphi(n) := \left|(\mathbb{Z}/n\mathbb{Z})^\times\right|$$

とおくことで, オイラー関数 $\varphi$ を定める.

**命題 1.15**　$n, m$ が自然数で, $\gcd(n,m)=1$ とする. このとき, 以下の写像が全単射である.

$$\begin{aligned} \alpha\colon \mathbb{Z}/nm\mathbb{Z} &\longrightarrow \mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/m\mathbb{Z} \\ k+mn\mathbb{Z} &\longmapsto (k+n\mathbb{Z},\ k+m\mathbb{Z}) \end{aligned}$$

**証明**

- $\alpha$ が全射であることを示す. 仮定より, $um+nv=1$ となる $u, v\in\mathbb{Z}$ が存在する. $x_1=um$, $x_2=nv$ とおく. 明らかに, $x_1\equiv 1 \pmod n$, $x_1\equiv 0 \pmod m$ である. 同様に, $x_2\equiv 0 \pmod n$, $x_1\equiv 1 \pmod m$ である. ゆえに, $k_1, k_2\in\mathbb{Z}$ に対して, $z=k_1x_1+k_2x_2$ とおくと, $z\equiv k_1 \pmod n$, $z\equiv k_2 \pmod m$ である. したがって, $\alpha$ は全射である.
- $\alpha$ が単射であることを示す. $a, b\in\mathbb{Z}$ で, $a\equiv b \pmod n$, $a\equiv b \pmod m$ とする. このとき $n\mid b-a$ かつ $m\mid b-a$ である. 命題 1.6(2) より, $nm\mid b-a$ となり, ゆえに $a\equiv b \pmod{nm}$ である. よって, $\alpha$ は単射である.

$k\in\mathbb{Z}$ に対し,

$$\gcd(k,nm)=1 \quad\Longleftrightarrow\quad \gcd(k,n)=1 \ \text{ かつ } \ \gcd(k,m)=1$$

が成り立つので, $\alpha$ は全単射

$$\begin{aligned} \alpha\colon (\mathbb{Z}/nm\mathbb{Z})^\times &\longrightarrow (\mathbb{Z}/n\mathbb{Z})^\times\times(\mathbb{Z}/m\mathbb{Z})^\times \\ k+mn\mathbb{Z} &\longmapsto (k+n\mathbb{Z},\ k+m\mathbb{Z}) \end{aligned}$$

を誘導する.

**系 1.16**　$\gcd(n,m)=1$ のとき, $\varphi(nm)=\varphi(n)\varphi(m)$ が成り立つ.

**証明**

以上より

$$\varphi(nm)=\left|(\mathbb{Z}/nm\mathbb{Z})^\times\right|=\left|(\mathbb{Z}/n\mathbb{Z})^\times\right|\cdot\left|(\mathbb{Z}/m\mathbb{Z})^\times\right|=\varphi(n)\varphi(m).$$

**命題 1.17**

(1) $p$ を素数とし, $k\geq 1$ とする. このとき, $\varphi(p^k)=p^k-p^{k-1}=p^{k-1}(p-1)$ である.

(2) $n$ が自然数で, $n$ の素因数分解を $p_1^{k_1}\dots p_r^{k_r}$ と書く. このとき, 以下が成り立つ.

$$\varphi(n)=(p_1^{k_1}-p_1^{k_1-1})\dots(p_r^{k_r}-p_r^{k_r-1})=n\left(1-\frac{1}{p_1}\right)\dots\left(1-\frac{1}{p_r}\right).$$

**証明**

- (1) を示す. 元 $0, 1, \dots, p^k-1$ のうち, $p$ で割り切れるものは $0, p, 2p, \dots, (p^{k-1}-1)p$ の $p^{k-1}$ 個の元である. ゆえに,

  $$\varphi(p^k)=p^k-p^{k-1}=p^{k-1}(p-1)$$

  である.
- (2) を示す. 系 1.16 により

  $$\begin{aligned} \varphi(n)&=\varphi(p_1^{k_1})\dots\varphi(p_r^{k_r}) \\ &=(p_1^{k_1}-p_1^{k_1-1})\dots(p_r^{k_r}-p_r^{k_r-1})=n\left(1-\frac{1}{p_1}\right)\dots\left(1-\frac{1}{p_r}\right). \end{aligned}$$

## 1.7　フェルマーの小定理・ウイルソンの定理

**定理 1.18: (フェルマーの小定理)**　$p$ を素数とし, $a$ を $p$ の倍数でない整数とする. このとき,

$$a^{p-1} \equiv 1 \pmod{p}$$

が成り立つ.

**証明**

$\mathbb{Z}/p\mathbb{Z}$ における $a$ の剰余類を $x$ とおく. すなわち, $x = a + p\mathbb{Z}$ である. 積 $S := \prod_{y \in (\mathbb{Z}/p\mathbb{Z})^\times} y$ について考える. $x$ が $\mathbb{Z}/p\mathbb{Z}$ の逆元であるので, 写像 $y \mapsto xy$ が全単射である. ゆえに,

$$S = \prod_{y \in (\mathbb{Z}/p\mathbb{Z})^\times} (xy) = x^{p-1} \left( \prod_{y \in (\mathbb{Z}/p\mathbb{Z})^\times} y \right) = x^{p-1} S.$$

両辺に $S^{-1}$ をかけ, $x^{p-1} = \overline{1}$ となる. よって, $a^{p-1} \equiv 1 \pmod{p}$ である.

**定理 1.19: (ウイルソンの定理)**　$p$ を自然数とする. このとき,

$$p \text{ が素数である} \iff (p-1)! \equiv -1 \pmod{p}$$

が成り立つ.

**証明**

- 「$\Longrightarrow$」を示す. $T = (p-1)!$ とおき, $\mathbb{Z}/p\mathbb{Z}$ における $T$ の剰余類 $\overline{T}$ を考える. $(\mathbb{Z}/p\mathbb{Z})^\times = \{\overline{1}, \ldots, \overline{p-1}\}$ であるので,
$$\overline{T} = \prod_{x \in (\mathbb{Z}/p\mathbb{Z})^\times} x$$
となる. $(\mathbb{Z}/p\mathbb{Z})^\times$ の元で, $x = x^{-1}$ を満たすものは $x = \pm\overline{1}$ に限ることに注意する. じっさい, $x = \overline{k}$ $(\gcd(k, p) = 1)$ とおくと,
$$\begin{aligned} x^{-1} = x &\iff x^2 = \overline{1} \\ &\iff p \mid k^2 - 1 = (k-1)(k+1) \\ &\iff p \mid k-1 \text{ または } p \mid k+1 \\ &\iff x = \pm\overline{1}. \end{aligned}$$
よって, $x_1, \ldots, x_m$ が存在し,
$$(\mathbb{Z}/p\mathbb{Z})^\times = \{\pm 1\} \sqcup \{x_1, \ldots, x_m, x_1^{-1}, \ldots, x_m^{-1}\}$$
と表せる. ただし, $x_1, \ldots, x_m, x_1^{-1}, \ldots, x_m^{-1}$ は相異なる元である. ゆえに,
$$\overline{T} = (-\overline{1}) \times \left( \prod_{i=1}^{m} x_i x_i^{-1} \right) = -\overline{1}.$$
である. ゆえに, $T \equiv -1 \pmod{p}$ である.
- 逆に, $(p-1)! \equiv -1 \pmod{p}$ とする. このとき, $1 = pm - (p-1)!$ を満たす $m \in \mathbb{Z}$ が存在するので, $1, \ldots, p-1$ が全て $p$ と互いに素である. したがって, $p$ が素数である.

# 2　群論

## 2.1　群の定義

$G$ を空でない集合とする．$G$ 上の演算とは, 写像 $G \times G \to G$ のことをいう．$G$ 上の演算 $(x, y) \mapsto x \cdot y$ が与えられているとする．

**定義 2.1**　$G$ が群であるとは, 以下の条件を満たすときにいう．
(a) 任意の $x, y, z \in G$ について $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ である．
(b) $G$ の元 $e$ が存在し, 任意の $x \in G$ に対し, $e \cdot x = x \cdot e = x$ である．
(c) 任意の $x \in G$ に対し, $x' \in G$ が存在し, $x \cdot x' = x' \cdot x = e$ である．

(a) が成り立つときに, 演算が結合法則を満たすという．条件 (b) を満たす元 $e$ を単位元という．単位元は一意的に定まる．また, (c) の元 $x'$ を $x$ の逆元といい, $x^{-1}$ と表す．$x$ の逆元は一意に定まる．任意の $x, y \in G$ に対し,

$$(xy)^{-1} = y^{-1}x^{-1}$$

が成り立つ．$x \in G$, $k \in \mathbb{Z}$ に対し,

$$x^k = \begin{cases} x \cdots x \quad (k \text{ 個}) & \text{if } \ k > 0 \\ e & \text{if } \ k = 0 \\ x^{-1} \cdots x^{-1} \quad (-k \text{ 個}) & \text{if } \ k < 0 \end{cases}$$

と定める．全ての $x, y \in G$ に対し

$$x \cdot y = y \cdot x$$

が成り立つときに, $G$ がアーベル群 (あるいは可換群) であるという．$x \cdot y$ を単に $xy$ と表すこともある．また, $G$ がアーベル群のとき, その演算を $(x, y) \mapsto x + y$ と表す場合がある．このとき, 合わせて単位元を $0$ で表す．

**例 2.2.**

- $(\mathbb{Z}, +)$ はアーベル群である．単位元は $0$ であり, $k \in \mathbb{Z}$ の逆元は $-k$ である．
- $(\mathbb{R}^*, \times)$ は $1$ を単位元とするアーベル群である．$x \in \mathbb{R}^*$ の逆元は $\frac{1}{x}$ である．
- $\{1, \ldots, n\}$ の置換全体の集合を $\mathfrak{S}_n$ とおく．置換の積に関して $\mathfrak{S}_n$ は群をなす．
- $(\mathbb{Z}/n\mathbb{Z}, +)$ は $\overline{0}$ を単位元とするアーベル群である．$\overline{k}$ の逆元は $-\overline{k}$ である．
- $((\mathbb{Z}/n\mathbb{Z})^\times, \times)$ は $\overline{1}$ を単位元とするアーベル群である．$\overline{k} \in (\mathbb{Z}/n\mathbb{Z})^\times$ の逆元は $\overline{k}^{-1}$ である．
- 正則 $n$ 次実行列全体の集合を $\mathrm{GL}_n(\mathbb{R})$ とおく．行列の積に関して $\mathrm{GL}_n(\mathbb{R})$ は群をなす．$n \geq 2$ のとき可換群でない．

$G_1$, $G_2$ を群とする．このとき, 直積 $G_1 \times G_2$ の 2 つの元 $(g_1, g_2)$ 及び $(g_1', g_2')$ に対し

$$(g_1, g_2) \cdot (g_1', g_2') := (g_1 g_1', g_2 g_2')$$

とおくことで, 直積 $G_1 \times G_2$ に演算を入れる．$G_1 \times G_2$ はこの演算に関して群であり, $G_1$ と $G_2$ の直積と呼ばれる．

**定義 2.3**　$G$ を群とし, $H \subset G$ を部分集合とする．$G$ の単位元を $e$ とおく．$H$ が部分群であるとは, 以下が成り立つときにいう．
(a) $e \in H$.
(b) $x, y \in H$ ならば, $xy \in H$ である．
(c) $x \in H$ ならば, $x^{-1} \in H$ である．

**注意 2.4.** $H$ が部分群になるためには, 「$H$ が空でなく, かつ任意の $x, y \in H$ に対し $xy^{-1} \in H$」が成り立つことが必要十分である.

**命題 2.5** 群 $(\mathbb{Z}, +)$ の部分群は $n\mathbb{Z}$ $(n \geq 0)$ という形の部分集合である.

**証明**

- $n\mathbb{Z}$ が部分群であることを示す. 明らかに, $0 \in n\mathbb{Z}$ である. また, $x, y$ が $n$ の倍数であるならば, $x - y$ も $n$ の倍数である. よって, $n\mathbb{Z}$ は $\mathbb{Z}$ の部分群である.
- 逆に, $H \subset \mathbb{Z}$ を部分群とする. $H = n\mathbb{Z}$ となる $n \geq 0$ が存在することを示す. $H = \{0\}$ のとき $n = 0$ とおけば良い. そうでなければ, 0 でない元 $k \in H$ が存在する. $\pm k \in H$ より, $H \cap \mathbb{N}$ が空でない. $H \cap \mathbb{N}$ の最小のものを $n$ とおく. $H$ が部分群だから, $n\mathbb{Z} \subset H$ である. 逆に, $a \in H$ とすると, 割り算の定理より $a = qn + r$ $(0 \leq r < n)$ と表せる. ゆえに $r = a - qn$ である. $a, n \in H$ より, $r \in H$ である. また, $n$ の最小性より $r = 0$ となり, すなわち $a = qn$ である. したがって, $H = n\mathbb{Z}$ が成り立つ.

**命題 2.6** $G$ を群とし, $S \subset G$ を空でない部分集合とする. $S$ を含む $G$ の部分群のうち, 最小のものが存在する. また, それを $\langle S \rangle$ とおくと, 以下が成り立つ.

$$\langle S \rangle = \{ s_1^{k_1} \dots s_m^{k_m} \mid s_i \in S,\ k_i \in \mathbb{Z} \}. \tag{2.1}$$

任意の部分群 $H \subset G$ に対し, 「$S \subset H \iff \langle S \rangle \subset H$」が成り立つ.

**証明**

まず, 上の集合 (2.1) が $G$ の部分群であることを示す. $S \neq \emptyset$ より $\langle S \rangle \neq \emptyset$ である. また, $x, y \in \langle S \rangle$ で, $x = s_1^{k_1} \dots s_m^{k_m}$, $y = t_1^{r_1} \dots t_d^{r_d}$ $(s_i, t_i \in S,\ k_i, r_i \in \mathbb{Z})$ とする. このとき,

$$xy^{-1} = s_1^{k_1} \dots s_m^{k_m} t_d^{-r_d} \dots t_1^{-r_1}$$

となり, とくに $xy^{-1} \in \langle S \rangle$ である. したがって, $\langle S \rangle$ は部分群である. $H$ を部分群とし, $S \subset H$ とする. このとき, 任意の $s_1, \dots, s_m \in S$ 及び $k_1, \dots, k_m \in \mathbb{Z}$ に対し $s_1^{k_1} \dots s_m^{k_m} \in H$ である. よって, $\langle S \rangle \subset H$ となる. 以上より, $\langle S \rangle$ は $S$ を含む部分群の中で最小のものである. また, 「$S \subset H \iff \langle S \rangle \subset H$」も示せた.

**定義 2.7**

(a) $\langle S \rangle$ は $S$ で生成される部分群と呼ばれる.

(b) $\langle S \rangle = G$ のとき, $S$ が $G$ を生成する (または, $S$ が $G$ の生成系である) という.

(c) $S = \{x_1, \dots, x_n\}$ のとき, $\langle S \rangle$ を単に $\langle x_1, \dots, x_n \rangle$ と書く.

**定義 2.8** $G = \langle x \rangle$ となる $x \in G$ が存在するとき, $G$ が巡回群であるという. また, このとき $x$ を $G$ の生成元という.

命題 2.6 より, $\langle x \rangle = \{ x^k \mid k \in \mathbb{Z} \}$ である.

**定義 2.9** $\langle x \rangle$ の元の個数を $x$ の位数といい, $\mathrm{ord}(x)$ と表す.

**定理 2.10**　$x$ を有限位数の元とし, $m := \mathrm{ord}(x)$ とおく.
(1) このとき, $\langle x\rangle = \{e, x, \dots, x^{m-1}\}$ が成り立つ. 但し, $e, x, \dots, x^{m-1}$ は相異なる元である.
(2) さらに, 任意の $k \in \mathbb{Z}$ に対し, $x^k = e \iff m \mid k$ が成り立つ.

**証明**

- (1) を示す. 仮定より $\langle x\rangle = \{x^k \mid k \in \mathbb{Z}\}$ は有限集合である. よって, $x^i = x^j$ を満たす整数 $j > i$ が存在する. $k = j - i$ とおくと,
$$x^{i+k} = x^i x^k = x^i$$
が成り立つ. 両辺に $x^{-i}$ をかけると, $x^k = e$ となる. 次に,
$$n := \min\{k \geq 1 \mid g^k = e\}$$
と定義する. 但し, 上の集合が空でないことを確認したので, $n$ が well-defined であることに注意する. 以下が成り立つことを示す.
$$\langle x\rangle = \{e, x, \dots, x^{n-1}\} \tag{2.2}$$
任意の整数 $k$ に対し, $k = qn + r$ かつ $0 \leq r < n$ を満たす整数 $q, r$ が存在する. よって,
$$x^k = x^{qn+r} = (x^n)^q \cdot x^r = e \cdot x^r = x^r$$
である. したがって, (2.2) が成り立つ. また, $0 \leq i < j < n$ のとき $x^i \neq x^j$ である. なぜならば, $x^i = x^j$ とすると, $x^{j-i} = e$ である. $0 < j - i < n$ であるので, $n$ の最小性に矛盾する. よって, $e, x, \dots, x^{n-1}$ は相異なる. 以上より, $|\langle x\rangle| = m = n$ が成り立つ. ゆえに, (1) が示せた.
- (2) を示す. $k \in \mathbb{Z}$ に対し, $k = qm + r$ かつ $0 \leq r < m$ と書くと $x^k = x^r$ である. よって,
$$x^k = e \iff r = 0 \iff m \mid k.$$

**例 2.11.** $G = \mathrm{GL}_2(\mathbb{R})$ とし, $x = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$, $y = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ とする.
$$x^2 = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}, \quad x^3 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$
より, $x$ の位数は 3 である. 同様に, $y^2 = -E_2$, $y^3 = -y$, $y^4 = E_2$ より $y$ の位数は 4 である. 一方,
$$xy = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \qquad (xy)^n = \begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix}$$
より, $xy$ の位数は無限である.

上の例は, $x$, $y$ が有限位数のとき, $xy$ が有限位数とは限らないことを示している. $x, y$ が交換するとは, $xy = yx$ が成り立つことをいう. このとき, 任意の $N \geq 1$ に対し
$$(xy)^N = x^N y^N$$
が成り立つ. ゆえに, $x^n = e$ かつ $y^m$ ならば, $(xy)^{nm} = x^{nm} y^{nm} = e$ となり, ゆえに $xy$ は有限位数の元である.

**命題 2.12**
(1) $x \in G$ を有限位数の元とし, $n = \mathrm{ord}(x)$ とおく. 任意の $k \in \mathbb{Z}$ に対し, $\mathrm{ord}(x^k) = \frac{n}{\gcd(k,n)}$ が成り立つ.
(2) $x, y \in G$ が交換するもので, $n := \mathrm{ord}(x)$ と $m := \mathrm{ord}(y)$ が互いに素であるとする. このとき, $\mathrm{ord}(xy) = nm$ が成り立つ.

**証明**

レポート 1 .

## 2.2 準同型

**定義 2.13** $G, G'$ を群とし, $f\colon G \to G'$ を写像とする. $f$ が群準同型であるとは, 任意の $x, y \in G$ に対し

$$f(x \cdot y) = f(x) \cdot f(y)$$

が成り立つことをいう.

**例 2.14.**

- $(\mathbb{R}, +)$ と $(\mathbb{R}^*, \times)$ は明らかにアーベル群である. 写像 $\exp\colon \mathbb{R} \to \mathbb{R}^*$, $x \mapsto \exp(x)$ は $\exp(x+y) = \exp(x)\exp(y)$ を満たすので, $(\mathbb{R}, +)$ から $(\mathbb{R}^*, \times)$ への群準同型である.
- 写像 $\det\colon \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^*$ は $\det(AB) = \det(A)\det(B)$ を満たすので, $\mathrm{GL}_n(\mathbb{R})$ から $\mathbb{R}^*$ への群準同型である.

**補題 2.15** $f\colon G \to G'$ を群準同型とする. $G, G'$ の単位元をそれぞれ $e, e'$ とおく. このとき, 以下が成り立つ.
(1) $f(e) = e'$ である.
(2) 任意の $x \in G$ に対し $f(x^{-1}) = f(x)^{-1}$ である.

**証明**

- $f(e) = f(ee) = f(e)f(e)$ である. よって, 両辺に $f(e)^{-1}$ をかけて, $f(e) = e'$ となる.
- $f(x)f(x^{-1}) = f(xx^{-1}) = f(e) = e'$ である. よって, $f(x^{-1}) = f(x)^{-1}$ である.

**命題 2.16** $f\colon G \to G'$ を群準同型とする.
(1) $H$ が $G$ の部分群ならば, $f(H)$ は $G'$ の部分群である.
(2) $H'$ が $G'$ の部分群ならば, $f^{-1}(H') = \{x \in G \mid f(x) \in H'\}$ は $G$ の部分群である.

**証明**

- (1) を示す. $f(e) = e'$ かつ $e \in H$ より $e' \in f(H)$ である. また, $x, y \in f(H)$ で, $x = f(a)$, $y = f(b)$ $(a, b \in H)$ とする. このとき, $xy^{-1} = f(a)f(b)^{-1} = f(ab^{-1})$ となる. $H$ が部分群だから, $ab^{-1} \in H$ である. ゆえに $xy^{-1} \in f(H)$ となり, $f(H)$ は $G'$ の部分群である.
- (2) を示す. $f(e) = e'$ かつ $e' \in H'$ より, $e \in f^{-1}(H')$ である. また, $a, b \in f^{-1}(H')$ ならば, $f(ab^{-1}) = f(a)f(b^{-1}) = f(a)f(b)^{-1}$ である. $f(a), f(b) \in H'$ より, $f(a)f(b)^{-1} \in H'$ となる. よって, $ab^{-1} \in f^{-1}(H')$ であり, ゆえに $f^{-1}(H')$ は $G$ の部分群である.

