代数学基礎 B 講義ノート (環論)

作成者：石川雅雄

平成 29 年 2 月 6 日

環・加群・単因子論について勉強する.

目 次

第1章　環の定義

1.1　準備

$\mathbb{P} = \{1, 2, \dots\}$ 自然数の集合, $\mathbb{N} = \{0, 1, 2, \dots\}$ 非負整数の集合, $\mathbb{Z} = \{-2, -1, 0, 1, 2, \dots\}$ 整数の集合, $\mathbb{Q}$ 有理数の集合, $\mathbb{R}$ 実数の集合, $\mathbb{C}$ 複素数の集合.

1.1.1　半群

定義 1.1.1. (半群)　集合 S 上に **二項演算 (binary operation)** $S \times S \to S$, $(x, y) \mapsto x \cdot y$ が定義されていて

(i) $(x \cdot y) \cdot z = x \cdot (y \cdot z)$　　(結合律 associative law)

をみたすとき S を **半群 (semigroup)** という. 乗法の記号 $\cdot$ を省略して $x \cdot y$ を単に xy と書くこともある.

例 1.1.2. $\mathbb{P}$ は加法 $+$ に関して半群である.

定義 1.1.3. (部分半群)　S が半群で S' が S の部分集合のとき,

(S-i) $x, y \in S'$ ならば $x, y \in S'$)

が成り立つならば S' は S の**部分半群 (subsemigroup)** という.

例 1.1.4. $S' = (\mathbb{P}, +)$ は $S = (\mathbb{N}, +)$ の部分半群である.

定義 1.1.5. (半群としての準同型)　S, S' が半群で $f : S \to S'$ が写像のとき,

(H-i) $f(x \cdot y) = f(x) \cdot f(y)$　　$(^\forall x, y \in S)$

が成り立つならば f は **半群としての準同型 (semigroup homomorphism)** という.

例 1.1.6. $S = S' = (\mathbb{P}, +)$ のとき $f : \mathbb{P} \to \mathbb{P}$, $x \mapsto 2x$ は半群としての準同型である.

命題 1.1.7. S, S' が半群で $f : S \to S'$ が半群としての準同型写像のとき, $\operatorname{Im} f$ は S' の部分半群である.

命題 1.1.8. 命題 1.1.7 を証明せよ.

1.1.2　モノイド

定義 1.1.9. (モノイド)　半群 M において $1_M \in S$ が存在して,

(ii) $1_M \cdot x = x \cdot 1_M = x$　　$(^\forall x \in M)$

が成り立つならば 1_M は M の**単位元 (identity** または **unit)** という. また, このとき, M を**モノイド** または **単位元をもつ半群 (monoid)** という.

例 1.1.10. $\mathbb{N}$ は加法 $+$ に関して monoid である. このときの単位元は 0 である.
$\mathbb{P}$ は乗法 $\cdot$ に関して monoid である. このときの単位元は 1 である.

問題 1.1.11. 半群 S に, ある元 $1_S \in S$ が存在して

(ii') $1_S \cdot x = x$　　$(^\forall x \in S)$

が成り立つとき, 1_S を **左単位元 (left identity)** という.

同様にして, ある元 $1'_S \in S$ が存在して

(ii") $x \cdot 1'_S = x \qquad ({}^{\forall}x \in M)$

が成り立つとき, $1'_S$ を **右単位元 (right identity)** という. 半群 S に, 左単位元 1_S と右単位元 $1'_S$ が存在すれば $1_S = 1'_S$ であることを示せ. したがって, 単位元は存在すれば一意である.

定義 1.1.12. (部分モノイド) M がモノイドで M' が M の部分集合のとき,

(S-i) M' は M の部分半群
(S-ii) $1_M \in M'$

が成り立つならば M' は M の**部分モノイド (submonoid)** という.

例 1.1.13. $\mathbb{Z}$ は 加法 $+$ に関して $\mathbb{Q}$ の部分モノイドである.

例 1.1.14. $\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$ は乗法 $\cdot$ に関して $\mathbb{R}^\times = \mathbb{R} \setminus \{0\}$ の部分モノイドである.

定義 1.1.15. (モノイドとしての準同型) M, M' がモノイドで $f : M \to M'$ が写像のとき,

(H-i) f は半群としての準同型
(H-ii) $f(1_M) = 1_{M'}$

が成り立つならば f は モノイドとしての**準同型 (homomorphism)** という.

命題 1.1.16. M, M' がモノイドで $f : M \to M'$ がモノイドとしての準同型写像のとき, $\operatorname{Im} f$ は M' の部分モノイドである.

命題 1.1.17. 命題 1.1.16 を証明せよ.

1.1.3 群

定義 1.1.18. (群) 単位元を持つ半群 G において,

(iii) ${}^{\forall}x \in G$ に対して ${}^{\exists}y \in G$ が存在して $x \cdot y = y \cdot x = 1_G$

が成り立つとき, G を **群 (group)** という. このとき, y を x の**逆元 (inverse)** といい, x^{-1} と書く.

例 1.1.19. $\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$, $\mathbb{R}^\times = \mathbb{R} \setminus \{0\}$, $\mathbb{C}^\times = \mathbb{C} \setminus \{0\}$ は乗法 $\cdot$ に関して群である.

問題 1.1.20. モノイド M において, ある $x \in M$ に対して

(ii') $y \cdot x = 1_M$

が成り立つとき, y を x の **左逆元 (left inverse)** という.

同様にして, ある元 $1'_M \in M$ が存在して

(ii") $x \cdot z = 1_M$

が成り立つとき, z を x の **右逆元 (right inverse)** という. x の左逆元 y と右逆元 z が存在すれば $y = z$ であることを示せ. したがって, $x \in G$ の逆元 x^{-1} は存在すれば一意である.

定義 1.1.21. (群) G が群で G' が G の部分集合のとき

(S-i) G' は G の部分半群である.
(S-iii) $x \in G'$ ならば $x^{-1} \in G$ である.

が成り立つとき, G' を G の**部分群 (subgroup)** という.

問題 1.1.22. 上の (S-i) と (S-iii) から (S-ii) を導け.

命題 1.1.23. (群としての準同型写像)　群 G, G' とモノイドとしての準同型写像 $f : G \to G'$ に対して,

$$f(x^{-1}) = f(x)^{-1} \qquad ({}^{\forall}x \in S)$$

が成り立つ. よって, このとき, f は**群としての準同型写像 (group homomorphism)** という.

問題 1.1.24. 命題 1.1.23 を示せ.

命題 1.1.25. G, G' が群で $f : G \to G'$ が群としての準同型写像のとき, $\mathrm{Im}\, f$ は G' の部分群である.

命題 1.1.26. 命題 1.1.16 を証明せよ.

定義 1.1.27. (アーベル群)　群 A において,

(iv) $x \cdot y = y \cdot x$ (可換律 commutative law)

が成り立つとき, A を **アーベル群 (Abelian group)** という. 特に, 群の演算を, 乗法 $\cdot$ の代わりに加法 $+$ で書き $x+y$ と書いたとき **加群 (additive group)** という. また, このとき x の逆元を $-x$ と書く.

例 1.1.28. $\mathbb{Z}$ は加法 $+$ に関して加群である.

1.2　環の定義

1.2.1　環と単位的環

定義 1.2.1. (環と単位的環) 集合 R において, 2 つの二項演算 $R \times R \to R$, 加法 $(x, y) \mapsto x + y$, 乗法 $(x, y) \mapsto x \cdot y$ が定義されていて,

(1) 加法 $+$ に関して R は加群である.
(2) 乗法 $\cdot$ に関して $R \setminus \{0\}$ は半群である.
(3) 次の分配律が成り立つ.

(3l) $x \cdot (y + z) = x \cdot y + z \cdot z$　　**左分配律 (left distributive law)**
(3r) $(x + y) \cdot z = x \cdot z + y \cdot z$　　**右分配律 (right distributive law)**

が成り立つとき, R は**環 (ring)** という. さらに (2) の代わりに

(2') 乗法 $\cdot$ に関して $R \setminus \{0\}$ は monoid である.

を仮定するとき, R は**単位的環 (unitary ring)** または**単位元を持つ環 (ring with unity)** という.[1]

命題 1.2.2. (環の性質)　環 R においては, 次が成り立つ.

1) 任意の元 x について $x0 = 0x = 0$ が成り立つ.
2) 単位的環において $1 = 0$ ならば、その環にはたった一つの元 0 しか含まれない.
3) 乗法の単位元が存在するとき $-1a = (-1)a$ が成り立つ。
4) $(-a)(-b) = ab$ が成り立つ.

したがって, 今後 $1 \neq 0$ と仮定する.

問題 1.2.3. 命題 1.2.2 を証明せよ.

定義 1.2.4. (環の準同型写像) R, R' が環であり, $f : R \to R'$ が写像であるとき

(H1) 加法 $+$ に関して f は群としての準同型である.
(H2) 乗法 $\cdot$ に関して f は半群としての準同型である.

[1] 環の概念は, 1880 年代のデデキントに始まる, フェルマーの最終定理に対する証明の試みの中で形成されていった. 他分野（主に数論）からの寄与もあって, 環の概念は一般化されていき, 1920 年代のうちにエミー・ネーター, ヴォルフガング・クルルらによって確立される.

を満たすとき, f は**環としての準同型 (homomorphism as ring)** という.

さらに, R, R' が単位的環であり, f が (H2) の代わりに

(H2') 乗法 $\cdot$ に関して f はモノイドとしての準同型である.

をみたすとき, f は**単位的環としての準同型 (homomorphism as unitary ring)** という. 特に, f が単射のとき, **単準同型 (injective homomorphism)**, f が全射のとき, **全準同型 (surjective homomorphism)**, f が全単射のとき, **同型 (R-isomorphism)** という. また, 同型写像 $f : M \to M$ を**自己同型 (automorphism)** という.

定義 1.2.5. (部分環) R が環であり, R' が R の部分集合であるとき

(S1) 加法 $+$ に関して R' は R の部分群である.
(S2) 乗法 $\cdot$ に関して R' は R の部分半群である.

を満たすとき, R' は R の**部分環 (subring)** という.

さらに, R が単位的環であり, R' が (S2) の代わりに

(S2') 乗法 $\cdot$ に関して R' は R の部分モノイドである.

をみたすとき, f は**単位的部分環 (unitary subring)** という.

命題 1.2.6. R, R' が環 (resp. 単位的環) で $f : R \to R'$ が環としての準同型写像 (resp. 単位的環としての準同型写像) のとき, $\mathrm{Im}\, f$ は R' の部分環 (resp. 単位的部分環) である.

問題 1.2.7. 命題 1.2.6 を証明せよ.

1.2.2 域 (domain)

定義 1.2.8. (零因子・域) R を単位元をもつ環とするとき, $x \neq 0 \in R$ であるとき, $y \neq 0 \in R$ が存在して $xy = 0$ となるとき, x を**左零因子**という. 同様に $y \neq 0 \in R$ が存在して $yx = 0$ となるとき, x を**右零因子**という. R に左零因子も右零因子も存在しないとき, すなわち

(4) $x, y \in R$ に対して $x \cdot y$ ならば $x = 0$ または $y = 0$ である.

が成り立つとき, R を**域 (domain)** という.

定義 1.2.9. 単位元をもつ可換環環 D が域であるとき, **整域 (integral doman)** という.

例 1.2.10. $\mathbb{Z}$ は加法 $+$ と乗法 $\cdot$ に関して整域である.

問題 1.2.11. $R = \mathbb{Z}[\sqrt{-1}] = \mathbb{Z} + \mathbb{Z}\sqrt{-1} = \{x + y\sqrt{-1} | x, y \in \mathbb{Z}\}$ は整域であることを示せ.

1.2.3 可換環 (commutative ring)

定義 1.2.12. (斜体) R を単位元をもつ環とするとき, さらに

(2") 乗法 $\cdot$ に関して R は群である.

を仮定するとき, R は**斜体 (skew field)** という.

定義 1.2.13. (単位元を持つ可換環) 単位元を持つ環 R が, 乗法に関する可換律

(iv) $x \cdot y = y \cdot x$ (可換律 commutative law)

をみたすとき, **単位元を持つ可換環 (commutative ring with unit)** または, 単に, **可換環 (commutative ring)** という

1.2.4 体 (field)

定義 1.2.14. 単位元をもつ可換環環 F が斜体であるとき, **体 (field)** という.

例 1.2.15. $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ は体であるが $\mathbb{Z}$ は体でない.

問題 1.2.16. 四元数環 $\mathbb{H} = \{x + yi + jz + kw | x, y, z, w \in \mathbb{R}\}$ は斜体であることを示せ. ここで $i^2 = j^2 = k^2 = -1$, $ij = k$, $jk = i$, $ki = j$, $ji = -k$, $kj = -i$, $ik = -j$ とする.

注意 1.2.17. これまでに出てきた, i) 環, ii) 単位的環, iii) 可換環, iv) 体, の違いを憶えよう. i) ii) のような非可換環は群の表現論に使われ, iii) の可換環は可換環論・代数幾何などに使われる. iv) の体はガロア理論などで学習する. 数学の専門分野によって, 同じ「環」という言葉が違う意味を持つことに注意しよう.

	環	単位的環	域	斜体	可換環	整域	体
乗法の単位元	×	○	○	○	○	○	○
乗法の可換律	×	×	×	×	○	○	○
乗法の逆元	×	×	×	○	×	×	○

第2章　加群

2.1　R-加群

2.1.1　R-加群

定義 2.1.1. (左 R-加群)　R が環で, M が加群のとき, R の M に対する作用 $R \times M \to M$, $(a, x) \mapsto ax$ が定義されていて

(1) $a, b \in R$, $x \in M$ に対して $a(x+y) = ax + ay$ である
(2) $a, b \in R$, $x \in M$ に対して $(a+b)x = ax + bx$ である
(3) $a, b \in R$, $x \in M$ に対して $(ab)x = a(bx)$ である

が成り立つとき, M を**左 R-加群 (left R-module)** という. さらに, R が単位的環の場合には,

(4) $x \in M$ に対して $1x = x$ である

が成り立つことを仮定する.

問題 2.1.2. M が左 R-加群のときに, 任意の $x \in M$ に対して $0_R x = 0_M$ を示せ. また, R が単位的環のとき任意の $x \in M$ に対して $(-1_R)x = -x$ を示せ.

例 2.1.3. M が加群 (additive group) のとき, 整数環 $R = \mathbb{Z}$ の M への作用 $R \times M \to M$ を $x \in M$ に対して

$$nx = \underbrace{x + x + \cdots + x}_{n \text{ times}}$$

と定義すると, この作用は, 上の (1) (2) (3) をみたす. よって, 単なる加群は $\mathbb{Z}$-加群とみなせる.

問題 2.1.4. 上の例 2.1.3 の作用が (1) (2) (3) (4) をみたすことを示せ.

定義 2.1.5. (右 R-加群)　R が環で, M が加群のとき, R の M に対する作用 $M \times R \to M$, $(x, a) \mapsto ax$ が定義されていて

(1') $a, b \in R$, $x \in M$ に対して $(x+y)a = xa + ya$ である
(2') $a, b \in R$, $x \in M$ に対して $x(a+b) = xa + xb$ である
(3') $a, b \in R$, $x \in M$ に対して $x(ab) = (xa)b$ である

が成り立つとき, M を**右 R-加群 (right R-module)** という. さらに, R が単位的環の場合には,

(4') $x \in M$ に対して $x = x1$ である

が成り立つことを仮定する.

定義 2.1.6. (両側加群)　R, S が環 (または, 単位的環) で, M が左 R-加群かつ右 S-加群で,

(5) $a \in R$, $b \in S$, $x \in M$ に対して $(ax)b = a(xb)$ である　　**作用の可換性**

が成り立つとき, M を **(R, S)-両側加群 ((R, S)-bimodule)** という.

注意 2.1.7. 以後, 特に断らない限り, R を単位的環とし, M は左 R-加群と仮定する. 右 R-加群についても, ほぼ並行的に言えるので, 左 R-加群のみを扱い右 R-加群については述べない. 左 R-加群を, 単に, R-加群と書くこともある. これが, もっとも一般的な定義である.

注意 2.1.8. M が左 R-加群のとき, 特に, R が可換環ならば R の M への右からの作用を $a \in R$ と $x \in M$ に対して

$$xa := ax$$

によって定義することによって M は右 R-加群になる. また, この作用によって M は (R,R)-両側加群とすることもできる. よって, R が可換環のときは, 左加群か右加群か, または (R,R)-両側加群かを特に区別する必要はない.

また, R が体のときは R-加群を **R 上のベクトル空間 (vector space)** という.

しかし, ここでは, 主に非可換な単位的環を想定して欲しい.

問題 2.1.9. 注意 2.1.8 において定義した右からの作用が, 定義 2.1.5 の (1') (2') (3') (4') をみたすことを示せ. また, (R,R)-両側加群とみたときに, 定義 2.1.6 の (5) をみたすことを示せ.

2.1.2 部分加群

定義 2.1.10. (R-部分加群) R が (単位的) 環, M が左 R-加群のとき, 部分集合 $N \subseteq M$ が

(i) N は M の (addtive group として) 部分加群
(ii) 任意の $a \in R$ と $x \in N$ に対して $ax \in N$

をみたすとき, N は M の **R-部分加群 (R-submodule)** という. 特に $\mathbf{0} = \{0\}$ と M 自身は, M の R-部分加群であり, これらを**自明な (trivial)** R-部分加群という. 自明でない R-部分加群を**非自明な (non-trivial)** R-部分加群という. また, R が体のときは R-部分加群を**部分空間 (subspace)** という.

問題 2.1.11. R が (単位的) 環, M が左 R-加群のとき, 部分集合 $N \subseteq M$ が R-部分加群であるための必要十分条件は

(i') 任意の $x, y \in N$ に対して $x + y \in N$ である [1]
(ii) 任意の $a \in R$ と $x \in N$ に対して $ax \in N$ である

をみたすことであることを示せ.

定義 2.1.12. R, S が (単位的) 環, M が (R,S)-両側加群のとき, 部分集合 $N \subseteq M$ が左 R-部分加群かつ右 S-部分加群であるとき N は M の **(R,S)-両側部分加群 ((R,S)-sub-bimodule)** という.

2.1.3 加群としての準同型写像

定義 2.1.13. (準同型写像) R を (単位的) 環, M, M' を左 R-加群とするとき, 写像 $f : M \to M'$ が

(I) f は加群 (addtive group) としての準同型写像 である
(II) 任意の $a \in R$ と $x \in M$ に対して $f(ax) = af(x)$ である

をみたすとき, f は**左 R-加群としての準同型写像 (homomorphism as left R-module)** または **R-準同型 (R-homomorphism)** という. 特に, f が単射のとき, **R-単準同型 (injective R-homomorphism)**, f が全射のとき, **R-全準同型 (surjective R-homomorphism)**, f が全単射のとき, **R-同型 (R-isomorphism)** という. また, R-同型写像 $f : M \to M$ を **R-自己同型 (R-automorphism)** という. また, R が体のときは, R-準同型写像を **R-線形写像 (R-linear map)** という.

問題 2.1.14. R を (単位的) 環, M, M' を左 R-加群とするとき, 写像 $f : M \to M'$ が R-準同型であるための必要十分条件は

(I') 任意の $x, y \in M$ に対して $f(x + y) = f(x) + f(y)$ である [2]

---

[1] 群論で習うように N が M の部分加群であるための必要十分条件は
(i'') 任意の $x, y \in N$ に対して $x - y \in N$ である
である. この条件はさらに弱い.

[2] 群論で習うように f が加群としての準同型であるための必要十分条件は
(I'') 任意の $x, y \in M$ に対して $f(x - y) = f(x) - f(y)$ である
である. この条件はさらに弱い.

(II) 任意の $a \in R$ と $x \in M$ に対して $f(ax) = af(x)$ である

をみたすことであることを示せ.

命題 2.1.15. R を (単位的) 環, M, M' を左 R-加群とし, 写像 $f : M \to M'$ が R-準同型であるとする. N が M の R-部分加群 N' が M' の R-部分加群とするとき, 次が成り立つ.

1) $f(N)$ は M' の R-部分加群である.
2) $f^{-1}(N')$ は M の R-部分加群である.

特に, $\mathrm{Im}\, f = f(M)$ は M' の R-部分加群, $\mathrm{Ker}\, f = f^{-1}(\mathbf{0})$ は M の R-部分加群である.

証明. 易しいので省略. □

問題 2.1.16. 命題 2.1.15 を証明せよ.

定義 2.1.17. (完全列)　R を (単位的) 環, $\mathscr{M} = \{M_i\}_{i \in I}$ を左 R-加群の有限または可算列, 写像 $f_i : M_i \to M_{i+1}$ が R-準同型写像の列

$$\cdots \xrightarrow{f_{i-2}} M_{i-1} \xrightarrow{f_{i-1}} M_i \xrightarrow{f_i} M_{i+1} \xrightarrow{f_{i+1}} \cdots$$

のとき

(III) $\mathrm{Im}\, f_i = \mathrm{Ker}\, f_{i+1}$

が両辺が定義される任意の $i \in I$ に対して成り立つとき, $\{f_i\}$ を**完全系列 (exact sequence)** という.

命題 2.1.18. R を (単位的) 環, M, M' を左 R-加群, f, g, h を R-準同型写像とする.

1) $\mathbf{0} \xrightarrow{f} M$ が exact であるための必要十分条件は f が単射である.
2) $M \xrightarrow{f} \mathbf{0}$ が exact であるための必要十分条件は f が全射である.
3) $\mathbf{0} \xrightarrow{f} M \xrightarrow{g} M' \xrightarrow{h} \mathbf{0}$ が exact であるとき g は全単射である.

証明. 易しいので省略. □

問題 2.1.19. 命題 2.1.18 を証明せよ.

2.1.4　剰余加群

定理 2.1.20. (剰余加群)　R を (単位的) 環, M を左 R-加群, N を M の左 R-部分加群とする. M に関係 $\equiv$ を次のように定義する.

$$x \equiv y \Leftrightarrow y - x \in N$$

このとき, $\equiv$ は同値関係であり, この同値関係による $x \in M$ の剰余類を $[x] := x + N := \{y \in M | y \equiv x\} = \{x + y | y \in N\}$ と書く. 剰余類全体の集合を

$$M/N = \{x + N \,|\, x \in M\}$$

と書く. このとき, $a \in R$ の M/N への作用を

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

によって定義すると, M/N は左 R-加群の構造が入る. また, 写像 $\pi : M \to M/N$ を $x \in M$ に対して $\pi(x) = x + N$ によって定義すると π は R-全準同型写像である.

証明. 1) $\equiv$ が同値関係であることを示す, 2) $x \in M$ の同値類が $[x] = x + N$ であることを示す, 3) $a \in R$ の M/N への作用 $a(x + N) = ax + N$ が well-defined (代表元の取り方に依存しない) ことを示す, 4) この作用で M/N が左 R-加群であることを示す, 5) $\pi : x \mapsto x + N$ が準同型写像であることを示す, の順に示す. □

定義 2.1.21. (剰余加群)　R を (単位的) 環, M を左 R-加群, N を M の左 R-部分加群とするとき, M/N を**剰余 R-加群 (quotient R-module)**, $\pi : M \to M/N$ を自然な準同型写像という.

定理 2.1.22. (準同型定理)　R を (単位的) 環, M, N を左 R-加群, $f : M \to N$ を全射 R-準同型写像とする. このとき

$$M/\operatorname{Ker} f \simeq N$$

が成り立つ.

証明. 命題 2.1.15 より, $\operatorname{Ker} f = f^{-1}(\mathbf{0})$ は M の R-部分加群である. このとき, $\overline{f} : M/\operatorname{Ker} f \to N$ を

$$\overline{f}(x + \operatorname{Ker} f) = f(x)$$

によって, 定義する. このとき, 1) $\overline{f}$ は well-defined, 2) $\overline{f}$ は単射, 3) $\overline{f}$ は全射であることを示す.