**定義 2.17** $f\colon G \to G'$ を群準同型とする.
(a) $\mathrm{Ker}(f) := \{x \in G \mid f(x) = e'\}$ とおき, $f$ の核という.
(b) $\mathrm{Im}(f) := \{f(x) \mid x \in G\}$ とおき, $f$ の像という.

**補題 2.18**　$f\colon G \to G'$ を群準同型とする．$\mathrm{Ker}(f)$ は $G$ の部分群であり，$\mathrm{Im}(f)$ は $G'$ の部分群である．

**証明**

$\mathrm{Ker}(f) = f^{-1}(\{e'\})$, $\mathrm{Im}(f) = f(G)$ であるので，主張は命題 2.16 より従う．

**命題 2.19**　$f\colon G \to G'$ を群準同型とする．このとき，

$$f \text{ が単射である} \iff \mathrm{Ker}(f) = \{e\} \text{ である．}$$

**証明**

- 「$\Longrightarrow$」を示す．$f$ が単射であることを仮定し，$x \in \mathrm{Ker}(f)$ とすると，$f(x) = e' = f(e)$ である．ただし，$e, e'$ はそれぞれ $G, G'$ の単位元である．$f$ の単射性より，$x = e$ となる．ゆえに，$\mathrm{Ker}(f) = \{e\}$ である．
- 「$\Longleftarrow$」を示す．$\mathrm{Ker}(f) = \{e\}$ とする．$f(x) = f(y)$ $(x, y \in G)$ ならば，

$$f(x^{-1}y) = f(x^{-1})f(y) = f(x)^{-1}f(y) = e'$$

である．ゆえに，$x^{-1}y \in \mathrm{Ker}(f) = \{e\}$ である．ゆえに，$x^{-1}y = e$ であり，よって $x = y$ が成り立つ．したがって，$f$ は単射である．

**定義 2.20**

(a) 群準同型 $f\colon G \to G'$ が全単射であるとき，$f$ を群同型という．
(b) 群準同型 $G \to G$ のことを $G$ の自己準同型という．
(c) 群同型 $G \to G$ のことを $G$ の自己同型という．

$G_1, G_2$ が群で，群同型 $G_1 \to G_2$ が存在するとき，$G_1 \simeq G_2$ と表す．

**定理 2.21: (中国の剰余定理)**　$n, m$ を互いに素な自然数とする．写像

$$\begin{aligned} \alpha\colon \mathbb{Z}/nm\mathbb{Z} &\longrightarrow \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \\ k + mn\mathbb{Z} &\longmapsto (k + n\mathbb{Z},\ k + m\mathbb{Z}) \end{aligned}$$

は群同型である．

**証明**

命題 1.15 により $\alpha$ は全単射である．$\alpha$ は明らかに群準同型であるので，群同型である．

## 2.3 剰余類

**定義 2.22** $G$ を群とし, $H$ を $G$ の部分群とする. $x \in G$ に対し, 部分集合 $xH$, $Hx$ を以下のように定める.

$$xH := \{xh \mid h \in H\}$$
$$Hx := \{hx \mid h \in H\}.$$

$xH$, $Hx$ をそれぞれ $x$ の左剰余類, 右剰余類という.

**補題 2.23** $x, x' \in H$ に対し, 以下が同値である.

(i) $xH = x'H$

(ii) $x \in x'H$

(iii) $x' \in xH$

(iv) $xH \cap x'H \neq \emptyset$

**証明**

(i)$\Longrightarrow$(ii) $\Longrightarrow$ (iv), また (i)$\Longrightarrow$(iii) $\Longrightarrow$ (iv) は明らかである. 最後に, (iv) $\Longrightarrow$ (i) を示す. $y \in xH \cap x'H$ とする. このとき, $y = xh = x'h'$ となる $h, h' \in H$ が取れる. よって, 任意の $k \in H$ に対し,

$$xk = (xh)h^{-1}k = (x'h')h^{-1}k = x'(h'h^{-1}k) \in x'H$$

となる. ゆえに, $xH \subset x'H$ である. 同様の議論で $x'H \subset xH$ が分かる. ゆえに, $xH = x'H$ である.

$H$ による左剰余類全体の集合, 右剰余類全体の集合をそれぞれ $G/H$, $H\backslash G$ と表す.

**命題 2.24** $G$ が $H$ による左剰余類に分割される. つまり, $G$ の元の族 $\{x_i\}_{i \in I}$ が存在し,

$$G = \bigsqcup_{i \in I} x_i H \tag{2.3}$$

が成り立つ (ただし, 記号 $\bigsqcup$ は共通部分を持たない和集合を意味する). 同様に, $G$ が $H$ による右剰余類に分割される.

**証明**

左剰余類全体の族を $(C_i)_{i \in I}$ とおく. 各 $i \in I$ に対し, $C_i$ から代表元 $x_i \in C_i$ を一つ取る. このとき, $C_i = x_i H$ である. 各 $x \in G$ が自分の左剰余類 $xH$ に属するので, $G = \bigcup_{i \in I} C_i$ が成り立つ. また, 補題 2.23 より, $i \neq j$ のとき $C_i \cap C_j = \emptyset$ である. 主張が従う.

上の (2.3) を満たす $G$ の元の族 $\{x_i\}_{i \in I}$ を左剰余類の代表系という. 右剰余類の代表系は同様に定義する.

**定義 2.25** $G/H$ が有限集合のとき, $H$ を有限指数の部分群という. $G/H$ の元の個数を $G$ における $H$ の指数といい, $[G : H]$ と表す.

**注意 2.26.** 写像 $G/H \to H\backslash G$, $xH \mapsto Hx^{-1}$ は全単射であるので, 左剰余類の個数は右剰余類の個数と一致する.

**定理 2.27: (ラグランジュの定理)** $G$ が有限群で, $H$ を $G$ の部分群とする. このとき,

$$|G| = |H| \times [G : H]$$

が成り立つ.

**証明**

$H$ の左剰余類の代表系 $\{x_1, \ldots, x_m\}$ を考える. 但し, $m = [G : H]$ である. 命題 2.24 より

$$G = \bigsqcup_{j=1}^{m} x_i H \tag{2.4}$$

が成り立つ. 写像 $H \to x_i H$, $h \mapsto x_i h$ は全単射である (その逆写像は $h \mapsto x_i^{-1} h$ である). とくに, $|x_i H| = |H|$ である. ゆえに,

$$|G| = \sum_{j=1}^{m} |x_i H| = \sum_{j=1}^{m} |H| = |H| \times m = |H| \times [G : H]$$

が成り立つ.

$G$ が有限群のとき, $|G|$ を $G$ の位数という.

**系 2.28** $|H|$ は $|G|$ の約数である. とくに, $x \in G$ のとき $\mathrm{ord}(x)$ は $|G|$ の約数である.

**系 2.29** $n = |G|$ とおくと, 任意の $x \in G$ に対し, $x^n = e$ が成り立つ.

**証明**

定理 2.10 より従う.

**例 2.30.** $G = (\mathbb{Z}/n\mathbb{Z})^\times$ を考える. $G$ の位数は $\varphi(n)$ である. ゆえに, $\gcd(k, n) = 1$ を満たす任意の整数 $k$ に対し,

$$k^{\varphi(n)} \equiv 1 \pmod{n}$$

が成り立つ.

## 2.4 正規部分群・剰余群

**定義 2.31** $G$ を群とし, $H \subset G$ を部分群とする. $H$ が正規部分群であるとは, 以下が成り立つことをいう.

$$g \in G,\ h \in H \quad \Longrightarrow \quad ghg^{-1} \in H.$$

$H$ が正規部分群であるとき, $H \triangleleft G$ と表す.

$g \in G$ に対し,

$$gHg^{-1} := \{ghg^{-1} \mid h \in H\}$$

とおく. $gHg^{-1}$ は $G$ の部分群であることは容易に確認できる. $H$ が正規部分群であることは, 任意の $g \in G$ に対し $gHg^{-1} \subset H$ が成り立つことを意味する. また, $g$ と $g^{-1}$ を入れ替えて, $H$ が正規部分群のとき $g^{-1}Hg \subset H$

も成り立つ. ゆえに, $H \subset gHg^{-1}$ である. 以上より, 以下が成り立つ.

$$\begin{aligned} H \text{ が } G \text{ の正規部分群である} &\iff \text{任意の } g \in G \text{ に対し, } gHg^{-1} = H \\ &\iff \text{任意の } g \in G \text{ に対し, } gH = Hg. \end{aligned}$$

**例 2.32.**

- $\{e\}$ と $G$ は $G$ の正規部分群である. それ以外の正規部分群が存在しないときに, $G$ が単純群であるという.
- $G$ がアーベル群のとき, 全ての部分群が正規部分群である. 実際, このとき $g \in G$, $h \in H$ に対し $ghg^{-1} = gg^{-1}h = h \in H$ である.
- $G$ を群とする.

$$Z(G) := \{g \in G \mid \text{任意の } h \in G \text{ に対し } gh = hg \text{ である}\}$$

とおき, $G$ の中心という. $Z(G)$ は常に $G$ の正規部分群である. 明らかに,

$$G \text{ がアーベル群} \iff Z(G) = G.$$

- $G$ の部分群 $H$ に対し,

$$N_G(H) = \{g \in G \mid gHg^{-1} = H\}$$

とおき, $H$ の正規化群という. $N_G(H)$ は $H$ を含む部分群である. また, $H \triangleleft N_G(H)$ が成り立つ.

**命題 2.33** $f\colon G \to G'$ を群準同型とする. このとき, $\mathrm{Ker}(f)$ は $G$ の正規部分群である. また, $H' \subset G'$ が $G'$ の正規部分群ならば, $f^{-1}(H')$ は $G$ の正規部分群である.

**証明**

$H' \triangleleft G'$ とし, $H := f^{-1}(H')$ とおく. $g \in G$, $h \in H$ のとき,

$$f(ghg^{-1}) = f(g)f(h)f(g)^{-1}$$

である. $f(h) \in H'$ であるので, $H'$ の正規性より $f(g)f(h)f(g)^{-1} \in H'$ である. ゆえに $ghg^{-1} \in H$ となり, $H$ が正規部分群である. $\mathrm{Ker}(f) = f^{-1}(\{e'\})$ であるので, 正規部分群である.

$H$ を $G$ の正規部分群とする. このとき, 左剰余類全体の集合 $G/H$ に自然な演算を入れることができる. $g, g' \in G$ に対し,

$$(gH)(g'H) := (gg')H \tag{2.5}$$

とおくことで, $G/H$ の演算を定義する. この演算が well-defined であることを確認しよう. 結果が剰余類の代表元の取り方に依らないことを示せば良い. $g_1, g_2, g_1', g_2' \in G$ で, $g_1H = g_2H$, $g_1'H = g_2'H$ とする. このとき, $g_1g_2H = g_1'g_2'H$ を示せば良い. $G$ の元 $g, g'$ に対し,

$$gHg' := \{ghg' \mid h \in H\}$$

とおくことで部分集合 $gHg'$ を定義する (一般には部分群でない). $H$ の正規性より, 以下が成り立つ.

$$g_1g_2H = g_1g_2'H = g_1Hg_2' = g_1'Hg_2' = g_1'g_2'H.$$

ゆえに, (2.5) で定まる $G/H$ の演算は well-defined である.

**命題 2.34**

(1) この演算に関して $G/H$ は群をなす.

(2) $\pi(x) = xH$ で定まる写像 $\pi\colon G \to G/H$ は群準同型である.

(3) $\mathrm{Ker}(\pi) = H$ である.

**証明**

- 結合法則は容易に確認できる．また, $eH = H$ は明らかに単位元である．最後に, $x \in G$ のとき $(xH)(x^{-1}H) = (x^{-1}H)(xH) = eH = H$ であるので, 全ての元が可逆元である．
- $x, y \in G$ のとき, $\pi(xy) = xyH = (xH)(yH) = \pi(x)\pi(y)$ であり, $\pi$ は群準同型である．
- $\pi(x) = H \iff xH = H \iff x \in H$ である．

$\pi$ は「自然な射影」と呼ばれる．

**定理 2.35: (準同型定理)** $f\colon G \to G'$ を群準同型とする．このとき, 写像

$$\widetilde{f}\colon G/\operatorname{Ker}(f) \to \operatorname{Im}(f), \quad x\operatorname{Ker}(f) \mapsto f(x)$$

は well-defined であり, 群同型写像である．

**証明**

- $\widetilde{f}$ が well-defined であることを示す．$x\operatorname{Ker}(f) = y\operatorname{Ker}(f)$ $(x, y \in G)$ のとき, $f(x) = f(y)$ を示せば良い．$y = xz$ となる $z \in \operatorname{Ker}(f)$ が存在する．ゆえに, $f(y) = f(xz) = f(x)f(z) = f(x)e' = f(x)$ となる．
- $\widetilde{f}$ が単射であることを示す．$f(x) = f(y)$ $(x, y \in G)$ と仮定する．$z = x^{-1}y$ とおくと, $f(z) = f(x^{-1})f(y) = f(x)^{-1}f(y) = e'$ となる．よって, $z \in \operatorname{Ker}(f)$ である．$y = xz$ より, $x\operatorname{Ker}(f) = y\operatorname{Ker}(f)$ である．
- $\widetilde{f}$ が全射であることと, 群準同型写像であることは明らかである．以上より, $\widetilde{f}$ は群同型である．

**例 2.36.** $f\colon \mathbb{R} \to \mathbb{C}^*$, $x \mapsto \exp(2i\pi x)$ を考える．明らかに, $f$ は $(\mathbb{R}, +)$ から $(\mathbb{C}^*, \times)$ への準同型である．また, $f$ の像は $U = \{z \in \mathbb{C} \mid |z| = 1\}$ であり, $f$ の核は $\mathbb{Z}$ である．よって群同型

$$\mathbb{R}/\mathbb{Z} \simeq U, \quad x + \mathbb{Z} \mapsto \exp(2i\pi x)$$

が存在する．

$G$ が群で, $x \in G$ とする．写像

$$f\colon \mathbb{Z} \to \langle x \rangle, \quad k \mapsto x^k$$

を考える．明らかに, $f$ は全射準同型である．

- $\operatorname{ord}(x) = m$ が有限ならば, $\operatorname{Ker}(f) = m\mathbb{Z}$ である．ゆえに, $f$ は群同型 $\widetilde{f}\colon \mathbb{Z}/m\mathbb{Z} \to \langle x \rangle$ を引き起こす．
- $\operatorname{ord}(x) = \infty$ ならば, $\operatorname{Ker}(f) = 0$ であるので, $f$ は群同型 $\mathbb{Z} \to \langle x \rangle$ である．

**系 2.37** $G$ を巡回群とする．$G$ が有限群ならば, $G \simeq \mathbb{Z}/m\mathbb{Z}$ である (但し, $m$ は $G$ の位数である)．$G$ が無限ならば $G \simeq \mathbb{Z}$ である．

**定理 2.38** $p$ を素数とする．このとき, $(\mathbb{Z}/p\mathbb{Z})^\times$ は巡回群である．

**注意 2.39.** $p$ が奇素数で, $r \geq 1$ のとき, $(\mathbb{Z}/p^r\mathbb{Z})^\times$ も巡回群である．しかし, $p = 2$ のとき $(\mathbb{Z}/2^r\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/2^{r-2}\mathbb{Z})$ $(r \geq 2)$ であることが証明できる．とくに, $r \geq 3$ のとき $(\mathbb{Z}/2^r\mathbb{Z})^\times$ は巡回群でない．

**定理 2.40: (有限アーベル構造定理)** $G$ を有限アーベル群とする．このとき，

$$G \simeq \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$$

かつ $n_k \mid n_{k-1} \mid \ldots \mid n_1$ を満たす自然数 $n_1, \ldots, n_k$ $(n_i \geq 2)$ が一意的に存在する．

## 2.5 可解群

**定義 2.41** $G$ が可解群であるとは，以下の条件を満たす部分群の有限列 $G = G_0 \supsetneq G_1 \supsetneq G_2 \supsetneq \cdots \supsetneq G_m = \{e\}$ が存在することをいう．

(a) $G_i \triangleleft G_{i-1}$ $(i = 1, \ldots, m)$.

(b) $G_{i-1}/G_i$ はアーベル群である $(i = 1, \ldots, m)$.

$p$ を素数とする．$|G| = p^k$ $(k \geq 1)$ のとき，$G$ が $p$ 群であるという．

**命題 2.42** $G$ を $p$ 群とする．このとき，

(1) $G$ の中心 $Z(G)$ は非自明である (すなわち，$Z(G) \neq \{e\}$ である).

(2) 正規部分群の列 $G = G_0 \supsetneq G_1 \supsetneq G_2 \supsetneq \cdots \supsetneq G_m = \{e\}$ が存在し，$G_i/G_{i-1} \simeq \mathbb{Z}/p\mathbb{Z}$ である．とくに，$G$ は可解群である．

**例 2.43.** $p, q$ が相異なる素数で，$|G| = p^a q^b$ $(a, b \in \mathbb{N})$ のとき，$G$ が可解である (バーンサイドの定理).

**定理 2.44: (Feit-Thompson の定理)** $G$ が有限群で，その位数が奇数ならば，$G$ が可解である．

**定理 2.45** $n \geq 5$ のとき，$\mathfrak{A}_n = \{\sigma \in \mathfrak{S}_n \mid \text{偶置換}\}$ は単純群である．

とくに，$n \geq 5$ のとき $\mathfrak{A}_n$ は可解でない．$\mathfrak{A}_5$ は位数 $\frac{5!}{2} = 60$ の群であり，非可解群の中で位数最小のものである．

**例 2.46.** $G = \mathfrak{S}_4$ とする．$|G| = 4! = 24$ である．$\mathfrak{S}_4$ は以下のような形の元から構成されている．ただし，$a, b, c, d$ を $\{1, 2, 3, 4\}$ の相異なるものとする．

$$\mathfrak{S}_4 \;=\; \{\mathrm{id},\ (ab),\ (abc),\ (ab)(cd),\ (abcd)\}.$$

以下の部分群を考える．

- $G_1 = \mathfrak{A}_4$,
- $G_2 = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}$,
- $G_3 = \langle (12)(34) \rangle$.

但し，$G_2$ が $\mathfrak{S}_4$ の部分群であることは直ちに確認できる．また，$G_0 = G$ 及び $G_4 = \{\mathrm{id}\}$ とおく．このとき，$G_i \triangleleft G_{i-1}$ であり，かつ $G_{i-1}/G_i$ は巡回群である．さらに

$$G = G_0 \supsetneq G_1 \supsetneq G_2 \supsetneq G_3 \supsetneq G_4 = \{\mathrm{id}\}$$

である．以上より，$\mathfrak{S}_4$ は可解群である．

## 2.6　シローの定理

$G$ を有限群とし, その位数を $n$ と書く. $p$ を $n$ の素因数とする. $n = p^k m$ と書くことができる. ただし, $k \geq 1$, $\gcd(p, m) = 1$ とする.

**定義 2.47**　$H$ を $G$ の部分群とする.
(a) $|H| = p^d$ $(d \geq 1)$ のとき, $H$ を $p$ 部分群という.
(b) $|H| = p^k$ のとき, $H$ を $G$ の $p$ シロー部分群という.

すなわち, $p$ シロー部分群は $p$ 部分群の中で最大位数のものである.

**定理 2.48**　$G$ を有限群とし, $|G| = n$ とおく. $p$ を $n$ の素因数とする.
(1) $G$ は $p$ シロー部分群を持つ.
(2) $K$ が $G$ の $p$ 部分群ならば, $K$ を含む $G$ の $p$ シロー部分群が存在する.
(3) $S, S'$ が $p$ シロー部分群ならば, $S' = gSg^{-1}$ となる $g \in G$ が存在する.
(4) $p$ シロー部分群の個数を $n_p$ とおくと, $n_p \equiv 1 \pmod{p}$ かつ $n_p \mid n$ が成り立つ. また, $S$ が $G$ の $p$ シロー部分群ならば, $n_p = [G : N_G(S)]$ である.

とくに, $S$ が $p$ シロー部分群のとき, 「$S \triangleleft G \iff n_p = 1$」が成り立つ.

**例 2.49.**

- $G = \mathfrak{A}_4$ とすると, $|G| = \frac{4!}{2} = 12 = 2^2 \times 3$ である. よって, $\mathfrak{A}_4$ の位数 4 の部分群が存在する. 長さ 3 の巡回置換は位数 3 の元であるので, 2 シロー部分群に属さない. ゆえに,

$$H = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}$$

が唯一の 2 シロー部分群である.　また, $\mathfrak{A}_4$ の 3 シロー部分群は

$$\langle (123) \rangle, \quad \langle (124) \rangle, \quad \langle (134) \rangle, \quad \langle (234) \rangle$$

の 4 つである.

- $G = \mathfrak{S}_4$ とすると, $|G| = 4! = 24 = 2^3 \times 3$ である. $a, b, c, d$ を $\{1, 2, 3, 4\}$ の相異なるものとする. このとき,

$$\langle (abcd), (ac) \rangle$$

は位数 8 の部分群であることが確認できる. ゆえに $\mathfrak{S}_4$ の 2 シロー部分群である. $\mathfrak{S}_4$ の 2 シロー部分群の個数は 3 である.

**系 2.50: コーシーの定理**　$G$ を位数 $n$ の群とし, $p$ を $n$ の素因数とする. このとき, $G$ は位数 $p$ の元を持つ.

**証明**

$H \subset G$ を $p$ シロー部分群とする. $x \in H$, $x \neq e$ ならば, $x$ の位数は $p^k$, $k \geq 1$ である. よって, 命題 2.12(1) により

$$\mathrm{ord}(x^{p^{k-1}}) = \frac{p^k}{p^{k-1}} = p$$

である.

# 3　可換環

## 3.1　定義

$A$ を空でない集合とし, $A$ 上の 2 つの演算 $(a,b) \mapsto a+b$ (足し算), $(a,b) \mapsto a \times b$ (掛け算) が与えられているとする. 掛け算は $a \times b = a \cdot b = ab$ とも書く. $(A,+,\times)$ が可換環であるとは, 以下が成り立つことをいう.