1) は $x - y \in \operatorname{Ker} f$ ならば $f(x) = f(y)$ だから成り立つ. 2) は $f(x) = f(y)$ ならば $x - y \in \operatorname{Ker} f$ なので $x + \operatorname{Ker} f = y + \operatorname{Ker} f$ である. 3) は明らかである. □

2.1.5　生成される部分加群

命題 2.1.23. R が (単位的) 環, M_λ ($\lambda \in \Lambda$) が左 R-加群の族 (family) のとき, $\bigcap_{\lambda\in\Lambda} M_\lambda$ も左 R-加群である.

問題 2.1.24. 命題 2.1.23 を証明せよ.

命題 2.1.25. (生成される部分加群)　R が (単位的) 環, M を左 R-加群, S が M の任意の部分集合であるとき, S を含む M の R-部分加群全体の交わり (intersection) は S を含む最小の R-部分加群になる. 明らかに, この部分 R-加群は

$$\sum_i r_i s_i$$

($r_i \in R$, $s_i \in S$) の形の有限和全体の集合であり, この集合を RS と書くことにする. RS を S から生成される R-部分加群 (R-**submodule generated by** S) という.

定義 2.1.26. (生成される部分加群)　R が (単位的) 環, M を左 R-加群のとき, 有限集合 S が存在して $M = RS$ となるならば, M は **有限生成 (finitely generated)** という.

第3章　イデアル・剰余環

3.1　イデアル

この節では, R は単位的環とする. このとき, R 自身に対する R の左からの作用を $a, x \in R$ に対して ax を普通の R の掛け算で定義することによって, R に左 R-加群の構造が入る. 右 R-加群に関しても同様である. また, これらによって R は (R, R)-両側加群でもある.

3.1.1　イデアル

定義 3.1.1. (イデアル)　R が (単位的) 環のとき R の部分集合 I が, 左 R-部分加群であるとき, I を R の**左イデアル (left ideal)** という. すなわち, I が左イデアルであるための必要十分条件は, 以下の 1) 2) をみたすことである.

1) 任意の $x, y \in I$ に対して $x + y \in I$ である
2) 任意の $a \in R$, $x \in I$ に対して $ax \in I$ である.

右イデアル (right ideal) の定義も同様である. I が左イデアルかつ右イデアルであるとき, I は R の**両側イデアル (two-sided ideal)** という. 両側イデアルを単に**イデアル (ideal)** という. 可換環においては, すべての 左 (または右) イデアルは両側イデアルである.

問題 3.1.2. $\mathbf{0} = \{0\}$ および R 自身は R の両側イデアルであることを示せ.

問題 3.1.3. $m \in \mathbb{Z}$ のとき, 単位的可換環 $R = \mathbb{Z}$ において

$$I = m\mathbb{Z} = \{mx | x \in \mathbb{Z}\}$$

はイデアルであることを示せ.

略解. 左イデアルことを示すには, 上の 1) 2) を示せばよい. これは $x, y \in \mathbb{Z}$ のとき

$$mx + my = m(x + y) \in m\mathbb{Z}$$

と, $a, x \in \mathbb{Z}$ のとき

$$a(mx) = m(ax) \in m\mathbb{Z}$$

に帰着する. 可換環なので, 左イデアルは両側イデアルであるであることを示せ.

問題 3.1.4. 実数を成分とする 2×2 行列全体の集合を

$$R = \mathrm{M}_2(\mathbb{R}) = \left\{ \begin{pmatrix} x & y \\ z & w \end{pmatrix} \,\middle|\, x, y, z, w \in \mathbb{R} \right\}$$

と書くことにすると R は非可換な単位的環である. 第 2 列 (resp. 第 2 列) の成分がすべて 0 である行列全体の集合を I (resp. J) と書くと, I (resp. J) は R の左イデアル (resp. 右イデアル) であることを示せ.

略解. 第 2 列の成分がすべて 0 である行列全体は

$$I = \left\{ \begin{pmatrix} x & 0 \\ z & 0 \end{pmatrix} \,\middle|\, x, z \in \mathbb{R} \right\}$$

と書ける. 1) を示すのは容易. 2) を示すには

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x & 0 \\ z & 0 \end{pmatrix} = \begin{pmatrix} ax+bz & 0 \\ cx+dz & 0 \end{pmatrix}$$

を使え.

命題 3.1.5. I_λ ($\lambda \in \Lambda$) が左イデアル (resp. 右イデアル, 両側イデアル) の族 (family) のとき, $\bigcap_{\lambda\in\Lambda} I_\lambda$ も左イデアル (resp. 右イデアル, 両側イデアル) である.

問題 3.1.6. 上を示せ.

略解. 1) を示すには, $x, y \in \bigcap_{\lambda\in\Lambda} I_\lambda$ ならば, すべての $\lambda \in \Lambda$ に対して, $x, y \in I_\lambda$ なので

$$x + y \in \bigcap_{\lambda\in\Lambda} I_\lambda$$

である. 2) も同様.

定義 3.1.7. (生成されるイデアル)　(単位的) 環 R の任意の部分集合 S に対して, S を含む左 (resp. 右, 両側) イデアル全体の集合を $\Lambda_{\mathrm{L}}(S)$ (resp. $\Lambda_{\mathrm{R}}(S)$, $\Lambda(S)$) と書き, $\Lambda_{\mathrm{L}}(S)$ (resp. $\Lambda_{\mathrm{R}}(S)$, $\Lambda(S)$) の元全体の交わり

$$(S)_{\mathrm{L}} = \bigcap_{I\in\Lambda_{\mathrm{L}}(S)} I \qquad (\text{resp. } (S)_{\mathrm{R}} = \bigcap_{I\in\Lambda_{\mathrm{R}}(S)} I, \quad (S) = \bigcap_{I\in\Lambda(S)} I\ )$$

をは S を含む最小の左 (resp. 右, 両側) イデアルである. 特に, $S = \{a_1, \ldots, a_s\}$ のとき, $(\{a_1, \ldots, a_s\})_{\mathrm{L}}$ 等を $(a_1, \ldots, a_s)_{\mathrm{L}}$ のようにと書く. また, 特に $s = 1$ のとき, 1 個の元から生成されるイデアル $(a)_{\mathrm{L}}$ (resp. $(a)_{\mathrm{R}}$ (a)) を**単項左イデアル (pricipal left ideal)** (resp. **単項右イデアル (pricipal right ideal)**, **単項イデアル (pricipal ideal)**) という.

定義 3.1.8. (単項イデアル整域)　単位的可換環 R において, そのイデアルがすべて単項イデアルである整域を, **単項イデアル整域 (Pricipal Ideal Domain)** という.

問題 3.1.9. 整数環 $\mathbb{Z}$ は単項イデアル整域であることを示せ.

略解. I が $\mathbb{Z}$ のイデアルで $I \neq \mathbf{0}$ とする. I に含まれる元の中で $x > 0$ で最小のものを a とする. 任意の $x \in I$ に対して, $x < 0$ ならば $-x$ を考えることにして $x > 0$ としてよい.

$$x = aq + r$$

となる整数 q と $0 \leq r < a$ が存在する. もし $r \neq 0$ ならば $r = x - aq \in I$ となり, a の最小性に反する. よって, $x = aq$ となり $I = (a)$ である.

問題 3.1.10. $(S)_{\mathrm{L}} = \left\{ \sum_{i=1}^{k} r_i a_i | r_i \in R, a_i \in S, k \in \mathbb{N} \right\}$ を示せ.

略解. $I = (S)_{\mathrm{L}}$, $J = \left\{ \sum_{i=1}^{k} r_i a_i | r_i \in R, a_i \in S, k \in \mathbb{N} \right\}$ とおくと, $a_i \in S \subseteq I$ なので

$$\sum_{i=1}^{k} r_i a_i \in I$$

だから $J \subseteq I$ である. よって J がイデアルであることを示せばよい.

定義 3.1.11. (イデアルの和)　(単位的) 環 R の左 (resp. 右, 両側) イデアルの族 I_λ ($\lambda \in \Lambda$) に対して

$$\left(\bigcup_{\lambda\in\Lambda} I_\lambda\right)_{\mathrm{L}} \qquad (\text{resp. } \left(\bigcup_{\lambda\in\Lambda} I_\lambda\right)_{\mathrm{R}} \quad \left(\bigcup_{\lambda\in\Lambda} I_\lambda\right)\ )$$

をイデアルの和といい

$$\sum_{\lambda\in\Lambda} I_\lambda$$

という.

問題 3.1.12. $4\mathbb{Z}+6\mathbb{Z}=2\mathbb{Z}$ を示せ. もっと一般的に $a,b\in\mathbb{Z}$ の最大公約数を d とすると, $a\mathbb{Z}+b\mathbb{Z}=d\mathbb{Z}$ を示せ.

証明. $\mathbb{Z}$ は単項イデアル整域なので $a\mathbb{Z}+b\mathbb{Z}=c\mathbb{Z}$ となる $c\in\mathbb{Z}$ が存在する. $c\in a\mathbb{Z}+b\mathbb{Z}$ なので $c=ax+by$ となる整数 $x,y\in\mathbb{Z}$ が存在する.

$$d|ax+by=c$$

となる.[1] 逆に $a,b\in c\mathbb{Z}$ より, $c|a,b$ となる. よって, c は a,b の公約数なので $c|d$ である.

命題 3.1.13. R, R' が (単位的) 環, $f:R\to R'$ が準同型写像のとき,

(1) f が全射で S が R の部分環ならば $f(S)$ は R' の部分環である.
(2) f が全射で I が R の左イデアル (resp. 右イデアル, 両側イデアル) ならば $f(I)$ は R' の左イデアル (resp. 右イデアル, 両側イデアル) である.
(3) S' が R' の部分環ならば $f^{-1}(S)$ は R の部分環である.
(4) I' が R' の左イデアル (resp. 右イデアル, 両側イデアル) ならば $I=f^{-1}(')$ は R の左イデアル (resp. 右イデアル, 両側イデアル) である. 特に, **核** $\operatorname{Ker} f=f^{-1}(\mathbf{0})$ は R の両側イデアルである.

問題 3.1.14. 上の命題 3.1.13 を示せ.

定義 3.1.15. I を単位的可換環 R のイデアルとする. $x,y\in R$ に対して

$$y-x\in I$$

のとき, $x\equiv y\pmod{I}$ と書き, x と y は I **を法として合同**という. 特に, $R=\mathbb{Z}$, $I=m\mathbb{Z}$ のときは $x\equiv y\pmod{m}$ と書き, x と y は m **を法として合同**という.

問題 3.1.16. 「I を法として合同」は, 同値関係であることを示せ.

問題 3.1.17. 「I を法として合同」について, 次が成り立つことを示せ.

1) $x_1\equiv y_1\pmod{I}$ かつ $x_2\equiv y_2\pmod{I}$ ならば $x_1+x_2\equiv y_1+y_2\pmod{I}$
2) $x_1\equiv y_1\pmod{I}$ かつ $x_2\equiv y_2\pmod{I}$ ならば $x_1x_2\equiv y_1y_2\pmod{I}$

補題 3.1.18. 与えられた二つの整数 m, n が互いに素[2] ならば, 任意に与えられる整数 a, b に対し,

$$\begin{aligned}x&\equiv a\pmod{m},\\ x&\equiv b\pmod{n}\end{aligned}$$

を満たす整数 x が mn を法として一意的に存在する.[3]

証明. (解の存在)　二つの整数 m, n が互いに素ならば, 問題 3.1.12 により[4] 適当な整数 u, v が存在して

$$mu+nv=1$$

となるようにできる. このとき,

$$\begin{aligned}mu&\equiv 1\pmod{n},\\ nv&\equiv 1\pmod{m}\end{aligned}$$

がなりたつので

$$x\equiv anv+bmu\pmod{mn}$$

とおくと, x は与えられた連立合同式の解となる.

---

[1] y が x で割り切れるとき $x|y$ と書く.
[2] m と n の最大公約数が 1 という意味
[3] x と y が両方とも解ならば $x\equiv y\pmod{mn}$ になる.
[4] ユークリッドの互除法でも証明できる.

(解の一意性)　y を任意の解とすると, $x-y$ は

$$x-y\equiv 0 \pmod{m},$$
$$x-y\equiv 0 \pmod{n}$$

を満たす. よって, $x-y$ は法 m および法 n で割り切れる. m と n とは互いに素なので, $x-y$ は m と n との最小公倍数 mn で割り切れる.

$$x-y\equiv 0 \pmod{mn}$$

すなわち, x と y とは法 mn に関して合同になる. □

定理 3.1.19. (中国の剰余定理[5])　与えられた k 個の整数 $m_1, m_2, \ldots, m_k$ がどの二つも互いに素ならば, 任意に与えられる整数 $a_1, a_2, \ldots, a_k$ に対し

$$x\equiv a_1 \pmod{m_1},$$
$$x\equiv a_2 \pmod{m_2},$$
$$\vdots$$
$$x\equiv a_k \pmod{m_k}$$

を満たす整数 x が $m_1m_2\cdots m_k$ を法として一意的に存在する.

証明. ガウスは『整数論』(1801 年) において, 法 $m_1, m_2, \ldots, m_k$ に関して対称な解法を示した.
(解の存在)　整数 $m_1, m_2, \ldots, m_k$ がどの二つも互いに素ならば,

$$M=m_1m_2...m_k,$$
$$M=m_1M_1=m_2M_2=\cdots=m_kM_k$$

と置くと, 各 m_i と M_i とは互いに素なので, 補題 3.1.18 により, $i=1,2,\cdots,k$ に対して,

$$M_it_i\equiv 1 \pmod{m_i},$$

となる t_i が存在する. このとき,

$$x\equiv a_1M_1t_1+a_2M_2t_2+\cdots+a_kM_kt_k \pmod{M}$$

は与えられた連立合同式の解になる. 例えば, x の第 1 項の法 m_1 に関する剰余は a_1 に合同であり, 第 2 項から第 k 項は M_2 から M_k が m_1 の倍数となるので, x は法 m_1 に関して a_1 と合同になる. $i=2,3,\ldots,k$ に関しても同様にして,

$$x\equiv a_i \pmod{m_i}$$

を満たすことがわかる.
(解の一意性)　y を任意の解とすると, $x-y$ は

$$x-y\equiv 0 \pmod{m_1},$$
$$x-y\equiv 0 \pmod{m_2},$$
$$\vdots$$
$$x-y\equiv 0 \pmod{m_k}$$

を満たす. よって, $x-y$ は法 $m_1, m_2, \ldots, m_k$ で割り切れる. $m_1, m_2, \ldots, m_k$ は互いに素なので, $x-y$ は法の最小公倍数 M で割り切れる.

$$x-y\equiv 0 \pmod{M}$$

すなわち, x と y とは法 M に関して合同になる.

[5] 3〜5 世紀頃成立したといわれている中国の算術書『孫子算経』に由来する

問題 3.1.20. 3 で割って 2 余り, 5 で割って 4 余る 15 $(= 3 \times 5)$ 未満の非負整数 n を求めよ [6]

問題 3.1.21. 中国の算術書『孫子算経』の問題を解け.

> 今物が有るが, その数はわからない. 三つずつにして物を数えると二余る. 五で割ると三余る. 七で割ると二余る. 物はいくつあるか？[7]

定理 3.1.22. (商体)　R を単位的可換環とし, $T \neq \emptyset$ は $R^\times$ 部分モノイドのとき, 次の性質をもつ単位的可換環 $\widetilde{R}$ および写像 $f : R \to \widetilde{R}$ が存在する.

1) f は単準同型である.
2) $f(T)$ の元は $\widetilde{R}$ において単元である.
3) $\widetilde{R}$ の任意の元 x は $x = f(a)(f(b))^{-1}$ $(a \in R, b \in T)$ の形に書かれる.

また, $(\widetilde{R}_1, f_1)$, $(\widetilde{R}_2, f_2)$ がともに 1) 2) 3) をみたすならば, 同型写像 $\varphi : \widetilde{R}_1 \to \widetilde{R}_2$ で $f_2 = \varphi \circ f_1$ となるものが存在する.

証明.

3.2　剰余環

この節では, R は単位的環とする.

3.2.1　単元群

定義 3.2.1. (逆元)　R が単位的環, $a \in R$ であるとき, $ba = 1$ となるとき b を a の**左可逆元 (left inverse)** といい, $ac = 1$ となるとき c を a の**右可逆元 (right inverse)** という. a が左逆元 b と 右逆元 c を両方持つとき, $b = c$ であり, これを a の**逆元 (inverse)**, a は**単元 (unit)** であるという. R の単元全体の集合を

$$R^\times$$

と書くことにすると, これは, 乗法に関して群であり, R の**単元群 (group of units)** と呼ばれる.

3.2.2　直積・直和

定義 3.2.2. (直積)　R_λ $(\lambda \in \Lambda)$ が (単位的) 環の族のとき, $R = \prod_{\lambda \in \Lambda} R_\lambda$ に

$$(x_\lambda)_{\lambda \in \Lambda} + (y_\lambda)_{\lambda \in \Lambda} = (x_\lambda + y_\lambda)_{\lambda \in \Lambda} \qquad (x_\lambda)_{\lambda \in \Lambda}(y_\lambda)_{\lambda \in \Lambda} = (x_\lambda y_\lambda)_{\lambda \in \Lambda}$$

によって和と乗法を定義すると, R は (単位的) 環になる. これを R_λ $(\lambda \in \Lambda)$ の**直積 (direct product)**, という. また, $\lambda \in \Lambda$ に対して, λ 番目の座標に関する射影

$$\pi_\lambda : R \to R_\lambda, \quad (x_\lambda)_{\lambda \in \Lambda} \mapsto x_\lambda$$

は全射環準同型である.

命題 3.2.3. 環の直積 $R = \prod_{\lambda \in \Lambda} R_\lambda$ と射影 π_λ の組は以下の普遍性をもっている：

> S が任意の環で $f_\lambda : S \to R_\lambda$ がすべての $\lambda \in \Lambda$ に対して環準同型であれば, ちょうど 1 つの環準同型 $f : S \to R$ が存在してすべての $\lambda \in \Lambda$ に対して $\pi_\lambda \circ f = f_\lambda$ である.

このような R は同型を除いて一意である.

証明.

[6] 答は 14.
[7] 答は 23.

注意 3.2.4. Λ が有限集合のときは, 直積と直和は同じものである.

定義 3.2.5. (直和)　R_λ $(\lambda \in \Lambda)$ が (単位的) 環の族のとき, $\prod_{\lambda\in\Lambda} R_\lambda$ の部分集合を

$$R = \sum_{\lambda\in\Lambda} R_\lambda = \{(x_\lambda)_{\lambda\in\Lambda} \mid x_\lambda \text{ は有限個を除いて } 0\ \}$$

と定義するとき, R は $\prod_{\lambda\in\Lambda} R_\lambda$ (単位的) 部分環になる. これを R_λ $(\lambda \in \Lambda)$ の**直和 (direct product)**, という. また, $\lambda \in \Lambda$ に対して, λ 番目の座標に関する埋込み

$$\iota_\lambda : R_\lambda \to R, \quad x_\lambda \mapsto (\dots, 0, 0, x_\lambda, 0, 0, \dots)$$

は単射環準同型である.

命題 3.2.6. 環の直和 $R = \sum_{\lambda\in\Lambda} R_\lambda$ と射影 π_λ の組は以下の普遍性をもっている：

> S が任意の環で $f_\lambda : R_\lambda \to S$ がすべての $\lambda \in \Lambda$ に対して環準同型であれば, ちょうど 1 つの環準同型 $f : R \to S$ が存在してすべての $\lambda \in \Lambda$ に対して $f \circ \iota_\lambda = f_\lambda$ である.

このような R は同型を除いて一意である.

証明.

3.2.3　剰余環

定義 3.2.7. (剰余環)　R が (単位的) 環, I が R の両側イデアルとする. このとき R を同値関係

$$x \equiv y \pmod{I} \quad \Leftrightarrow \quad y - x \in I$$

によって定義する. R を, この同値関係で類別した集合を R/I と書き, $x \in R$ の同値類を

$$[x] = \{y \in T \mid y \equiv x \pmod{I}\}$$

と書く. このとき, R/I に

$$[x] + [y] = [x + y], \qquad [x][y] = [xy]$$

によって, 和と積を定義すると, well-defined であり, この演算に関して R/I は (単位的) 環になる. これを R の I による**剰余環**という. また, $[x]$ を $x + I$ と書く.

証明.　1) 同値関係であること

2) well-defined であることは $x_1 \equiv x_2 \pmod{I}$ かつ $y_1 \equiv y_2 \pmod{I}$ ならば

$$x_1 + y_1 \equiv x_2 + y_2 \pmod{I} \qquad x_1 y_1 \equiv x_2 y_2 \pmod{I}$$

を示せばよい.

3) R/I が単位的環であることを示すには

(1) 加法 $+$ に関して R は加群である.
(2) 乗法に関して $R \setminus \{0\}$ は半群 (モノイド) である.
(3) 次の分配律が成り立つ.
(3l) $x(y + z) = xy + zz$　　**左分配律 (left distributive law)**
(3r) $(x + y)z = xz + yz$　　**右分配律 (right distributive law)**

を示さなければならない. (1) は容易である. (2) を示すには結合律

$$([x][y])[z] = [(xy)z] = [x(yz)] = [x]([y][z])$$

と $[1]$ が単位元であることを示す. (3) も直接示す.

例 3.2.8. 整数環 $R = \mathbb{Z}$ において, m の倍数全体の集合 $(m) = m\mathbb{Z} = \{mx | x \in \mathbb{Z}\}$ はイデアルである. $\mathbb{Z}/(m) = \mathbb{Z}/m\mathbb{Z}$ は単位的可換環で, $\sharp\mathbb{Z}/(m) = m$ である.

問題 3.2.9. $3 + 12\mathbb{Z}$ は $\mathbb{Z}/12\mathbb{Z}$ の零因子であることを示せ.

3.3 整数環の剰余環

3.3.1 倍数の判定法

以下のような倍数の判定法を憶えておこう.

- $256 \equiv 0 \pmod{2}$ を示せ.[8]
- $512 \equiv 0 \pmod{4}$ を示せ.[9]
- $17848978 \equiv 0 \pmod{7}$ を示せ.[10] $(17848978 \to (17 + 978) - 848 = 147$ は 7 の倍数)
- $1024 \equiv 0 \pmod{8}$ を示せ.[11]
- $1515809277 \equiv 0 \pmod{9}$ を示せ.[12] $(1 + 5 + 1 + 5 + 8 + 0 + 9 + 2 + 7 + 7 = 45$ は 9 の倍数)
- $175428 \equiv 0 \pmod{11}$ を示せ.[13] $(175428 \to (1 + 5 + 2) - (7 + 4 + 8) = -11$ は 11 の倍数)
- $2032264 \equiv 0 \pmod{13}$ を示せ.[14] $(2032264 \to (2 + 264) - 032 = 234$ は 13 の倍数)

3.3.2 オイラーのファイ関数

定義 3.3.1. (オイラーのトーシェント関数) 正の整数 n に対して, 1 から n までの自然数のうち n と互いに素なものの個数を $\varphi(n)$ と書き, **オイラーのトーシェント関数 (Euler's totient function)** という. 慣例的に $\varphi(n)$ と表記されるため、オイラーのファイ関数 (phi function) とも呼ばれる. また, 簡略的にオイラーの関数と呼ぶこともある. また $(\mathbb{Z}/n\mathbb{Z})^\times$ を **既約剰余類群** という. 一般に

$$\varphi(n) = \sharp(\mathbb{Z}/n\mathbb{Z})^\times$$

である.

表 3.3.1: $\varphi(n)$ の値

n	1	2	3	4	5	6	7	8	9	10	11	12
$\varphi(n)$	1	1	2	2	4	2	6	4	6	4	10	4

命題 3.3.2. 正整数 n に対して, $n = n_1 n_2 \cdots n_r$, かつ $i \neq j$ のとき n_i と n_j は互いに素であるとき,

$$\mathbb{Z}/(n) \simeq \mathbb{Z}/(n_1) \times \mathbb{Z}/(n_2) \times \cdots \mathbb{Z}/(n_r)$$

である. 特に,

$$(\mathbb{Z}/(n))^\times \simeq (\mathbb{Z}/(n_1))^\times \times (\mathbb{Z}/(n_2))^\times \times \cdots (\mathbb{Z}/(n_r))^\times$$

である.

[8] 2 の倍数の判定法 — 1 の位の数が, 0, 2, 4, 6, 8 であれば, その数字は 2 の倍数である.
[9] 4 の倍数の判定法 — 下二桁が 4 で割り切れれば, その数字は 4 の倍数である.
[10] 7 の倍数の判定法 — 1 の位から 3 桁ずつの群に分けて, (左から) 奇数番目の群の和と偶数番目の群の和との差が 7 の倍数であること.
[11] 8 の倍数の判定法 — 下三桁が 8 の倍数であれば、その数字は 8 の倍数である.
[12] 9 の倍数の判定法 — 各位の数字の和が 9 で割り切れれば, その数字は 9 の倍数である.
[13] 11 の倍数の判定法 — 各位を一つ飛ばしに足した ” 和 ” の ” 差 ” が 11 の倍数であれば, その数は 11 の倍数である.
[14] 13 の倍数の判定法 — 3 桁ごとに区切った数字を一つ飛ばしに足す. その和の差が 13 の倍数であれば, その数は 13 の倍数である.

証明. 中国の剰余定理を使う.

命題 3.3.3.

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

である.

証明. $1, \ldots, p^e$ の中で p^e と互いに素であるないものは

$$px \qquad (x = 1, 2, \ldots, p^{e-1} - 1)$$

だから $\varphi(p^e) = p^e - p^{e-1}$ である.

系 3.3.4. 正整数 n に対して, $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ (各 p_i は素数) を n の素因数分解とするとき,

$$\varphi(n) = \prod_{i=1}^{r} p_i^{e_i} \left(1 - \frac{1}{p_i}\right)$$

である.

命題 3.3.5. 正整数 n に対して,

$$a^{\varphi(m)} \equiv 1 \qquad (\mathrm{mod}\ m)$$

である (Euler の等式). 特に, $m = p$ が素数のとき

$$a^{p-1} \equiv 1 \qquad (\mathrm{mod}\ p)$$

である (Fermat の小定理).

証明. Lagrange の定理 (元の位数は群の位数の約数) を使う.

定義 3.3.6. 正整数 n とある a $(1 \leq a < n)$ に対して

$$a^{n-1} \equiv 1 \qquad (\mathrm{mod}\ n)$$

が成り立つかどうか判定するアルゴリズムを **Fermat テスト (Fermat test)** という.[15] $a = 1, 2, \ldots, n-1$ の中からランダムに値を選び出し, その a に対して $a^{n-1} \equiv 1 \pmod{n}$ **確率的素数判定法**という. 確率的素数判定法に合格した n を**偽素数 (pseudoprime)** という.[16]

定義 3.3.7. 合成数 n が任意の整数 a に対して, $(a, n) = 1$ を満たすならば

$$a^{n-1} \equiv 1 \qquad (\mathrm{mod}\ n)$$

となるとき, 合成数 n を **Carmichael 数** と呼ぶ。

問題 3.3.8. $(a, n) \neq 1$ ならば $a^{n-1} \not\equiv 1 \pmod{n}$ を示せ.

問題 3.3.9. (Korselt's criterion)　整数 n を合成数とする. このとき次の二つは同値であることを示せ.[17]

(1) n は Carmichael 数

(2) n は平方数で割り切ることができず (square-free), かつ $\forall p | n$ なる素数 p に対して $(p-1) | (n-1)$.

[15] Fermat テストの計算量は $O(\log n)$ であるため, このアルゴリズムは高速に動作する.

[16] 量子コンピュータ （quantum computer） は, 量子力学的な重ね合わせを用いて並列性を実現するとされるコンピュータ. 従来のコンピュータの論理ゲートに代えて,「量子ゲート」を用いて量子計算を行う原理のものについて研究がさかんであるが, 他の方式についても研究・開発は行われている. ショアのアルゴリズム (Shor's factorization) とは, 素因数分解問題を高速に解くことができるアルゴリズムのことである. 古典コンピュータでは非現実的な時間で解くアルゴリズムしか知られていない.

[17] http://www.epii.jp/articles/note/computer/primality/fermat_test#article_chapter_1

命題 3.3.10. 自然数 $n \in \mathbb{N}$ に対して

$$\sum_{d|n} \varphi(d) = n$$

が成り立つ.

証明. d が自然数で $d|n$ とする. 1 から n までの自然数のうち n との最大公約数が n/d であるものは, $n/d \cdot x$ $(x = 1, 2, \ldots, d)$ かつ x と d は互いに素の形をしているので, その個数は $\varphi(d)$ 個である. d を n の約数全てをわたる和をとると, 等式

$$\sum_{d|n} \varphi(d) = n$$

が成り立つ.

例 3.3.11. $n = 12$ のとき

$$\varphi(1) + \varphi(2) + \varphi(3) + \varphi(4) + \varphi(6) + \varphi(12) = 1 + 1 + 2 + 2 + 2 + 4 = 12$$

が成り立つ.

定理 3.3.12. 有限群 G において, 任意の正の整数 d に対して $x^d = 1$ となる元 $x \in G$ が高々 d 個しか含まれないとき G は巡回群である.

証明. $|D| = n$ とする. 自然数 d で $d|n$ となるものに対して, 位数が d の元の個数を $\psi(d)$ とする. もし, 位数が d の元 a が存在したら, $1, a, a^2, \ldots, a^{d-1}$ は, すべて $x^d = 1$ をみたすから, 位数 d の元は a^k, $(k, d) = 1$, という形の元以外には存在しない. この形の元は, 全部で $\varphi(d)$ 個なので, もし, 位数 d の元が存在すれば $\psi(d) = \varphi(d)$, 存在しなければ $\psi(d) = 0$ である. ゆえに $\psi(d) \leq \varphi(d)$ としてよい. Langrange の定理より, 元の位数は n の約数だから

$$n = \sum_{d|n} \psi(d) \leq \sum_{d|n} \varphi(d) = n$$

となり, 常に $\psi(d) = \varphi(d)$ が成り立つ. 特に, $\psi(n) = \varphi(n) > 0$ なので位数 n の元が存在する.

定義 3.3.13. (リーマンゼータ関数関数) **ゼータ関数** $\zeta(s)$ は, 複素数 $s = x + iy$ $(\mathrm{Re}\, s = x > 1)$ のとき,

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \cdots$$

によって定義される。$s = x + iy$ $(x > 0)$ とすると, 解析学で習うように $n^s = n^{x+iy} = n^x \cdot n^{iy} = n^x \cdot e^{iy \log n} = n^x(\cos(y \log n) + i \sin(y \log n))$ なので $|1/n^s| = 1/n^x$ である.

$$\sum_{n=1}^{\infty} \left| \frac{1}{n^s} \right| = \sum_{n=1}^{\infty} \frac{1}{n^x}$$

なので, $x > 1$ のとき, この級数は絶対収束する. $x \leq 1$ に対するゼータ関数は解析接続で定義される.[18]

命題 3.3.14.

$$\zeta(s) = \prod_{p\,:\,\text{素数}} \frac{1}{1 - \frac{1}{p^s}} = \frac{1}{\left(1 - \frac{1}{2^s}\right)\left(1 - \frac{1}{3^s}\right)\left(1 - \frac{1}{5^s}\right)\cdots}$$

が成り立つ.

証明. 右辺を展開し [19]

$$\left(1 + \frac{1}{2} + \frac{1}{2^2} + \cdots\right)\left(1 + \frac{1}{3} + \frac{1}{3^2} + \cdots\right)\left(1 + \frac{1}{5} + \frac{1}{5^2} + \cdots\right)$$

を掛け合わせて素因数分解を使う.

[18] リーマン予想 (Riemann hypothesis) は, ドイツの数学者ベルンハルト・リーマンによって提唱された, ゼータ関数の零点の分布に関する予想である. それは「$\zeta(s)$ の自明でない零点 s は、全て実部が 1/2 の直線上に存在する.」というものである。数学上の未解決問題の一つであり, クレイ数学研究所はミレニアム懸賞問題の一つとしてリーマン予想の解決者に対して 100 万ドルの懸賞金を支払うことを約束している.

[19] 幾何級数 $\frac{1}{1-x} = 1 + x + x^2 + \cdots$ を使う.

3.3.3 1 の冪根

定義 3.3.15. (1 の原始 n 乗根) $n \in \mathbb{N}$ に対して n 乗して初めて 1 になる複素数を **1 の原始 n 乗根 (nth primitiveroot of unity)** という.

$$\zeta_n = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$$

とおくと, ζ_n^k $(1 \le k \le n,\ k$ と n が互いに素$)$ はすべて原始 n 乗根なので, 全部で $\varphi(n)$ 個ある. ζ が 1 の原始 n 乗根ならば $\zeta^n = 1$ である.[20]

例 3.3.16. $n = 3$ のとき

$$\omega = \frac{-1+i\sqrt{3}}{2}, \qquad \omega^2 = \frac{-1-i\sqrt{3}}{2}$$

が原始立方根であり, $n = 4$ のとき $\pm i$ が原始 4 乗根である.

定義 3.3.17. (円分多項式) $n \in \mathbb{N}$ に対して

$$\Phi_n(X) = \prod_{k:(k,n)=1} \left(X - \zeta_n^k\right)$$

を, **円分多項式 (cyclotomic polynomial)** という.

$$\prod_{d|n} \Phi_n(X) = X^n - 1$$

が成り立つ. また $\deg \Phi_n(X) = \varphi(n)$ である.

例 3.3.18. 小さい n に対して

$$\begin{aligned}
\Phi_1(X) &= X - 1\\
\Phi_2(X) &= X + 1\\
\Phi_3(X) &= X^2 + X + 1\\
\Phi_4(X) &= X^2 + 1\\
\Phi_5(X) &= X^4 + X^3 + X^2 + X + 1\\
\Phi_6(X) &= X^2 - X + 1
\end{aligned}$$

である.

3.3.4 Möbius の逆転公式

定義 3.3.19. (Möbius 関数) $n \in \mathbb{N}$ に対して $\mu(n)$ を次のように定義する. $\mu(1) = 1$ であり, $n > 1$ のとき, $n = \prod_{i=1}^r p_i^{e_i}$ を n の素因数分解とすれば

$$\mu(n) = \begin{cases} (-1)^r & e_1 = \cdots = e_r = 1,\\ 0 & \text{otherwise.} \end{cases}$$

$\mu(n)$ を n の **Möbius 関数**という.

表 3.3.2: $\mu(n)$ の値

n	1	2	3	4	5	6	7	8	9	10	11	12
$\mu(n)$	1	−1	−1	0	−1	1	−1	0	0	1	−1	0

[20] 逆は正しくない.

問題 3.3.20. $n \in \mathbb{Z}$, $n > 1$ ならば

$$\sum_{d|n} \mu(d) = 0$$

を示せ.

証明. n の素因数分解を $n = p_1^{e_1} \cdots p_r^{e_r}$ $(r \geq 1)$ とすると

$$\sum_{d|n} \mu(d) = \sum_{0 \leq x_1 \leq e_1, \ldots, 0 \leq x_r \leq e_r} \mu\left(p_1^{x_1} \cdots p_r^{x_r}\right) = \sum_{0 \leq x_1 \leq 1, \ldots, 0 \leq x_r \leq 1} (-1)^{x_1 + \cdots + x_r} = \sum_{x=0}^{r} (-1)^r \binom{r}{x} = (1-1)^r = 0$$

ここで, 最後の和は $x_1 + \cdots + x_r = x$ とおいた. □

例 3.3.21. $n = 12$ のとき

$$\mu(1) + \mu(2) + \mu(3) + \mu(4) + \mu(6) + \mu(12) = 1 - 1 - 1 + 0 + 1 + 0 = 0$$

が成り立つ.

定理 3.3.22. (逆転公式 1)　f を $\mathbb{N}$ 上の任意の関数とし, 自然数 $n \in \mathbb{N}$ に対して

$$\sum_{d|n} f(d) = g(n)$$

とすれば

$$\sum_{d|n} \mu\left(\frac{n}{d}\right) g(d) = f(n)$$

が成り立つ.

証明.

$$\sum_{d|n} \mu\left(\frac{n}{d}\right) g(d) = \sum_{d|n} \mu\left(\frac{n}{d}\right) \sum_{d'|d} f(d') = \sum_{d'|d|n} \mu\left(\frac{n}{d}\right) f(d') = \sum_{d'|n} f(d') \sum_{t|\frac{n}{d'}} \mu(t)$$

ここで,

$$\sum_{t|a} \mu(t) = \begin{cases} 1 & a = 1, \\ 0 & a > 1. \end{cases}$$

を使えば, 証明が終わる.

系 3.3.23. 自然数 $n \in \mathbb{N}$ に対して

$$\sum_{d|n} \mu\left(\frac{n}{d}\right) d = \varphi(n)$$

が成り立つ.

例 3.3.24. $n = 12$ のとき

$$\mu(12) \cdot 1 + \mu(6) \cdot 2 + \mu(4) \cdot 3 + \mu(3) \cdot 4 + \mu(2) \cdot 6 + \mu(1) \cdot 12 = 0 \cdot 1 + 1 \cdot 2 + 0 \cdot 3 - 1 \cdot 4 - 1 \cdot 6 + 1 \cdot 12 = 4$$

が成り立つ.

系 3.3.25. (逆転公式 2)　f を $\mathbb{N}$ 上の任意の関数とし, 自然数 $n \in \mathbb{N}$ に対して

$$\prod_{d|n} f(d) = g(n)$$

とすれば

$$\prod_{d|n} g(d)^{\mu\left(\frac{n}{d}\right)} = f(n)$$

が成り立つ.

証明. 上の証明で和を積に変えると並行的に証明できる.

問題 3.3.26. 系 3.3.25 の証明を書け.

系 3.3.27.

$$\Phi_n(X) = \prod_{d|n} (X^d - 1)^{\mu\left(\frac{n}{d}\right)}$$

が成り立つ.

例 3.3.28. $n = 12$ のとき, 12 の約数は $\{1, 2, 3, 4, 6, 12\}$ で, $\mu(1) = \mu(6) = 1$, $\mu(2) = \mu(3) = -1$, $mu(4) = \mu(12) = 0$ なので

$$\Phi_{12}(X) = (X-1)^{\mu(12)}(X^2-1)^{\mu(6)}(X^3-1)^{\mu(4)}(X^4-1)^{\mu(3)}(X^6-1)^{\mu(2)}(X^{12}-1)^{\mu(1)} = \frac{(X^2-1)(X^{12}-1)}{(X^4-1)(X^6-1)} = X^4 - X^2 + 1$$

となる.

3.3.5 Euclid の互除法

命題 3.3.29. (Euclid の互除法) $a, b \in \mathbb{Z}$ が与えられたときに, $ax + by = d$ となる $x, y \in \mathbb{Z}$ を見つける方法 $(d = (a, b))$

証明. $0 < a < b$ としてよい. $b = r_0$, $a = r_1$ として, b を a で割った商を q_1, 余りを r_2 とすると

$$b = aq_1 + r_2$$

である. もし $r_2 \neq 0$ のときは, これを繰り返し,

$$r_{i-1} = r_i q_i + r_{i+1} \qquad (i = 1, 2, \ldots, n)$$

$r_n \neq 0$, $r_{n+1} = 0$ とすると $d = r_n$ で

$$\begin{aligned}
r_n &= r_{n-2} - q_{n-1} r_{n-1} \\
&= r_{n-2} - q_{n-1}(r_{n-3} - q_{n-2} r_{n-2}) \\
&= (1 + q_{n-1}q_{n-2}) r_{n-2} - q_{n-1} r_{n-3} \\
&= (1 + q_{n-1}q_{n-2})(r_{n-4} - q_{n-3} r_{n-3}) - q_{n-1} r_{n-3} \\
&= (1 + q_{n-1}q_{n-2}) r_{n-4} - (q_{n-1} + q_{n-1}q_{n-2}q_{n-3}) r_{n-3} \\
&= \cdots
\end{aligned}$$

これを繰り返していって $r_n = ax + by$ となる x, y を見つける.

問題 3.3.30. $9x + 16y = 1$ となる $x, y \in \mathbb{Z}$ を見つけよ.

解答. Euclid の互除法を使って, 割算を次々とやると

$$\begin{aligned}
16 \div 9 &= 1 \cdots 7 \\
9 \div 7 &= 1 \cdots 2 \\
7 \div 2 &= 3 \cdots 1 \\
2 \div 1 &= 2 \cdots 0
\end{aligned}$$

だから $(9, 16) = 1$ で

$$\begin{aligned}
16 &= 9 \cdot 1 + 7 \\
9 &= 7 \cdot 1 + 2 \\
7 &= 2 \cdot 3 + 1
\end{aligned}$$

なので

$$1 = 7 - (9 - 7 \cdot 1) \cdot 3 = 7 \cdot (1 + 1 \cdot 3) - 9 \cdot 3 = (16 - 9 \cdot 1)(1 + 1 \cdot 3) - 9 \cdot 3 = 16 \cdot (1 + 1 \cdot 3) - 9 \cdot (3 + 1 \cdot 1 + 1 \cdot 1 \cdot 3)$$

より $1 = 16 \cdot 4 - 9 \cdot 7$ である. □

問題 3.3.31.

$$x \equiv 1 \pmod{9}, \qquad x \equiv 1 \pmod{16}$$

となる $x, y \in \mathbb{Z}$ を見つけよ.

解答. Euclid の互除法を使って, 割算を次々とやると

$$16 \div 9 = 1 \cdots 7$$
$$9 \div 7 = 1 \cdots 2$$
$$7 \div 2 = 3 \cdots 1$$
$$2 \div 1 = 2 \cdots 0$$

だから $(9, 16) = 1$ で

$$16 = 9 \cdot 1 + 7$$
$$9 = 7 \cdot 1 + 2$$
$$7 = 2 \cdot 3 + 1$$

なので

$$1 = 7 - (9 - 7 \cdot 1) \cdot 3 = 7 \cdot (1 + 1 \cdot 3) - 9 \cdot 3 = (16 - 9 \cdot 1)(1 + 1 \cdot 3) - 9 \cdot 3 = 16 \cdot (1 + 1 \cdot 3) - 9 \cdot (3 + 1 \cdot 1 + 1 \cdot 1 \cdot 3)$$

より $1 = 16 \cdot 4 - 9 \cdot 7$ である. □

3.3.6 既約剰余類群

定義 3.3.32. 整数環の剰余群 $\mathbb{Z}/n\mathbb{Z}$ の単元群 $(\mathbb{Z}/n\mathbb{Z})^\times$ を**既約剰余類群**という.

定理 3.3.33. (整数環の剰余環の単元群の構造)　一般に, 既約剰余類群 $(\mathbb{Z}/p^e\mathbb{Z})^\times$ の構造について

i) p が奇素数ならば, 乗法群 $(\mathbb{Z}/p^e\mathbb{Z})^\times$ は, 位数 $p^e(p-1)$ の巡回群である.[21]
ii) $p = 2$ ならば, $e = 1, 2$ のとき巡回群であり, $e \geq 3$ のとき, 乗法群 $(\mathbb{Z}/2^e\mathbb{Z})^\times$ は $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{e-2}\mathbb{Z}$ と同型である.[22]

ということが知られている.[23]

問題 3.3.34. $123456789^{123456789}$ を 144 で割った余りを求めよ.

解答. 割算を行うと $1234567 \equiv 55 \pmod{144}$ であるので

$$x \equiv 55^{123456789} \pmod{144}$$

となる x を求めればよい. $144 = 2^4 \cdot 3^2$ なので

$$\mathbb{Z}/144\mathbb{Z} \simeq \mathbb{Z}/2^4\mathbb{Z} \times \mathbb{Z}/3^2\mathbb{Z}$$

である.

$$55 \equiv 7 \pmod{2^4}, \qquad 55 \equiv 1 \pmod{3^2}$$

より

$$55 \equiv (7, 1) \in \left(\mathbb{Z}/2^4\mathbb{Z}\right)^\times \times \left(\mathbb{Z}/3^2\mathbb{Z}\right)^\times \simeq (\mathbb{Z}/144\mathbb{Z})^\times$$

であり $7^2 = 49 \equiv 1 \pmod{2^4}$ なので

$$55^{123456789} \equiv (7^{123456789}, 1) \equiv (7, 1) \equiv 55$$

したがって, 答は 55 である. □

[21] 例えば $(\mathbb{Z}/5\mathbb{Z})^\times$ は位数 $5 - 1 = 4$ の巡回群, $\left(\mathbb{Z}/5^2\mathbb{Z}\right)^\times$ は位数 $5 \times (5 - 1) = 20$ の巡回群, $\left(\mathbb{Z}/5^3\mathbb{Z}\right)^\times$ は位数 $5^2 \times (5 - 1) = 100$ の巡回群に同型である.

[22] 例えば $\left(\mathbb{Z}/2^2\mathbb{Z}\right)^\times$ は位数 2 の巡回群, $\left(\mathbb{Z}/2^3\mathbb{Z}\right)^\times$ はクラインの四元群 $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $\left(\mathbb{Z}/2^4\mathbb{Z}\right)^\times$ は $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ に同型である.

[23] 群論 (岩波基礎数学選書) 近藤 武 (著) または http://pisan-dub.jp/doc/2011/20110114001/5_6.html

問題 3.3.35. 83^{1234} の一の位の数は $\boxed{34}$ である.[24]

解答. $83 \equiv 3 \pmod{10}$ より $3^2 \equiv 9 \equiv -1 \pmod{10}$, $3^4 \equiv (-1)^2 \equiv 1 \pmod{10}$ である. 指数法則を使って $3^{1234} \equiv 3^{4\times 308+2} \equiv \left(3^4\right)^{308} \times 3^2 \equiv 1^{308} \times 3^2 \equiv 3^2$ と変形せよ. さらに専門的な知識 (後述の整数環の構造) を使って解くならば 3 と 10 は互いに素なので 3 は $\mathbb{Z}/10\mathbb{Z}$ の単元である. (単元とは, 可換環で乗法の逆元をもつ元のことである.) すなわち $3 \in (\mathbb{Z}/10\mathbb{Z})^\times$ で, $(\mathbb{Z}/10\mathbb{Z})^\times = \{1,3,7,9\}$ は位数 4 の巡回群で 3 は生成元である. $1234 = 4 \times 308 + 2$ なので $3^{1234} \equiv 3^2 \equiv 9 \pmod{10}$ となる.□

問題 3.3.36. 2000^{2000} を 12 で割った余りは $\boxed{34}$ である.[25]

解答. $2000 \equiv 8 \pmod{12}$ である. $8^2 \equiv 4 \pmod{12}$, $8^3 \equiv 8 \pmod{12}$ と繰り返していくので, 非負整数 n に対して $8^{2n} \equiv 4 \pmod{12}$, $8^{2n+1} \equiv 8 \pmod{12}$ である. さらに専門的な見方をすれば, 8 と 12 の最大公約数は $(8,12) = 4$ なので, 8 は $\mathbb{Z}/12\mathbb{Z}$ の単元ではない, すなわち, 8^n は 12 を法として常に 4 の倍数である. $12 = 2^2 \cdot 3$ なので, $f : \mathbb{Z}/3\mathbb{Z} \to \mathbb{Z}/12\mathbb{Z}$, $x \mapsto 4x$ は、このような整数の全単射を与える. ここで $f(2) = 8$ であり, $(\mathbb{Z}/3\mathbb{Z})^\times$ は位数 2 の巡回群であるから, $8^{2000} \equiv f\left(2^{2000}\right) \equiv f(1) \equiv 4 \pmod{12}$ となる.□

問題 3.3.37. 2017^{2017} の下 2 桁を求めよ.