(a) $(A,+)$ はアーベル群である.
(b) $x(yz) = (xy)z$　(結合則)
(c) $xy = yx$　(交換則)
(d) $x(y+x) = xy + xz$　(分配則)
(e) $1 \in A$ が存在し, 任意の $x \in A$ に対し, $x1 = 1x = x$ である (単位元).

$1 = 0$ を満たす環は零環と呼び, 単に 0 で表す. このとき, 任意の $x$ に対し $x = x \cdot 1 = x \cdot 0 = 0$ であるので, 零環は元として 0 しか持たない. $A$ が可換環で, 部分集合 $B \subset A$ がを満たすとき, $A$ の部分環という.

- $0, 1 \in B$,
- $x, y \in B \implies x - y \in B$,
- $x, y \in B \implies xy \in B$

**例 3.1.** 通常の足し算・掛け算に関して, $\mathbb{Z}$ 及び $\mathbb{Z}/n\mathbb{Z}$ は可換環である. $\mathbb{Z}$ は $\mathbb{Q}$ の部分環である.

**例 3.2.**

- 以下の集合は $\mathbb{Q}$ の部分環である.

$$\mathbb{Z}\left[\frac{1}{2}\right] := \left\{ \frac{a}{2^m} \;\middle|\; a \in \mathbb{Z},\ m \geq 0 \right\}.$$

- 以下の集合は $\mathbb{C}$ の部分環である.

$$\mathbb{Z}[i] := \{a + ib \mid a, b \in \mathbb{Z}\}.$$

**定義 3.3**　$A$ を可換環とする. $x \in A$ が単元であるとは, $xy = 1$ を満たす $y \in A$ が存在することをいう. このとき, $y$ が一意的に定まり, $y = x^{-1}$ と書く.

$A$ の単元全体の部分集合を $A^\times$ と書き, 単元群という. $A^\times$ は乗法に関して群をなす.

**例 3.4.**

- $\mathbb{Z}^\times = \{\pm 1\}$ である.
- $\mathbb{Z}/n\mathbb{Z}$ の単元群は $(\mathbb{Z}/n\mathbb{Z})^\times = \left\{ \overline{k} \in \mathbb{Z}/m\mathbb{Z} \;\middle|\; \gcd(k,n) = 1 \right\}$ である.
- $\mathbb{Z}\left[\frac{1}{2}\right]$ の単元群は $\mathbb{Z}\left[\frac{1}{2}\right]^\times = \{\pm 2^k \mid k \in \mathbb{Z}\}$ である.
- $\mathbb{Z}[i]$ の単元群は $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$ である.

**定義 3.5**　$A$ が整域であるとは, 零環でなく, かつ任意の $x, y \in A$ に対し

$$xy = 0 \quad \Longrightarrow \quad x = 0 \ \text{ または } \ y = 0$$

が成り立つことをいう.

$A$ が整域のとき, $a, x, y \in A$ $(a \neq 0)$ で, $ax = ay$ ならば $x = y$ となる.

**例 3.6.** $\mathbb{Z}$, $\mathbb{Z}[i]$, $\mathbb{Z}\left[\frac{1}{2}\right]$ は整域である. $\mathbb{Z}/4\mathbb{Z}$ において $\overline{2} \times \overline{2} = \overline{0}$ であるので, $\mathbb{Z}/4\mathbb{Z}$ は整域でない.

**定義 3.7**　$A \neq 0$ を可換環とする．0 以外の元が全て単元のとき，$A$ が可換体であるという．

例えば，以下の集合は通常の演算に関して可換体をなす．

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

また，自然数 $n$ に対し，以下が同値である．

$$\mathbb{Z}/n\mathbb{Z} \text{ が整域である} \iff \mathbb{Z}/n\mathbb{Z} \text{ が可換体である} \iff n \text{ が素数である}.$$

$A$ が整域のとき，$A$ の商体 $\mathrm{Frac}(A)$ が定義できる．$\mathrm{Frac}(A)$ は可換体であり，$A$ を部分環として含む．さらに，$A$ を含む可換体の中で最小のものである．

$$\mathrm{Frac}(A) = \left\{ \frac{a}{b} \;\middle|\; a, b \in A,\ b \neq 0 \right\}$$

が成り立つ．例えば，$\mathbb{Z}$ の商体は $\mathbb{Q}$ である．$A$ が可換環で，多項式環 $A[X]$ を

$$A[X] = \left\{ \sum_{i=0}^{n} a_i X^i \;\middle|\; a_i \in A \right\}$$

によって定義する．$A[X]$ は可換環である．$P(X) \in A[X]$ に対し，$P$ の次数を $\deg(P)$ で表す．$A$ が整域のとき，$\deg(PQ) = \deg(P) + \deg(Q)$ が成り立つ．$A$ が整域ならば $A[X]$ も整域であり，その単元は $A^\times$ と一致する．

**定理 3.8: (多項式の除法原理)**　$A$ を整域とする．$P, M \in A[X]$ とし，$M$ の最高次係数が $A$ の単元であるとする．このとき，

$$P = QM + R \quad \text{かつ} \quad \deg(R) < \deg(M)$$

を満たす $Q, R \in A[X]$ が一意的に存在する．

**証明**

- $Q, R$ の一意性を示す．$P = Q_1 M + R_1 = Q_2 M + R_2$ かつ $\deg(R_1) < \deg(M), \deg(R_2) < \deg(M)$ とする．このとき，$M(Q_1 - Q_2) = R_2 - R_1$ である．$\deg(R_2 - R_1) \leq \max(\deg(R_1), \deg(R_2)) < \deg(M)$ より，$R_2 = R_1$ かつ $Q_1 = Q_2$ である．
- $Q, R$ の存在性を $P$ の次数に関する帰納法により証明する．$\deg(P) < \deg(M)$ のとき $Q = 0$, $R = P$ とおけば良い．$\deg(P) \geq \deg(M)$ とし，$M = \sum_{k=0}^{n} a_k X^k$, $P = \sum_{k=0}^{m} b_k X^k$ とおく．但し，$a_n, b_m \neq 0$ とする．仮定より，$a_n$ が単元である．

  $$P_1 := P - b_m a_n^{-1} X^{m-n} M$$

  と定める．$P_1$ の次数 $m$ の項は 0 であるので，$\deg(P_1) < \deg(P)$ である．帰納法の仮定より，$P_1 = Q_1 M + R_1$ かつ $\deg(R_1) < \deg(M)$ を満たす多項式 $Q_1, R_1$ が存在する．よって，

  $$P = P_1 + b_m a_n^{-1} X^{m-n} M = M(b_m a_n^{-1} X^{m-n} + Q_1) + R_1$$

  である．よって，$R = R_1$, $Q = b_m a_n^{-1} X^{m-n} + Q_1$ とおけば良い．

**定義 3.9**　$A, B$ を可換環とし，$f\colon A \to B$ を写像とする．$f$ が環の準同型であるとは，

- $f(x + y) = f(x) + f(y),\ \ x, y \in A,$
- $f(xy) = f(x)f(y),\ \ x, y \in A,$
- $f(1) = 1$

が成り立つことをいう．

**例 3.10.** $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $k \mapsto \overline{k}$ は環の準同型である. 一般的に, $A$ が可換環ならば, 写像

$$f_A \colon \mathbb{Z} \to A, \quad k \mapsto k \cdot 1$$

は環の準同型である. さらに, 環の準同型 $\mathbb{Z} \to A$ は $f_A$ に限る.

環の準同型 $f \colon A \to B$ が全単射ならば, $f$ を同型写像という.

## 3.2 イデアル

$A$ を可換環とする. $A$ のイデアルとは, 以下の 2 つの条件を満たす部分集合 $I \subset A$ のことをいう.

(a) $I$ は $(A, +)$ の部分群である.

(b) $a \in A,\ x \in I \implies ax \in I$.

例えば, $x_1, \ldots, x_n \in A$ に対し,

$$(x_1, \ldots, x_n) := \left\{ \sum_{i=1}^{n} a_i x_i \;\middle|\; a_i \in A \right\}$$

は $A$ のイデアルであり, $x_1, \ldots, x_n$ で生成されるイデアルという. このイデアルを $Ax_1 + \cdots + Ax_n$ と表すこともある. とくに, 一つの元 $x \in A$ で生成されるイデアルは

$$Ax = (x) = \{ax \mid a \in A\}$$

である. イデアル $I$ に対し, $I = Ax_1 + \cdots + Ax_n$ となる元 $x_1, \ldots, x_n$ が存在するときに, $I$ が有限生成イデアルであるという. また, $I = Ax$ を満たす $x \in A$ が存在するとき, $I$ が単項イデアルであるという. イデアル $I$ 内に単元 $u$ が存在するとき, $I = A$ である. なぜならば, 任意の $x \in A$ に対し, $x = (xu^{-1})u$ と書けるので, $x \in I$ となる.

**定義 3.11** $A$ を整域とする. $b = ac$ となる $c \in A$ が存在するとき, $a$ が $b$ の約数であるといい, $a \mid b$ と表す.

**注意 3.12.** 明らかに, $a \mid b \iff (b) \subset (a)$ が成り立つ. 例えば, $A = \mathbb{Z}$ の場合に, $4\mathbb{Z} \subset 2\mathbb{Z}$ が成り立つ.

$A$ を整域とする. $a, b \in A \setminus \{0\}$ に対し, $b = au$ となる単元が存在するとき, $a, b$ が同伴であるといい, $a \sim b$ と書く. 「$\sim$」は $A$ 上の同値関係である. 0 でない元 $a, b \in A$ に対し,

$$\begin{aligned} a \sim b &\iff (a) = (b) \\ &\iff a \mid b \ \text{ かつ } \ b \mid a \end{aligned}$$

が成り立つ. 実際, $c, d \in A$ で $b = ac$ かつ $a = bd$ と表せるならば, $a = acd$ となる. $A$ が整域だから, $1 = cd$ となり, ゆえに $c, d \in A^\times$ である. よって $a \sim b$ である. 逆は自明である.

**補題 3.13** $A$ が可換体である $\iff$ $A \neq 0$, かつ 0, $A$ 以外のイデアルを持たない.

**証明**

「$\Longrightarrow$」は明らかである. 逆に, $A \neq 0$ が 0, $A$ 以外のイデアルを持たないとする. このとき, $x \in A \setminus \{0\}$ とすると, $(x) = A$ が成り立つ. よって, $xy = 1$ となる $y \in A$ が存在する.

言い換えれば, $A$ が可換体であることは, $A$ がちょうど 2 つのイデアル (すなわち 0 と $A$) を持つことと同値である.

**定義 3.14**　$A$ を可換環とする.
(a) $A$ の全てのイデアルが有限生成であるときに, $A$ をネーター環という.
(b) $A$ が整域で, $A$ の全てのイデアルが単項イデアルであるとき, $A$ を単項イデアル整域という.

明らかに, 単項イデアル整域はネーター環である.

**例 3.15.** $\mathbb{Z}$ のイデアルは, $\mathbb{Z}$ の部分群に他ならない. ゆえに, $\mathbb{Z}$ のイデアルは $n\mathbb{Z}$, $n \geq 0$ である. とくに, それらは単項イデアルであるので, $\mathbb{Z}$ は単項イデアル整域である.

**例 3.16.** $A = \mathcal{C}([0,1], \mathbb{R})$ を区間 $[0,1]$ 上の連続関数全体のなす可換環とする (ただし, 通常の足し算と掛け算を考える). $n \geq 1$ に対し,

$$J_n = \left\{ f \colon [0,1] \to \mathbb{R} \mid 0 \leq x \leq \frac{1}{n} \text{ に対し } \ f(x) = 0 \right\}$$

と定める. $(J_n)$ は $A$ のイデアルの昇鎖である (すなわち, $J_n \subset J_{n+1}$ が成り立つ). $J = \bigcup_{n \geq 1} J_n$ とおくと, $J$ は $A$ のイデアルであるが, 有限生成でない (レポート 2 参照). よって, $A$ はネーター環でない.

**定理 3.17**　$K$ を可換体とする. このとき, 多項式環 $K[X]$ は単項イデアル整域である.

**証明**

$I \subset K[X]$ $(I \neq 0)$ をイデアルとする. $I \setminus \{0\}$ の元の中から, 次数が最小のものを一つとり, それを $M$ とおく. このとき, $P \in I$ ならば, 除法の原理より $P = MQ + R$ かつ $\deg(R) < \deg(M)$ を満たす多項式 $Q, R$ が存在する. $P, M \in I$ より, $R = P - MQ$ も $I$ に属する. $M$ の最小性より, $R = 0$ となり, すなわち $P = MQ$ である. よって, $I = (M(X))$ が成り立つ. 以上より, $K[X]$ は単項イデアル整域である.

**注意 3.18.** $M(X)$ を多項式とし, $a \neq 0$ を $M(X)$ の最高次係数とする. $M(X)$ と $a^{-1}M(X)$ が同伴であるので, それらは同じイデアルを生成する. ゆえに, $K[X]$ の任意のイデアル $I \neq 0$ に対し, $I = (M(X))$ を満たすモニックな多項式 $M(X)$ が一意的に存在する.

**定理 3.19: (ヒルベルトの定理)**　$A$ がネーター環ならば, 多項式環 $A[X]$ もネーター環である.

$X_1, \ldots, X_n$ を有限個の変数とする. $X_1, \ldots, X_n$ に関する多変数多項式環 $K[X_1, \ldots, X_n]$ を帰納法的に

$$K[X_1, \ldots, X_n] = (K[X_1, \ldots, X_{n-1}])[X_n]$$

によって定義する. ヒルベルトの定理より, $K[X_1, \ldots, X_n]$ はネーター環であることが分かる. しかし, $n \geq 2$ のとき単項イデアル整域ではない. また, 無限個の変数に関する多項式環 $A = K[X_1, X_2, \ldots]$ はネーター環でない. 実際, イデアル $\{P \in A \mid P(0) = 0\}$ は有限生成でない.

## 3.3　可換体の準同型定理

$A$ を可換環とし, $I$ を $A$ のイデアルとする. とくに $I$ は $A$ の部分群であるので, 剰余群 $A/I$ を考えることができる. $x, y \in A$ に対し,

$$(x + I) \cdot (y + I) \ = \ xy + I$$

とおくことによって, $A/I$ に掛け算を入れる. 但し, この演算が well-defined であることに注意する. 実際, $x, y, x', y' \in A$ で $x + I = x' + I$ かつ $y + I = y' + I$ が成り立つならば,

$$x'y' = xy + x'(y' - y) + y(x' - x)$$

と書ける．$x'-x$ 及び $y'-y$ は $I$ に属するので，$a=x'(y'-y)+y(x'-x)$ も $I$ の元である．ゆえに，$x'y'+I=xy+I$ となり，演算は剰余類の代表元の取り方に依らない．$A/I$ は可換環であり，イデアル $I$ による $A$ の剰余環と呼ばれる．写像 $\pi\colon A\to A/I$, $x\mapsto x+I$ は環の準同型である．

**例 3.20.** $A=\mathbb{Z}$, $I=n\mathbb{Z}$ とする．$n\mathbb{Z}$ による $\mathbb{Z}$ の剰余環は $\mathbb{Z}/n\mathbb{Z}$ に他ならない．

$f\colon A\to B$ を環の準同型とする．このとき，

$$\mathrm{Ker}(f):=\{x\in A\mid f(x)=0\}$$

とおき，$f$ の核という．$\mathrm{Ker}(f)$ は $A$ のイデアルである．

**定理 3.21: (環の準同型定理)** $f\colon A\to B$ を可換環の準同型とし，$I=\mathrm{Ker}(f)$ とおく．このとき，$\mathrm{Im}(f)$ は $B$ の部分環であり，さらに以下の写像は環の同型写像である．

$$A/I\to\mathrm{Im}(f),\quad x+I\mapsto f(x).$$

**証明**

上の写像が群同型であることは既に知っている．$f$ は明らかに環の準同型であるので，主張がわかる．

**例 3.22.** $A=\mathbb{R}[X]$, $B=\mathbb{C}$ とし，写像

$$f\colon\mathbb{R}[X]\to\mathbb{C},\quad P(X)\mapsto P(i)$$

を考える．$f$ は環の準同型であり，$\mathrm{Ker}(f)$ は多項式 $X^2+1$ で生成されるイデアルである．また，明らかに $\mathrm{Im}(f)=\mathbb{C}$ である．ゆえに，環の同型写像

$$\frac{\mathbb{R}[X]}{(X^2+1)}\to\mathbb{C},\qquad P(X)+(X^2+1)\mapsto P(i)$$

が得られる．

**定義 3.23** $I$ を $A$ のイデアルとする．
(a) $A/I$ が整域であるとき，$I$ が素イデアルであるという．
(b) $A/I$ が可換体であるとき，$I$ が極大イデアルであるという．

$I,J$ が $A$ のイデアルで，$I\subset J$ のとき $J/I$ は $A/I$ のイデアルである．$J\mapsto J/I$ という対応により，$I$ を含む $A$ のイデアル全体と $A/I$ のイデアル全体は一対一で対応している．このことから以下がわかる．

$$\begin{aligned}I\text{ が極大イデアルである}&\iff A/I\text{ が可換体である}\\&\iff I\neq A\text{ かつ }I\subsetneq J\subsetneq A\text{ を満たすイデアル }J\text{ が存在しない．}\end{aligned}$$

ゆえに，$I$ が極大イデアルであるならば，$I$ より大きいイデアルは $A$ に限る．零環でない可換環においては常に極大イデアルが存在する (一般には複数の極大イデアルが存在する)．さらに，$J\neq A$ がイデアルならば $J$ を含む極大イデアルが存在する．明らかに，以下が成り立つ．

$$\begin{aligned}A\text{ が可換体である}&\iff 0\text{ が極大イデアルである}\\A\text{ が整域である}&\iff 0\text{ が素イデアルである}\end{aligned}$$

**例 3.24.**

- $A=\mathbb{Z}$ とする．$n\geq 1$ に対し 「$n\mathbb{Z}$ が素イデアル」 $\iff$ 「$n\mathbb{Z}$ が極大イデアル」 $\iff$ 「$n$ が素数」．しかし，零イデアル 0 は素イデアルであるが，極大イデアルでない．

- $A = \mathbb{Z}[X]$ とし, $\mathfrak{p} = (2)$, $\mathfrak{m} = (2, X)$ とおく. 写像

$$f\colon \mathbb{Z}[X] \to (\mathbb{Z}/2\mathbb{Z})[X], \quad \sum_{i=0}^{n} a_i X^i \mapsto \sum_{i=0}^{n} \overline{a}_i X^i \qquad (\text{但し}, \overline{a}_i = a_i + 2\mathbb{Z})$$

は全射環準同型であり, $\mathrm{Ker}(f) = \mathfrak{p}$ が成り立つ. 準同型定理により, $\mathbb{Z}[X]/\mathfrak{p} \simeq (\mathbb{Z}/2\mathbb{Z})[X]$ である. よって, $\mathfrak{p}$ は素イデアルであるが極大イデアルでない. また, 写像

$$f\colon \mathbb{Z}[X] \to \mathbb{Z}/2\mathbb{Z}, \quad \sum_{i=0}^{n} a_i X^i \mapsto \overline{a}_0$$

は $\mathfrak{m}$ を核とする全射準同型だから, $\mathbb{Z}[X]/\mathfrak{m} \simeq \mathbb{Z}/2\mathbb{Z}$ である. とくに, $\mathfrak{m}$ は極大イデアルである.

$A$ を可換環とし, 自然な準同型

$$f\colon \mathbb{Z} \to A, \quad k \mapsto k \cdot 1$$

を考える. $\mathrm{Ker}(f)$ は $\mathbb{Z}$ のイデアルであるので, $\mathrm{Ker}(f) = n\mathbb{Z}$ となる $n \geq 0$ が一意的に存在する. $n$ を $A$ の標数といい, $n = \mathrm{char}(A)$ とおく. 準同型定理により同型写像 $\mathbb{Z}/n\mathbb{Z} \simeq \mathrm{Im}(f)$ が存在する. よって

$$\begin{cases} \mathrm{char}(A) = 0 & \text{のとき} \quad \mathbb{Z} \subset A \\ \mathrm{char}(A) = n & \text{のとき} \quad \mathbb{Z}/n\mathbb{Z} \subset A. \end{cases}$$

$A$ が整域である場合に, $\mathbb{Z}/n\mathbb{Z}$ も整域になり, ゆえに $n = \mathrm{char}(A)$ が 0 または素数である. 例えば, 多項式環 $(\mathbb{Z}/p\mathbb{Z})[X]$ は標数 $p$ の整域である.

**命題 3.25** $p$ が素数で, $A$ を標数 $p$ の可換環とする. このとき, 以下が成り立つ.

$$(x + y)^p = x^p + y^p \qquad x, y \in A.$$

**証明**

二項式により,

$$(x + y)^p = \sum_{i=0}^{p} \binom{p}{i} x^i y^{p-i} \qquad x, y \in A.$$

が成り立つ. また, 任意の $1 \leq i \leq p-1$ に対し, $\binom{p}{i}$ は $p$ の倍数である. なぜならば, $\binom{p}{i} \times i! = p! \equiv 0 \pmod{p}$ かつ $\gcd(i!, p) = 1$ より, $\binom{p}{i} \equiv 0 \pmod{p}$ である. $A$ の標数が $p$ だから, $A$ において $p \cdot 1 = 0$ である. ゆえに, $(x + y)^p = x^p + y^p$ となる.

明らかに, $(xy)^p = x^p y^p$ も成り立つので, 写像 $F_A\colon A \to A$, $x \mapsto x^p$ は環の準同型写像である. $F_A$ は $A$ のフロベニウス自己準同型と呼ばれる.

## 3.4 素元, 既約元

$A$ を整域とする.