解法のテクニック 以上の整数環に関する基本事項をもとに「a^m を n で割った余りを求めよ」という問題の一般的な解法を述べると以下のようになる.[26] まず a が $\mathbb{Z}/n\mathbb{Z}$ の単元であるかどうかを調べる. (1) a と n が互いに素のときは a は $\mathbb{Z}/n\mathbb{Z}$ の単元であり, (2) 素でないときは単元でない.

(1) a が $\mathbb{Z}/n\mathbb{Z}$ の単元であるとき, まず a が大きいならば a を n で割った余りを b として $a \equiv b \pmod{n}$ を使う. 次に $b^k \equiv 1 \pmod{n}$ となる最小の自然数 k を見つけよ. 見つかったら, m を k で割った商を q, 余りを r とする. 指数法則を使って

$$a^m \equiv b^{kq+r} \equiv \left(b^k\right)^q \times b^r \equiv b^r \pmod{n}$$

によって余りを計算する. 例えば 2015^{2015} を 49 で割った余りを求めてみよう.[27]

(2) a が $\mathbb{Z}/n\mathbb{Z}$ の単元でないときは, 基本的には (1) と同じ方針であるが, もう少し注意深く整数環の構造を考察する必要がある. まず a と n の最大公約数 (a,n) を l とおく. また, $n = p_1^{e_1} \cdots p_r^{e_r}$, $l = p_1^{f_1} \cdots p_r^{f_r}$ とおくことができる. ここで $0 \le f_i \le e_i$ $(1 \le i \le r)$ とする. $S = \{i; f_i = 0\}$ とおくと,

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{e_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_r^{e_e}\mathbb{Z}$$

より, m が十分大きいならば a^m は

$$\prod_{i\in S} \mathbb{Z}/p_i^{e_i}\mathbb{Z}$$

の中で考えればよい. したがって, a^m の $\mathbb{Z}/n\mathbb{Z}$ の周期は m が十分大きければ高々

$$\prod_{i\in S} \varphi\left(p_i^{e_i}\right) = \prod_{i\in S} p_i^{e_i-1}(p_i - 1)$$

のはずである. 例えば 2015^{2015} の下 2 桁を求めてみよう.[28]

---

[24](平成 27 年度沖縄県教員採用試験, 三-問 13)

[25](平成 26 年度沖縄県教員採用試験, 三-問 13)

[26]このような群論の知識を使った解答は, 記述式の試験では採点者を唸らせるほどのペダンティックで完璧な解答としてお勧めするが, 沖縄県の教員採用試験のようなマークの問題では, とりあえず法として合同と指数法則を使って法則を見つけるのが推奨される. 間違っても 2000^{2000} を直接計算したりしないように心してかかろう. mod が大事である.

[27]まず $2015 \equiv 6 \pmod{49}$ である. $49 = 7^2$ なので $(\mathbb{Z}/49\mathbb{Z})^\times$ の位数は 42 である. よって 6 の $(\mathbb{Z}/49\mathbb{Z})^\times$ における位数は 42 の約数であるが $6^7 \equiv -1$, $6^{14} \equiv 1$ より, 6 の位数は 14 であることがわかる. 2015 を 14 で割った商は 143, 余りは 13 なので, $2015^{2015} \equiv 6^{13} \pmod{49}$ である.

[28]まず $(2015, 100) = 5$ なので, 2015 と 100 は互いに素でない. $2015 \equiv 15 \pmod{100}$ $100 = 2^2 \cdot 5^2$ なので $\varphi(2^2) = 2$ が高々周期になる. 実際 $15^2 \equiv 25 \pmod{100}$, $15^3 \equiv 75 \pmod{100}$, $15^4 \equiv 75 \pmod{100}$ となり, 以下 25 と 75 を繰り返す.

第4章　部分環

4.1　多項式環

この章では R を単位的可換環とする.

定義 4.1.1. R を単位的可換環とするとき, R の元を係数とする n 変数 $X_1, \dots, X_n$ の多項式

$$f(X) = f(X_1, \dots, X_n) = \sum_{i_1, \dots, i_n \geq 0} a_{i_1, \dots, i_n} X^{i_1} \cdots X^{i_n}$$

全体のなす環を $R[X_1, \dots, X_n]$ と書き, R 上の n **変数多項式環**という. 特に $aX^{i_1} \cdots X^{i_n}$ の形の多項式を**単項式**といい, $i_1 + \cdots + i_n$ を, この単項式の**次数**という. 多項式 f に現れる各単項式の中で次数が最大のものを, $f(X)$ の**次数**といい, $\deg f$ と書く. $\deg 0 = -\infty$ とする.

例 4.1.2. $f(X, Y) = 2\,X^3 + X^2Y + X^2 + 2\,Y \in \mathbb{Z}[X, Y]$ は 3 次多項式, $g(X) = X^2 + \frac{1}{2}\,X + \frac{2}{3} \in \mathbb{Q}[X]$ は 2 次多項式.

この節では, 実際は R を整域と仮定することが多い.

命題 4.1.3. R が整域ならば $f(X), g(X) \in R[X]$ に対して $\deg fg = \deg f + \deg g$ である.

4.2　生成される部分環

定義 4.2.1. R を単位的可換環とする. S が R の部分集合であるとき, S を含む R の部分環全体の交わりは R の部分環である. これを S が生成する R の部分環といい, $[S]$ と書く.

定義 4.2.2. R を単位的可換環とする. R_0 が R の部分環で S が R の部分集合であるとき, $[R_0 \cup S]$ を $R_0[S]$ と書く.

例 4.2.3. $R_0 = \mathbb{Z}$ は $R = \mathbb{C}$ の部分環である. $S = \{i\}$ のとき, $\mathbb{Z}[i]$ を**ガウス整数環**という.

定理 4.2.4. R を単位的可換環とする. R_0 が R の部分環で S が R の部分集合であるとき,

$$R_0[S] = \{f(s_1, \dots, s_n) \,|\, n \text{ は自然数で } f \in R'[X_1, \dots, X_n],\ s_1, \dots, s_n \in S\}$$

である.

証明. 証明の方針は以下のようである. 右辺の集合を

$$R_1 = \{f(s_1, \dots, s_n) \,|\, n \text{ は自然数で } f \in R'[X_1, \dots, X_n],\ s_1, \dots, s_n \in S\}$$

とおく. 1) R' が R の部分環で $S \subseteq R'$ ならば $R_1 \subseteq R'$ であることを示す. 2) R_1 が R の部分環であることを示す.

例 4.2.5. $R' = \mathbb{Z}$ は $R = \mathbb{C}$ の部分環である. $S = \{i\}$ のとき, $i^2 = -1$ なので

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

である.

例 4.2.6. $\mathbb{Z}[i]$ は整域であることを示せ.[1]

[1] 整域の部分環は整域であることを使え.

命題 4.2.7. $x = a + bi \in \mathbb{Z}[i]$ に対して $\overline{x} = a - bi$ をその共役複素数とする. $N(x) = x\overline{x} = a^2 + b^2$ とおく. $x, y \in \mathbb{Z}[i]$, $x \neq 0$ ならば $q, r \in \mathbb{Z}[i]$ が存在して $y = xq + r$ かつ $N(r) \leq \frac{1}{2} N(x)$ とできる.

証明. $x = a + ib$, $y = c + id$ とすると

$$\frac{y}{x} = \frac{c + id}{a + ib} = \frac{(a - ib)(c + id)}{a^2 + b^2} = \frac{ac + bd}{a^2 + b^2} + i\frac{ad - bc}{a^2 + b^2}$$

である. $u, v \in \mathbb{Z}$ で

$$\left|\frac{ac + bd}{a^2 + b^2} - u\right| \leq \frac{1}{2}, \qquad \left|\frac{ad - bc}{a^2 + b^2} - v\right| \leq \frac{1}{2}$$

となるものが取れる. $q = u + iv \in \mathbb{Z}[i]$ とおき, $r = y - xq$ とすると

$$N\left(\frac{r}{x}\right) = N\left(\frac{y}{x} - q\right) = \left(\frac{ac + bd}{a^2 + b^2} - u\right)^2 + \left(\frac{ad - bc}{a^2 + b^2} - v\right)^2 \leq \frac{1}{4} + \frac{1}{4} = \frac{1}{2}$$

である. また

$$N\left(\frac{r}{x}\right) = \frac{r}{x} \cdot \frac{\overline{r}}{\overline{x}} = \frac{N(r)}{N(x)} \leq \frac{1}{2}$$

なので $N(r) \leq \frac{1}{2} N(x)$ である.

例 4.2.8. $R' = \mathbb{Z}$ は $R = \mathbb{C}$ の部分環である. $S = \{\omega\}$ のとき, $\omega^2 + \omega + 1 = 0$ なので

$$\mathbb{Z}[\omega] = \{a + \omega b \,|\, a, b \in \mathbb{Z}\}$$

である.

第5章　可換環論初歩

5.1　準備

定義 5.1.1. $(P, \leq)$ が**半順序集合 (partially ordered set, poset)** とは, $x, y \in P$ に二項関係 $x \leq y$ が定義されて

(i) $x \leq x$ (反射律 reflexivity)
(ii) $x \leq y$ かつ $y \leq x \Rightarrow x = y$ (反対称律 anti-symmetry)
(iii) $x \leq y$ かつ $y \leq z \Rightarrow x \leq z$ (推移律 transtivity)

が成り立つこと.

定義 5.1.2. $\emptyset \neq S \subseteq P$ のとき

- a が S の**上界 (upper bound)**（resp. **下界 (lower bound)**）: $^\forall x \in S : x \leq a$ (resp. $x \geq a$)
- a が S の**最大元 (maximum element)**（resp. **最小元 (minimum element)**）: $a \in S$ かつ a は S の上界 (resp. 下界)
- a が S の**極大元 (maximal element)**（resp. **極小元 (minimul element)**）: $a \in S$ かつ $x \gneqq a$ (resp. $x \lneqq a$) を満たす $x \in P$ が存在しない

$S = P$ に最大元 (resp. 最小元) が存在するとき, それを $\widehat{1}_P$ (resp. $\widehat{0}_P$), または, 単に $\widehat{1}$ (resp. $\widehat{0}$) と書く.

定義 5.1.3. (帰納的集合) 半順序集合 P の任意の全順序部分集合が P に上界を持つとき, P は**帰納的集合**という.

定理 5.1.4. (**Zorn の補題**)　帰納的集合には極大元が存在する.

5.2　可換環

ここでは R は常に単位的可換環とする.

5.2.1　素イデアル

命題 5.2.1. R が単位的可換環で, $\mathfrak{p} \neq R$ がイデアルのとき, 次は同値である.

(1) $R/\mathfrak{p}$ は整域
(2) $a, b \in \mathfrak{p}$ のとき, $ab \in \mathfrak{p} \Rightarrow a \in \mathfrak{p}$ または $b \in \mathfrak{p}$
(3) R のイデアル $\mathfrak{a}, \mathfrak{b}$ に対して, $\mathfrak{ab} \subseteq \mathfrak{p} \Rightarrow \mathfrak{a} \subseteq \mathfrak{p}$ または $\mathfrak{b} \subseteq \mathfrak{p}$
(4) R のイデアル $\mathfrak{a}, \mathfrak{b}$ に対して, $\mathfrak{a} \not\subseteq \mathfrak{p}$ かつ $\mathfrak{b} \not\subseteq \mathfrak{p} \Rightarrow \mathfrak{ab} \not\subseteq \mathfrak{p}$

このいずれかが成り立つとき $\mathfrak{p}$ は**素イデアル (prime ideal)** という.[1]

証明. (1) $\Rightarrow$ (2)
$ab \in \mathfrak{p}$ ならば, $R/\mathfrak{p}$ において $(a + \mathfrak{p})(b + \mathfrak{p}) = \mathfrak{p}$ なので, $R/\mathfrak{p}$ が整域であることから $a + \mathfrak{p} = \mathfrak{p}$ または $b + \mathfrak{p} = \mathfrak{p}$ である. すなわち $a \in \mathfrak{p}$ または $b \in \mathfrak{p}$ である.
(2) $\Rightarrow$ (4)
R のイデアル $\mathfrak{a}, \mathfrak{b}$ に対して, $\mathfrak{a} \not\subseteq \mathfrak{p}$ かつ $\mathfrak{b} \not\subseteq \mathfrak{p}$ であるとすると $^\exists a \in \mathfrak{a} \setminus \mathfrak{p}$, $^\exists b \in \mathfrak{b} \setminus \mathfrak{p}$ が存在する. (2) より $ab \notin \mathfrak{p}$ だから $\mathfrak{ab} \not\subseteq \mathfrak{p}$ である.

[1] 定義から R は素イデアルではない.

(4) ⇒ (3)
対偶

(3) ⇒ (1)
$R/\mathfrak{p}$ の定義より明らか. □

5.2.2 極大イデアル

命題 5.2.2. R が単位元 1 をもつ可換環で, $\mathfrak{m} \neq R$ がイデアルのとき, 次は同値である.

(1) $\mathfrak{a}$ がイデアルで, $\mathfrak{m} \subseteq \mathfrak{a} \subseteq R \Rightarrow \mathfrak{a} = \mathfrak{m}$ または $\mathfrak{a} = R$. (すなわち $\mathfrak{m}$ は包含関係に関して極大)
(2) $R/\mathfrak{m}$ は体

このいずれかが成り立つとき $\mathfrak{m}$ は**極大イデアル (maximal ideal)** という

証明. (1) ⇒ (2)
$a + \mathfrak{m} \neq \mathfrak{m}$ ならば $a \notin \mathfrak{m}$ なので $\mathfrak{m} \subsetneq (a) + \mathfrak{m}$ となり, $\mathfrak{m}$ が極大イデアルであることより $(a) + \mathfrak{m} = R$ である. すなわち $r \in R$, $m \in \mathfrak{m}$ が存在して $ra + m = 1$ となる. ゆえに $r + \mathfrak{m}$ は $a + \mathfrak{m}$ の逆元である.

(2) ⇒ (1)
$\mathfrak{m} \subsetneq \mathfrak{a} \subseteq R$ とすると $^{\exists}x \in \mathfrak{a} \setminus \mathfrak{m}$ が存在する. $R/\mathfrak{m}$ において $x + \mathfrak{m} \neq \mathfrak{m}$ なので $^{\exists}y \in R$ が存在して $(x + \mathfrak{m})(y + \mathfrak{m}) = 1 + \mathfrak{m}$ となる. よって $1 \in \mathfrak{a}$ となり $\mathfrak{a} = R$ が示される. □

系 5.2.3. 極大イデアルは素イデアルである.

定理 5.2.4. R が単位元 1 をもつ可換環で, $S \neq \emptyset$ $(0 \notin S)$ が積に関して閉じている R の部分集合 (i.e. $a, b \in S \Rightarrow ab \in S$), $\mathfrak{a}$ が R のイデアル s.t. $\mathfrak{a} \cap S = \emptyset$ とする. このとき, R のイデアルの族

$$\mathscr{I} = \{\mathfrak{b} | \mathfrak{b} \supseteq \mathfrak{a} \text{ かつ } \mathfrak{b} \cap S = \emptyset\}$$

には包含関係で極大元が存在する. $\mathfrak{p}$ を極大元の 1 つを $\mathfrak{p}$ とすれば, $\mathfrak{p}$ は素イデアルである.

証明. $\mathscr{I}$ が帰納的集合であることを示す. $\mathfrak{b}_\iota$ $(\iota \in I)$ が $\mathscr{I}$ の全順序集合であるとき, $\mathfrak{c} = \bigcup_{\iota \in I} \mathfrak{b}_\iota$ とおくと, $\mathfrak{c}$ はイデアルであり, $\mathfrak{c} \in \mathscr{I}$ である.[2] よって, 帰納的集合であることが示された. ゆえに, Zorn の補題より, 極大元 $\mathfrak{p} \in \mathscr{I}$ が存在する. $\mathfrak{p}$ が素イデアルであることを示す. $b \notin \mathfrak{p}$, $c \notin \mathfrak{p}$, $bc \in \mathfrak{p}$ とすると $\mathfrak{p} \subsetneq (b) + \mathfrak{p}$, $\mathfrak{p} \subsetneq (c) + \mathfrak{p}$ だから $((b) + \mathfrak{p}) \cap S \neq \emptyset$, $((c) + \mathfrak{p}) \cap S \neq \emptyset$ であり, $s_1 = r_1 b + p_1$, $s_2 = r_2 c + p_2$ となる $s_1, s_2 \in S$, $r_1, r_2 \in R$, $p_1, p_2 \in \mathfrak{p}$ が存在する. このとき, $S \ni s_1 s_2 = r_1 r_2 bc + r_1 b p_2 + r_2 c p_1 + p_1 p_2 \in \mathfrak{p}$ となり $\mathfrak{p} \cap S = \emptyset$ に矛盾する. □

系 5.2.5. R が単位元 1 をもつ可換環で, $\mathfrak{a} \neq R$ がイデアルのとき, $\mathfrak{a}$ を含む R の極大イデアル $\mathfrak{m}$ が存在する.

証明. 上の定理で $S = \{1\}$ とせよ.

系 5.2.6. R が単位元 1 をもつ可換環ならば R の極大イデアル $\mathfrak{m}$ が存在する.

証明. 上の系で $\mathfrak{a} = \mathbf{0}$ とせよ.

定理 5.2.7. 単位元 1 をもつ可換環 $R \neq \mathbf{0}$ について, 次は同値である.

(1) R は体
(2) R のイデアルは $\mathbf{0}$, R 以外に存在しない.

系 5.2.8. 有限個の元からなる整域 R は体である.

証明. $\mathfrak{a} \neq \mathbf{0}$ を R のイデアルとせよ. $0 \neq {}^{\exists}a \in \mathfrak{a}$ を 1 つ取る. $f_a : R \to \mathfrak{a}, x \mapsto xa$ は R から $\mathfrak{a}$ への単射, よって全射でなければならない. すなわち $\mathfrak{a} = R$ である. R のイデアルは $\mathbf{0}$ と R のみである.

[2] $\mathfrak{a} \subseteq \mathfrak{c}$ は明らか. $\mathfrak{c} \cap S = \emptyset$ を自分で示せ.

5.2.3 素元・既約元・同伴元

定義 5.2.9. R が整域のとき,

- $a, b \in R$ に対して $b = ac$ ($^{\exists}c \in R$) のとき, $a|b$ と書き, b は a の**倍元**, a は b の**約元**という.
- $a \in R$ に対して $x \in R$ が, $x = \epsilon a$ となる単元 ϵ が存在するとき, a と x は**同伴元**といい, $x \approx a$ と書く.[3]
- $a_1, a_2, \ldots, a_n \in R$ $(n \geq 2)$ に対して
  - $d|a_i$ ($^{\forall}i$)
  - $x|a_i$ ($^{\forall}i$) ならば $x|d$

  をみたす $d \in R$ を $a_1, a_2, \ldots, a_n$ の**最大公約元**という. 最大公約元は, 単元を除いて一意に決まる. すなわち, d, d' が共に $a_1, a_2, \ldots, a_n$ の最大公約元ならば $d \approx d'$ である. $a_1, a_2, \ldots, a_n$ の最大公約元が単元のとき $a_1, a_2, \ldots, a_n$ は**互いに疎**という.
- $a_1, a_2, \ldots, a_n \in R$ に対して
  - $a_i|m$ ($^{\forall}i$)
  - $a_i|x$ ($^{\forall}i$) ならば $m|x$

  をみたす m を $a_1, a_2, \ldots, a_n$ の**最小公倍元**という. 最小公倍元も, 単元を除いて一意に決まる.

命題 5.2.10. $a, x \in R$ に対して, 次は同値

(i) $x|a$ ならば $x = \epsilon$ または $x = \epsilon a$ (ただし ϵ は単元) と書ける
(ii) $x|a \Leftrightarrow x$ は単元か, または $x \approx a$
(iii) $(a) \subseteq (x) \subseteq R \Rightarrow (x) = (a)$ または $(x) = R$

証明. 易しいので省略. □

定義 5.2.11. R が整域のとき,

- $a \in R$ が, $x \notin R^{\times}$, かつ $x|a$ ならば $x = \epsilon$ または $x = \epsilon a$ (ただし ϵ は単元) をみたすとき, a は**既約元 (irreducible element)** という.
- $p \notin R^{\times}$ が $p|ab \Rightarrow p|a$ または $p|b$ をみたすとき, p を R の**素元**という.[4]

命題 5.2.12. 整域 R において, 素元は既約元である.

証明. $p \in R$ が素元であり, $p = ab$ と書けたとすると $p \,|\, ab$ なので, $p \,|\, a$ または $p \,|\, b$ である. たとえば $p \,|\, a$ のときは, $p = ab$ より $a|p$ だから $a \approx p$ となり, p は既約元である. $b \in (p)$ のときも同様. □

5.2.4 素元分解整域 (UFD)

定義 5.2.13. 整域 R において, R の単元でない元 a $(a \neq 0)$ はすべて有限個の素元の積 $a = p_1 p_2 \cdots p_r$ と書けるとき, **素元分解整域** または **一意分解整域 (Unique Factorization Domain)** という.

定理 5.2.14. 素元分解整域において, 素元への分解は順序と単を除いて一意的である. すなわち, $a \in R$ が $a = p_1 \cdots p_r = q_1 \cdots q_s$ と 2 通りの方法で素元の積に分解したとすると, $r = s$ であり, 適当に順番を付け替えることによって $p_1 \approx q_1, \ldots, p_r \approx q_r$ となる.

証明. r に関する数学的帰納法で証明する. $r = 1$ のとき, $p_1 = q_1 \cdots q_s$ とすると, $q_1 \cdots q_s \in (p_1)$ だから $q_1 \in (p_1)$ としてよい. このとき, $p_1 \approx q_1$ であり, $q_2 \cdots q_s$ は単元だから $s = 1$ でなければならない. $r > 1$ のとき, $p_1 \cdots p_r = q_1 \cdots q_s$ だから $q_1 \cdots q_s \in (p_1)$ であり, 今と同じ議論により, $p_1 \approx q_1$ としてよい. $q_1 = \epsilon_1 p_1$ (ϵ_1 は単元) とおくと $p_1 \cdots p_r = \epsilon_1 p_1 \cdots q_s$ より $p_2 \cdots p_r = \epsilon_1 q_2 \cdots q_s$ となり, 帰納法の仮定より $r - 1 = s - 1$ で, 適当に番号を付け替えて $p_2 \approx q_2, \ldots, p_r \approx q_r$ とできる. □

[3] $x \approx a \Leftrightarrow a|x$ かつ $x|a$.
[4] 命題 5.2.1 より (p) が素イデアルであると同値

命題 5.2.15. 素元分解整域において, 既約元は素元である. (よって, 既約元であることと素元であることは同値)

証明. 素元分解を考えると明らかである. □

問題 5.2.16. $R = \mathbb{Z}[\sqrt{-5}] = \{x + y\sqrt{-5} \mid x, y \in \mathbb{Z}\}$ を考える. $w = x + y\sqrt{-5} \in R$ に対して, $\overline{w} = x - y\sqrt{-5}$, $N(w) = w\overline{w} = x^2 + 5\,y^2 \in \mathbb{Z}$ と定義すると $N(w_1w_2) = N(w_1)N(w_2)$ である.