**定義 3.26** $a \in A$ $(a \neq 0)$ とする.

- $a$ が既約元であるとは, $a$ が単元でなく, かつ以下が成り立つことをいう.

$$a = bc \quad \Longrightarrow \quad b \in A^\times \text{ または } c \in A^\times.$$

- $a$ が素元であるとは, $a$ が単元でなく, かつ以下が成り立つことをいう.

$$a \mid bc \quad \Longrightarrow \quad a \mid b \text{ または } a \mid c.$$

**補題 3.27**　素元は既約元である.

**証明**

$a$ が素元で, $a = bc$ $(b, c \in A)$ とする. このとき $a \mid bc$ であるので, $a \mid b$ または $a \mid c$ となる. 前者の場合を考えれば十分である. このとき, $b = ad$ と表すことができる. よって, $b = ad = bcd$ となる. $b \neq 0$ より $1 = cd$ となる. よって $b \in A^\times$. ゆえに $a$ が既約元である.

**注意 3.28.**

- $a$ が素元である $\iff$ $(a)$ が素イデアルである.
- $a$ が既約元である $\iff$ $(a)$ が単項イデアルの中で極大元である. 但し, ここでいう「単項イデアルの中で極大元」とは, $(a)$ を含む単項イデアルが $(a)$ と $A = (1)$ に限ることを意味する. (但し, 一般には単項イデアルでないイデアルも存在するので, このとき $(a)$ が極大イデアルとは限らない).

**定義 3.29**　単元でない任意の $x \in A$ $(x \neq 0)$ が有限個の素元の積で表すことができるとき, $A$ が一意分解環であるという.

一意分解環において「既約元」$\iff$「素元」が成り立つ. つまり, 既約元と素元は一致する. ネーター環の場合はその逆も成り立つ.

**命題 3.30**　$A$ をネーター整域とする. このとき, 以下が同値である.

(i)　$A$ が一意分解環である.

(ii)　既約元と素元が一致する.

**定理 3.31**　単項イデアル整域は一意分解環である.

例えば, $K$ が可換体のとき, 多項式環 $K[X]$ は単項イデアル整域であるので, 一意分解環である. $P(X)$ が $K[X]$ の既約元ならば, $P(X)$ を $K$ 上の既約多項式という.

**例 3.32.**

- $K = \mathbb{C}$ とする. このとき, 任意の多項式 $P(X) \in \mathbb{C}[X]$ $(\deg(P) \geq 1)$ が $P(X) = u(X - a_1) \dots (X - a_n)$ と分解できる (但し $u \in \mathbb{C}^*$, $a_i \in \mathbb{C}$ である). ゆえに, $\mathbb{C}[X]$ の既約元は一次式 $aX + b$ $(a \in \mathbb{C}^*, b \in \mathbb{C})$ に限る.
- $K = \mathbb{R}$ とする. $\mathbb{R}[X]$ の既約元は

$$\{aX + b \mid a \neq 0\} \cup \{aX^2 + bX + c \mid \text{判別式 } b^2 - 4ac < 0\}$$

である.

**命題 3.33**　$A$ が単項イデアル整域で, $I$ を 0 でないイデアルとする. このとき, 以下が成り立つ.

$$I \text{ が素イデアル} \iff I \text{ が極大イデアル}$$

**証明**

$I$ が素イデアルであるとし, $I \subset J \subset A$ とする. $A$ が単項イデアル整域だから, $x, y \in A$ が存在し $I = (x)$, $J = (y)$ である. 仮定より $x = yz$ となる $z \in A$ が存在する. $x$ が既約元であるので, $z \in A^\times$ または $y \in A^\times$ である. ゆえに, $J = I$ または $J = A$ である. 以上より, $I$ は極大イデアルである.

$x$ が既約元で, $x \sim y$ であるならば, 明らかに $y$ も既約元である. 但し, ここで「$\sim$」は同伴関係である. 各既約元の同値類から一つの代表元を選び, それらを集めた集合を $\mathcal{P}$ とおく. $\mathcal{P}$ は既約元の完全代表系と呼ばれる. 例えば, $A = \mathbb{Z}$ のとき, $\mathcal{P} = \{ \text{素数} \} = \{2, 3, 5, \dots\}$ は既約元の完全代表系である. $A$ の既約元の完全代表系 $\mathcal{P}$ を固定する. このとき, 任意の $x \in A \setminus \{0\}$ が一意的に

$$x = u \prod_{p \in \mathcal{P}} p^{v_p(x)}, \qquad u \in A^\times,\ v_p(x) \geq 0$$

と表すことができる. ただし, 有限個を除き全ての $v_p(x)$ が 0 であるので, 上の積は有限積である.

**例 3.34.** $A = \mathbb{Z}$ のとき, $\mathcal{P}$ として素数全体の集合をとる. $v_p(a)$ は $a$ の $p$ 進付値という. 例えば,

$$-24 = (-1) \times 2^3 \times 3^1$$

である. よって, $v_2(24) = 3$, $v_3(24) = 1$, 他の素数 $p$ に対し $v_p(24) = 0$ である.

0 でない元 $x_1, \dots, x_m$ に対し,

$$\gcd(x_1, \dots, x_m) := \prod_{p \in \mathcal{P}} p^{\min(v_p(x_1), \dots, v_p(x_m))}$$
$$\mathrm{lcm}(x_1, \dots, x_m) := \prod_{p \in \mathcal{P}} p^{\max(v_p(x_1), \dots, v_p(x_m))}$$

とおき, それぞれを $x_1, \dots, x_m$ の最大公約数, 最小公倍数という. $\gcd(x_1, \dots, x_m)$ と $\mathrm{lcm}(x_1, \dots, x_m)$ は 既約元の完全代表系 $\mathcal{P}$ の選び方に依存するが, 同伴を除いては一意的に定まることに注意する. $x_1, \dots, x_m$ が $A$ の元で, その中で少なくとも 1 つが 0 でないときに, 0 でない $x_i$ の最大公約数を $\gcd(x_1, \dots, x_m)$ とおき, 最大公約数の定義をこの場合に拡張する.

**定義 3.35** $P(X) = \sum_{i=0}^n a_i X^i$ を 0 でない $A[X]$ の多項式とする. このとき,

$$c(P) := \gcd(a_0, a_1, \dots, a_n)$$

とおき, $P(X)$ の内容という. $P(X)$ の内容が単元であるとき, $P(X)$ が原始多項式であるという.

**例 3.36.** 例えば, $A = \mathbb{Z}$ の場合に, $P = 2X^3 - 4X + 7$ は原始多項式である ($\gcd(2, -4, 7) = 1$ である).

多項式の内容は乗法的関数である. すなわち, 任意の $P, Q \in A[X]$ $(P, Q \neq 0)$ に対し, 同伴を除いて

$$c(PQ) = c(P)c(Q)$$

が成り立つ. このことから, 以下の定理が証明できる.

**定理 3.37** $A$ を一意分解環とし, その商体を $K$ とおく. このとき, $A[X]$ も一意分解環である. さらに, $A[X]$ の既約元は以下の形の元である.

- (次数 0 の多項式として考えた)$A$ の既約元.
- 一意分解環 $K[X]$ において既約である $A[X]$ の原始多項式.

**例 3.38.** $\mathbb{Z}[X]$ の既約元は

$$\{\pm p \mid p : \text{素数}\} \cup \{ \text{原始多項式} \mid \mathbb{Q}[X] \text{ において既約} \}$$

例えば, 次の元は $\mathbb{Z}[X]$ の既約元である：$-11$, $4X + 1$, $2X^2 - 1$.

# 4　体論

## 4.1　代数的拡大

**定義 4.1**　$L$ が可換体で, $K \subset L$ を部分集合とする. $K$ が $L$ の部分体であるとは, 以下が成り立つことをいう.

(i) $0, 1 \in K$

(ii) $x, y \in K \implies x - y \in K$

(iii) $x, y \in K \implies xy \in K$

(iv) $x \in K,\ x \neq 0 \implies \frac{1}{x} \in K$.

すなわち, $L$ の部分体は, 体である $L$ の部分環に他ならない. 例えば, $\mathbb{Q}$ は $\mathbb{R}$ の部分体であり, $\mathbb{R}$ は $\mathbb{C}$ の部分体である.

**例 4.2.** 以下の集合を考える.

$$\mathbb{Q}(\sqrt{3}) := \{a + b\sqrt{3} \mid a, b \in \mathbb{Q}\}.$$

$\sqrt{3}$ が無理数だから, $\mathbb{Q}(\sqrt{3})$ は $(1, \sqrt{3})$ を基底とする $\mathbb{Q}$ ベクトル空間である. $\mathbb{Q}(\sqrt{3})$ が $\mathbb{R}$ の部分体であることを確認する. 定義 4.1 の (i), (ii) は明らかに成り立つ. (iii) について考える. $x = a + b\sqrt{3}$, $y = c + d\sqrt{3}$ $(a, b, c, d \in \mathbb{Q})$ とすると,

$$xy = (a + b\sqrt{3})(c + d\sqrt{3}) = (ac + 3bd) + (ad + bc)\sqrt{3}$$

となり, $xy \in \mathbb{Q}(\sqrt{3})$ である. 最後に, (iv) について考える. $x = a + b\sqrt{3}$ $(a, b \in \mathbb{Q})$ で $x \neq 0$ とする. このとき,

$$\frac{1}{x} = \frac{1}{a + b\sqrt{3}} = \frac{a - b\sqrt{3}}{(a + b\sqrt{3})(a - b\sqrt{3})} = \frac{a - b\sqrt{3}}{a^2 - 3b^2} = \frac{a}{a^2 - 3b^2} - \frac{b}{a^2 - 3b^2}\sqrt{3}$$

である. 但し, $a^2 - 3b^2 \neq 0$ であることに注意する. ゆえに, $\frac{1}{x} \in \mathbb{Q}(\sqrt{3})$ である.

**定義 4.3**

(a) $K$ が $L$ の部分体のとき, $L$ を $K$ の体拡大といい, $L/K$ と表す.

(b) $K \subset L' \subset L$ を満たす部分体 $L'$ を $L/K$ の中間体という. または, $L'/K$ が $L/K$ の部分拡大であるという.

$L/K$ が体拡大ならば, $L$ を自然に $K$ ベクトル空間と見ることができる. $L$ が有限次元 $K$ ベクトル空間であるとき, $L/K$ を有限次拡大という.

$$[L : K] := \dim_K(L)$$

とおき, $L/K$ の次数という. 例えば, $\mathbb{C}$ は 2 次元 $\mathbb{R}$ ベクトル空間であるので, $[\mathbb{C} : \mathbb{R}] = 2$ である. $K \subset L' \subset L$ のとき,

$$[L : K] = [L : L'] \times [L' : K]$$

が成り立つ. 実際, $(e_i)_i$ と $(f_j)_j$ がそれぞれ $L'/K$ と $L/L'$ の基底ならば, $(e_i f_j)_{i,j}$ は $L/K$ の基底である.

$L/K$ を体拡大とし, $\alpha \in L$ とする. 環準同型

$$\varphi_\alpha \colon K[X] \to L, \qquad P(X) \mapsto P(\alpha)$$

を考える. $\varphi_\alpha$ の像を $K[\alpha]$ とおく. 具体的に,

$$K[\alpha] = \mathrm{Span}_K(1, \alpha, \alpha^2, \dots)$$

である．但し，$\mathrm{Span}_K(1,\alpha,\alpha^2,\dots)$ とは，$1,\alpha,\alpha^2,\dots$ の $K$-線形結合全体の集合のことである．$K[\alpha]$ は $L$ の部分環である．$K[\alpha]$ の商体を $K(\alpha)$ とおく．$K(\alpha)$ は，$\alpha$ を含む $L/K$ の部分拡大の中で最小のものであり，$\alpha$ で生成される部分拡大 (または $K$ に $\alpha$ を添加した拡大) と呼ばれる．同様に，$\alpha_1,\dots,\alpha_n \in L$ に対し，$P \in K[X_1,\dots,X_n]$ で $P(\alpha_1,\dots,\alpha_n)$ という形の元全体の集合を $K[\alpha_1,\dots,\alpha_n]$ とおき，その商体を $K(\alpha_1,\dots,\alpha_n)$ とおく．$\alpha_1,\dots,\alpha_n$ を含む部分拡大の中で最小のものである．

**定義 4.4**

(a) $\alpha \in L$ が $K$ 上代数的であるとは，多項式 $M(X) \in K[X]$ $(M \neq 0)$ が存在し，$M(\alpha) = 0$ であることをいう．

(b) $L$ の全ての元が $K$ 上代数的ならば，$L/K$ を代数的拡大という．

環準同型 $\varphi_\alpha \colon K[X] \to L$, $P(X) \mapsto P(\alpha)$ を考える．準同型の定理により，同型写像

$$\frac{K[X]}{\mathrm{Ker}(\varphi_\alpha)} \simeq K[\alpha]$$

が得られる．$K[\alpha]$ は $L$ の部分環であるので，整域である．ゆえに，$\mathrm{Ker}(\varphi_\alpha)$ は $K[X]$ の素イデアルである．$K[X]$ が単項イデアル整域なので，

$$\mathrm{Ker}(\varphi_\alpha) = (\mu_{\alpha,K}(X))$$

を満たすモニックな多項式 $\mu_{\alpha,K}(X)$ が一意的に存在する．$\mathrm{Ker}(\varphi_\alpha)$ が素イデアルであるので，$\mu_{\alpha,K}$ は $K[X]$ の既約多項式である．

**定義 4.5** $\mu_{\alpha,K}(X)$ は $\alpha$ の $K$ 上の最小多項式と呼ばれる．

具体的に，$\mu_{\alpha,K}(X)$ は $P(\alpha) = 0$ を満たすモニックな多項式 $P(X) \in K[X] \setminus \{0\}$ の中で，次数が最小のものである．

**例 4.6.** 複素数 $i$ は $\mathbb{Q}$ 上代数的であり，$\mu_{i,\mathbb{Q}}(X) = X^2+1$ である．同様に，$\mu_{i,\mathbb{R}}(X) = X^2+1$ である．しかし，$\mu_{i,\mathbb{C}}(X) = X - i$ であることに注意する．

命題 3.33 により

$$\begin{aligned} \alpha \text{ が } K \text{ 上代数的である} &\iff \mathrm{Ker}(\varphi_\alpha) \neq 0 \\ &\iff \mathrm{Ker}(\varphi_\alpha) \text{ が極大イデアルである} \\ &\iff K[\alpha] \text{ が可換体である} \\ &\iff K[\alpha] = K(\alpha). \end{aligned}$$

**命題 4.7** $\alpha$ が $K$ 上代数的である $\iff$ $[K(\alpha):K] < \infty$ である．さらに，このとき

$$[K(\alpha):K] = \deg(\mu_{\alpha,K}).$$

**証明**

- $\alpha$ を $K$ 上代数的な元とし，$M(X) := \mu_{\alpha,K}(X)$, $m = \deg(\mu_{\alpha,K})$ とおく．多項式の除法より，$P \in K[X]$ に対し，$P = MQ + R$ かつ $\deg(R) < m$ を満たす $Q, R \in K[X]$ が存在する．よって，

  $$P(\alpha) = M(\alpha)P(\alpha) + R(\alpha) = R(\alpha)$$

  となる．したがって，$K[\alpha] = \mathrm{Span}_K(1,\alpha,\dots,\alpha^{m-1})$ である．また，$\mu_{\alpha,K}(X)$ の次数の最小性より，$1,\alpha,\dots,\alpha^{m-1}$ は $K$ 上線形独立である．$K(\alpha) = K[\alpha]$ より，$[K(\alpha):K] = m$ となる．
- 逆に，$m = [K(\alpha):K] < \infty$ とする．このとき，$\{1,\alpha,\alpha^2,\dots,\alpha^m\}$ は線形従属である．ゆえに，

$M(\alpha) = 0$ となる $M \in K[X]$ $(M \neq 0)$ が存在する.

**系 4.8** $\alpha_1, \ldots, \alpha_n \in L$ を $K$ 上代数的な元とする. このとき, $K(\alpha_1, \ldots, \alpha_n)$ は $K$ の有限次拡大である.

**証明**

$n$ に関する帰納法によって示す. $n = 1$ のとき命題 4.7 から従う. $n > 1$ とする. $\alpha_n$ が $K$ 上代数的であるので, とくに $K' = K(\alpha_1, \ldots, \alpha_{n-1})$ 上代数的である. よって, $K'(\alpha_n)$ は $K'$ の有限次拡大である. また, 帰納法の仮定より, $K'/K$ も有限次拡大である.

$$[K'(x_n) : K] = [K'(x) : K'][K' : K]$$

より, $K'(x_n) = K(\alpha_1, \ldots, \alpha_n)$ は $K$ の有限次拡大である.

**系 4.9** $L/K$ を体拡大とする. このとき, $K$ 上代数的である $L$ の元全体の集合は $K$ を含む $L$ の部分体である.

**証明**

$K$ 上代数的である $L$ の元全体の集合を $L'$ とおく. 明らかに, $a \in K$ ならば $a \in L'$ である (多項式 $M(X) = X - a$ は $M(a) = 0$ を満たす). $x, y \in L'$ とする. 系 4.8 により, $K(x, y)$ は $K$ の有限次拡大である. $K(x - y)$ 及び $K(xy)$ は $K(x, y)$ の部分拡大であるので, $K$ 上有限次拡大である. よって, $x - y, xy \in L'$ である.

## 4.2 代数的閉体

多項式 $P(X) \in K[X]$ $(\deg(P) \geq 1)$ が $K$ で分解するとは,

$$P(X) = u(X - a_1) \ldots (X - a_n)$$

となる $u \in K^*$ 及び $a_1, \ldots, a_n \in K$ が存在することをいう.

**定義 4.10** 可換体 $K$ が代数的閉体であるとは, 任意の多項式 $P(X) \in K[X]$ $(\deg(P) \geq 1)$ が $K$ で分解することをいう.

**命題 4.11** 以下が同値である.

(i) $K$ が代数的閉体である.

(ii) 任意の多項式 $P(X) \in K[X]$ $(\deg(P) \geq 1)$ が $K$ 内に根をもつ.

(iii) $K$ が非自明な代数的拡大を持たない.

**証明**

- 「(i) $\Longrightarrow$ (ii)」は明らかである.
- 「(ii) $\Longrightarrow$ (iii)」を示す. $L/K$ を代数的拡大とし, $x \in L$ とする. $M(X) = \mu_{x,K}(X)$ とおく. (ii) より, $M(y) = 0$ を満たす $y \in K$ が存在する. このとき $X - y \mid M(X)$ となるので, 既約性より $M(X) = X - y$, すなわち $x = y \in K$ となる. よって $L = K$ である.
- 「(iii) $\Longrightarrow$ (i)」を示す. $M(X) \in K[X]$ を既約多項式とする. このとき, $(M(X))$ は $K[X]$ の極大イ

デアルであるので,

$$L := \frac{K[X]}{(M(X))}$$

は可換体である. また, 自然な体の準同型 $K \to L$, $a \mapsto a + (M(X))$ が存在するので, $L$ を $K$ の体拡大とみなすことができる. (iii) より, $L = K$ であるので, $\deg(M) = 1$ となる. ゆえに, $K[X]$ の任意の多項式一次式の積で表せる.

**定理 4.12: (代数学の基本定理)** $\mathbb{C}$ は代数的閉体である.

## 4.3 $K$-準同型, $K$-自己同型

$L_1, L_2$ を可換体とする. 体の準同型 $f\colon L_1 \to L_2$ は常に単射であることに注意する. なぜならば, $\mathrm{Ker}(f)$ は $L_1$ とは異なるイデアルだから, $\mathrm{Ker}(f) = 0$ である. よって, $f$ は単射である. とくに, $L_1$ と $f(L_1)$ は同型である. 今, $L_1/K$ と $L_2/K$ を $K$ の 2 つの体拡大とする.

**定義 4.13** 写像 $\sigma\colon L_1 \to L_2$ が $K$-準同型であるとは, 以下の 2 つ条件を満たすことをいう.

- $\sigma$ が体の準同型である.
- $\sigma(x) = x, \quad x \in K.$

また, $L_1 = L_2 = L$ のとき, $\sigma$ を $L$ の $K$-自己同型という.

$K, K'$ を可換体とし, $\sigma\colon K \to K'$ を体の準同型とする. 多項式 $P(X) = \sum_{i=0}^{n} a_i X^i \in K[X]$ に対し,

$$\sigma(P)(X) := \sum_{i=0}^{n} \sigma(a_i) X^i \in K'[X]$$

と定義する. 明らかに, $\sigma(P)$ の係数は部分体 $\sigma(K)$ に属する. 任意の $z \in \overline{K}$ に対し

$$\sigma(P(z)) = \sigma(P)(\sigma(z))$$

が成り立つので, $z \in K$ が $P(X)$ の根ならば, $\sigma(z)$ は $\sigma(P)(X)$ の根である.

**命題 4.14** $\sigma\colon K \to K'$ を体の準同型とし, $P \in K[X]$ を既約多項式とする. $L/K$ 及び $L'/K'$ を体拡大とし, $\alpha \in L$, $\alpha' \in L'$ をそれぞれ $M(X)$, $\sigma(M)(X)$ の根とする. このとき, $\sigma(\alpha) = \alpha'$ となるように $\sigma$ が体の準同型

$$\sigma\colon K(\alpha) \to L'$$

に一意的に延長できる.

$$\begin{array}{ccc} K(\alpha) & \xrightarrow{\sigma} & L' \\ \cup & & \cup \\ K & \xrightarrow[\sigma]{} & K' \end{array}$$

**証明**

$M(\alpha) = 0$ より $\mu_{\alpha,K}(X) \mid M(X)$ である. $M(X)$ が $K$ 上既約であるので, 同伴を除いて $\mu_{\alpha,K}(X) = M(X)$ である. 環の準同型 $\varphi_\alpha\colon K[X] \to L$, $P(X) \mapsto P(\alpha)$ を考える. $\mathrm{Im}(\varphi_\alpha) = K[\alpha] = K(\alpha)$ であり,

$\mathrm{Ker}(\varphi_\alpha) = (\mu_{\alpha,K}(X)) = (M(X))$ である. 準同型定理により体の同型写像

$$\widetilde{\varphi}_\alpha \colon \frac{K[X]}{(M(X))} \to K(\alpha), \quad P(X) + (M(X)) \mapsto P(\alpha)$$

が得られる. 同様に, $\sigma \colon K \to \sigma(K)$ が体の同型写像であるので, $\sigma(M)(X)$ は $\sigma(K)[X]$ の既約多項式である. ゆえに, $\mu_{\alpha',\sigma(K)}(X) = \sigma(M)(X)$ である. また, 上と同様に体の同型写像

$$\widetilde{\varphi}_{\alpha'} \colon \frac{\sigma(K)[X]}{(\sigma(M)(X))} \to \sigma(K)(\alpha'), \quad Q(X) + (\sigma(M)(X)) \mapsto Q(\alpha')$$

が存在する. 以下の図式を考える.

$$\begin{array}{ccc} K(\alpha) & \longrightarrow & \sigma(K)(\alpha') \\ {\scriptstyle \widetilde{\varphi}_\alpha^{-1}}\downarrow & & \uparrow{\scriptstyle \widetilde{\varphi}_{\alpha'}} \\ \frac{K[X]}{(M(X))} & \xrightarrow[\sigma]{} & \frac{\sigma(K)[X]}{(\sigma(M)(X))} \end{array}$$

但し, 下段の写像は $P(X) + (M(X)) \mapsto \sigma(P)(X) + (\sigma(M)(X))$ で定まる自然な同型写像である. 以上より,

$$\widetilde{\varphi}_{\alpha'} \circ \sigma \circ \widetilde{\varphi}_\alpha^{-1}$$

は体の同型写像 $K(\alpha) \to \sigma(K)(\alpha')$ であり, $\sigma \colon K \to \sigma(K)$ を延長するものである. 延長の一意性は明らかである.

**系 4.15** $L/K$ を体拡大とし, $M(X)$ を $K[X]$ の既約多項式とする. また, $\alpha, \beta \in L$ で $M(\alpha) = M(\beta) = 0$ とする. このとき, $\sigma(\alpha) = \beta$ を満たす $K$-同型写像

$$K(\alpha) \to K(\beta)$$

が存在する.

**証明**

$K = K'$, $L = L'$, $\mathrm{id}_K \colon K \to K$ の場合を考える. 主張は命題 4.14 より従う.

**例 4.16.**

- $M(X) = X^2 + 1$ とする. $M(X)$ は $\mathbb{R}$ 上既約多項式であり, $\pm i$ を根として持つ. また, $\mathbb{R}(i) = \mathbb{R}(-i) = \mathbb{C}$ である. ゆえに, $\sigma(i) = -i$ を満たす $\mathbb{R}$-自己同型 $\sigma \colon \mathbb{C} \to \mathbb{C}$ が一意的に存在する. $\sigma$ は複素共役 $z \mapsto \overline{z}$ に他ならない.
- $M(X) = X^2 - 2$ とする. $\sqrt{2} \notin \mathbb{Q}$ より, $M(X)$ は $\mathbb{Q}$ 上既約多項式であり, その根は $\pm\sqrt{2}$ である. ゆえに, $\sigma(\sqrt{2}) = -\sqrt{2}$ を満たす $\mathbb{Q}$-自己同型 $\sigma \colon \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$ が一意的に存在する. 具体的に, 任意の $a + b\sqrt{2}$ に対し,

  $$\sigma(a + b\sqrt{2}) = a - b\sqrt{2}$$

  である.

体拡大 $L/K$ に対し, $L$ の $K$-自己同型全体の集合を

$$\mathrm{Aut}_K(L) := \{\sigma \colon L \to L \mid \text{体同型 } \sigma|_K = \mathrm{id}_K\}$$

とおき, $L/K$ の自己同型群という. 明らかに, 写像の合成に関して $\mathrm{Aut}_K(L)$ は群をなす.

**命題 4.17**　$L/K$ を有限拡大とし, $\Omega$ を代数的閉体とする. また, $\sigma\colon K \to \Omega$ を体の準同型とする. このとき, $\sigma$ が体の準同型 $\sigma\colon L \to \Omega$ に延長できる.

$$\begin{array}{ccc} L & & \\ \cup & \overset{\sigma}{\searrow} & \\ K & \xrightarrow[\sigma]{} & \Omega \end{array}$$

**証明**

$[L:K]$ に関する帰納法により示す. $[L:K]=1$ のとき $K=L$ だから明らかである. $[L:K]>1$ とし, $\alpha \in L$ かつ $\alpha \notin K$ とする. 最小多項式 $M(X)=\mu_{\alpha,K}(X)$ を考える. $\Omega$ が代数的閉体だから, $\sigma(M)(X)$ は $\Omega$ 内に根 $\alpha'$ を持つ. このとき, 命題 4.14 により, 体の準同型 $\sigma\colon K(\alpha) \to \Omega$ で, $\sigma\colon K \to \Omega$ を延長するものが存在する. $[L:K(\alpha)] < [L:K]$ より, 帰納法の仮定より $\sigma$ が体の準同型 $L \to \Omega$ に延長できる. 主張が従う.

**注意 4.18.** ツォルンの補題を用いて, 命題 4.17 の主張は $L/K$ が代数的拡大である場合に拡張できる.

## 4.4　代数的閉包

複素数 $\alpha$ が $\mathbb{Q}$ 上代数的のとき, $\alpha$ を代数的数という. 代数的数全体の集合を $\overline{\mathbb{Q}}$ とおく. すなわち

$$\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} \mid \exists M \in \mathbb{Q}[X],\ M \neq 0,\ M(\alpha)=0\}.$$

系 4.9 により, $\overline{\mathbb{Q}}$ は $\mathbb{C}$ の部分体である.

**補題 4.19**　$\overline{\mathbb{Q}}$ は代数的閉体である.

**証明**

$P(X)=\sum_{i=0}^{n} a_i X^i \in \overline{\mathbb{Q}}[X]$ $(\deg(P) \geq 1)$ とする. $P(X)$ は $\mathbb{C}$ 内に根 $\beta$ を持つ. $K=\mathbb{Q}(a_1,\ldots,a_n)$ とおく. $a_i$ が $\mathbb{Q}$ 上代数的であるので, $K$ が $\mathbb{Q}$ の有限次拡大である. また, $\beta$ は $K$ 上代数的であるので, $K(\beta)$ は $K$ の有限次拡大である. $[K(\beta):\mathbb{Q}]=[K(\beta):K][K:\mathbb{Q}]$ より, $K(\beta)$ も $\mathbb{Q}$ の有限次拡大となる. ゆえに, $\beta \in \overline{\mathbb{Q}}$ となる.

$\overline{\mathbb{Q}}$ は $\mathbb{Q}$ の代数的閉包と呼ばれる. 一般には, 可換体 $K$ の拡大体 $K'$ が $K$ の代数的閉包であるとは, 以下の 2 つ条件を満たすことをいう.

- $K'/K$ が代数的拡大である.
- $K'$ が代数的閉体である.

$K$ の代数的閉包は常に存在し, さらに同型を除いて一意的である. すなわち, $K'$ 及び $K''$ が $K$ の代数的閉包ならば, $f|_K = \mathrm{id}_K$ を満たす体の同型写像 $f\colon K' \to K''$ が存在する.

代数的でない複素数を超越という.

**補題 4.20**　$\overline{\mathbb{Q}}$ は可算集合である.

集合 $X$ が可算集合であるとは, 全射 $\mathbb{N} \to X$ が存在することをいう. 例えば, $\mathbb{N}^2$, $\mathbb{Q}$ は可算集合であり, $\mathbb{R}$, $\mathbb{C}$ は非可算集合である. また, $(A_i)_{i\in I}$ が $X$ の部分集合の族で, $X=\bigcup_{i\in I} A_i$ とする. $I$ が可算であり, かつ 各 $A_i$

が可算集合ならば, $X$ も可算集合である. なぜならば, 全射 $\gamma\colon \mathbb{N} \to I$ 及び $f_i\colon \mathbb{N} \to A_i$ が存在する. ゆえに, 写像

$$\mathbb{N}^2 \to X, \quad (k,n) \mapsto f_{\gamma(n)}(k)$$

は全射となる. $\mathbb{N}^2$ が可算集合だから, $X$ も可算となる.

**証明 : (補題 4.20 の証明)**

多項式 $P \in \mathbb{Q}[X]$ に対し, $P(X)$ の複素根全体の集合を $Z(P)$ とおく. $\overline{\mathbb{Q}}$ を以下のように表すことができる.

$$\overline{\mathbb{Q}} = \bigcup_{\substack{P \in \mathbb{Q}[X] \\ P \neq 0}} Z(P)$$

である. $Z(P)$ が有限だから, 可算である. また, $\mathbb{Q}[X] = \bigcup_{n \geq 1} \mathbb{Q}_n[X]$ と表せるので, $\mathbb{Q}[X]$ が可算である (但し, $\mathbb{Q}_n[X]$ は次数 $n$ 以下の多項式全体の集合とする). 以上より, $\overline{\mathbb{Q}}$ も可算集合となる.

**系 4.21** 超越複素数の集合は非可算集合である. とくに, 超越数が存在する.

**証明**

$\mathbb{C}$ が非可算集合であることからわかる.

**補題 4.22** $f(X) \in \mathbb{Q}[X]$ を次数 $n$ の多項式とし, $\alpha \in \mathbb{R}$ で $f(\alpha) = 0$ とする. また, $f$ が $\mathbb{Q}$ 内に根を持たないとする. このとき, 以下を満たす実数 $R > 0$ が存在する.

$$\text{任意の整数 } p, q \ (q > 0) \text{ に対し, } \left|\alpha - \frac{p}{q}\right| \geq \frac{1}{Rq^n} \text{ である.}$$

**証明**

$f(X) = a_n X^n + \cdots + a_1 X + a_0$ $(a_i \in \mathbb{Q})$ とおく. $a_i$ の分母を払い, $a_i \in \mathbb{Z}$ として良い. 明らかに, $q^n f\left(\frac{p}{q}\right) \in \mathbb{Z}$ である. $f$ が $\mathbb{Q}$ 内に根を持たないので, $f\left(\frac{p}{q}\right) \neq 0$ である. よって, $q^n \left|f\left(\frac{p}{q}\right)\right| \geq 1$ である. $f$ の微分多項式 $f'$ が連続関数であるので, 閉区間 $[\alpha - 1, \alpha + 1]$ の上で有界である. よって, $|f'(x)| \leq R$ $(x \in [\alpha - 1, \alpha + 1])$ となる $R > 0$ が存在する. 任意の $x \in [\alpha - 1, \alpha + 1]$ に対し, $|f(x)| = |f(x) - f(\alpha)| = \left|\int_x^\alpha f'(t)dt\right| \leq \int_x^\alpha |f'(t)|dt \leq R|x - \alpha|$ である. よって, $\frac{p}{q} \in [\alpha - 1, \alpha + 1]$ のとき

$$\frac{1}{q^n} \leq \left|f\left(\frac{p}{q}\right)\right| \leq R\left|\frac{p}{q} - \alpha\right|$$

である. ゆえに, $\left|\alpha - \frac{p}{q}\right| \geq \frac{1}{Rq^n}$ となる. また, $\frac{p}{q} \notin [\alpha - 1, \alpha + 1]$ の場合に, $R \geq 1$ とすると $\left|\alpha - \frac{p}{q}\right| \geq 1 \geq \frac{1}{Rq^n}$ である.

**例 4.23.** $f(X) = X^2 - 2$, $\alpha = \sqrt{2}$ とする. $f'(X) = 2X$ であるので, 補題 4.22 の証明により $R = 2(\sqrt{2} + 1)$ とおけば良い. すなわち

$$\left|\sqrt{2} - \frac{p}{q}\right| \geq \frac{1}{2(\sqrt{2} + 1)q^2}$$

**定理 4.24: (Liouville)**

$$\sum_{k=1}^{\infty} \frac{1}{10^{k!}} \quad \text{は超越数である.}$$

**証明**

$\alpha = \sum_{k=1}^{\infty} \frac{1}{10^{k!}}$ とおく. $\alpha$ が代数的であるとし, $f(X)$ を $\alpha$ の最小多項式とする. $\deg(f) = n$ とおく. 補題 4.22 により実数 $R > 0$ が存在し, 任意の整数 $p, q$ $(q > 0)$ に対し, $\left|\alpha - \frac{p}{q}\right| \geq \frac{1}{Rq^n}$ である. $m \geq 1$ で, $\sum_{k=1}^{m} \frac{1}{10^{k!}} = \frac{p}{10^{m!}}$ $(p \in \mathbb{Z})$ と書ける. ゆえに,

$$\sum_{k=m+1}^{+\infty} \frac{1}{10^{k!}} = \left|\alpha - \frac{p}{10^{m!}}\right| \geq \frac{1}{R \times (10^{m!})^n}$$

である. 一方,

$$\sum_{k=m+1}^{+\infty} \frac{1}{10^{k!}} \leq \frac{1}{10^{(m+1)!}} \sum_{k=0}^{+\infty} \frac{1}{10^k} = \frac{1}{10^{(m+1)!}} \times \frac{10}{9}$$

である. したがって,

$$\frac{1}{10^{(m+1)!}} \times \frac{10}{9} \geq \frac{1}{R \times 10^{m!n}}$$

となる. よって, $10^{m!n-(m+1)!} \geq \frac{1}{R}$ となり, $\lim_{m\to\infty} 10^{m!n-(m+1)!} = 0$ に矛盾する.

## 4.5 ガロア拡大

$K$ が可換体で, $P(X) = \sum_{i=0}^{n} a_i X^i \in K[X]$ とする. このとき,

$$P'(X) := \sum_{i=1}^{n} i a_i X^{i-1}$$

とおき, $P$ の微分多項式という. $\mathrm{char}(K) = 0$ かつ $\deg(P) \geq 1$ のとき, $\deg(P') = \deg(P) - 1$ が成り立つ. しかし, $\mathrm{char}(K) = p$ (素数) のとき, $\deg(P') = \deg(P) - 1$ が成り立つとは限らない. 例えば, $P(X) = X^p$ とすると, $P' = pX^{p-1} = 0$ である. 多項式 $P(X)$ が分離多項式であるとは,

$$\gcd(P, P') = 1$$

が成り立つことをいう.

**注意 4.25.** $\overline{K}$ を $K$ の代数的閉包とする. $a_1, \ldots, a_n \in \overline{K}$ で, $P(X) = (X - a_1) \ldots (X - a_n)$ と表せる. このとき,

$$P \text{ が分離多項式である} \iff a_1, \ldots, a_n \text{ が相異なる.}$$

**補題 4.26** $\mathrm{char}(K) = 0$ のとき, $K[X]$ の任意の既約多項式が分離多項式である.

**証明**

$P(X) \in K[X]$ を既約多項式とする. $K$ の標数が 0 であるので, $P'(X) \neq 0$ である. また, $\deg(P') < \deg(P)$ より, $P'$ は $P$ の倍数でない. $P$ が既約多項式なので, $\gcd(P, P') = 1$ となる.

**定義 4.27**　$L/K$ を代数的拡大とする.
(a) $L/K$ が分離拡大であるとは, 全ての $x \in L$ に対し, $\mu_{x,K}(X)$ が分離多項式であるという.
(b) $L/K$ が正規拡大であるとは, 全ての $x \in L$ に対し, $\mu_{x,K}(X)$ が $L$ で分解することをいう.
(c) $L/K$ が分離拡大かつ正規拡大のとき, ガロア拡大であるという.

$\mathrm{char}(K) = 0$ のとき, 任意の拡大 $L/K$ が分離拡大である. 実際, $\alpha \in L$ のとき $\mu_{\alpha,K}(X)$ は $K[X]$ の既約多項式であるので, 補題 4.26 により分離多項式である. したがって, 標数 0 の場合に,「ガロア拡大」と「正規拡大」は同値である.

**例 4.28.**　$\alpha = \sqrt[3]{2}$ とし, $L = \mathbb{Q}(\alpha)$ とおく. 明らかに $\mu_{\alpha,\mathbb{Q}}(X) = X^3 - 2$ である. $j = \exp\left(\frac{2i\pi}{3}\right)$ とおくと,

$$X^3 - 2 = (X - \alpha)(X - j\alpha)(X - j^2\alpha)$$

と分解できる. $j\alpha$ は実数でないので, とくに $j\alpha \notin \mathbb{Q}(\alpha)$ である. したがって, $\mathbb{Q}(\alpha)$ は $\mathbb{Q}$ の正規拡大でない.

$L/K$ を有限次拡大とする. また, $L$ を含む $K$ の代数的閉包 $\overline{K}$ を固定する.

**命題 4.29**　以下が同値である.
(i) $L/K$ が正規拡大である.
(ii) 任意の $K$-準同型 $\sigma\colon L \to \overline{K}$ に対し, $\sigma(L) = L$ が成り立つ.

**証明**

- 「(i) $\Longrightarrow$ (ii)」を示す. $\sigma\colon L \to \overline{K}$ を $K$-準同型とし, $x \in L$ とする. $x$ の $K$ 上の最小多項式 $M(X) = \mu_{x,K}(X)$ を考える. $\sigma$ が $K$-準同型なので, $\sigma(M)(X) = M(X)$ が成り立つ. ゆえに, $\sigma(x)$ も $M(X)$ の根である. $L/K$ が正規拡大だから, $M(X)$ の全ての根が $L$ に属する. ゆえに $\sigma(x) \in L$ となり, $\sigma(L) \subset L$ が成り立つ. $[L : K] = [\sigma(L) : K]$ より, $L = \sigma(L)$ である.
- 「(ii) $\Longrightarrow$ (i)」を示す. $x \in L$ とし, $M(X) = \mu_{x,K}(X)$ とおく. $M(X)$ の全ての根が $L$ に属することを示せば良い. $y \in \overline{K}$ を $M(X)$ の根とする. 命題 4.14 により, $\sigma(x) = y$ を満たす $K$-準同型 $\sigma\colon K(\alpha) \to \overline{K}$ が存在する. また, 命題 4.17 により, $\sigma$ を $K$-準同型 $\sigma\colon L \to \overline{K}$ に延長できる. 仮定より $\sigma(L) = L$ であるので, $y \in L$ となる.

## 4.6　ガロア理論の主定理

$K$ を可換体とし, $\overline{K}$ を $K$ の代数的閉包とする. $P(X) \in K[X]$ $(\deg(P) \geq 1)$ に対し, $\alpha_1, \ldots, \alpha_n \in \overline{K}$, $u \in K^\times$ を用いて $P(X) = (X - \alpha_1)\ldots(X - \alpha_n)$ と分解できる. このとき,

$$K(\alpha_1, \ldots, \alpha_n)$$

は多項式 $P(X)$ の分解体と呼ばれる.

**系 4.30**　$P(X)$ の分解体は $K$ の正規拡大である.

**証明**

$\overline{K}$ に属する $P(X)$ の全ての根を $\alpha_1, \ldots, \alpha_n$ とおき, $L = K(\alpha_1, \ldots, \alpha_n)$ とおく. $\sigma\colon L \to \overline{K}$ を $K$-準同型とする. 任意の $z \in \overline{K}$ に対し $\sigma(P(z)) = P(\sigma(z))$ が成り立つので, $z \in \overline{K}$ が $P(X)$ の根ならば, $\sigma(z)$ も $P(X)$ の根である. よって, $\sigma$ は根 $\alpha_1, \ldots, \alpha_n$ の置換を引き起こす. とくに, $\sigma(L) = L$ が成り立つ. ゆ

えに, $L/K$ が正規拡大である.

**例 4.31.** $K=\mathbb{Q}$ とし, $P(X)=X^3-2$ とする. $\alpha=\sqrt[3]{2}$, $j=\exp\left(\frac{2i\pi}{3}\right)$ とおくと, $P(X)$ の根は $\alpha, j\alpha, j^2\alpha$ の 3 つである. ゆえに, $P(X)$ の分解体は

$$L=\mathbb{Q}(\alpha, j\alpha, j^2\alpha)=\mathbb{Q}(\alpha, j)$$

である.

$L/K$ を有限次拡大とし, $L$ を含む $K$ の代数的閉包 $\overline{K}$ を固定する. このとき, $\overline{K}$ に含まれる $K$ の有限次正規拡大で, $L$ を含むものが存在する. 実際, $L/K$ の生成系 $\{x_1,\dots,x_r\}$ を固定する (つまり, $L=K(x_1,\dots,x_r)$ とする). 各 $i$ に対し $M_i(X):=\mu_{x_i,K}(X)$ とおき, $M(X)=M_1(X)\cdots M_r(X)$ と定める. $E$ を $M(X)$ の分解体とする. 系 4.30 により, $E$ は $K$ の正規拡大である. $x_1,\dots,x_r\in E$ より, $L\subset E$ である. さらに, $L$ を含む $K$ の正規拡大のうち, $E$ は最小のものである.

**定義 4.32** 上の拡大体 $E$ は $L/K$ の正規閉包と呼ばれる.

**定義 4.33** $L/K$ をガロア拡大とする. このとき,

$$\mathrm{Gal}(L/K):=\mathrm{Aut}_K(L)$$

とおき, $L/K$ のガロア群という.

$L$ を可換体とし, $\mathrm{Aut}(L)$ を $L$ の自己同型群とする. $H\subset\mathrm{Aut}(L)$ を部分群とする. $H$ の固定体とは,

$$L^H:=\{x\in L\mid \forall\sigma\in H,\ \sigma(x)=x\}$$

で定まる $L$ の部分体である. 以下の定理はガロア理論の基本定理である.