(i) 2, 3, $1 \pm \sqrt{-5}$ は R の素元であることを示せ.
(ii) (2) は R の素イデアルでないことを示せ.
(iii) $(2, 1 + \sqrt{-5})$ は単項イデアルでないことを示せ.
(iv) R は UFD でないことを示せ. $(6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ を使え).

5.2.5 単項イデアル整域 (PID)

定義 5.2.17. 整域 R において, すべてのイデアルが単項イデアルであるとき, **単項イデアル整域 (Principal Integral Domain)** という.

補題 5.2.18. 単項イデアル整域において, 既約元は素元である. (よって, 既約元であることと素元であることは同値)

証明. 単項イデアル整域においては, 命題 5.2.10 より p が既約元 $\Leftrightarrow$ (p) が極大イデアル $\Rightarrow$ (p) が素イデアル $\Leftrightarrow$ p は素元 □

同様に, 次も, すぐわかる.

命題 5.2.19. R が単項イデアル整域のとき, $p \in R$ に対して, 次は同値.

(i) (p) は素イデアル
(ii) (p) は極大イデアル

定理 5.2.20. 単項イデアル整域 R は素元分解整域である.

証明. (背理法) $a \neq 0 \in R$ が単元でないとし, 素元の積として表せないと仮定する. したがって, a は既約元でないから $a = a_1a_1'$ $(a_1, a_1'$ は単元でない) と分解され, a_1, a_1' のうち, どちらか 1 つは既約元でない. たとえば, a_1 が既約元でないならば, $a_1 = a_2a_2'$ $(a_2, a_2'$ は単元でない) と分解され, a_2, a_2' のうち, どちらか 1 つ, 例えば a_2 が既約元でない. これを繰り返していくことにより, 増大するイデアルの無限列

$$(a) \subsetneq (a_1) \subsetneq (a_2) \subsetneq (a_3) \subsetneq \cdots \subsetneq R$$

が得られる. このとき $\bigcup_i (a_i)$ はイデアルである.[5] R は単項イデアル整域だから $\bigcup_i (a_i) = (b)$ となる $b \in R$ が存在する. このとき, $^{\exists}i_0$ が存在して $b \in (a_{i_0})$ となるので,

$$(a_{i_0}) = (a_{i_0+1}) = (a_{i_0+2}) = \cdots$$

となり, 矛盾する. □

命題 5.2.21. 単項イデアル整域 R の元 a, b について次は同値.

(i) a と b の最大公約元は d である.
(ii) $(a, b) = (d)$.

証明. (i) $\Rightarrow$ (ii)
$(a, b) = (c)$ となる $c \in R$ が存在する. $c|a$ かつ $c|b$ なので $c|d$ である. また, $c = ax + by$ となる $x, y \in R$ が存在するが, $d|a$ かつ $d|b$ なので $d|c$ である. したがって $c \approx d$ となる.

(ii) $\Rightarrow$ (i)
$d = ax + by$ となる $x, y \in R$ が存在する. c を a, b の公約元とすると, $c|a$, $c|b$ より $c|d$ である. $a, b \in (d)$ より, $d|a$ かつ $b|d$ である. □

例 5.2.22. X, Y を変数として, $R = \mathbb{Z}[X, Y]$ は UFD である. (後出) $I = (X, Y) \subsetneq R$ は単項イデアルではないことを示せ. よって, R は PID ではない.

[5] これを示せ.

5.2.6 ユークリッド整域

定義 5.2.23. 整域 R の 0 でない各元 a に非負整数 $v(a) \geq 0$ が対応し, 次の条件をみたすとき, **Euclid 整域 (Euclidian Domain)** という.

(1) $^{\forall}a, b \in R$ s.t. $a \neq 0$, $^{\exists}q, r$ such that $b = aq + r$ で, $r = 0$ または $v(r) < v(a)$
(2) $a \neq 0$, $b \neq 0$ に対して $v(a) \leq v(ab)$.

定理 5.2.24. Euclid 整域 R は単項イデアル整域である.

証明. $\mathfrak{a} \neq 0$ を R のイデアルとする.

$$S = \{v(x) | x \in \mathfrak{a} \text{ かつ } x \neq 0\}$$

は $\mathbb{N}$ の空でない部分集合なので最小値 $v(a)$ が存在する. このとき $\mathfrak{a} = (a)$ であることを示す. 実際, $x \in \mathfrak{a}$ として $x = aq + r$ と表すと $r = 0$ または $r \neq 0$ かつ $v(r) < v(a)$ であるが, もし後者だとすると $r = x - qa \in \mathfrak{a}$ となり, $v(a)$ の最小性に矛盾する. □

5.2.7 商体

定理 5.2.25. (商体) R が整域のとき, 次をみたす体 F と写像 $f : R \to F$ が存在する.

(1) f は単準同型写像
(2) F の任意の元は $x = f(a)f(b)^{-1}$ の形に書かれる.

また, (F, f), (F', f') がともに (1) (2) をみたせば, 同型写像 $\varphi : F \to F'$ が存在して $f' = \varphi \circ f$ となる.

証明.

$$\overline{F} = \{(a, b) | a, b \in R,\ b \neq 0\}$$

とし, $\overline{F}$ に同値関係 $\sim$ を

$$(a, b) = (c, d) \Leftrightarrow ad = bc$$

で定義する. $F = \overline{F}/\sim$ とおき, F の加法と乗法を

$$\overline{(a, b)} + \overline{(c, d)} = \overline{(ad + bc, bd)},\ \overline{(a, b)(c, d)} = \overline{(ac, bd)}$$

によって定義すると, この二項演算は well-defined で, $0_F = \overline{(0_R, 1_R)}$ が零元で, $1_F = \overline{(1_R, 1_R)}$ が単位元となる. $f : R \to F$ を $f(a) = \overline{(a, 1_R)}$ で定義する.

問題 5.2.26. 上の定理の詳細を述べよ.

定義 5.2.27. R が整域のとき, 上の F を R の**商体 (field of quotients)** という.

以後, R は (単位元をもつ可換環でかつ) 整域とする.

第6章　多項式環

この節では, 実際は R を整域と仮定することが多い. $\deg f \geq 1$ である多項式 $f \in R[X_1, \ldots, X_n]$ について,

$$f = gh, \qquad 1 \leq \deg g, \deg h < f$$

となる $g, h \in R[X_1, \ldots, X_n]$ が存在するとき, f は**次数可約 (degreewise reducible)** であるという. $f \in R[X_1, \ldots, X_n]$ が $\deg f \geq 1$, かつ可約でないとき, **次数既約 (degreewise irreducible)** という.

例 6.0.1. $h(X) = 2\,X^3 + 2\,X^2 + 2\,X + 2 \in \mathbb{Z}[X]$ は次数可約, $g(X) = X^2 + \frac{1}{2}\,X + \frac{2}{3} \in \mathbb{Q}[X]$ は次数既約.

命題 6.0.2. $f \in R[X_1, \ldots, X_n]$ が単元 $\Leftrightarrow$ f は R の単元

証明. $\Leftarrow$　$f \in R[X_1, \ldots, X_n]$ が単元ならば $\deg f = 0$ である.
$\Rightarrow$　明らか □

例 6.0.3. $\mathbb{Z}[X_1, \ldots, X_n]$ の単元は ± 1 のみである.

注意 6.0.4. F が体ならば, 『$f \in F[X]$ が次数既約 $\Leftrightarrow$ f は $F[X]$ の既約元』であるが, 一般には, R が整域のとき, $f \in R[X]$ が次数既約と $R[X]$ の元として既約であることは違う. 例えば $f(X) = 6(X^2 + X + 1) \in \mathbb{Z}[X]$ は, より次数の小さな多項式の積に書けないので次数既約であるが, $f(X)$ は $\mathbb{Z}[X]$ の素元 2, 3, $X^2 + X + 1$ の積に書けるので $\mathbb{Z}[X]$ の既約元ではない. $\mathbb{Q}[X]$ で考えれば 6 は単元なので既約元である.

6.1　1 変数多項式環

$R[X]$ を R 上の 1 変数多項式環とする. $f \in R[X]$ は

$$f = a_0 + a_1 X + \cdots + a_m X^m = \sum_{i=0}^{m} a_i X^i \qquad (a_i \in R,\ a_m \neq 0)$$

と書けて, m を**次数 (degree)**, a_m を**最高次の係数 (leading coefficient)** という. $a_m = 1$ のとき**モニック (monic)** な多項式という. また, 上の f に対して, $\sum_{i=1}^{m} i a_i X^{i-1}$ で定義される多項式を f' と書き, f の**導関数 (derivative)** とよぶ.

例 6.1.1. $h(X) = 2\,X^3 + 2\,X^2 + 2\,X + 2 \in \mathbb{Z}[X]$ は 3 次多項式で, 最高次の係数が 2 なので monic でなく, $h'(X) = 6\,X^2 + 4\,X + 2 \in \mathbb{Z}[X]$ である.

命題 6.1.2. R が整域 $\Rightarrow$ $R[X]$ も整域, $f, g \in R[X]$ に対して, $\deg(fg) = \deg f + \deg g$

証明. $f = \sum_{i=0}^{m} a_i X^i$, $g = \sum_{j=0}^{n} b_j X^j$ とすると $fg = \sum_{i=0}^{m} \sum_{j=0}^{n} a_i b_j X^{i+j}$ で $a_m b_n \neq 0$ である.

系 6.1.3. R が整域 $\Rightarrow$ $R[X_1, \ldots, x_n]$ も整域, $f, g \in R[X]$ に対して, $\deg(fg) = \deg f + \deg g$

証明. $R[X_1, \ldots, x_n] = R[X_1][X_2] \cdots [X_n]$ を使え.

定義 6.1.4. R が整域のとき, $R[X_1, \ldots, x_n]$ の商体を

$$R(X_1, \ldots, X_n) = \left\{ \frac{f(X_1, \ldots, X_n)}{g(X_1, \ldots, X_n)} \mid f(X_1, \ldots, X_n), g(X_1, \ldots, X_n) \in R[X_1, \ldots, X_n],\ g(X_1, \ldots, X_n) \neq 0 \right\}$$

と書く.

定理 6.1.5. R が整域, $f, g \in R[X]$ で g の最高次の係数が R の単元ならば

$$f = gq + r, \qquad r = 0 \text{ または } \deg f < \deg g$$

となる $q, r \in R[X]$ が一意的に存在する.

証明. まず, 存在を示す. $f = \sum_{i=0}^{m} a_i X^i$, $g = \sum_{j=0}^{n} b_j X^j$ とすると, $\deg f < \deg g$ のときは明らかである. $\deg f = \deg g$ のときは, 多項式の割算をやれば, q, r が求められる.

次に一意性をいう. $f = gq_1 + r_1 = gq_2 + r_2$, $\deg r_1, \deg r_2 < \deg g$ とすると $g(q_1 - q_2) = r_2 - r_1$ である. $q_1 - q_2 \neq 0$ ならば $\deg g(q_1 - q_2) \geq \deg g > \deg r_2 - r_1$ となり矛盾である. よって $q_1 = q_2$, $r_1 = r_2$.

系 6.1.6. R が整域 のとき, $f \in R[X]$, $a \in R$ に対して,

$$f(X) = (X - a)q(X) + f(a),$$

となる $q(X) \in R[X]$ が一意的に存在する. 特に,

$$X - a | f(X) \quad \Leftrightarrow \quad f(a) = 0$$

証明. 上の定理で $g(X) = X - a$ とすると

$$f(X) = (X - a)q(X) + r$$

である. $X = a$ を代入すると $r = f(a)$. 残りは明らか.

系 6.1.7. 整域 R 上の m 次多項式, $f(X) \in R[X]$ は m 個より多くの根を持たない.

証明. m に関する数学的帰納法.

(i) $m = 1$ のときは, 明らか.

(ii) $m > 2$ とし, $m - 1$ まで正しいとする. m 次多項式, $f(X) \in R[X]$ が根 a を持つとすると $f(X) = (X - a)f_1(X)$ と書ける. ここで, $f_1(X)$ は $m - 1$ 次式だから, 高々 $m - 1$ 個の根しかもたない. よって, $f(X)$ は高々 m 個の根しかもたない.

残りは明らか.

系 6.1.8. 整域 R 上の次多項式, $f(X) \in R[X]$ が無限に多くの相異なる R の元 a に対し, $f(a) = 0$ ならば $f(X) = 0$ である.

定義 6.1.9. $f \in R[X]$, $a \in R$ のとき,

$$(X - a)^k | f(X) \qquad \text{かつ} \qquad (X - a)^{k+1} \not| f(X)$$

ならば, a は $f(X)$ の k **重根**, k を $f(X)$ の根 a の**重複度**という. 少なくとも 2 重根となっているとき, 単に, **重根**という.

命題 6.1.10. R が整域のとき, $a \in R$ が $f(X) \in R[X]$ の k 重根 $(k \geq 2)$ ならば, a は $f'(X)$ の少なくとも $k - 1$ 重根である.

$$a \in R \text{ が } f(X) \text{ の重根} \Leftrightarrow f(a) = f'(a) = 0.$$

証明. 仮定より, $f(X) = (X - a)^k g(X)$, $g(a) \neq 0$ である. このとき,

$$f'(X) = k(X - a)^{k-1} g(X) + (x - a)kg'(X) = (X - a)^{k-1} \{kg(X) + (X - a)g'(X)\}$$

なので $(X - a)^{k-1} | f(X)$ である.

6.2 体の上の 1 変数多項式環

命題 6.2.1. 体 F 上の 1 変数多項式環 $F[X]$ は Euclid 整域である.

証明. 定理 6.1.5 を使え.

系 6.2.2. 体 F 上の 1 変数多項式環 $F[X]$ は PID である.

証明. 定理 5.2.24 を使え.

命題 6.2.3. 体 F 上の 1 変数多項式 $f(X), g(X) \in F[X]$ について, 次は同値.

(i) $f(X), g(X)$ は定数以外に公約元をもたない.
(ii) $f(X)u(X) + g(X)v(X) = 1$ となる $u(X), v(X) \in F[X]$ が存在する.

命題 6.2.4. 体 F 上の 1 変数多項式 $p(X) \in F[X]$ について, 次はすべて同値.

(i) $p(X)$ は $F[X]$ の次数既約
(ii) $p(X)$ は $F[X]$ の素元
(iii) $(p(X))$ は $F[X]$ の素イデアル
(iv) $(p(X))$ は $F[X]$ の極大イデアル

6.3 UFD 上の 1 変数多項式環

この節では, R は UFD とする. また, F を R の商体とする.

定義 6.3.1. $f(X) \in R[X]$ の全ての係数の最大公約元が単元であるとき, $f(X)$ は**原始多項式 (primitive polynomial)** という.

例 6.3.2. $h(X) = 2\,X^3+2\,X^2+2\,X+2 \in \mathbb{Z}[X]$ は全ての係数が 2 で割れるので primitive でないが, $k(X) = 6\,X^2+3\,X+4 \in \mathbb{Z}[X]$ は primitive である.

補題 6.3.3. $p \in R$ が R の素元であるならば p は $R[X]$ の素元, i.e.,
$f(X), g(X) \in R[X]$ について $p \not| f(X)$ かつ $p \not| g(X) \Rightarrow p \not| f(X)g(X)$.

証明. $f(X) = a_0 + a_1X + \cdots + a_mX^m$, $g(X) = b_0 + b_1X + \cdots + b_nX^n$ $(a_m, b_n \neq 0)$ とする. $f(X), g(X)$ の最初に p で割れない係数を, それぞれ a_j, b_k とすると, 積 $f(X)g(X)$ の X^{j+k} の係数は

$$c_{j+k} = a_{j+k}b_0 + \cdots + a_{j+1}b_{k-1} + a_jb_k + a_{j-1}b_{k+1} + \cdots + a_0b_{j+k}$$

である. $p \not| a_kb_k$ で, 他の項は全て p で割れるので, $p \not| c_{j+k}$ であるから $p \not| f(X)g(X)$. □

定理 6.3.4. (Gauss's Lemma) $f(X), g(X) \in R[X]$ が原始多項式ならば, その積 $f(X)g(X)$ も原始多項式である.

証明. もし, $f(X)g(X)$ が原始多項式でないならば, $p|f(X)g(X)$ となる素元 $p \in R$ が存在する. 補題 6.3.3 より $p|f(X)$ または $p|g(X)$ となり, $f(X), g(X)$ が原始多項式であることに反する. □

例 6.3.5. $f(X) = 2\,X^2 + 3\,X + 3$, $g(X) = 2\,X^2 + 5\,X + 2 \in \mathbb{Z}[X]$ は原始多項式であり, その積

$$f(X)g(X) = 4\,x^4 + 16\,x^3 + 25\,x^2 + 21\,x + 6 \in \mathbb{Z}[X]$$

も原始多項式である.

定義 6.3.6. 商体の元 $a, b \in F$ に対して, $b = a\epsilon$ となる R の単元 $\epsilon \in R^\times$ が存在するとき, $a \approx b$ と書き [1], a と b は同伴元という.

[1] $approx$ は同値関係

例 6.3.7. $R=\mathbb{Z}$ のとき, その商体は $F=\mathbb{Q}$ で, $\mathbb{Z}^\times=\{\pm1\}$ なので, $\frac{2}{3}$ と同伴な元は $\pm\frac{2}{3}$ である. また, $R=\mathbb{Z}[i]$ $(i=\sqrt{-1})$ のとき, その商体は $F=\mathbb{Q}[i]$ であり, $\mathbb{Z}^\times=\{\pm1,\pm i\}$ なので, $\frac{2}{3}$ と同伴な元は $\pm\frac{2}{3}$, $\pm\frac{2}{3}\,i$ である.

命題 6.3.8. $f(X)\in F[X]$ ならば $f(X)=cg(X)$ となる $c\in F$ と原始多項式 $g(X)\in R[X]$ が存在する. c は同伴元を除いて一意的であり, これを $c=c(f)$ と書き $f(X)$ の**コンテント (content)** という.

証明. $f(X)=\dfrac{a_0}{b_0}+\dfrac{a_1}{b_1}X+\cdots+\dfrac{a_m}{b_m}X^m$ とするとき, $b_0,b_1,\ldots,b_m$ の最小公倍元を B とおくと

$$f(X)=\frac{1}{B}\left(a_0\cdot\frac{B}{b_0}+a_1\cdot\frac{B}{b_1}X+\cdots+a_m\cdot\frac{B}{b_m}X^m\right)$$

と書けて, $a_i\cdot\dfrac{B}{b_i}\in R$ の R での最大公約元を $A\in R$ とすると,

$$f(X)=\frac{A}{B}\,(c_0+c_1X+\cdots+c_mX^m)$$

という形になる. ここで, $c=\frac{A}{B}$, $f_0(X)=c_0+c_1X+\cdots+c_mX^m$ とおくと, 作り方から $f_0(X)\in R[X]$ は原始的である.

もし, $f(X)=cf_0(X)=c'f_0'(X)$ $(f_0(X),f_0'(X)\in R[X]$ は原始的$)$ と書けたとすると, $c=\dfrac{a}{b}$, $c'=\dfrac{a'}{b'}$ とおくと $ab'f_0(X)=a'bf_0'(X)\in R[X]$ となる. 両辺の係数の最大公約元を考えると, $f_0(X),f_0'(X)$ が原始的であることより $ab'\approx a'b$ でなければならない. すなわち $ab'=a'b\epsilon$ となる単元 $\epsilon\in R^\times$ が存在する. よって, $c'=c\epsilon$ かつ $f_0(X)=\epsilon f_0'(X)$ となる. □

例 6.3.9. $R=\mathbb{Z}$ のとき, その商体は $F=\mathbb{Q}$ で, $g(X)=X^2+\frac{1}{2}\,X+\frac{2}{3}\in\mathbb{Q}[X]$ の場合は. $c(g)=\frac{1}{6}$, と primitive な多項式 $k(X)=6\,X^2+3\,X+4\in\mathbb{Z}[X]$ を使って, $g(X)=c(g)\,k(X)$ と分解する.

命題 6.3.10. 次は明らか

- $f\in F[X]$ に対して, $f\in R[X]\Leftrightarrow c(f)\in R$
- $f\in R[X]$ に対して, f が原始多項式 $\Leftrightarrow c(f)\approx1$
- $f,g\in F[X]$ に対して, $c(fg)=c(f)c(g)$.[2] □

補題 6.3.11. $f(X),g(X)\in R[X]$ で, $g(X)$ が原始多項式のとき, $f(X)=g(X)h(X)$ となる $h(X)\in F[X]$ が存在すれば $h(X)\in R[X]$.

証明. $f(X)=g(X)h(X)$ より $R\ni c(f)=c(g)c(h)=c(h)$ だから, 命題 6.3.10 より $h(X)\in R[X]$. □

補題 6.3.12. $f(X)\in R[X]$ が, $f(X)=g(X)h(X)$ となる $g(X),h(X)\in F[X]$ が存在したとすれば

$$f(X)=g_1(X)h_1(X),\quad \deg g=\deg g_1,\quad \deg h=\deg h_1$$

となる $g_1(X),h_1(X)\in R[X]$ が存在する.

証明. $g(X)=c(g)g_0(X)$, $h(X)=c(h)h_0(X)$ $(g_0,h_0\in R[X]$ は原始多項式$)$ とすると $f(X)=c(g)c(h)g_0(X)h_0(X)$ で, 定理 6.3.4 より, $g_0(X)h_0(X)$ は原始的で, 命題 6.3.10 より $c(g)c(h)\in R$ でなければならない. よって, 例えば, $g_1(X)=g_0(X)\in R[X]$, $h_1(X)=c(g)c(h)h_0(X)\in R[X]$ とおけばよい. □

定理 6.3.13. $f(X)\in R[X]$ が, $R[X]$ において次数既約ならば $F[X]$ において既約である.

定理 6.3.14. 素元分解整域 R 上の多項式環 $R[X]$ の元 $f(X)$ について, 次は同値

(1) $f(X)$ は $R[X]$ の素元である
(2) f は R の素元 $(\deg f=0)$, または, f は原始的かつ次数既約 $(\deg f\geq1)$.

証明. (1) ⇒ (2)
$f(X)\in R[X]$ が素元のとき, 命題 6.3.8 より $f(X)=c(f)f_0(X)$ $(f_0(X)\in R[X]$ は原始多項式$)$ とすれば, $f(X)|c(f)f_0(X)$ より $f(X)|c(f)$ または $f(X)|f_0(X)$ である. 前者の場合は $f(X)\approx c(f)$ は R の素元, 後者の場合は $f(X)\approx f_0(A)$ で $c(f)\approx1$ でなければならない.

(2) ⇒ (1)
明らか. □

[2]定理 6.3.4 を使え.

定理 6.3.15. 素元分解整域 R 上の多項式環 $R[X]$ は素元分解整域である.

証明. $f(X) \in R[X]$ のとき, 命題 6.3.8 より $f(X) = c(f)f_0(X)$ ($c(f) \in R$, $f_0(X) \in R[X]$ は原始多項式) と書ける. $c(f)$ は R の素元の積で $c(f) = p_1 \cdots p_r$ と書ける. また, R の商体 F 上の多項式環 $F[X]$ は素元分解整域だから, $F[X]$ の中で $f_0(X) = g_1(X) \cdots g_s(X)$ ($g_i(X) \in F[X]$) と書ける. 補題 6.3.12 より, $h_1, \ldots, h_s \in R[X]$ が存在し,

$$f_0(X) = h_1(X) \cdots h_s(X), \deg g_i = \deg g_i$$

となる. このとき, f_0 が原始多項式だから $1 \approx c(h_1) \cdots c(h_s)$ となり, h_i も原始多項式で $F[X]$ で次数既約だから $R[X]$ でも次数既約である. したがって, 定理 6.3.14 より, $f(X) = p_1 \cdots p_r h_1(X) \cdots h_s(X)$ は f の素元分解を与える. □

系 6.3.16. 素元分解整域 R 上の多項式環 $R[X_1, \ldots, X_n]$ は素元分解整域である.