**定理 4.34: (ガロア理論の主定理)** $L/K$ を有限次ガロア拡大とする．このとき, 以下の写像により, $L/K$ の中間体と $\mathrm{Gal}(L/K)$ の部分群は一対一に対応している．

$$\{L/K \text{ の中間体 }\} \overset{1:1}{\longleftrightarrow} \{\mathrm{Gal}(L/K) \text{ の部分群 }\}$$

$$F \longmapsto \mathrm{Gal}(L/F)$$

$$L^H \longmapsfrom H$$

さらに, 以下が成り立つ．

(1) 上の 2 つの写像は互いに逆写像である．つまり,
- $L^{\mathrm{Gal}(L/F)} = F$ (中間体 $K \subset F \subset L$)
- $\mathrm{Gal}(L/L^H) = H$ (部分群 $H \subset \mathrm{Gal}(L/K)$)

(2) 中間体 $F$ と部分群 $H$ が対応しているならば, $[F : K] = [G : H]$ が成り立つ．つまり, 指数 $k$ の部分群は次数 $k$ の部分拡大に対応する．

(3) 中間体 $F$ と分群 $H$ が対応しているならば,

$$F/K \text{ がガロア拡大} \iff H \triangleleft \mathrm{Gal}(L/K)$$

また, このとき $\mathrm{Gal}(F/K) \simeq \mathrm{Gal}(L/K)/H$ が成り立つ．

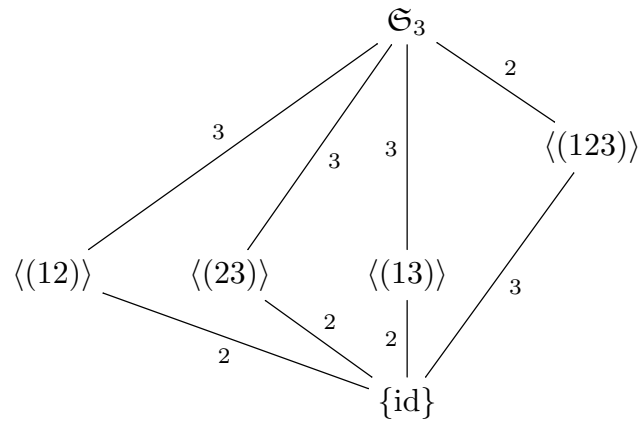
(4) 部分群 $H_1, H_2$ がそれぞれ中間体 $F_1, F_2$ に対応しているとする．このとき,

$$F_1 \subset F_2 \iff H_1 \supset H_2.$$

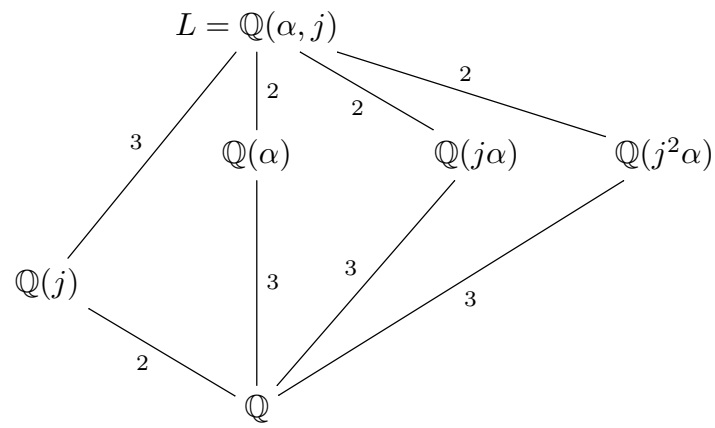
**例 4.35.** $\alpha = \sqrt[3]{2}$, $j = \exp\left(\frac{2i\pi}{3}\right)$ とし, $L = \mathbb{Q}(\alpha, j)$ とおく．例 4.31 により, $L$ は多項式 $P(X) = X^3 - 2$ の分解体であるので, $L/\mathbb{Q}$ はガロア拡大である．明らかに, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$ である．また, $j \notin \mathbb{Q}(\alpha)$ であるので, $[\mathbb{Q}(\alpha)(j) : \mathbb{Q}(\alpha)] = 2$ である ($\mu_{j,\mathbb{Q}(\alpha)}(X) = \mu_{j,\mathbb{Q}}(X) = X^2 + X + 1$ である)．よって, $[L : \mathbb{Q}] = 2 \times 3 = 6$ が成り立つ．$\sigma \in \mathrm{Gal}(L/K)$ のとき, $\sigma$ は $P(X)$ の根を置き換えるので, $\alpha, j\alpha, j^2\alpha$ の置換を誘導する．よって, 群の準同型写像

$$\rho\colon \mathrm{Gal}(L/\mathbb{Q}) \to \mathfrak{S}(\{\alpha, j\alpha, j^2\alpha\}) \simeq \mathfrak{S}_3$$

が得られる．また, $L$ が $\alpha, j\alpha, j^2\alpha$ で生成されるので, $\rho$ は単射である．$[L : \mathbb{Q}] = |\mathrm{Gal}(L/\mathbb{Q})| = 6 = |\mathfrak{S}_3|$ より, $\rho$ は群同型である．よって, $\mathrm{Gal}(L/\mathbb{Q}) \simeq \mathfrak{S}_3$ である．$\mathfrak{S}_3$ の部分群とそれぞれに対応する $L/\mathbb{Q}$ の部分拡大について調べる．




よって, $L/\mathbb{Q}$ の部分拡大は以下の通りである．




$\mathfrak{S}_3$ の正規部分群は $\{\mathrm{id}\}$, $\langle(123)\rangle$, $\mathfrak{S}_3$ の 3 つに限る. よって, $L/\mathbb{Q}$ の中間体の中で, $\mathbb{Q}$ のガロア拡大であるものは $L$, $\mathbb{Q}(j)$, $\mathbb{Q}$ のみである.

## 4.7 円分体多項式

$\zeta \in \mathbb{C}$ が 1 の冪根であるとは, $\zeta^n = 1$ となる $n \geq 1$ が存在することをいう. 1 の $n$ 乗根全体の集合を

$$\mu_n := \{\zeta \in \mathbb{C} \mid \zeta^n = 1\}$$

とおく. 明らかに, $\mu_n$ は $\mathbb{C}^*$ の部分群であり, 位数 $n$ の巡回群である. 1 の冪根 $\zeta$ に対し, $\zeta$ の位数を $\mathrm{ord}(\zeta)$ とおく. $\mathrm{ord}(\zeta) = n$ のとき, $z$ が 1 の $n$ 次原始根であるという. 例えば, $\mathrm{ord}(1) = 1$, $\mathrm{ord}(-1) = 2$, $\mathrm{ord}(i) = 4$ である. $\zeta_n := \exp\left(\frac{2i\pi}{n}\right)$ とおくと, $\mathrm{ord}(\zeta_n) = n$ である. 任意の自然数 $k$ に対し, 命題 2.12(1) により

$$\mathrm{ord}(\zeta_n^k) = \frac{n}{\gcd(n,k)}$$

が成り立つ. とくに, $d \geq 1$ が $n$ の約数ならば, $\mathrm{ord}(\zeta_n^d) = \frac{n}{d}$ である. また,

$$\mathrm{ord}(\zeta_n^k) = n \quad \Longleftrightarrow \quad \gcd(k,n) = 1 \tag{4.1}$$

が成り立つ.

**定義 4.36**

$$\Phi_n(X) = \prod_{\substack{1 \leq i \leq n \\ \gcd(i,n)=1}} (X - \zeta_n^i)$$

とおき, $n$ 次円分多項式と呼ぶ.

**例 4.37.**

$$\begin{aligned}
\Phi_1(X) &= X - 1 \\
\Phi_2(X) &= X + 1 \\
\Phi_3(X) &= (X - e^{\frac{2i\pi}{3}})(X - e^{\frac{4i\pi}{3}}) = X^2 + X + 1 \\
\Phi_4(X) &= (X - i)(X + i) = X^2 + 1
\end{aligned}$$

上の (4.1) により, 円分多項式 $\Phi_n(X)$ を以下のように書き換えることができる.

$$\Phi_n(X) = \prod_{\substack{\zeta \in \mu_n \\ \mathrm{ord}(\zeta)=n}} (X - \zeta)$$

**命題 4.38**　以下が成り立つ.

$$X^n - 1 = \prod_{\substack{d \mid n \\ d \geq 1}} \Phi_d(X).$$

**証明**

$$X^n - 1 = \prod_{\zeta \in \mu_n} (X - \zeta) = \prod_{\substack{d \mid n \\ d \geq 1}} \left( \prod_{\substack{\zeta \in \mu_n \\ \mathrm{ord}(\zeta) = d}} (X - \zeta) \right) = \prod_{\substack{d \mid n \\ d \geq 1}} \left( \prod_{\substack{\zeta \in \mu_d \\ \mathrm{ord}(\zeta) = d}} (X - \zeta) \right) = \prod_{\substack{d \mid n \\ d \geq 1}} \Phi_d(X).$$

次に, $\Phi_n(X)$ の係数が有理整数であることを証明する.

**補題 4.39**　$A$ を一意分解環とし, その商体を $K$ とおく. $P \in A[X]$, $P_1, P_2 \in K[X]$ で, $P = P_1 P_2$ とする.

(1) $P_1$ が $A[X]$ のモニックな多項式ならば, $P_2 \in A[X]$ である.

(2) $P_1$, $P_2$ がモニックな多項式ならば, $P_1, P_2 \in A[X]$ が成り立つ.

**証明**

- (1) を示す. 定理 3.8 により, $P = P_1 Q + R$ かつ $\deg(R_1) < \deg(P_1)$ を満たす $Q, R \in A[X]$ が存在する. 一方, 仮定より $P = P_1 P_2$ が成り立つ. $K[X]$ における除法の一意性より, $Q = P_2$ かつ $R = 0$ となる. とくに, $P_2 \in A[X]$ である.
- (2) を示す. 適当な $a_1, a_2 \in A \setminus \{0\}$ が存在し, $a_1 P_1$, $a_2 P_2$ が $A[X]$ に属する. $a_1 a_2 P = (a_1 P_1)(a_2 P_2)$ と書ける. 両辺の多項式の内容をとれば

  $$a_1 a_2 = c((a_1 P_1)(a_2 P_2)) = c(a_1 P_1) c(a_2 P_2)$$

  となる (但し, $P$ がモニックなので $c(P) = 1$ であることに注意する). ゆえに,

  $$P = P_1 P_2 = \frac{a_1 P_1}{c(a_1 P_1)} \frac{a_2 P_2}{c(a_2 P_2)}$$

  となる. $\frac{a_1 P_1}{c(a_1 P_1)}$ と $\frac{a_2 P_2}{c(a_2 P_2)}$ は $A[X]$ に属することに注意する. また, $P$ がモニックなので, それらの最高次係数は単元である. また, $P_1$, $P_2$ もモニックであるので, 同伴を除いて $c(a_i P_i) = a_i$ である $(i = 1, 2)$. ゆえに, $P_i \in A[X]$ が成り立つ.

**命題 4.40**　$\Phi_n(X)$ は次数 $\varphi(n)$ の有理整数係数多項式である.

**証明**

$\Phi_n(X)$ は明らかに次数 $\varphi(n)$ のモニックな多項式である. $\Phi_n(X) \in \mathbb{Z}[X]$ であることを $n$ に関する帰納法により示す. $n = 1$ のとき明らかである. $n > 1$ とし, 全ての $1 \leq k < n$ に対し, $\Phi_k(X) \in \mathbb{Z}[X]$ であるとする. $\prod_{\substack{d \mid n \\ 1 \leq d < n}} \Phi_d(X) = P(X)$ とおくと,

$$X^n - 1 = \prod_{\substack{d \mid n \\ d \geq 1}} \Phi_d(X) = P(X) \Phi_n(X)$$

である．帰納法の仮定より，$P(X) \in \mathbb{Z}[X]$ である．除法原理より，$\Phi_n(X) \in \mathbb{Q}[X]$ となる．また，補題 4.39 により，$\Phi_n(X) \in \mathbb{Z}[X]$ である．

次に，円分多項式の既約性について考える．$\zeta_n$ の $\mathbb{Q}$ 上の最小多項式を $M_n(X)$ とおく．$M_n(X) = \Phi_n(X)$ を示せば良い．$\Phi_n(\zeta_n) = 0$ より，$M_n(X)$ は $\Phi_n(X)$ の約数である．補題 4.39(2) より，$M_n(X) \in \mathbb{Z}[X]$ である．

**補題 4.41**　$n$ を割らない任意の素数 $p$ に対し，$\zeta_n^p$ は $M_n(X)$ の根である．

**証明**

$\Phi_n(X) = M_n(X)R(X)$ を満たす $R(X) \in \mathbb{Z}[X]$ が存在する．$\gcd(p, n) = 1$ より，$\zeta_n^p$ は $\Phi_n(X)$ の根である．$M_n(\zeta_n^p) \neq 0$ と仮定する．このとき，$\zeta_n^p$ は $R(X)$ の根であり，すなわち $R(\zeta_n^p) = 0$ である．したがって，多項式 $R(X^p)$ が 根として $\zeta_n$ を持ち，ゆえに $R(X^p) = M_n(X)S(X)$ と書ける．また，補題 4.39 により $S(X) \in \mathbb{Z}[X]$ である．多項式 $Q = \sum_{i=0}^{m} a_i X^i \in \mathbb{Z}[X]$ に対し，$\overline{Q} := \sum_{i=0}^{m} \overline{a}_i X^i \in \mathbb{Z}/p\mathbb{Z}[X]$ と定める．但し，$\overline{a} = a + p\mathbb{Z} \in \mathbb{Z}/p\mathbb{Z}$ とする．$\overline{R}(X^p) = \overline{M}_n(X)\overline{S}(X)$ が成り立つ．また，$\overline{R} = \sum_{j=0}^{m} \overline{r}_j X^j$ とおくと，命題 3.25 により

$$\overline{R}(X)^p = \left( \sum_{j=0}^{m} \overline{r}_j X^j \right)^p = \sum_{j=0}^{m} \overline{r}_j^p X^{pj} = \sum_{j=0}^{m} \overline{r}_j X^{pj} = \overline{R}(X^p)$$

以上より，$\overline{R}(X)^p = \overline{M}_n(X)\overline{S}(X)$ となる．一意分解環 $\mathbb{Z}/p\mathbb{Z}[X]$ における $\overline{M}_n(X)$ の一つの素因数 $T(X) \in \mathbb{Z}/p\mathbb{Z}[X]$ を考える．$T(X)$ が $\overline{R}(X)^p$ の素因数であるので，$T$ の既約性より $T \mid \overline{R}$ となる．$\overline{\Phi}_n = \overline{M}_n\overline{R}$ が成り立つので，$T^2 \mid \overline{\Phi}_n$ であり，ゆえに $T^2 \mid X^n - \overline{1}$ となる．$H(X) := X^n - \overline{1}$ の微分多項式は $\overline{n}X^{n-1}$ である．$\gcd(p, n) = 1$ という仮定より $\overline{n} \neq \overline{0}$ であることに注意する．明らかに，$\gcd(H, H') = 1$ が成り立つ．しかし，$T^2 \mid H$ より，$T \mid H'$ となり，$\gcd(H, H') = 1$ に矛盾する．したがって，$\zeta_n^p$ は $M_n(X)$ の根である．

**命題 4.42**　$\Phi_n(X) = M_n(X)$ である．とくに，$\Phi_n(X)$ は $\mathbb{Q}$ 上既約である．

**証明**

$m$ が自然数で，$\gcd(m, n) = 1$ とする．$m$ を素数の積で $m = p_1 \dots p_r$ と書ける．明らかに $p_i$ が $n$ を割らない．補題 4.41 を帰納法的に使えば，$\zeta_n^m$ が $M_n(X)$ の根であることが分かる．よって，$\Phi_n(X) \mid M_n(X)$ となる．したがって，$\Phi_n(X) = M_n(X)$ が成り立つ．

## 4.8　ディリクレの弱定理

**補題 4.43**　$a \in \mathbb{Z}$ とし，$p$ を素数とする．$\gcd(p, n) = 1$ かつ $p \mid \Phi_n(a)$ ならば，$p \equiv 1 \pmod{n}$ が成り立つ．

**証明**

$p \mid \Phi_n(a)$ より，$\mathbb{Z}/p\mathbb{Z}$ において $\overline{\Phi}_n(\overline{a}) = 0$ である．

$$X^n - 1 = \prod_{d \mid n} \Phi_d(X)$$

であるので, $\overline{a}^n = \overline{1}$ が成り立つ (とくに, $\overline{a} \neq \overline{0}$ である). さらに, $d \mid n$ かつ $d \neq n$ のとき, $\overline{a}^d \neq \overline{1}$ が成り立つ. なぜならば, 上の公式より, $\Phi_n(X) \times (X^d - 1)$ が $X^n - 1$ の約数であることに注意する. $\overline{a}^d = \overline{1}$ ならば, $(X - \overline{a})^2$ が $H = X^n - \overline{1}$ の約数になり, 補題 4.41 の証明と同じく $\gcd(H, H') = 1$ に矛盾する. 以上より, 群 $(\mathbb{Z}/p\mathbb{Z})^\times$ における $\overline{a}$ の位数はちょうど $n$ である. ラグランジュの定理により, $n \mid p - 1$ となり, すなわち $p \equiv 1 \pmod{n}$ である.

**定理 4.44: (ディリクレの弱定理)** $p \equiv 1 \pmod{n}$ を満たす素数は無限に存在する.

**証明**

任意の自然数 $N$ に対し, $p \geq N$ かつ $p \equiv 1 \pmod{n}$ を満たす素数 $p$ が存在することを示せば良い. まず, $x > 1$ を満たす実数に対し,

$$|\Phi_n(x)| = \prod_{\substack{i=1 \\ \gcd(i,n)=1}}^{n} |x - \zeta_n^i| \ > \ |x - 1|^{\varphi(n)}$$

が成り立つことに注意する. よって, $x \geq 3$ のとき, $\Phi_n(x) \geq 2$ である. とくに, $\Phi_n(nN!) \neq \pm 1$ である. $p$ を $\Phi_n(nN!)$ の素因数とする. $\Phi_n(X)$ の定数項が $\pm 1$ であるので, $p$ は $nN!$ の約数でない. ゆえに, $p > N$ であり, $\gcd(p, n) = 1$ である. 補題 4.43 より, $p \equiv 1 \pmod{n}$ となる.

**例 4.45.** 補題 4.43 より, 任意の $n, k \geq 1$ に対し, $\Phi_n(kn)$ の全ての素因数が $\equiv 1 \pmod{n}$ である. 例えば,

$$\Phi_9(9) = 9^6 + 9^3 + 1 = 19 \times 37 \times 757.$$

**定理** (ディリクレの定理)**.** $m, a$ を互いに素な自然数とする. このとき, $p \equiv a \pmod{m}$ を満たす素数 $p$ が無限に存在する.

**例 4.46.** 下 4 桁 1111 の素数が無限に存在する. 実際, $a = 1111$, $m = 10000$ とすれば良い.

## 4.9 円分体

**定義 4.47** $\mathbb{Q}$ の拡大体 $F_n := \mathbb{Q}(\zeta_n)$ のことを円分体という.

例えば, $F_4 = \mathbb{Q}(i)$ である. 明らかに, $F_n$ は全ての 1 の $n$ 乗根を含む. さらに, $\zeta$ が 1 の原始 $n$ 乗根ならば, $F_n = \mathbb{Q}(\zeta)$ である.

**定理 4.48** 以下が成り立つ.
(1) $F_n/\mathbb{Q}$ はガロア拡大である.
(2) $[F_n : \mathbb{Q}] = \varphi(n)$ である.
(3) $\mathrm{Gal}(F_n/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$ である.