証明. $R[X_1, \ldots, X_n] = R[X_1, \ldots, X_{n-1}][X_n]$ を使え. □

第7章　単因子論

この章では, R を単位的可換環と仮定する.

7.1　行列の正則性

R の元を成分とする $m \times n$ 行列全体の集合を $\mathrm{M}_{m,n}(R)$ と記す. 特に, $m = n$ のとき, n 次正方行列全体の集合を, 略して $\mathrm{M}_n(R)$ と記す. n 次正方行列 $A \in \mathrm{M}_n(R)$ は

$$AB = BA = I$$

となる n 次正方行列 $B \in \mathrm{M}_n(R)$ が存在するとき, **正則 (non-singular)** といい, B を A の逆行列といい, A^{-1} と記す. ここで

$$I = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix}$$

は単位行列である. R 係数の n 次の正則行列全体の集合を $\mathrm{GL}_n(R)$ と書き, R 上の**一般線型群 (General Linear Group)** という.

定理 7.1.1. n 次正方行列 $A \in \mathrm{M}_n(R)$ が正則であるための必要十分条件は $\det A$ が R の単元であることである.

証明. $AB = I$ ならば, $\det A \det B = 1$ より $\det A \in R^\times$ である. 逆に, $\det A \in R^\times$ ならば A の余因子行列を $\widetilde{A}$ とすると

$$A^{-1} = \frac{1}{\det A}\, {}^tA$$

である. ここで, ${}^tA$ は A の転置行列を表す. □

7.2　行列の基本変形

次の 4 つの n 次正方行列 $P_n(i,j), Q_n(i;c), R_n(i,j;a) \in \mathrm{M}_n(R)$ を**基本変形行列**という.

$$P_n(i,j) = \begin{array}{c} \\ \\ \\ i \text{ 行} \\ \\ \\ j \text{ 行} \\ \\ \\ \end{array} \begin{array}{c} \begin{array}{ccccccccc} & & & & i \text{ 列} & & & & j \text{ 列} \end{array} \\ \begin{pmatrix} 1 & & & & \vdots & & & & \vdots & & \\ & \ddots & & & \vdots & & & & \vdots & & \\ & & 1 & & & & & & & & \\ \dots & \dots & & & 0 & & \dots & & 1 & \dots & \dots \\ & & & & & 1 & & & & & \\ & & & & \vdots & & \ddots & & \vdots & & \\ & & & & & & & 1 & & & \\ \dots & \dots & & & 1 & & \dots & & 0 & \dots & \dots \\ & & & & & & & & & 1 & \\ & & & & \vdots & & & & \vdots & \ddots & \\ & & & & \vdots & & & & \vdots & & 1 \end{pmatrix} \end{array}$$

$$Q_n(i;c) = \begin{array}{r} \\ \\ \\ \\ i\text{ 行} \\ \\ \\ \\ \end{array} \begin{array}{c} \begin{array}{ccccccc} &&& i\text{ 列} &&& \end{array} \\ \begin{pmatrix} 1 & & & \vdots & & & \\ & \ddots & & \vdots & & & \\ & & 1 & & & & \\ \cdots & \cdots & & c & & \cdots & \cdots \\ & & & & 1 & & \\ & & & \vdots & & \ddots & \\ & & & \vdots & & & 1 \end{pmatrix} \end{array}$$

ただし, $c \in R^{\times}$ とする.

$$R_n(i,j;a) = \begin{array}{r} \\ \\ \\ i\text{ 行} \\ \\ j\text{ 行} \\ \\ \\ \end{array} \begin{array}{c} \begin{array}{ccccccc} && i\text{ 列} && j\text{ 列} && \end{array} \\ \begin{pmatrix} 1 & & \vdots & & \vdots & & \\ & \ddots & \vdots & & \vdots & & \\ \cdots & \cdots & 1 & \cdots & a & & \\ & & & \ddots & \vdots & & \\ \cdots & \cdots & & \cdots & 1 & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{pmatrix} \end{array}$$

ただし, $a \in R$ とする.

$$S_n(i,j;\alpha,\beta,\gamma,\delta) = \begin{array}{r} \\ \\ \\ \\ i\text{ 行} \\ \\ \\ \\ j\text{ 行} \\ \\ \\ \\ \end{array} \begin{array}{c} \begin{array}{ccccccccccc} &&& i\text{ 列} &&&& j\text{ 列} &&& \end{array} \\ \begin{pmatrix} 1 & & & \vdots & & & & \vdots & & & \\ & \ddots & & \vdots & & & & \vdots & & & \\ & & 1 & & & & & & & & \\ \cdots & \cdots & & \alpha & & \cdots & & \beta & & \cdots & \cdots \\ & & & & 1 & & & & & & \\ & & & \vdots & & \ddots & & \vdots & & & \\ & & & & & & 1 & & & & \\ \cdots & \cdots & & \gamma & & \cdots & & \delta & & \cdots & \cdots \\ & & & & & & & & 1 & & \\ & & & \vdots & & & & \vdots & & \ddots & \\ & & & \vdots & & & & \vdots & & & 1 \end{pmatrix} \end{array}$$

ただし, $\alpha\delta - \beta\gamma \in R^{\times}$, とする.

命題 7.2.1. $a \in R$, $c \in R^{\times}$, $\alpha\delta - \beta\gamma \in R^{\times}$ のとき, 上の 4 つの n 次正方行列 $P_n(i,j), Q_n(i;c), R_n(i,j;a), S_n(i,j;\alpha,\beta,\gamma,\delta) \in \mathrm{M}_n(R)$ は正則行列である.

証明. 行列式を計算すると

$$\det P_n(i,j) = -1, \qquad \det Q_n(i;c) = c, \qquad \det R_n(i,j;a) = 1, \qquad \det S_n(i,j;\alpha,\beta,\gamma,\delta) = \alpha\delta - \beta\gamma$$

なので, Theorem 7.1.1 を使うと正則であることがわかる.

または, 直接計算で

$$P_n(i,j)^{-1} = P_n(i,j), \quad Q_n(i;c)^{-1} = Q_n(i;c^{-1}), \quad R_n(i,j;a)^{-1} = R_n(i,j;-a), \quad S_n(i,j;\alpha,\beta,\gamma,\delta) = S_n(i,j;\alpha',\beta',\gamma',\delta')$$

であることも確かめられる. ここで, $\alpha' = (\alpha\delta - \beta\gamma)^{-1}\delta$, $\beta' = -(\alpha\delta - \beta\gamma)^{-1}\beta$, $\gamma' = -(\alpha\delta - \beta\gamma)^{-1}\gamma$, $\delta' = (\alpha\delta - \beta\gamma)^{-1}\alpha$ とする. □

定義 7.2.2. $m \times n$ 行列 $A \in \mathrm{M}_{m,n}(R)$ に対して, 次の 3 つの変形を行って, 新しい行列 B を得ることを A の**行の基本変形 (elementary row operations)** (resp. **列の基本変形 (elementary column operations)**) という.

(L1) 2 つの行 (resp. 列) を入れ替える.

(L2) ある行 (resp. 列) に R の単元 c をかける.

(L3) ある行 (resp. 列) に R の元 a をかけて, 他の行 (resp. 列) に加える.

(L4) $\alpha\delta - \beta\gamma$ が R の単元のとき, 第 i 行を, 元の行列の第 i 行の α 倍と第 j 行の β 倍で置き換え第 j 行を, 元の行列の第 i 行の γ 倍と第 j 行の δ 倍で置き換える.

列の基本変形のときは上の操作をそれぞれ (R1), (R2), (R3) とよぶ. また

(R4) $\alpha\delta - \beta\gamma$ が R の単元のとき, 第 i 列を, 元の行列の第 i 列の α 倍と第 j 列の γ 倍で置き換え第 j 列を, 元の行列の第 i 列の β 倍と第 j 列の δ 倍で置き換える.

とする. 行の基本変形と列の基本変形を総称して, 単に, **基本変形 (elementary operations)** という.

例 7.2.3. (L1) の第 1 行と第 2 行を入れ替える操作

$$\begin{pmatrix} 1 & 0 & -2 \\ 2 & 3 & 1 \end{pmatrix} \xrightarrow{①\leftrightarrow②} \begin{pmatrix} 2 & 3 & 1 \\ 1 & 0 & -2 \end{pmatrix}$$

は行の基本変形である. この操作を ①↔② と記す. これに対して, 第 1 行と第 3 行を入れ替える操作

$$\begin{pmatrix} 1 & 0 & -2 \\ 2 & 3 & 1 \end{pmatrix} \xrightarrow{\boxed{1}\leftrightarrow\boxed{3}} \begin{pmatrix} -2 & 0 & 1 \\ 1 & 3 & 2 \end{pmatrix}$$

を $\boxed{1}\leftrightarrow\boxed{3}$ と記す.

例 7.2.4. $\mathbb{Z}$ の単元は ± 1 のみである. (L2) の第 1 行に単元 -1 をかける操作

$$\begin{pmatrix} 1 & 0 & -2 \\ 2 & 3 & 1 \end{pmatrix} \xrightarrow{①\times(-1)} \begin{pmatrix} -1 & 0 & 2 \\ 2 & 3 & 1 \end{pmatrix}$$

を ①×(−1) と記す. これに対して, 第 2 列に単元 -1 をかける操作

$$\begin{pmatrix} 1 & 0 & -2 \\ 2 & 3 & 1 \end{pmatrix} \xrightarrow{\boxed{2}\times(-1)} \begin{pmatrix} 1 & 0 & -2 \\ 2 & -3 & 1 \end{pmatrix}$$

を $\boxed{2}\times(-1)$ と記す.

例 7.2.5. (L3) の第 2 行に $2 \in R$ をかけて第 1 行に加える操作

$$\begin{pmatrix} 1 & 0 & -2 \\ 2 & 3 & 1 \end{pmatrix} \xrightarrow{①+②\times 2} \begin{pmatrix} 5 & 6 & 0 \\ 2 & 3 & 1 \end{pmatrix}$$

を ①+②×2 と記す. これに対して, 第 1 列に 2 をかけて第 3 列に加える操作

$$\begin{pmatrix} 1 & 0 & -2 \\ 2 & 3 & 1 \end{pmatrix} \xrightarrow{\boxed{3}+\boxed{1}\times 2} \begin{pmatrix} 1 & 0 & 0 \\ 2 & 3 & 5 \end{pmatrix}$$

を $\boxed{3}+\boxed{1}\times 2$ と記す.

例 7.2.6. 例えば $i = 1$, $j = 2$, $a = 3$, $b = 7$, $c = 2$, $d = 5$ のとき (L4) の操作は

$$\begin{pmatrix} 1 & 0 & -2 \\ 2 & 3 & 1 \end{pmatrix} \xrightarrow[①\times 2+②\times 5]{①\times 3+②\times 7} \begin{pmatrix} 17 & 21 & 1 \\ 12 & 15 & 1 \end{pmatrix}$$

を $\begin{smallmatrix} ①\times 3+②\times 7 \\ ①\times 2+②\times 5 \end{smallmatrix}$ と記す. これに対して, $i = 1$, $j = 3$, $a = 3$, $b = 7$, $c = 2$, $d = 5$ のとき (R4) の操作

$$\begin{pmatrix} 1 & 0 & -2 \\ 2 & 3 & 1 \end{pmatrix} \xrightarrow[\boxed{1}\times 2+\boxed{3}\times 5]{\boxed{1}\times 3+\boxed{3}\times 7} \begin{pmatrix} -11 & 0 & -8 \\ 13 & 3 & 9 \end{pmatrix}$$

を $\begin{smallmatrix} \boxed{1}\times 3+\boxed{3}\times 7 \\ \boxed{1}\times 2+\boxed{3}\times 5 \end{smallmatrix}$ と記す.

命題 7.2.7. $m \times n$ 行列 $A \in \mathrm{M}_{m,n}(R)$ に対して, 次の 3 つの行の基本変形 (L1), (L2), (L3), (L4) は, それぞれ $P_m(i,j)$, $Q_m(i;c)$ $(c \in R^\times)$, $R_m(i,j;a)$ $(a \in R)$, $S_m(i,j;\alpha,\beta,\gamma,\delta)$ $(\alpha,\beta,\gamma,\delta \in R,\ \alpha\delta-\beta\gamma \in R^\times)$ を左からかけることによって得られる. また, 次の 3 つの列の基本変形 (R1), (R2), (R3), (R4) は, それぞれ $P_n(i,j)$, $Q_n(i;c)$ $(c \in R^\times)$, $R_n(i,j;a)$ $(a \in R)$, $S_n(i,j;\alpha,\beta,\gamma,\delta)$ $(\alpha,\beta,\gamma,\delta \in R,\ \alpha\delta-\beta\gamma \in R^\times)$ を右からかけることによって得られる.

証明. (1) $B = P_m(i,j)A$ (resp. $B = AP_n(i,j)$) とすると, B は A の第 i 行と第 j 行 (resp. 第 i 列と第 j 列) を入れ替えたものである.

(2) $B = Q_m(i;c)A$ (resp. $B = AQ_n(i;c)$) とすると, B は A の第 i 行 (resp. 第 i 列) を c 倍したものである.

(3) $B = R_m(i,j;a)A$ (resp. $B = AR_n(i,j;a)$) とすると, B は A の第 i 行に第 j 行の (resp. 第 j 列に第 i 列の) c 倍を加えたものである.

(4) も同様に直接計算で確かめよ. □

定義 7.2.8. R を単位的可換環とする. $A, B \in \mathrm{M}_{m,n}(R)$ に対して, $P \in \mathrm{GL}_m(R)$ と $Q \in \mathrm{GL}_n(R)$ が存在して

$$B = PAQ$$

となるとき, A と B は**対等 (equivalent)** であるといい, $A \sim B$ と記す.

命題 7.2.9. 行列の対等は $\mathrm{M}_{m,n}(R)$ の同値関係である.

証明. 同値関係の 3 つの公理

(1) (反射律) $A \sim A$

(2) (対称律) $A \sim B$ ならば $B \sim A$

(3) (推移律) $A \sim B$ かつ $B \sim C$ ならば $A \sim C$

を確かめよ. □

7.3 コーシー・ビネの公式

$A \in \mathrm{M}_{m,n}(R)$ を $m \times n$ 行列とする. $1 \le k \le \min(m,n)$ のとき, 行の添字 $1 \le i_1 < \cdots < i_k \le m$ と, 列の添字 $1 \le j_1 < \cdots < j_k \le n$ に対して, A から第 $i_1, \ldots, i_k$ 行と第 $j_1, \ldots, j_k$ 列を選んで得られる k 次の正方行列を $A^{i_1,\ldots,i_k}_{j_1,\ldots,j_k}$ と書く. 例えば,

$$A = \begin{pmatrix} 1 & 0 & -2 & -5 \\ 2 & 4 & -3 & 0 \\ -3 & 1 & 3 & 4 \end{pmatrix}$$

のとき

$$A^{1,3}_{2,4} = \begin{pmatrix} 0 & -5 \\ 1 & 4 \end{pmatrix}$$

である. 特に, $k = m$ で $\{i_1, \ldots, i_m\} = \{1, \ldots, m\}$ のとき, $A^{1,\ldots,m}_{j_1,\ldots,j_m}$ を, 略して $A_{j_1,\ldots,j_m}$ と書く. 同様に, $k = n$ で $\{i_1, \ldots, i_n\} = \{1, \ldots, n\}$ のとき, $A^{i_1,\ldots,i_n}_{1,\ldots,n}$ を, 略して $A^{i_1,\ldots,i_n}$ と書く.

定理 7.3.1. (Cauchy-Binet formula) m, n が自然数で $m \le n$ とする. $A \in \mathrm{M}_{m,n}(R)$, $B \in \mathrm{M}_{n,m}(R)$ とする. このとき

$$\det AB = \sum_{1 \le i_1 < \cdots < i_m \le n} \det A_{i_1,\ldots,i_m} \det B^{i_1,\ldots,i_m}$$

である.

証明. 公式は

$$\begin{vmatrix} \sum_{k=1}^n a_{1k}b_{k1} & \cdots & \sum_{k=1}^n a_{1k}b_{km} \\ \vdots & \ddots & \vdots \\ \sum_{k=1}^n a_{mk}b_{k1} & \cdots & \sum_{k=1}^n a_{mk}b_{km} \end{vmatrix} = \sum_{1 \le k_1 < \cdots < k_m \le n} \begin{vmatrix} a_{1k_1} & \cdots & a_{1k_m} \\ \vdots & \ddots & \vdots \\ a_{mk_1} & \cdots & a_{mk_m} \end{vmatrix} \begin{vmatrix} b_{k_1 1} & \cdots & b_{k_1 m} \\ \vdots & \ddots & \vdots \\ b_{k_m 1} & \cdots & b_{k_m m} \end{vmatrix}$$

と書ける. 多重線形性より

$$\mathrm{LHS} = \begin{vmatrix} \sum_{k_1=1}^n a_{1k} b_{k1} & \cdots & \sum_{k_m=1}^n a_{1k} b_{km} \\ \vdots & \ddots & \vdots \\ \sum_{k_1=1}^n a_{mk} b_{k1} & \cdots & \sum_{k_m=1}^n a_{mk} b_{km} \end{vmatrix} = \sum_{k_1=1}^n \cdots \sum_{k_m=1}^n b_{k_1 1} \cdots b_{k_m m} \begin{vmatrix} a_{1k_1} & \cdots & a_{1k_m} \\ \vdots & \ddots & \vdots \\ a_{mk_1} & \cdots & a_{mk_m} \end{vmatrix}$$

添字 $k_1, \ldots, k_m$ は互いに相異なるので

$$= \sum_{1 \le k_1 < \cdots < k_m \le n} \sum_{\sigma \in \mathfrak{S}_m} b_{k_{\sigma(1)} 1} \cdots b_{k_{\sigma(m)} m} \begin{vmatrix} a_{1k_{\sigma(1)}} & \cdots & a_{1k_{\sigma(m)}} \\ \vdots & \ddots & \vdots \\ a_{mk_{\sigma(1)}} & \cdots & a_{mk_{\sigma(m)}} \end{vmatrix}$$

行列式の交代性より

$$= \sum_{1 \le k_1 < \cdots < k_m \le n} \sum_{\sigma \in \mathfrak{S}_m} \operatorname{sgn} \sigma \, b_{k_{\sigma(1)} 1} \cdots b_{k_{\sigma(m)} m} \begin{vmatrix} a_{1k_1} & \cdots & a_{1k_m} \\ \vdots & \ddots & \vdots \\ a_{mk_1} & \cdots & a_{mk_m} \end{vmatrix}$$

行列式の定義より

$$= \sum_{1 \le k_1 < \cdots < k_m \le n} \begin{vmatrix} a_{1k_1} & \cdots & a_{1k_m} \\ \vdots & \ddots & \vdots \\ a_{mk_1} & \cdots & a_{mk_m} \end{vmatrix} \cdot \begin{vmatrix} b_{k_1 1} & \cdots & b_{k_1 m} \\ \vdots & \ddots & \vdots \\ b_{k_m 1} & \cdots & b_{k_m m} \end{vmatrix} = \mathrm{RHS}$$

を得る. □

例 7.3.2. $m = 2, n = 3$ とする. $A, B \in \mathrm{M}_{m,n}(R)$ を

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \end{pmatrix}, \qquad B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \\ b_{31} & b_{32} \end{pmatrix}$$

とするとき

$$\det AB = \det \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \det \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} + \det \begin{pmatrix} a_{11} & a_{13} \\ a_{21} & a_{23} \end{pmatrix} \det \begin{pmatrix} b_{11} & b_{12} \\ b_{31} & b_{32} \end{pmatrix} + \det \begin{pmatrix} a_{12} & a_{13} \\ a_{22} & a_{23} \end{pmatrix} \det \begin{pmatrix} b_{21} & b_{22} \\ b_{31} & b_{32} \end{pmatrix}$$

である.

7.4 スミス標準形の存在

定理 7.4.1. R をユークリッド整域とする. 任意の行列 $A \in \mathrm{M}_{m,n}(R)$ は次のような標準形の対角行列と対等である.

$$B = \begin{pmatrix} e_1 & & & & & & \\ & e_2 & & & & & \\ & & \ddots & & & & \\ & & & e_r & & & \\ & & & & 0 & & \\ & & & & & \ddots & \\ & & & & & & 0 \end{pmatrix} \tag{7.4.1}$$

ここで $e_i \neq 0$ $(1 \le i \le r)$ かつ $e_i | e_{i+1}$ $(1 \le i < r)$ である.

証明. R がユークリッド整域で v をその valuation とする. $A = O$ (零行列) ならば, A 自身が標準形であるから, 定理は自明である. そこで以下 $A \neq O$ と仮定する. O でない行列 $A \in \mathrm{M}_{m,n}(R)$ に対して,

$$v(A) = \min\{v(a_{ij}) \,|\, a_{ij} \neq 0\}$$

と定義する. すなわち, $v(A)$ は A の 0 でない成分の valuation の最小値である. 証明が長いので, 以下, いくつかのステップにわける.

1° 任意の (i,j) に対し, A に対等な行列 B で, その $(1,1)$ 成分 b_{11} が, A の (i,j) 成分 a_{ij} に等しいものが存在する. このとき, $v(A)=v(B)$ である.

∴ 例えぱ $i\neq 1$, $j\neq 1$ ならば, A に ① ↔ ⓘ を施してから, その結果の行列に $\boxed{1}\leftrightarrow\boxed{j}$ を施すと B が得られる.

2° A の $(1,1)$ 成分 a_{11} が第 1 行 (または第 1 列) のすべての成分を割り切るならぱ, A と対等な行列 B で, その $(1,1)$ 成分 b_{11} は a_{11} に等しく, 他の第 1 行 (または第 1 列) の元はすべて 0 に等しいものが存在する.

∴ 例えぱ, 第 1 行の $(1,j)$ 成分について $a_{1j}=qa_{11}$ $(j\neq 1)$ ならぱ, 操作 $\boxed{j}+\boxed{1}\times(-q)$ を行えば $(1,j)$ 成分は 0 となる. この操作を第 1 行の元 a_{1j} を**掃き出す**という. この操作を繰り返せば, 第 1 行の $(1,1)$ 以外の成分 (または第 1 列) の $(1,1)$ 以外の成分をすべて 0 にできる.

3° A の成分で valuation が最小なものが a_{11} であるとき (i.e. $v(a_{11})=v(A)$), A の第 1 行または第 1 列の成分で a_{11} で割り切れないのがあるならば, A と対等な行列 B で, $v(B)<v(A)$ となるようなものが存在する.

∴ 例えぱ, 第 1 列の成分 a_{i1} が a_{11} で割り切れないとすれぱ, R がユークリッド整域であることより

$$a_{i1}=qa_{11}+r,\qquad v(r)<v(a_{11}) \tag{7.4.2}$$

となるような元 $q,r\neq 0\in R$ が存在する. そこで A に対して操作 ⓘ + ① × $(-q)$ を行った行列を B とすれば B の $(i,1)$ 成分は r だから, $v(B)<v(A)$ となる.

4° 行列 $A\neq O$ の成分で valuation が最小なものが a_{ij} であるとき (i.e. $v(a_{ij})=v(A)$), 行列 A の 0 でない成分 a_{kl} で a_{ij} で割り切れないものが存在すれぱ, A と対等な行列 B であって, $v(B)<v(A)$ となるものが存在する.