**証明**

命題 4.42 により, $\zeta_n$ の $\mathbb{Q}$ 上の最小多項式は $\Phi_n(X)$ である. $\Phi_n(X)$ の全ての根が $F_n$ に属するので, $F_n$ は $\Phi_n(X)$ の分解体と一致し, ゆえにガロア拡大になる (系 4.30 参照). また, $[F_n : \mathbb{Q}] = \deg(\Phi_n) = \varphi(n)$ となる. 最後に, 同型写像 $\mathrm{Gal}(F_n/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$ を作る. $\sigma \in \mathrm{Gal}(F_n/\mathbb{Q})$ のとき, $\sigma(\zeta_n)$ は明らかに $\mathrm{ord}(\sigma(\zeta_n)) = \mathrm{ord}(\zeta_n) = n$ を満たすので, 1 の原始 $n$ 乗根である. ゆえに, $\sigma(\zeta_n) = \zeta_n^k$ かつ

$\gcd(k,n)=1$ を満たす $k\in\mathbb{Z}$ が存在する．$u(\sigma):=k+n\mathbb{Z}$ とおくと，$u(\sigma)\in(\mathbb{Z}/n\mathbb{Z})^\times$ であり，$k$ の取り方に依らない．よって，写像

$$u\colon\ \mathrm{Gal}(F_n/\mathbb{Q})\to(\mathbb{Z}/n\mathbb{Z})^\times$$

が定まる．$u$ が単射準同型であることは容易に確認できる．

$$|\,\mathrm{Gal}(F_n/\mathbb{Q})|=[F_n:\mathbb{Q}]=\varphi(n)=|(\mathbb{Z}/n\mathbb{Z})^\times|$$

より，$u$ は全単射である．主張が従う．

## 4.10　ガロアの逆問題

**問題 4.49: (ガロアの逆問題)**　有限群 $G$ が与えられているとき，$\mathrm{Gal}(L/\mathbb{Q})\simeq G$ を満たすガロア拡大 $L/\mathbb{Q}$ が存在するか?

**定理 4.50**　$G$ を有限アーベル群とする．このとき，$\mathrm{Gal}(L/\mathbb{Q})\simeq G$ を満たすガロア拡大 $L/\mathbb{Q}$ が存在する．

**証明**

定理 2.40 により

$$G\ \simeq\ \mathbb{Z}/n_1\mathbb{Z}\times\cdots\times\mathbb{Z}/n_k\mathbb{Z}$$

となる自然数 $n_1,\dots,n_k\geq 2$ が存在する．ディリクレの弱定理により，$p_i\equiv 1\pmod{n_i}$ $(1\leq i\leq k)$ を満たす相異なる素数 $p_1,\dots,p_k$ がとれる．$N:=p_1\dots p_k$ と定める．このとき，

$$(\mathbb{Z}/N\mathbb{Z})^\times\ \simeq\ (\mathbb{Z}/p_1\mathbb{Z})^\times\times\cdots\times(\mathbb{Z}/p_k\mathbb{Z})^\times\ \simeq\ (\mathbb{Z}/(p_1-1)\mathbb{Z})\times\cdots\times(\mathbb{Z}/(p_k-1)\mathbb{Z})\tag{4.2}$$

である (定理 2.38 により，$(\mathbb{Z}/p_i\mathbb{Z})^\times$ は位数 $p_i-1$ の巡回群であることに注意する)．$p_i-1=n_id_i$ $(d_i\in\mathbb{N})$ とおく．このとき，

$$d_i\mathbb{Z}/(p_i-1)\mathbb{Z}=d_i\mathbb{Z}/(d_in_i)\mathbb{Z}\ \simeq\ \mathbb{Z}/n_i\mathbb{Z}$$

である．群同型 (4.2) によって部分群 $(d_1\mathbb{Z}/(p_1-1)\mathbb{Z})\times\cdots\times(d_k\mathbb{Z}/(p_k-1)\mathbb{Z})$ に対応する $(\mathbb{Z}/N\mathbb{Z})^\times$ の部分群を $H$ とおく．以上より，

$$\frac{(\mathbb{Z}/N\mathbb{Z})^\times}{H}\ \simeq\ \mathbb{Z}/n_1\mathbb{Z}\times\cdots\times\mathbb{Z}/n_k\mathbb{Z}\ \simeq\ G$$

となる．$L:=\mathbb{Q}(\zeta_N)$ とおき，$F:=L^H$ と定める．但し，ここで定理 4.48 を用いて $\mathrm{Gal}(L/\mathbb{Q})$ と $(\mathbb{Z}/N\mathbb{Z})^\times$ を同一視する．$L/\mathbb{Q}$ のガロア群がアーベル群であるので，全ての部分群は正規部分群である．定理 4.34 により，

$$\mathrm{Gal}(F/\mathbb{Q})\ \simeq\ \frac{(\mathbb{Z}/N\mathbb{Z})^\times}{H}\ \simeq\ G.$$

**定理 4.51: (Shafarevich)**　$G$ を有限可解群とする．このとき，$\mathrm{Gal}(K/\mathbb{Q})\simeq G$ となるガロア拡大 $K/\mathbb{Q}$ が存在する．

一般の有限群の場合はガロア逆問題は未解決である. 上の定理 4.50 の証明では, $\mathrm{Gal}(F/\mathbb{Q}) \simeq G$ を満たす拡大体 $F$ を適当な円分体の部分拡大として作った. 以下の定理により, $G$ がアーベル群のとき, 問題 4.49 の解は全て円分体の部分拡大として現れる.

**定理 4.52: (クロネッカー・ウェーバーの定理)** $L/\mathbb{Q}$ をガロア拡大とし, $\mathrm{Gal}(L/\mathbb{Q})$ がアーベル群であるとする. このとき, $L$ は適当な円分体に含まれる.

**例 4.53.** $p$ を素数とし, $p^* := (-1)^{\frac{p-1}{2}} p$ とおく. このとき,

$$\mathbb{Q}(\sqrt{p^*}) \subset \mathbb{Q}(\zeta_p)$$

が成り立つ.

# 5 加群

## 5.1 定義

$A$ を可換環とし, $(M, +)$ をアーベル群とする. また, 写像 $f\colon A \times M \to M$ が与えられているとする. $a \in A$, $x \in M$ に対し, $f(a, x)$ を単に $a \cdot x$, または $ax$ と表す.

**定義 5.1** $M$ が $A$ 加群であるとは, 任意の $a, b \in A$, $x, y \in M$ に対して, 以下が成り立つことをいう.

- $a(bx) = (ab)x$,
- $(a + b)x = ax + bx$,
- $a(x + y) = ax + ay$,
- $1x = x$.

**例 5.2.**

- $K$ が可換体のとき, $K$ 加群は $K$ ベクトル空間に他ならない.
- $M$ をアーベル群とする. $k \in \mathbb{Z}$, $x \in M$ に対して,

$$kx = \begin{cases} \underbrace{x + \cdots + x}_{k \text{ 個}} & \text{if } k > 0 \\ \underbrace{(-x) + \cdots + (-x)}_{-k \text{ 個}} & \text{if } k < 0 \\ 0 & \text{if } k = 0 \end{cases}$$

  とおくによって, $M$ は自然に $\mathbb{Z}$ 加群とみなすことができる. ゆえに, 「$\mathbb{Z}$ 加群」と「アーベル群」というのは全く同じものである.
- $A$ を可換環とする. $A$ 自分自身を $A$ 加群として考えることができる. 実際, $A$ の掛け算 $A \times A \to A$, $(a, b) \mapsto ab$ は定義 5.1 の条件を満たす.
- $f\colon A \to B$ を可換環の準同型とする. 任意の $a \in A$, $b \in B$ に対し, $a \cdot b = f(a)b$ とおくことによって, $B$ を $A$ 加群とみなすことができる. 特に, $A \subset B$ が部分環のとき, $B$ が自然に $A$ 加群である.

**定義 5.3** $M$ を $A$ 加群とし, $N \subset M$ を部分群とする. 任意の $a \in A$, $x \in N$ に対して, $ax \in N$ が成り立つとき, $N$ が $M$ の部分加群であるという.

**注意 5.4.**

- $\{0\}$ と $M$ は明らかに $M$ の部分加群である.
- $A$ の部分加群は $A$ のイデアルに他ならない.
- $A = K$ が可換体のとき, 部分加群は線形部分空間に他ならない.

## 5.2 $A$ 加群の準同型写像

**定義 5.5** $M$, $M'$ を $A$ 加群とし, $f\colon M \to M'$ を群の準同型写像とする. 任意の $a \in A$, $x \in M$ に対して $f(ax) = af(x)$ が成り立つとき, $f$ が $A$ 加群の準同型写像 (または $A$ 線形写像) であるという.

$A$ 線形写像 $f\colon M \to M'$ に対し,

$$\mathrm{Ker}(f) = \{x \in M \mid f(x) = 0\}$$
$$\mathrm{Im}(f) = \{f(x) \mid x \in M\}$$

とおき, それぞれ $f$ の核, $f$ の像という. $\mathrm{Ker}(f)$, $\mathrm{Im}(f)$ はそれぞれ $M$, $N$ の部分加群である. $f$ が全単射であるときに, $f$ を同型写像という. このとき, $f^{-1}\colon M' \to M$ も $A$ 線形写像である. 同型写像 $M \to M'$ が存在するときに $M \simeq M'$ と表す. $M$ が $A$ 加群で, $N$ を $M$ の部分加群とし, 剰余群 $M/N$ を考える. $a \in A$, $x \in M$ に対して

$$a(x + N) = ax + N$$

とおくことによって, $M/N$ は自然に $A$ 加群になる. 群の場合と同じく, 準同型定理と呼ばれる以下の定理が成り立つ.

**定理 5.6: (加群の準同型定理)** $f\colon M \to M'$ を $A$ 加群の準同型とする. このとき, 以下の写像は $A$ 加群の同型写像である.

$$M/\mathrm{Ker}(f) \to \mathrm{Im}(f) \qquad x + \mathrm{Ker}(f) \mapsto f(x).$$

**証明**

群の準同型定理により, この写像は群同型である. 明らかに $A$ 線形性を満たすので, $A$ 加群の同型写像である.

準同型写像 $f\colon M \to M'$ について, 群の準同型の場合と同様に

$$f \text{ が単射} \quad \Longleftrightarrow \quad \mathrm{Ker}(f) = 0$$

が成り立つ.

## 5.3 部分加群の和, イデアルと部分加群の積

$M$ を $A$ 加群とし, $M_1, \ldots, M_n$ を $M$ の部分加群とする.

$$M_1 + \cdots + M_n = \left\{ \sum_{i=1}^{n} x_i \;\middle|\; x_i \in M_i \right\}$$

とおき, 部分加群 $M_1, \ldots, M_n$ の和という. 明らかに, $M_1 + \cdots + M_n$ は $M$ の部分加群である. さらに, 全ての $M_i$ を含む部分加群の中で最小のものである. $M_1, \ldots, M_n$ の共通部分 $\bigcap_{i=1}^{n} M_i$ も明らかに $M$ の部分加群をなす. $x$ を $M$ の元とする. $x$ で生成される巡回加群とは

$$Ax = \{ax \mid a \in A\}$$

のことである. 同様に, 有限個の元 $x_1, \ldots, x_n$ で生成される部分加群とは,

$$Ax_1 + \cdots + Ax_n \quad = \left\{ \sum_{i=1}^{n} a_i x_i \;\middle|\; a_i \in A,\ x_i \in M_i \right\}$$

で定まるものである.

**定義 5.7**　$A$ 加群 $M$ に対し, $M = Ax_1 + \cdots + Ax_n$ となる $x_1, \ldots, x_n \in M$ が存在するとき, $M$ が有限生成であるという. このとき, $x_1, \ldots, x_n$ を $M$ の生成系という.

写像 $f\colon A \to Ax,\ a \mapsto ax$ は明らかに $A$ 加群の全射準同型である. $f$ の核は

$$\mathrm{Ann}(x) = \{a \in A \mid ax = 0\}$$

である ($\mathrm{Ann}(x)$ は $x$ の零化イデアルと呼ばれる). 準同型定理により, $A$ 加群の同型写像

$$A/\mathrm{Ann}(x) \simeq Ax$$

が存在する. $\mathfrak{a} \subset A$ をイデアルとし, $N \subset M$ を部分加群とする. このとき,

$$\mathfrak{a}N = \left\{ \sum_{j=1}^{n} a_j x_j \;\middle|\; n \geq 1,\ a_j \in \mathfrak{a},\ x_j \in N \right\}$$

とおき, $\mathfrak{a}$ と $N$ の積という. 明らかに, $\mathfrak{a}N$ は部分加群であり, $\mathfrak{a}N \subset N$ が成り立つ. とくに, $A$ の 2 つのイデアル $\mathfrak{a}, \mathfrak{b}$ に対し, それらの積 $\mathfrak{a}\mathfrak{b}$ が定義されている. 具体的に

$$\mathfrak{a}\mathfrak{b} = \left\{ \sum_{j=1}^{n} a_j b_j \;\middle|\; n \geq 1,\ a_j \in \mathfrak{a},\ \ b_j \in \mathfrak{b} \right\}$$

である. 明らかに, $\mathfrak{a}\mathfrak{b} \subset \mathfrak{a} \cap \mathfrak{b}$ が成り立つ.

$\mathfrak{a} \subset A$ をイデアルとし, $M$ を $A$ 加群とする. 部分加群 $\mathfrak{a}M$ による $M$ の商加群 $M/\mathfrak{a}M$ を考える. $M/\mathfrak{a}M$ は自然に $A/\mathfrak{a}$ 加群とみなすことができる. 実際, $s \in A$, $x \in M$ に対し,

$$(s + \mathfrak{a}) \cdot (x + \mathfrak{a}M) := sx + \mathfrak{a}M$$

とおくことによって, $M/\mathfrak{a}M$ が $A/\mathfrak{a}$ 加群となる.

## 5.4　加群の直積, 加群の直和

$(M_i)_{i \in I}$ を $A$ 加群の族とする. 足し算とスカラー倍を成分ごとに定義することによって直積

$$\prod_{i \in I} M_i$$

は自然に $A$ 加群となる. 一方,

$$\bigoplus_{i \in I} M_i = \left\{ (x_i)_{i \in I} \in \prod_{i \in I} M_i \;\middle|\; \text{有限個を除き } x_i = 0 \right\}$$

とおき, 族 $(M_i)_{i \in I}$ の直和という. $\bigoplus_{i \in I} M_i$ は $\prod_{i \in I} M_i$ の部分加群である. また, $I$ が有限集合ならば, 直和と直積は一致する. $M_1, M_2$ を $M$ の部分加群とする. $M$ の任意の元 $x$ が一意的に $x = x_1 + x_2$ ($x_1 \in M_1$, $x_2 \in M_2$) と表せるとき, $M$ が部分加群 $M_1$ と $M_2$ の直和であるといい, $M = M_1 \oplus M_2$ と書く. 明らかに,

$$M = M_1 \oplus M_2 \quad \Longleftrightarrow \quad \begin{cases} M = M_1 + M_2 \\ M_1 \cap M_2 = \{0\} \end{cases}$$

が成り立つ.

## 5.5　自由加群

全ての $i \in I$ に対して, $M_i = A$ とする. このとき, 族 $(M_i)_{i\in I}$ の直積と直和をそれぞれ $A^I$ と $A^{(I)}$ で表す. すなわち

$$A^I = \{(a_i)_{i\in I} \mid a_i \in A\}$$
$$A^{(I)} = \{(a_i)_{i\in I} \mid a_i \in A,\ \text{有限個を除き } a_i = 0\}$$

である. 各 $j \in I$ に対し,

$$e_j = (\delta_{i,j})_{i\in I}$$

と定める. 任意の元 $x \in A^{(I)}$ が一意的に

$$x = \sum_{i\in I} a_i e_i \quad \text{有限個を除き, } a_i = 0$$

と表すことができる. $(e_j)_{j\in I}$ は $A^{(I)}$ の標準基底と呼ばれる.

**補題 5.8**　$M$ を $A$ 加群とし, $(x_i)_{i\in I}$ を $M$ の元の族とする. このとき, $f(e_i) = x_i$ $(i \in I)$ を満たす $A$ 加群の準同型 $f\colon A^{(I)} \to M$ が一意的に存在する.

**証明**

$f\left(\sum_{i\in I} a_i e_i\right) = \sum_{i\in I} a_i x_i$ とおけば良い. 但し, 有限個を除き $(a_i)_{i\in I}$ の全ての元が 0 であるので, これは有限和であることに注意する. $f$ の一意性は明らかである.

**定義 5.9**　$M$ を $A$ 加群とする. $M$ の元の族 $(u_i)_{i\in I}$ が $M$ の基底であるとは, 任意の元 $x \in M$ が一意的に

$$x = \sum_{i\in I} a_i u_i \qquad (\text{有限個を除き, } a_i = 0)$$

と表せることをいう. $M$ が基底を持つときに, $M$ を自由加群という.

言い換えれば, $(u_i)_{i\in I}$ が $M$ の基底であるためには, 写像

$$A^{(I)} \longrightarrow M, \quad (a_i)_{i\in I} \mapsto \sum_{i\in I} a_i u_i$$

が同型写像であることが必要十分である. とくに, 自由加群は $A^{(I)}$ という形の加群と同型になる. $M$ の元の族 $(u_i)_{i\in I}$ が「$A$ 線形独立」であるとは, $\sum_{i\in I} a_i u_i = 0 \implies \forall i \in I, a_i = 0$ が成り立つことをいう. 明らかに, $(u_i)_{i\in I}$ が基底ならば, $A$ 線形独立である.

**例 5.10.**

- $A^n$ は自由 $A$ 加群である.
- $A[X]$ は自由 $A$ 加群であり, 族 $(1, X, X^2, X^3, \dots)$ はその基底をなす.
- $\mathbb{Q}$ は自由 $\mathbb{Z}$ 加群でない. なぜならば, 有理数 $x = \frac{p}{q}$ および $x' = \frac{p'}{q'}$ $(p, p', q, q' \neq 0)$ に対し, $p'qx - pq'y = 0$ である. よって $(x, y)$ は $\mathbb{Z}$ 線形独立でない.
- アーベル群 $\mathbb{Q}_{>0}$ を $\mathbb{Z}$ 加群としてみると, 自由 $\mathbb{Z}$ 加群であり, 素数全体の集合を基底として持つ.

**命題 5.11**　$M$ を有限生成加群とする．このとき，$n \geq 1$ 及び $A^n$ の部分加群 $L \subset A^n$ が存在し，

$$M \simeq A^n/L$$

である．

**証明**

$x_1, \ldots, x_n \in M$ を生成系とする．$(e_1, \ldots, e_n)$ を $A^n$ の標準基底とする．$f(e_i) = x_i$ を満たす $A$ 加群の準同型 $f\colon A^n \to M$ が存在する．$M = Ax_1 + \cdots + Ax_n$ より，$f$ は全射である．$L = \mathrm{Ker}(f)$ とおくと，準同型定理により $A^n/L \simeq M$ となる．

**命題 5.12**　$L$ が自由加群で，$f\colon M \to L$ を $A$ 加群の全射準同型とする．このとき，部分加群 $M_0 \subset M$ が存在し，

$$M = M_0 \oplus \mathrm{Ker}(f)$$

が成り立つ．さらに，$f$ の $M_0$ への制限は同型写像 $f\colon M_0 \to L$ である．

**証明**

$(e_i)_{i \in I}$ を $L$ の基底とする．$f$ が全射であるので，$f(u_i) = e_i$ を満たす $u_i \in M$ がとれる．補題 5.8 により，$g(e_i) = u_i$ $(i \in I)$ を満たす準同型 $g\colon L \to M$ が存在する．$M_0 := \mathrm{Im}(g)$ と定める．明らかに，$f \circ g = \mathrm{id}_L$ が成り立つ．$x \in M_0 \cap \mathrm{Ker}(f)$ とすると，$x = g(y)$ $(y \in L)$ と書ける．さらに，$0 = f(x) = f(g(y)) = y$ となり，ゆえに $x = 0$ である．したがって，$M_0 \cap \mathrm{Ker}(f) = 0$ である．さらに，$z \in M$ とすると，

$$z = g(f(z)) + z', \qquad z' = z - g(f(z))$$

である．$f(z') = f(z) - f(g(f(z))) = f(z) - f(z) = 0$ である．よって，$z' \in \mathrm{Ker}(f)$ である．ゆえに，$M_0 + \mathrm{Ker}(f) = M$ が成り立つ．以上より，$M = M_0 \oplus \mathrm{Ker}(f)$ である．最後に，$f$ の $M_0$ への制限 $M_0 \to L$, $x \mapsto f(x)$ が同型写像であることを確認する．$M_0 \cap \mathrm{Ker}(f) = 0$ より単射性は明らかである．全射性については，任意の $x \in L$ に対し $x = f(g(x))$ と書けるので成り立つ．

## 5.6　階数

**補題 5.13**　$n, m$ が自然数で，$A$ 加群の同型写像 $f\colon A^m \to A^n$ が存在するならば，$n = m$ が成り立つ．

**証明**

$A$ の極大イデアル $\mathfrak{m}$ を固定し，$k := A/\mathfrak{m}$ とおく．$A$ 加群 $M$ に対し，

$$\overline{M} := M/\mathfrak{m}M$$

と定義する．$\overline{M}$ は $k$ ベクトル空間である．明らかに，$A$ 加群 $M_1$, $M_2$ に対し，自然な同型 $\overline{M_1 \oplus M_2} \simeq \overline{M_1} \oplus \overline{M_2}$ が存在する．また，$\overline{A} = k$ である．ゆえに，$N = A^n$ のとくと，$\overline{N} \simeq k^n$ であり，$n$ 次元の $k$ ベクトル空間である．同様に，$M := A^m$ とおくと，$\overline{M}$ は $m$ 次元の $k$ ベクトル空間である．$f := M \to N$ が同型写像であるので，明らかに $f(\mathfrak{m}M) = \mathfrak{m}N$ が成り立つ．準同型定理により，$f$ は $k$ ベクトル空間の同型写像

$$\overline{f} := \overline{M} \to \overline{N}, \qquad x + \mathfrak{m}M \mapsto f(x) + \mathfrak{m}N$$

を誘導する．ゆえに，$m = \dim_k(\overline{M}) = \dim_k(\overline{N}) = n$ となる．

**系 5.14**　$M$ を有限生成自由 $A$ 加群とし，$\mathcal{B} = (x_1, \ldots, x_n)$ を $M$ の基底とする．このとき，自然数 $n$ は基底の取り方に依らない．$n = \mathrm{rank}(M)$ とおき，$A$ の階数 (またはランク) という．

**証明**

$\mathcal{B} = (x_1, \ldots, x_n)$ が基底であるので，写像 $A^n \to M$, $(a_1, \ldots, a_n) \mapsto \sum_{i=1}^n a_i x_i$ は同型写像である．特に $M \simeq A^n$ である．ゆえに，主張は補題 5.13 より従う．

## 5.7　単項イデアル整域上の加群

一般には，自由加群の部分加群は自由加群とは限らない．例えば，$A = \mathbb{Z}[X]$ とし，$\mathfrak{a} = (2, X)$ を 2 と $X$ で生成されるイデアルとする．このとき，$\mathfrak{a}$ は自由加群でないが，自由加群 $A$ に含まれる．

以下は，$A$ を単項イデアル整域とする．

**定理 5.15**　$M$ を有限生成自由 $A$ 加群とし，$N \subset M$ を部分加群とする．このとき，$N$ は自由加群である．さらに，$\mathrm{rank}(N) \leq \mathrm{rank}(M)$ が成り立つ．

**証明**

$A$ の階数に関する数学的帰納法によって証明する．$M = A^n$ とすれば良い．$\pi\colon A^n \to A$ を第一成分への射影とする．$N \cap \mathrm{Ker}(\pi) \subset \mathrm{Ker}(\pi) = \{0\} \times A^{n-1}$ だから，帰納法の仮定より $N \cap \mathrm{Ker}(\pi)$ は自由加群であり，その階数は $\leq n-1$ である．$L := \pi(N)$ とおくと，全射準同型 $\pi\colon N \to L$ が得られ，その核は $N \cap \mathrm{Ker}(\pi)$ である．$A$ が単項イデアル整域であるので，$L$ は単項イデアルである．とくに，$L$ は自由 $A$ 加群である．命題 5.12 により，$N = (N \cap \mathrm{Ker}(\pi)) \oplus N_0$ と分解できる．さらに，$N_0 \simeq L$ である．よって $N$ は自由加群であり，$\mathrm{rank}(N) \leq (n-1) + 1 = n$ が成り立つ．

**定義 5.16**　$A$ を整域とし，$M$ を $A$ 加群とする．$x \in M$ がねじれ元であるとは，$a \in A \setminus \{0\}$ が存在し，$ax = 0$ が成り立つ．$M$ のねじれ元全体の部分集合を $M_{\mathrm{tor}}$ とおく．

**補題 5.17**　$M_{\mathrm{tor}}$ は $M$ の部分加群である．

**証明**

$1 \cdot 0 = 0$ と書けるので，$0 \in M_{\mathrm{tor}}$ である．$x, x' \in M_{\mathrm{tor}}$ 及び $b \in A$ とする．このとき，$a, a' \in A \setminus \{0\}$ が存在し，$ax = a'x' = 0$ である．よって，$aa'(bx + x') = aa'bx + aa'x' = 0$ となる．$A$ が整域より $aa' \neq 0$ である．よって，$bx + x'$ がねじれ元である．よって，$M_{\mathrm{tor}}$ は $M$ の部分加群である．

$M_{\mathrm{tor}}$ を $M$ のねじれ部分加群という．$M = M_{\mathrm{tor}}$ のとき，$M$ がねじれ加群であるという．また，$M_{\mathrm{tor}} = 0$ のとき，$M$ がねじれを持たないという．明らかに，自由加群はねじれを持たない．

**補題 5.18**　商加群 $M/M_{\mathrm{tor}}$ はねじれを持たない．

**証明**

$x \in M$ に対し, $M_{\mathrm{tor}}$ による $x$ の剰余類を $\overline{x}$ と表す. $\overline{x}$ をねじれ元とする. このとき, $a \in A$ $(a \neq 0)$ が存在し, $a\overline{x} = \overline{0}$ である. ゆえに, $ax \in M_{\mathrm{tor}}$ である. すなわち, $b(ax) = 0$ となる $b \in A$ $(b \neq 0)$ が存在する. $A$ が整域であるので $ab \neq 0$ である. $(ab)x = 0$ より, $x \in M_{\mathrm{tor}}$ となる. したがって, $\overline{x} = \overline{0}$ である. 以上より, $M/M_{\mathrm{tor}}$ はねじれを持たない.

**例 5.19.** $\mathbb{Z}$ 加群 $M = \mathbb{R}/\mathbb{Z}$ を考える (写像 $x + \mathbb{Z} \mapsto \exp(2i\pi x)$ により, $M$ は絶対値 1 の複素数全体の群と同型である). このとき,

$$M_{\mathrm{tor}} = \mathbb{Q}/\mathbb{Z}$$

である.

**定理 5.20** $A$ を単項イデアル整域とし, $M$ を有限生成 $A$ 加群とする. このとき,

$$M \text{ がねじれをもたない} \quad \Longleftrightarrow \quad M \text{ が自由加群である}$$

**証明**

「$\Longleftarrow$」は明らかである. 逆に, $M$ がねじれを持たないとする. $(x_1, \ldots, x_n)$ を $M$ の生成系とする. $\{x_1, \ldots, x_n\}$ の中から $A$ 線形独立な族 $\mathcal{B} = (x_{i_1}, \ldots, x_{i_k})$ をとる. また, $k$ が最大であるとする. 添字を付け直して, $(x_1, \ldots, x_k)$ が $A$ 線形独立であるとして良い. このとき, 部分加群

$$M_1 := Ax_1 + \cdots + Ax_k$$

は $\mathcal{B}$ を基底とする自由加群である. $k = n$ の場合は $M = M_1$ となり, 主張が従う. よって, $k < n$ として良い. $i \in \{k+1, \ldots, n\}$ に対し, $k$ の最大性より $(x_1, \ldots, x_k, x_i)$ は線形従属である. ゆえに, $a_1x_1 + \ldots a_kx_k + b_ix_i = 0$ を満たす $(a_1, \ldots, a_k, b_i) \in A^{k+1} - \{(0, \ldots, 0)\}$ が存在する. $(x_1, \ldots, x_k)$ が $A$ 線形独立だから, $b_i \neq 0$ である. とくに, $b_ix_i \in M_1$ である. $b = b_{k+1} \ldots b_n$ とおく. $b \neq 0$ であり, かつ任意の $i \in \{1, \ldots, n\}$ に対して $bx_i \in M_1$ が成り立つ. $x_i$ たちが $M$ を生成するので, $bM \subset M_1$ となる. $M_1$ が自由加群であるので, 定理 5.15 により $bM$ も自由加群である. $M$ がねじれを持たないので, 写像 $M \to bM$, $x \mapsto bx$ は全単射である. したがって, $M$ が $bM$ と同型であり, ゆえに自由加群である.

**例 5.21.** 「有限生成」という仮定を外せば定理 5.20 の主張は成り立たない. 例えば, $\mathbb{Q}$ はねじれを持たない $\mathbb{Z}$ 加群であるが, 自由加群ではない.

**定理 5.22** $A$ を単項イデアル整域とし, $M$ を有限生成 $A$ 加群とする. このとき,

$$M \simeq A^d \oplus A/(a_1) \oplus \cdots \oplus A/(a_r)$$

かつ $a_{i+1} \mid a_i$ $(1 \leq i \leq r-1)$ を満たす整数 $d \geq 0$ および 単元でも 0 でもない元 $a_1, \ldots, a_r \in A$ が存在する. さらに, 整数 $d \geq 0$ と単項イデアル $(a_1)$, $\ldots$, $(a_r)$ は一意的に定まる.

**定理 5.23** $M$ を階数 $n$ の自由加群とし, $N \subset M$ を階数 $r \leq n$ の部分加群とする. このとき, 以下の条件を満たす $M$ の基底 $(x_1, \ldots, x_n)$ 及び $d_1, \ldots, d_r \in A - \{0\}$ が存在する ($d_i$ は単元可).

- $d_{i+1} \mid d_i$ $(1 \leq i \leq r-1)$ が成り立つ.
- $d_1x_1, \ldots, d_rx_r$ が $N$ の基底である.

さらに, 単項イデアル $(d_1), \ldots, (d_r)$ は一意的に定まる.

有理整数を成分とする $n$ 次正方行列全体の集合を $\mathrm{M}_n(\mathbb{Z})$ とおき,

$$\mathrm{GL}_n(\mathbb{Z}) = \{U \in \mathrm{M}_n(\mathbb{Z}) \mid \exists V \in \mathrm{M}_n(\mathbb{Z}),\ UV = VU = E_n\}$$

と定義する. 但し, $E_n$ は $n$ 次単位行列である. $UV = E_n$ より, $\det(U)\det(V) = 1$ となる. $\det(U)$, $\det(V)$ が有理整数であるので, $\det(U) = \pm 1$ となる. 逆に, $\det(U) = \pm 1$ とすると, $U\widetilde{U} = \widetilde{U}U = \det(U)E_n$ である (但し, $\widetilde{U}$ は $U$ の余因子行列である). $\widetilde{U} \in \mathrm{M}_n(\mathbb{Z})$ であるので, $U \in \mathrm{GL}_n(\mathbb{Z})$ となる. したがって,

$$\mathrm{GL}_n(\mathbb{Z}) = \{U \in \mathrm{M}_n(\mathbb{Z}) \mid \det(U) = \pm 1\}$$

が成り立つ.

**系 5.24** $B \in \mathrm{M}_n(\mathbb{Z})$ に対し, $d_{i+1} \mid d_i$ $(1 \leq i \leq r-1)$ を満たす整数 $d_1, \ldots, d_r$ 及び $U, V \in \mathrm{GL}_n(\mathbb{Z})$ が存在し, 以下が成り立つ.

$$B = U \begin{pmatrix} d_1 & & & & & \\ & \ddots & & & & \\ & & d_r & & & \\ & & & 0 & & \\ & & & & \ddots & \\ & & & & & 0 \end{pmatrix} V$$

さらに, 整数 $d_1, \ldots, d_r$ は符号を除いて一意的である.

**証明**

準同型 $f\colon \mathbb{Z}^n \to \mathbb{Z}^n$, $x \mapsto Bx$ を考え, $L = f(\mathbb{Z}^n)$ とおく. 命題 5.12 により, $\mathbb{Z}^n = \mathrm{Ker}(f) \oplus M_0$ と分解できる. さらに, 写像 $f\colon M_0 \to L$ は同型写像である. 定理 5.23 により, $\mathbb{Z}^n$ の基底 $\mathcal{B} = (x_1, \ldots, x_n)$ 及び $d_1, \ldots, d_r \in \mathbb{Z} - \{0\}$ が存在し, $d_{i+1} \mid d_i$ かつ $d_1x_1, \ldots, d_rx_r$ は $L$ の基底である. $f\colon M_0 \to L$ が全単射より, $d_ix_i = f(u_i)$ を満たす $u_i \in M_0$ が存在する. さらに, $(u_1, \ldots, u_r)$ は $M_0$ の基底をなす. $\mathrm{Ker}(f)$ の基底 $(u_{r+1}, \ldots, u_n)$ をとる. $M = M_0 \oplus \mathrm{Ker}(f)$ より, $\mathcal{C} := (u_1, \ldots, u_n)$ は $M$ の基底である. また, $\mathbb{Z}^n$ の標準基底を $\mathcal{D}$ とおく.

$$B = \mathrm{Mat}_{\mathcal{D},\mathcal{D}}(f_B) = \mathrm{Mat}_{\mathcal{B},\mathcal{D}}(\mathrm{id}) \times \mathrm{Mat}_{\mathcal{C},\mathcal{B}}(f) \times \mathrm{Mat}_{\mathcal{D},\mathcal{C}}(\mathrm{id})$$

と表せる. $U = \mathrm{Mat}_{\mathcal{B},\mathcal{D}}(\mathrm{id})$, $V = \mathrm{Mat}_{\mathcal{D},\mathcal{C}}(\mathrm{id})$ とおく. $\mathcal{B}, \mathcal{C}, \mathcal{D}$ が $\mathbb{Z}^n$ の基底であるので, $U, V \in \mathrm{GL}_n(\mathbb{Z})$ が成り立つ. また, $\mathrm{Mat}_{\mathcal{C},\mathcal{B}}(f)$ は対角行列であり, その対角成分が $d_1, \ldots, d_r, 0, \ldots, 0$ である. 最後に, 定理 5.23 により, イデアル $d_1\mathbb{Z}, \ldots, d_r\mathbb{Z}$ は一意的に定まるので, $d_1, \ldots, d_r$ は符号を除いて一意的である.

## 5.8 線形代数学への応用

### 5.8.1 $K[X]$ 加群

以下, $K$ を可換体とする. $V$ が $K$ ベクトル空間で, $f\colon V \to V$ を $K$ 線形写像とする. 多項式 $P(X) = \sum_{i=0}^{n} a_iX^i \in K[X]$ に対し,

$$P(f) := \sum_{i=0}^{n} a_i f^i$$

と定義する. 但し, $f^i = f \circ \cdots \circ f$ ($i$ 個) である. 多項式 $P(X) \in K[X]$ 及び $V$ のベクトル $v \in V$ に対して,

$$P(X)v = P(f)v$$

とおくことによって $V$ は $K[X]$ 加群になる. $W \subset V$ が線形部分空間のとき,

$$W \text{ が } V \text{ の部分 } K[X] \text{ 加群である} \iff f(W) \subset W$$

が成り立つ. 逆に, $M$ が $K[X]$ 加群ならば, 写像 $M \to M$, $a \mapsto Xa$ が $K$ 線形写像である. ゆえに, 「$K[X]$ 加群」というのは, 「線形写像 $f\colon V \to V$ を持つベクトル空間 $V$」に他ならない. $V$ が有限次元 $K$ ベクトル空間のとき, 明らかに有限生成 $K[X]$ 加群である.

### 5.8.2 巡回加群, 同伴行列

$V$ を有限次元 $K$ ベクトル空間とし, $f\colon V \to V$ を線形写像とする. 上のように $V$ を $K[X]$ として考える. $V$ が巡回加群になるための必要十分条件について考える. 但し, ここでいう「巡回加群」とは, 一つの元で生成される加群のことである. $v \in V$ に対し, $v$ で生成される部分 $K[X]$ 加群を $\langle v \rangle_f$ とおく. 具体的にいうと,

$$\langle v \rangle_f := \mathrm{Span}_K(v, f(v), f^2(v), \dots) \tag{5.1}$$

である.

**命題 5.25** 以下が同値である.

(i) $V$ が巡回 $K[X]$ 加群である.

(ii) $v \in V$ が存在し, $(v, f(v), \dots, f^{n-1}(v))$ が $V$ の基底である.

**証明**

- (ii) が成り立つとき, (5.1) により $\langle v \rangle_f = V$ である. よって, $V$ が巡回 $K[X]$ 加群である.
- 逆に, (i) を仮定し, $V = \langle v \rangle_f$ $(v \in V)$ とする. 写像 $f\colon K[X] \to V$, $P \mapsto Pv$ は全射である. $\mathrm{Ker}(f) = (M(X))$ を満たすモニックな多項式 $M$ が存在する. 準同型定理により, 同型写像 $\frac{K[X]}{(M(X))} \to V$ が得られる. $M(X)$ の次数を $n$ とおく. 多項式の除法原理により, $\frac{K[X]}{(M(X))}$ の各剰余類は次数 $< n$ の代表元をちょうど一つ持つ. ゆえに, $(1, X, \dots, X^{n-1})$ の剰余類は $K$ ベクトル空間 $\frac{K[X]}{(M(X))}$ の基底をなす. よって, $(v, f(v), \dots, f^{n-1}(v))$ は $V$ の基底をなす.

命題 5.25(ii) を満たすベクトル $v \in V$ を考える. $\mathcal{B} = (v, f(v), \dots, f^{n-1}(v))$ とおく. $\mathcal{B}$ が $V$ の基底であるので,

$$f^n(v) = \sum_{i=0}^{n-1} b_i f^i(v), \qquad b_i \in K$$

と書ける. したがって, 基底 $\mathcal{B}$ に関する $f$ の行列は以下の通りになる.

$$\mathrm{Mat}_{\mathcal{B}}(f) = \begin{pmatrix} 0 & 0 & \dots & 0 & b_0 \\ 1 & 0 & \dots & 0 & b_1 \\ 0 & 1 & \dots & 0 & b_2 \\ \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & \dots & 0 & 1 & b_{n-1} \end{pmatrix}$$

この形の行列を同伴行列という.

**定義 5.26** 多項式 $P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0$ $(a_i \in K)$ に対し

$$C(P) := \begin{pmatrix} 0 & 0 & \dots & 0 & -a_0 \\ 1 & 0 & \dots & 0 & -a_1 \\ 0 & 1 & \dots & 0 & -a_2 \\ \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & \dots & 0 & 1 & -a_{n-1} \end{pmatrix}$$

とおき, $P$ の同伴行列という.

$n$ 次正方行列 $B \in \mathrm{M}_n(K)$ に対し, $B$ の固有多項式, 最小多項式をそれぞれ $\chi_B(X)$, $\mu_B(X)$ とおく.

**補題 5.27** $\chi_{C(P)} = \mu_{C(P)} = P$ が成り立つ.

**証明**

帰納法によって示す.

$$\chi_{C(P)} = \begin{vmatrix} X & 0 & \dots & 0 & a_0 \\ -1 & X & \dots & 0 & a_1 \\ 0 & -1 & \dots & 0 & a_2 \\ \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & \dots & 0 & -1 & X + a_{n-1} \end{vmatrix} = X \begin{vmatrix} X & & & a_1 \\ -1 & \ddots & & a_2 \\ & \ddots & \ddots & \vdots \\ & & -1 & X + a_{n-1} \end{vmatrix} + (-1)^n \begin{vmatrix} -1 & X & & \\ & \ddots & \ddots & \\ & & \ddots & X \\ & & & -1 \end{vmatrix}$$
$$= X(X^{n-1} + a_{n-1}X^{n-2} + \cdots + a_2X + a_1) + a_0$$
$$= P.$$

次に, $C(P)$ の最小多項式について考える. $\mu_{C(P)} = \sum_{i=0}^{m} c_i X^i$ $(c_i \in K)$ とおく. ケイリー・ハミルトンの定理により, $\mu_{C(P)} \mid \chi_{C(P)} = P$ が成り立つ. とくに, $m \leq n$ である. 行列 $C(P)$ に対応する $K$ 線形写像 $K^n \to K^n$ を $f$ とおき, $K^n$ の標準基底を $(e_1, \dots, e_n)$ をとおく. 明らかに, $f^i(e_1) = e_{i+1}$ $(0 \leq i < n)$ が成り立つ. $\mu_{C(P)}(f) = 0$ より,

$$0 = \sum_{i=0}^{m} c_i f^i(e_1) = \sum_{i=0}^{m} c_i e_{i+1}$$

となる. $m < n$ ならば, これは $(e_1, \dots, e_n)$ の線形独立性に矛盾するので, $m = n$ であることがいえる. $\mu_{C(P)} \mid \chi_{C(P)}$ より $\mu_{C(P)} = \chi_{C(P)} = P$ となる.

### 5.8.3 有理標準形

$V$ を $n$ 次元 $K$ ベクトル空間とし, $f\colon V \to V$ を $K$ 線形写像とする. $P \in K[X]$, $v \in V$ に対して,

$$Pv := P(f)v$$

とおくことで $V$ を $K[X]$ 加群とみなす. $K[X]$ 加群として $V = V_{\mathrm{tor}}$ を満たす. 実際, $P$ を $f$ の最小多項式とすると, $P(f) = 0$ であるので, 任意の $v \in V$ に対し $Pv = 0$ である. $K[X]$ が単項イデアル整域であるので, 定理 5.22 により $K[X]$ 加群として $V$ が

$$V \simeq \frac{K[X]}{(P_1)} \oplus \cdots \oplus \frac{K[X]}{(P_r)} \tag{5.2}$$

と分解できる. 但し, $P_{i+1} \mid P_i$ $(1 \leq i \leq r-1)$ である. また, イデアル $(P_1), \dots, (P_r)$ が一意的である. よって, $P_1, \dots, P_r$ をモニックな多項式とすると, $P_1, \dots, P_r$ は一意的に定まる. (5.2) により,

$$V = W_1 \oplus \cdots \oplus W_r$$

となる線形部分空間 $W_1, \dots, W_r$ が存在し, 以下の 2 つ条件が満たされる.

- $f(W_i) \subset W_i$ である. さらに, $W_i$ が巡回 $K[X]$ 加群である.
- $f|_{W_i}\colon W_i \to W_i$ の固有多項式を $P_i$ とおくと, $P_{i+1} \mid P_i$ $(1 \leq i \leq r-1)$ である.

さらに, $P_1, \dots, P_r$ は一意的である (つまり, 上の条件を満たす $W_1, \dots, W_r$ の取り方に依らない). 命題 5.25 により, $v_i \in W_i$ が存在し, $\mathcal{B}_i = (v_1, f(v_i), \dots, f^{m_i-1}(v_i))$ が $W_i$ の基底である. 但し, $m_i = \dim_K(W_i)$ とする. $\mathcal{B} = (\mathcal{B}_1, \dots, \mathcal{B}_r)$ とおくと, $\mathcal{B}$ は $V$ の基底である. さらに,

$$\mathrm{Mat}_{\mathcal{B}}(f) = \begin{pmatrix} C(P_1) & & \\ & \ddots & \\ & & C(P_r) \end{pmatrix}$$

が成り立つ. ゆえに, 以下の定理が示せた.

**定理 5.28**　$B \in \mathrm{Mat}_n(K)$ を $n$ 次正方行列とする. このとき, $P_{i+1} \mid P_i$ $(1 \leq i \leq r-1)$ を満たすモニックな多項式 $P_1, \ldots, P_r$ が存在し, $B$ が以下の行列と相似である.

$$C(P_1, \ldots, P_r) := \begin{pmatrix} C(P_1) & & \\ & \ddots & \\ & & C(P_r) \end{pmatrix}$$

また, $P_1, \ldots, P_r$ が一意的に定まる.

**定義 5.29**　定理 5.28 によって得られた行列 $C(P_1, \ldots, P_r)$ は $B$ の有理標準形と呼ばれる. また, 多項式 $P_1, \ldots, P_r$ を $B$ の単因子という.

**補題 5.30**　$B \in \mathrm{M}_n(K)$ とし, $B' := C(P_1, \ldots, P_r)$ を $B$ の有理標準形とする. 但し, $P_1, \ldots, P_r$ はモニックな多項式で, $P_{i+1} \mid P_i$ $(1 \leq i \leq r-1)$ を満たすものとする. このとき, 以下が成り立つ.

$$\chi_B = P_1 \ldots P_r$$
$$\mu_B = P_1.$$

**証明**

$B$ と $B'$ が相似であるので, $\chi_B = \chi_{B'}$ かつ $\mu_B = \mu_{B'}$ が成り立つ. よって, $B = B'$ として良い. 各 $i$ に対し, $\chi_{C(P_i)} = P_i$ より $\chi_A = P_1 \ldots P_r$ がいえる. また, $P_i \mid P_1$ であるので, $P_1(B) = 0$ である. ゆえに, $\mu_B \mid P_1$ が成り立つ. また, $\mu_{C(P_1)} = P_1$ であるので, $P_1 \mid \mu_B$ である. 以上より, $\mu_B = P_1$ となる.

**例 5.31.** $B \in \mathrm{M}_n(\mathbb{R})$ で, $B^2 + E_n = 0$ とする. このとき, $\mu_B \mid X^2 + 1$ である. $X^2 + 1$ が $\mathbb{R}$ 上の既約多項式であるので, $\mu_B = X^2 + 1$ となる. また, $B$ の単因子は $(X^2 + 1, \ldots, X^2 + 1)$ となる (とくに, $n$ が偶数である). 定理 5.28 により, $B$ は以下の行列と相似である.

$$\begin{pmatrix} 0 & -1 & & & \\ 1 & 0 & & & \\ & & \ddots & & \\ & & & 0 & -1 \\ & & & 1 & 0 \end{pmatrix}$$