∴ 1° によって, 初めから $v(a_{11})=v(A)$ として構わない. もし A の第 1 行または第 1 列の成分で a_{11} で割り切れないものが存在するときは 3° により成り立つ. そこで A の第 1 行および第 1 列の成分はすべて a_{11} で割り切れる場合を考えればよい. そして a_{kl} $(k,l>1)$ が a_{11} で割り切れないとする. このとき, 行列 A に操作 $\boxed{1}+\boxed{l}\times 1$ を行った結果の行列を C とすれば C の $(k,1)$ 成分は $a_{k1}+a_{kl}$ である. a_{k1} は a_{11} で割り切れ, a_{kl} は割り切れないので, $a_{k1}+a_{kl}$ も a_{11} で割り切れない. よって, 3° に帰着する,

5° $A\neq O$ ならぱ, A と対等な行列 B であって, その一つの成分 b_{ij} が他のすべての成分を割り切るようなるのが存在する.

∴ $v(A)=v(a_{ij})$ となる A の成分 a_{ij} を取る. a_{ij} が A の他のすべての成分を割り切るときは, $B=A$ とすればよい. そうでなければ 4° により $v(B)<v(A)$ なる行列 B で A に対等なるものがある. そこで上の A の代りに B を取って考えれば, B の一つの成分が B のすべての成分を割り切るか, $v(C)<v(B)$ となる行列 C と B は対等になる. 以下これを繰り返せぱよい. $v(A)$ は非負整数だからこの操作は有限回の後に終り, A に対等な行列でその一つの成分 a_{ij} で他のすべての成分が切れるものが得られる.[1]

6° $A\neq O$ ならぱ A と対等な行列 B で次の (1),(2),(3) をみたすものが存在する.

(1) $b_{11}\neq 0$.
(2) $b_{i1}=b_{1j}=0$ $(i>1, j>1)$.
(3) b_{11} は b_{ij} $(i>1, j>1)$ を割り切る.

5° により A と対等な C で, c_{ij} が C の他のすべての要素を割り切るものが存在する. このとき, 1° により C の行, 列を入れ換えて C_{ij} を (1,1) 要素とする行列 D を作る. このとき D は A と対等で, d_{11} はすべての d_{ij} を割り切る. 次に 2° により D と対等な行列 B で上の (1), (2) をみたするのが存在する. このとき B は (3) をもみたす.

7° 6° により (m,n) 型の行列

$$A=\left(\begin{array}{c|ccc} a_{11} & a_{12} & \cdots & a_{1n} \\ \hline a_{21} & & & \\ \vdots & & A' & \\ a_{m1} & & & \end{array}\right)$$

[1] valuation の性質 $v(xy)\geq v(x)$ により $v(a_{ij})=v(A)$ である.

は

$$B = \left(\begin{array}{c|ccc} b_{11} & 0 & \dots & 0 \\ \hline 0 & & & \\ \vdots & & B' & \\ 0 & & & \end{array}\right)$$

と対等であることが示された. ここで B' の全ての成分は b_{11} で割り切れる. A の代りに B を考えて, この議論を続けて行けば有限回でスミス標準形に到達する. □

例 7.4.2.

$$A = \begin{pmatrix} 3 & -1 & -1 & -1 \\ -1 & 3 & -1 & -1 \\ -1 & -1 & 3 & -1 \\ -1 & -1 & -1 & 3 \end{pmatrix}$$

のとき, 標準形を求めよう. A に, 次々と, はきだし法を適用すると

3	−1	−1	−1	① ↔ ④
−1	3	−1	−1	
−1	−1	3	−1	
−1	−1	−1	3	
−1	−1	−1	3	① × (−1)
−1	3	−1	−1	
−1	−1	3	−1	
3	−1	−1	−1	
1	1	1	−3	
−1	3	−1	−1	② + ① × 1
−1	−1	3	−1	③ + ① × 1
3	−1	−1	−1	④ + ① × (−3)
1	1	1	−3	
0	4	0	−4	[2] + [1] × (−1)
0	0	4	−4	[3] + [1] × (−1)
0	−4	−4	8	[4] + [1] × 3
1	0	0	0	
0	4	0	−4	
0	0	4	−4	
0	−4	−4	8	④ + ② × 1
1	0	0	0	
0	4	0	−4	[4] + [2] × 1
0	0	4	−4	
0	0	−4	4	
1	0	0	0	
0	4	0	0	
0	0	4	−4	
0	0	−4	4	④ + ③ × 1
1	0	0	0	
0	4	0	0	[4] + [3] × 1
0	0	4	−4	
0	0	0	0	

で, 標準形は

$$B = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

となる.

系 7.4.3. R がユークリッド整域のとき, 任意の正則行列 $A \in \mathrm{GL}_n(R)$ は基本変形行列 $P_n(i,j)$, $Q_n(i;c)$ $(c \in R^\times)$, $R_n(i,j,a)$ $(a \in R)$ の積として表わされる.

証明. R がユークリッド整域のとき, $A \in \mathrm{M}_n(R)$ に対して, 定理 7.4.1 により,

$$P_k \cdots P_1 A Q_1 \cdots Q_l = B$$

となるような基本変形行列 $P_1, \ldots, P_k, Q_1, \ldots, Q_l$ が存在する. これらの基本変形行列は, $P_n(i,j)$, $Q_n(i;c)$ $(c \in R^\times)$, $R_n(i,j,a)$ $(a \in R)$ のどれかである. $\det B \in R^\times$ より, $r = n$ で, $e_1, \ldots, e_r \in R^\times$ がわかる.

7.5 スミス標準形の一意性

整域 R において, 任意の 2 つの 0 でない元が最大公約元 (greatest common divisor; GCD) をもつとき, **GCD 整域 (GCD domain)** という.[2] この条件は, 任意の 0 でない元が最小公倍元 (least common multiple; LCM) をもつことと同値である.

$$R \text{ はユークリッド整域} \Rightarrow R \text{ は単項イデアル整域} \Rightarrow R \text{ は一意分解整域} \Rightarrow R \text{ は GCD 整域}$$

が成り立つ.

問題 7.5.1. R が一意分解整域ならば GCD 整域であることを示せ.

定義 7.5.2. R を GCD 整域とする. $A \in \mathrm{M}_{m,n}(R)$ の k 次の小行列式全体の最大公約元を $d_k(A)$ と書く. すなわち

$$d_k(A) = \gcd\left\{ \det A^{i_1 \cdots i_k}_{j_1 \cdots j_k} \,|\, 1 \le i_1 < \cdots < i_k \le m,\ 1 \le j_1 < \cdots < j_k \le n \right\}$$

ただし, k 次の小行列式がすべて 0 のときは $d_k(A) = 0$ とする.

例 7.5.3.

$$A = \begin{pmatrix} 2 & -1 & -1 \\ -1 & 2 & -1 \\ -1 & -1 & 2 \end{pmatrix}$$

のとき, $d_1(A) = \gcd(2,-1) = 1$,

$$\det A^{12}_{12} = 3, \quad \det A^{12}_{13} = -3, \quad \det A^{12}_{23} = 3, \quad \det A^{13}_{12} = -3, \quad \det A^{13}_{13} = 3$$
$$\det A^{13}_{23} = -3, \quad \det A^{23}_{12} = 3, \quad \det A^{23}_{13} = -3, \quad \det A^{23}_{23} = 3$$

より $d_2(A) = 3$ である. $\det A^{123}_{123} = 0$ より $d_3(A) = 0$ である.

補題 7.5.4. R を GCD 整域とする. $A, B \in \mathrm{M}_{m,n}(R)$ を $m \times n$ 行列とする. 正則行列 $P \in \mathrm{M}_m(R)$, $Q \in \mathrm{M}_n(R)$ があって

$$B = PAQ$$

であるとき, $d_k(A) \approx d_k(B)$ である. ここで, $1 \le k \le \min(m,n)$ とする.

---

[2] $a, b \in R$ のとき, d が
(1) $d|a$ かつ $d|b$
(2) $c|a$ かつ $c|b$ ならば $c|d$
をみたすとき, d を a, b の**最大公約元 (greatest common divisor)** という. 同様に, l が
(1) $a|l$ かつ $b|l$
(2) $a|x$ かつ $b|x$ ならば $l|x$
をみたすとき l を a, b の**最小公倍元 (least common multiple)** という.

証明. $A=(a_{ij})$, $B=(b_{ij})$, $P=(p_{ij})$, $Q=(q_{ij})$ とすると

$$b_{ij}=\sum_{r=1}^{m}\sum_{s=1}^{n}p_{ir}a_{rs}q_{sj}$$

である. $1\leq i_1<\cdots<i_k\leq m$ と $1\leq j_1<\cdots<j_k\leq n$ を固定して $\det B^{i_1,\ldots,i_k}_{j_1,\ldots,j_k}$ を考える. 右辺を $P(AQ)$ と考えて Theorem 7.3.1 を使うと

$$\det B^{i_1,\ldots,i_k}_{j_1,\ldots,j_k}=\sum_{1\leq r_1<\cdots<r_k\leq m}\det P^{i_1,\ldots,i_k}_{r_1,\ldots,r_k}\det(AQ)^{r_1,\ldots,r_k}_{j_1,\ldots,j_k}$$

ここで, $\det(AQ)^{r_1,\ldots,r_k}_{j_1,\ldots,j_k}$ に再び Theorem 7.3.1 を使うと

$$\det B^{i_1,\ldots,i_k}_{j_1,\ldots,j_k}=\sum_{1\leq r_1<\cdots<r_k\leq m}\sum_{1\leq s_1<\cdots<s_k\leq n}\det P^{i_1,\ldots,i_k}_{r_1,\ldots,s_k}\det A^{r_1,\ldots,r_k}_{s_1,\ldots,s_k}\det Q^{s_1,\ldots,s_k}_{j_1,\ldots,j_k}$$

となる. ここで $d|\det A^{r_1,\ldots,r_k}_{s_1,\ldots,s_k}$ なので $d|\det B^{i_1,\ldots,i_k}_{j_1,\ldots,j_k}$ となり, $d|d'$ である. 一方, $A=P^{-1}BQ^{-1}$ なので, 同様にして $d'|d$ が得られる. したがって $d\approx d'$ である. □

定理 7.5.5. R をユークリッド整域とする. $A\in\mathrm{M}_{m,n}(R)$ のスミス標準形

$$B=\begin{pmatrix}e_1&&&&&&\\&e_2&&&&&\\&&\ddots&&&&\\&&&e_r&&&\\&&&&0&&\\&&&&&\ddots&\\&&&&&&0\end{pmatrix}\tag{7.5.1}$$

(ここで $e_i\neq 0$ $(1\leq i\leq r)$ かつ $e_i|e_{i+1}$ $(1\leq i<r)$ である) ば一意的である. すなわち, 単因子 $e_1,\ldots,e_r$ は A により, 単元倍を除いて一意的に定まる. このとき $d_k(x)=e_1e_2\cdots e_k$ である.

7.6 スミス標準形

ここでは, 上の標準形を, 一般の単位的可換環 R 上で考察する. そのために, 上の $e_i|e_{i+1}$ $(1\leq i<r)$ という条件を $(e_i)\supseteq(e_{i+1})$ $(1\leq i<r)$ という条件に置き換える.

定義 7.6.1. R を単位的可換環とし, $A\in\mathrm{M}_{m,n}(R)$ とする. A と対等な行列 $B\in\mathrm{M}_{m,n}(R)$ で, 次の形の対角行列が存在するとき, この B を A の**スミス標準形 (Smith Normal Form)** という.[3]

$$B=\begin{pmatrix}e_1&&&&&&\\&e_2&&&&&\\&&\ddots&&&&\\&&&e_r&&&\\&&&&0&&\\&&&&&\ddots&\\&&&&&&0\end{pmatrix}\tag{7.6.1}$$

ここで $e_i\neq 0$ $(1\leq i\leq r)$ かつ $(e_i)\supseteq(e_{i+1})$ $(1\leq i<r)$ である. このとき 0 でない対角成分 $e_1,\ldots,e_r$ を A の**単因子 (elementary divisors)** といい, 単因子の数を A の**階数 (rank)** という.

定理 7.6.2. R を単項イデアル整域とする. このとき, 任意の行列 $A\in\mathrm{M}_{m,n}(R)$ に対して, それと対等な上の意味でのスミス標準形が存在する. また, 単因子 $e_1,\ldots,e_r$ は A により, 単元倍を除いて一意的に定まる. このとき $d_k(x)=e_1e_2\cdots e_k$ である.

[3] $R=\mathbb{Z}$ の場合は Smith, Henry J. Stephen (1861). "On systems of linear indeterminate equations and congruences". *Phil. Trans. R. Soc. Lond.* **151** (1): 293–326.

ここでは, 証明を省略するが, 上の定理を証明するには, (L1), (L2), (L3), (R1), (R2), (R3) 以外に (L4), (R4) の基本変形を使う必要がある. したがって, 系 7.4.3 の代わりに, 次の系をえる.

系 7.6.3. R が単項イデアル整域のとき, 任意の正則行列 $A \in \mathrm{GL}_n(R)$ は基本変形行列 $P_n(i,j)$, $Q_n(i;c)$ $(c \in R^\times)$, $R_n(i,j,a)$ $(a \in R)$, $S_n(i,j;\alpha,\beta,\gamma,\delta)$ $(\alpha,\beta,\gamma,\delta \in R^\times)$ の積として表わされる.

定理 7.6.2 は古典的な結果であるが, 最近では以下のようなさらなる一般化もある.

定義 7.6.4. R を単位的可換環とする.

(1) R 上の任意の行列 $A \in \mathrm{M}_{m,n}(R)$ に対して, そのスミス標準形が必ず存在するような環 R を**単因子環 (elementary divisor ring)** ということにする.

(2) R 上の任意の $(1,2)$ 型の行列 $A \in \mathrm{M}_{1,2}(R)$ (または $(2,1)$ 型の行列 $A \in \mathrm{M}_{2,1}(R)$) に対して, そのスミス標準形が必ず存在するような環 R を**エルミート環 (Hermite ring)** ということにする.

(3) R において, 任意の 2 つの単項イデアルの和が単項イデアルになるとき, **ベズー環 (Bézout ring)** という. この条件は, 任意の有限生成イデアルが単項イデアルであることと同値である.

(4) R において, イデアルの昇鎖条件 (ascending chain condition)

任意のイデアルの昇鎖
$$I_1 \subseteq \cdots \subseteq I_{k-1} \subseteq I_k \subseteq I_{k+1} \subseteq \cdots$$
に対して, ある n が存在して
$$I_n = I_{n+1} = \cdots$$
となる

が満たされるとき, R を**ネーター環 (Noetherian Ring)** という.

(5) R において, イデアルの降鎖条件 (descending chain condition)

任意のイデアルの降鎖
$$I_1 \supseteq \cdots \supseteq I_{k-1} \supseteq I_k \supseteq I_{k+1} \supseteq \cdots$$
に対して, ある n が存在して
$$I_n = I_{n+1} = \cdots$$
となる

が満たされるとき, R を**アルティン環 (Artinian ring)** という.

(6) R において, 単項イデアルが等しい, すなわち $(a) = (b)$ が成り立つならば単元 $u \in R^\times$ が存在して $b = au$ となるとき, R を **同伴環 (associate ring)** という.

問題 7.6.5. R が単項イデアル整域ならば Bézout 整域であることを示せ.

問題 7.6.6. R が Bézout 整域ならば GCD 整域であることを示せ.

問題 7.6.7. R が GCD domain $\Leftrightarrow$ 任意の R の 0 でない 2 つの元が最小公倍元をもつ

問題 7.6.8. R が単項イデアル整域 $\Leftrightarrow$ R はネーター環かつ Bézout 整域

定理 7.6.9. R を単位的可換環とする.

(1) R がエルミート環ならば R は Bézout 環である.

(2) R 上の任意の対角行列がスミス標準形にできる必要十分条件は R が Bézout 環であることである.

(3) R が単因子環であるための必要十分条件は次の (i), (ii) が成り立つことである:

(i) R は Bézout 環

(ii) 任意の $a,b,c \in R$ について $(a,b,c) = R$ ならば $p,q \in R$ が存在して $(pa, pb+qc) = R$ となる.

(4) R が同伴環ならば, $A \in \mathrm{M}_{m,n}(R)$ と対等なスミス標準形 B に表われる単因子は単元倍を除いて一意に決まる.

証明. (1) [2, p.465] R がエルミート環ならば, 任意の 1×2 行列がスミス標準形が存在するので, $^\forall a,b \in R$ に対して, $^\exists d \in R$ と $\alpha\delta - \beta\gamma \in R^\times$ である $^\exists \alpha,\beta,\gamma,\delta \in R$ が存在して

$$\begin{pmatrix} a & b \end{pmatrix}\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} d & 0 \end{pmatrix}$$

となる. よって $d = a\alpha + b\gamma \in (a)+(b)$ なので $(d) \subseteq (a)+(b)$ である. 一方, 右から逆行列をかけると

$$\begin{pmatrix} a & b \end{pmatrix} = \begin{pmatrix} d & 0 \end{pmatrix}\begin{pmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{pmatrix}$$

となるので $a = d\alpha'$, $b = d\beta'$ となり, $a \in (d)$ かつ $b \in (d)$ より $(a)+(b) \subseteq (d)$ である. したがって, $^\forall a,b \in R$ に対して, $^\exists d \in R$ が存在して $(a)+(b) = (d)$ となるので, Bézout 環である.

(2) [4, (3.1)] (必要性) 任意の $^\forall a,b \in R$ に対して, $(d) \supseteq (e)$ であるような $^\exists d,e \in R$ が存在して対角行列 $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ がスミス標準形

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \sim \begin{pmatrix} d & 0 \\ 0 & e \end{pmatrix}$$

になったとする. このとき, $(a,b) = (d,e) = (d)$ なので, R は Bezout 環である.

(十分性) 十分性を示すために, R を Bezout 環とし, m に関する帰納法で A が $m\times n$ 対角行列ならばスミス標準形にできることを示す. $m = 1$ のときは示すことはない. $m > 1$ として,

$$A \sim \begin{pmatrix} a & 0 \\ 0 & A_1 \end{pmatrix}$$

とする. ここで A_1 は $(m-1)\times(n-1)$ 対角行列とする. 帰納法の仮定より, A_1 は次のようなスミス標準形にできる:

$$A_1 \sim \begin{pmatrix} c_1 & 0 & \dots & 0 \\ 0 & c_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \dots & \dots & \end{pmatrix}$$

ここで $(c_i) \supseteq (c_{i+1})$ である. ここで $d \in R$ を $(d) = (a, c_1)$ とすれば, $d = ma + nc_1$, $a = da'$ and $c_1 = dc_1'$ となる $m,n,a',c_1' \in R$ が存在する. このとき, 基本変形によって

$$\begin{pmatrix} a & 0 \\ 0 & c_1 \end{pmatrix} \sim \begin{pmatrix} a & ma+nc_1 \\ 0 & c_1 \end{pmatrix} \sim \begin{pmatrix} d & a \\ c_1 & 0 \end{pmatrix} \sim \begin{pmatrix} d & 0 \\ 0 & -a'c_1 \end{pmatrix}$$

と変形できるので, A は次のような行列と対等になる:

$$A \sim \begin{pmatrix} d & 0 & 0 & \dots & 0 \\ 0 & -a'c_1 & 0 & \dots & 0 \\ 0 & 0 & c_2 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \dots & \end{pmatrix}$$

d は c_1 を割り切るので, d は対角成分の全てを割り切らなければならない. 再び, 帰納法を第 1 行と第 1 列を除いた行列に適用すれば, 求める形に変形できることが証明できる.

(3) [2, Theorem 5.2] (必要性) R が単因子環ならば Hermite 環なので Bézout 環である. (ii) が成り立つことを示すために, $(a,b,c)=R$ となる $a,b,c\in R$ に対して

$$A=\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \tag{7.6.2}$$

とおき, PAQ を A のスミス標準形とする. PAQ の $(1,1)$ 成分は単元 u になることは明らかである. P の第 1 行が p,q で Q の第 1 列が x,y としよう. このとき, $pax+pby+qcy=u$ なので, $(pa,pb+qc)=1$ となり (ii) が成り立つ.

(十分性) 次に, 十分性を示すために, まず R がエルミート環であることを示す. $\begin{pmatrix} a & b \end{pmatrix}$ を任意の 1×2 行列として, $(a)+(b)=(d)$ となる $d\in R$ を取ると, $ap+bq=d$, $a=sd$, $b=-rd$ となる $p,q,r,s\in R$ が存在する. よって $d(ps-qr-l)=0$ である. We dismiss the cased = 0, and thus have that $ps-qr$ is a unit. The observation (6) completes the proof. It was remarked in § 2 that diagonal To prove the sufficiency we first observe (Theorem 3.2) that R is an Hermite ring. Given a 2 by 2 matrix, we may thus arrange to get a zero, say in the lower left corner. We thus reach the matrix A of (7.6.2). Write $(a,b,c)=d$, $d=xa+yb+zc$, $a=axd$, $b=bxd$, $c=Cxd$. We dismiss the case $d=0$ and thus find that $xax+ybx+zcx$ is a unit ; without loss of generality we may change notation and assume $(a,b,c)=1$. We now take the p and q offered us in hypothesis $(*)$, observe that necessarily $(p,q)=1$, complete the row p, q to a unimodular matrix, and use it to left-multiply A. The result is a matrix with pa, $pb+qc$ for its first row. Right multiplication by a suitable unimodular matrix converts this to $1,0$. We sweep out the element in the lower left corner and thus complete the reduction.

(4) □

7.7 砂山モデル (Abelian sandpile model)

この節では, 単因子論の応用として Abelian sandpile model というものを紹介する.

7.7.1 グラフ理論事始め

定義 7.7.1. グラフ **(Graph)** とは，点の集合 V と二点間を結ぶ辺 (二点の集合) の集合 E のペアで，$G=(V,E)$ と表す. 点のことを**頂点 (vertex)**，二点の集合のことを**辺 (edge)** と呼ぶ.

例えば $V=\{1,2,3,4\}$, $E=\{\{1,2\},\{1,3\},\{2,3\},\{2,4\},\{3,4\}\}$ のとき G は, 図 7.7.1 のようになる.

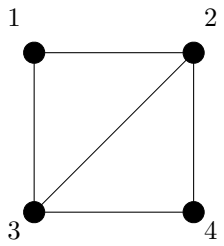

図 7.7.1: グラフ $G=(V,E)$

定義 7.7.2. $G=(V,E)$ をグラフとする.

(1) $v\in V$ に対して, 頂点 v から出ている辺の本数 $\deg v=\{\,u\,|\,\{u,v\}\in E\,\}$ を v の**次数 (degree)** という.
(2) どの頂点からどの頂点へも辺を伝っていくことができるようなグラフを**連結 (connected)** という.
(3) 頂点の列 $(v_1,v_2,\dots,v_r)$ で $\{v_i,v_{i+1}\}\in E$ $(i=1,2,\dots,r-1)$ となるものを**道 (path)** という.
(4) 道 $(v_1,v_2,\dots,v_r)$ が $v_0=v_r$ となるとき, **閉路 (cycle)** という.
(5) 2 つのグラフ $G=(V,E)$ と $G'=(V',E')$ について, G' の頂点集合と辺集合が共に G の頂点集合と辺集合の部分集合になっているとき, (i.e., $V'\subseteq V$ かつ $E'\subseteq E$ のとき) G' は G の**部分グラフ (subgraph)** であるという.

定義 7.7.3. (1) 閉路が存在しない連結なグラフを**木 (tree)** という.

(2) 連結グラフ $G = (V, E)$ の全ての点を通る部分グラフ $G' = (V, E')$ で木であるものを**全域木 (spanning tree)** という.

(3) 全ての頂点間に辺が引かれているグラフを**完全グラフ (complete graph)** という. 頂点数 n の完全グラフを K_n と書く

(4) 頂点が二つのグループに分かれており, 異なるグループの頂点間にのみ辺が引かれているグラフを**二部グラフ (bipertite graph)** という.

(5) 二部グラフで, 異なるグループの頂点間には全て辺が引かれているグラフを**完全二部グラフ (complete bipertite graph)** という. グループの頂点数がそれぞれ m, n である完全二部グラフを $K_{m,n}$ と書く

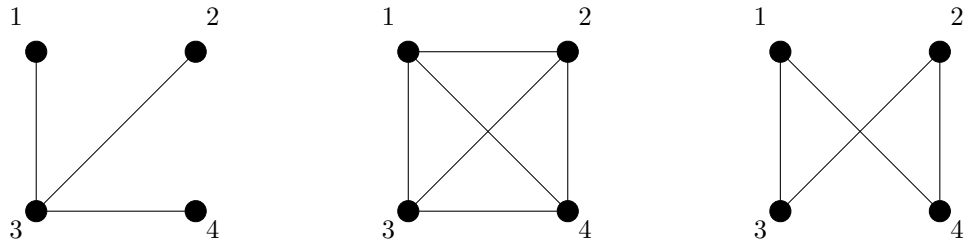

図 7.7.2: 木, 完全グラフ K_4, 及び, 完全二部グラフ $K_{2,2}$

7.7.2 砂山モデルって何？ (;･ ∀ ･)

連結な有限グラフ $G = (V, E)$ が与えられたとき, グラフの各頂点にいくつかの賭けコイン (chip) を置いた図形 σ を**コイン配置 (configuration)** という. すなわち, $\sigma : V \to \mathbb{N} = \{0, 1, 2, \dots\}$ は, 各頂点に非負整数を割り付ける関数である. 例えば, 図 7.7.1 のグラフの

$$\sigma(1) = 2, \qquad \sigma(2) = 4, \qquad \sigma(3) = 3, \qquad \sigma(4) = 0$$

というコイン配置は, 図 7.7.3 のように書くことにする. グラフ G のある頂点 v において $\sigma(v) \geq \deg(v)$ とする. 頂点 v に点

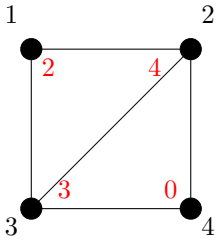

図 7.7.3: 図 7.7.1 のグラフのコイン配置

火する (firing) と, 現在のコイン配置の頂点の v のコインは, 辺によってそれに隣接した各頂点に送られ, 新しいコイン配置 τ が得られるとする. すなわち

$$\tau(u) = \begin{cases} \sigma(v) - \deg(v), & \text{if } u = v, \\ \sigma(u) + \mu(u, v), & \text{if } u \neq v. \end{cases}$$

である. ここで, $\mu(u, v)$ は u と v が隣接しているときは 1, 隣接していないときは 0 とする. (muliiple edge がないとする). 例えば, 図 7.7.3 のコイン配置 σ において頂点 2 を点火すると, コインは辺を通って隣接した頂点に移り

$$\tau(1) = 3, \qquad \tau(2) = 1, \qquad \tau(3) = 4, \qquad \tau(4) = 2$$

というコイン配置 τ を得る. これは, 図 7.7.4 のようになる. ここで G の頂点 w を選び, これを**コインの墓場 (sink)** としよう. この頂点 w に吸い込まれるコインはブラックホールのように二度と戻って来れないので, w のコインは無視することがで

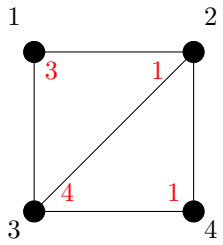

図 7.7.4: 図 7.7.3 のコイン配置 σ において頂点 2 を点火した結果のコイン配置 τ

きる. このようにして定義された**動的な系 (dynamical system)** を**砂山モデル (the abelian sandpile model)** ということにする. 頂点 v の点火は, v のコインがその次数 $\deg v$ 以上でないと出来ないことに注意しよう. **安定的コイン配置 (stable configuration)** とは点火できる頂点を持たないコイン配置のことである, i.e., $\sigma(v) < \deg(v)$ for $^\forall v \neq w$. 例えば, 図 7.7.4 のコイン配置で $w = 4$ をコインの墓場としよう. 図 7.7.4 のコイン配置は安定的ではないが, どのような連結の有限グラフのコイン配置も有限回の操作で安定的コイン配置に到達できるのは, 明らかであろう. 今後, コインの墓場 w を白丸で表し, w のコインの数は無視するので書かないことにする. 2 つ以上の頂点を点火できるとき, それらの操作は互いに可換で, それをやる順番に依存しないので最終的に到達する安定的コイン配置は最初の状態によって一意的に決まる. 例えば, 図 7.7.4 のコイン配置 τ

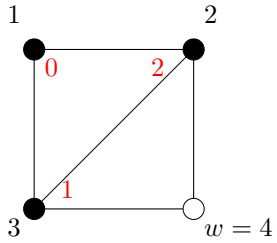

図 7.7.5: 図 7.7.3 のコイン配置 σ から得られる安定的コイン配置

において, さらに頂点の点火作業を続けていくと最終的に得られる安定的コイン配置は図 7.7.5 になる.

問題 7.7.4. 図 7.7.3 のコイン配置 σ から最終的に得られる安定的コイン配置が, 図 7.7.5 のようになることを示せ.

7.7.3 砂山モデルのモノイド構造

安定的コイン配置全体の集合を M とする. M 上の二項演算 $\oplus$ を次のように定義する. σ_1, σ_2 が安定的コイン配置のとき, $\sigma_1 \oplus \sigma_2$ は, σ_1 と σ_2 の各頂点のコイン数を頂点毎に足したあと, 次数以上のコインを持つ頂点に点火作業を行って得られる安定的コイン配置とする. この二項演算 $\oplus$ によって, M はモノイド (単位的半群) になる. モノイド M の**イデアル (ideal)** J とは, 部分集合 $J \subseteq M$ で, 任意の $\sigma \in M$ に対して $\sigma \oplus J \subseteq J$ となるものである. **砂山群 (sandpile group)** または **臨界群 (critical group)** $K(G)$ とは M の極小イデアル (minimal ideal), すなわち, 全てのイデアルの共通部分のことである. この砂山群 $K(G)$ は, コインの墓場 w をどの頂点に選ぶかに依存せず, 同型を除いて一意的に決まることが知られている.

問題 7.7.5. 有限な可換モノイド (単位的半群) の極小イデアルは群であることを示せ. [5]

例えば, 図 7.7.6 のような 1×1 格子のグラフにおいては, 各頂点の次数は 2 なので, 安定的コイン配置では, 各頂点におけるコインの枚数は $0, 1$ で, 全部で 2^3 個の状態がある. これらの間のモノイドとしての演算表は, 図 7.7.7 のようになる. コイン配置 σ を $\sigma(1)\sigma(2)\sigma(3)$ のような数字列で書くと, 演算表から $M = M000$ 以外のイデアルは

$$M100 = \{100, 110, 101, 011, 111\}$$
$$M010 = \{010, 100, 110, 101, 011, 111\}$$
$$M001 = \{001, 100, 110, 101, 011, 111\}$$
$$M110 = M101 = M011 = M111 = \{110, 101, 011, 111\}$$

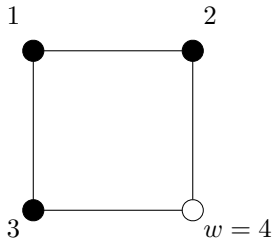

図 7.7.6: 1×1 格子 $G\ (V, E)$

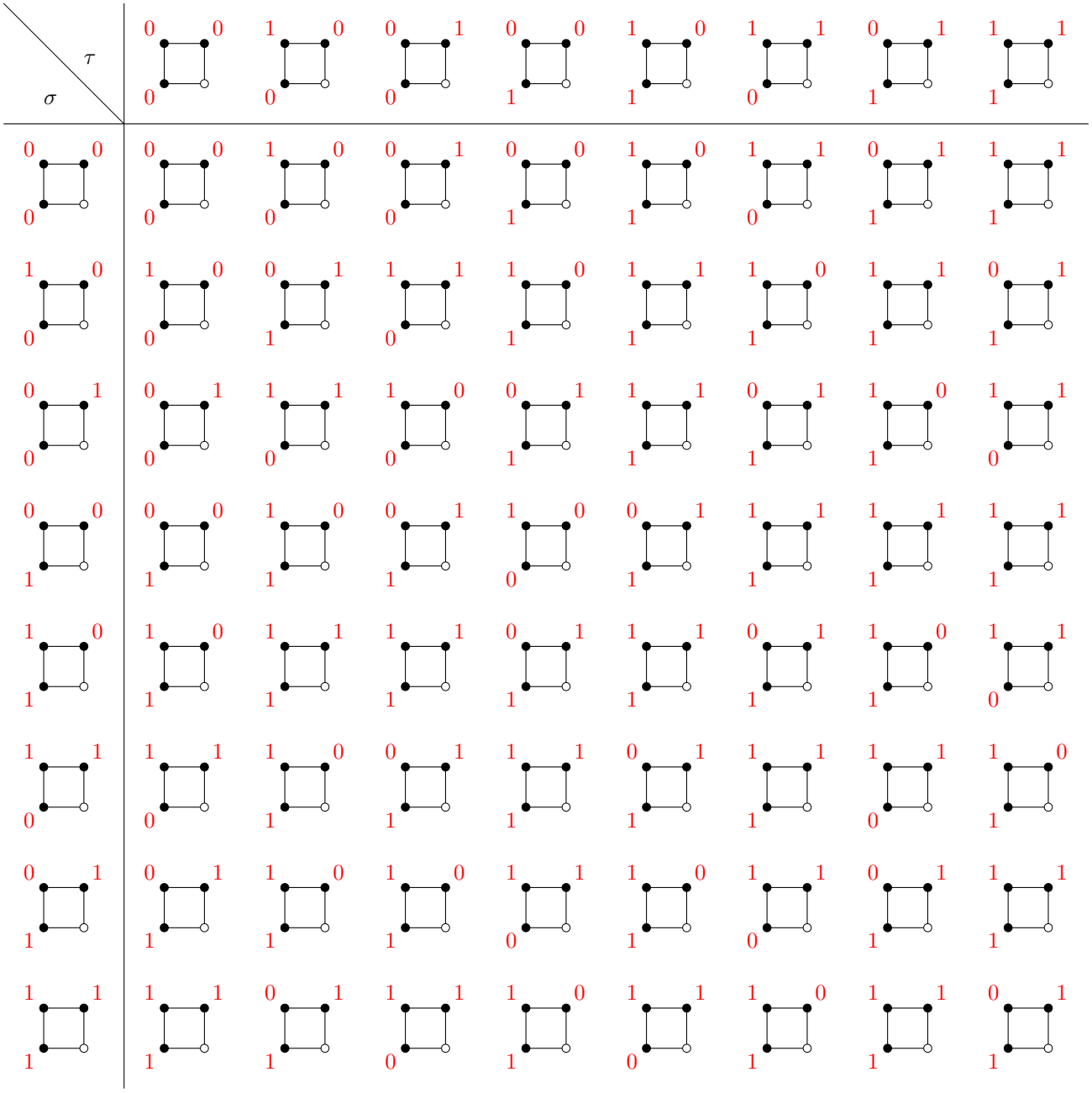

図 7.7.7: 図 7.7.6 のグラフの安定的コイン配置のなすモノイド M の演算 $\sigma \oplus \tau$

のみである. よって, 砂山群は

$$K(G) = \{101, 110, 011, 111\}$$

であり, 演算表は, 図 7.7.8 のようになる. 演算表から, この場合に単位元は $\sigma = 011$ である. 一般に, 砂山群 $K(G)$ の単位元が

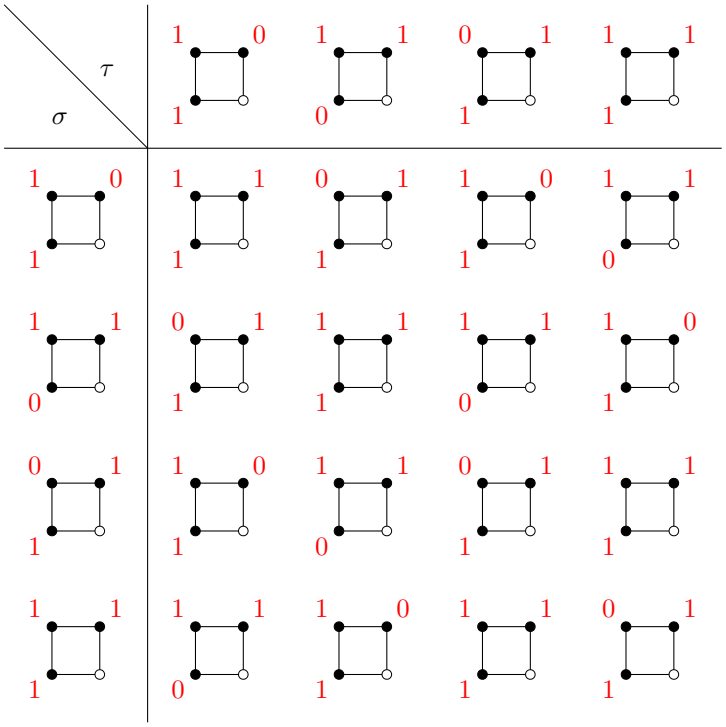

図 7.7.8: 図 7.7.6 のグラフの砂山群 $K(G)$ の演算 $\sigma \oplus \tau$

何になるのかは決して自明ではない. [5]

問題 7.7.6. 図 7.7.8 の演算表より

$$K(G) = \mathbb{Z}/4\mathbb{Z}$$

であることを示せ.

大きなグラフ $G = (V, E)$ の単位元になる安定的コイン配置 σ に対して $\sigma(v)$ の値によって頂点 $v \in V$ を色分けすると, 対称性の高い図形に」なることが多い. 例えば, 図 7.7.9 は 523×523 の正方格子に対応するグラフ $G = (V, E)$ に対して, その砂山群 $K(G)$ の単位元 σ の値を色分けしたもので, 境界の頂点をすべて同一視して, コインの墓場とする. また, 色分けは, 3 個の

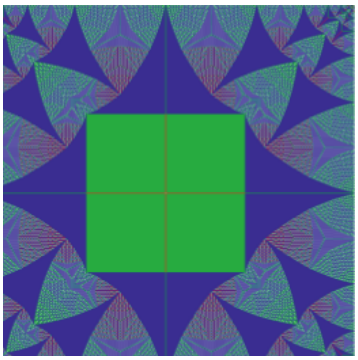

図 7.7.9: 523×523 の正方格子における砂山群 $K(G)$ の単位元

コインがあれば青, 2 個のコインがあれば緑, 1 個のコインがあれば赤, 0 個のコインがあればオレンジ色に色分けされている. (図は [5] からの引用). この形が, 砂山にできる紋様に似ていることから砂山群 (sandpile group) と呼ぶらしい.

問題 7.7.7. (難問)　完全グラフ K_n に対して

$$K(K_n) = (\mathbb{Z}/n\mathbb{Z})^{n-2}$$

となることを示せ.

問題 7.7.8. (難問)　完全二部グラフ $K_{m,n}$ び対して

$$K(K_{m,n}) = (\mathbb{Z}/mn\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})^{n-2} \times (\mathbb{Z}/n\mathbb{Z})^{m-2}$$

となることを示せ.

7.7.4　グラフのラプラス行列と単因子論

$G = (V, E)$ が連結な有限グラフとする. 頂点 u と v の間に辺があるときは $\mu(u, v) = 1$ で, ないときは $\mu(u, v) = 0$ とする. $\deg v$ は頂点 v の次数 (頂点 v に入る辺の個数) であった G の頂点 $u, v \in V$ を行と列の添字とする, 次のように定義される行列 $L = L(G) = (L_{uv})_{u,v\in V}$ を, グラフ G の**ラプラス行列 (Laplacian matrix)** という.

$$L_{uv} = \begin{cases} -\mu(u, v), & u \neq v \text{ のとき}, \\ \deg(v), & u = v \text{ のとき}. \end{cases}$$

例えば, 図 7.7.1 のグラフのラプラス行列は

$$L(G) = \begin{pmatrix} 2 & -1 & -1 & 0 \\ -1 & 3 & -1 & -1 \\ -1 & -1 & 3 & -1 \\ 0 & -1 & -1 & 2 \end{pmatrix}$$

である. 次数 $\deg v$ の定義から $L(G)$ の行ベクトルの和は 0 になり, 行ベクトルは線型従属なので $L(G)$ は正則行列ではない. $L_0 = L_0(G)$ を L からコインの墓場 (sink) になる頂点に対応する行と列を除いてできる行列とする. (本当は, 以下の議論は, どの頂点を除いてもよい). 有名な『木と行列の定理』 (Matrix-Tree Theorem) (e.g., [10, Thm. 5.6.8]) により

$$\det L_0 = \kappa(G),$$

は G の全域木 (spanning trees) の個数を与える. すなわちもし $\sharp V = n$ であり $L = L(G)$ の固有値が $\theta_1, \ldots, \theta_n$ であるとする. (ここで $\theta_n = 0$ としておく). このとき, 全域木 (spanning trees) の個数について $\kappa(G) = \theta_1 \cdots \theta_{n-1}/n$ が成り立つ. 例えば, 図 7.7.1 のグラフのラプラス行列については

$$\det L_0(G) = \det \begin{pmatrix} 2 & -1 & -1 \\ -1 & 3 & -1 \\ -1 & -1 & 3 \end{pmatrix} = 8$$

である. また, 図 7.7.6 のグラフのラプラス行列については

$$L(G) = \begin{pmatrix} 2 & -1 & -1 & 0 \\ -1 & 2 & 0 & -1 \\ -1 & 0 & 2 & -1 \\ 0 & -1 & -1 & 2 \end{pmatrix}, \qquad L_0(G) = \begin{pmatrix} 2 & -1 & -1 \\ -1 & 2 & 0 \\ -1 & 0 & 2 \end{pmatrix}$$

なので $\det L_0(G) = 4$ である. 図 7.7.6 のグラフのラプラス行列についてはその全域木は図 7.7.10 に挙げたとおりである.

問題 7.7.9. 図 7.7.1 のグラフの全域木を全てあげよ.

スミス標準形は行列式の一般化と考えることができる. なぜなら, 行列式の値は, 単因子の積と単元倍を除いて一致するからである. 一般に, 行列式を計算するよりもスミス標準形を計算する方が難しい. ここで, 行列 L と L_0 は有理整数環 $\mathbb{Z}$ 上の行列と考えてる. $L_0 \xrightarrow{\text{snf}} (\alpha_1, \ldots, \alpha_{n-1})$ と $L \xrightarrow{\text{snf}} (\alpha_1, \ldots, \alpha_{n-1}, 0)$ が同値であることは容易に示せる.

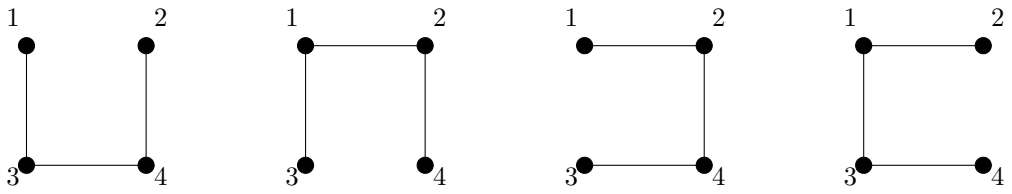

図 7.7.10: 図 7.7.6 のグラフの全域木

定理 7.7.10. $L_0(G)$ の単因子が $e_1, \ldots, e_{n-1}$ ならば, G の砂山群は

$$K(G) \simeq \mathbb{Z}/e_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/e_{n-1}\mathbb{Z}$$

である.

図 7.7.6 のグラフのラプラス行列のスミス標準形は

$$L_0(G) = \begin{pmatrix} 2 & -1 & -1 \\ -1 & 2 & 0 \\ -1 & 0 & 2 \end{pmatrix} \xrightarrow{\text{snf}} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 4 \end{pmatrix}$$

だから, 定理 7.7.10 を使って. 図 7.7.6 のグラフの砂山群は

$$K(G) \simeq \mathbb{Z}/4\mathbb{Z}$$

であることがわかる.

問題 7.7.11. 図 7.7.1 のグラフの砂山群を計算せよ.

第8章　R-加群の単因子論

8.1　R-加群再び

8.1.1　自由加群

定義 8.1.1. (独立)　R が (単位的) 環, M を左 R-加群とする. M の元の族 $\{x_\lambda\}_{\lambda\in\Lambda}$ に対して

$$\sum_i a_i x_{\lambda_i} \qquad \text{(有限和)}$$

の形の M の元を x_λ の一次結合という.

$$\sum_i a_i x_{\lambda_i} = 0 \Leftrightarrow \text{ すべての } a_i = 0$$

が成り立つならば $\{x_\lambda\}_{\lambda\in\Lambda}$ は**独立 (independent)** という.

定義 8.1.2. (自由加群)　R が (単位的) 環, M を左 R-加群とする. K が M の独立な集合で $RK = M$ のとき, K は M の**基底 (base)** という. M に基底が存在するとき, M を**自由 R-加群 (free R-module)** という.

注意 8.1.3. 一般には, 基底が存在するとは限らない. R が体のときは, 線形代数学で習うように, ベクトル空間には必ず基底が存在することを Zorn の補題を使って証明できる.

定理 8.1.4. R : 単項イデアル整域, M, N : R 上の有限生成自由加群のとき, R-準同型写像 $f : N \to M$ に対して, N, M の基底 $B_N = (\boldsymbol{v}_1, \ldots, v_n)$, $B_M = (\boldsymbol{u}_1, \ldots, \boldsymbol{u}_m)$ を適当に選べば, 次の条件をみたす:

(i) $f(\boldsymbol{v}_i) = e_i \boldsymbol{u}_i \quad (1 \le i \le r), \qquad f(\boldsymbol{v}_i) = 0 \quad (r < i \le n),$
(ii) $e_i | e_{i+1} \quad (1 \le i < r)$

証明. N, M の任意の基底 $B_N = (\boldsymbol{v}'_1, \ldots, v'_n)$, $B_M = (\boldsymbol{u}'_1, \ldots, \boldsymbol{u}'_m)$ に関する表現行列を $A = (a_{ij}) \in \mathrm{M}_{m,n}(R)$ とする. すなわち

$$(f(\boldsymbol{v}'_1), \ldots, f(v'_n)) = (\boldsymbol{u}'_1, \ldots, \boldsymbol{u}'_m)A$$

とする. 定理 7.4.1 により $P \in \mathrm{GL}_n(R)$, $Q \in \mathrm{GL}_m(R)$ が存在して

$$QAP = \begin{pmatrix} e_1 & & & & & & \\ & e_2 & & & & & \\ & & \ddots & & & & \\ & & & e_r & & & \\ & & & & 0 & & \\ & & & & & \ddots & \\ & & & & & & 0 \end{pmatrix} = B$$

とできる. ここで $e_i \neq 0$ $(1 \le i \le r)$ かつ $e_i | e_{i+1}$ $(1 \le i < r)$ である. ゆえに

$$(\boldsymbol{u}'_1, \ldots, \boldsymbol{u}'_m)Q^{-1} = (\boldsymbol{u}_1, \ldots, \boldsymbol{u}_m), \qquad (\boldsymbol{v}'_1, \ldots, v'_n)P = (\boldsymbol{v}_1, \ldots, v_n)$$

とおけば

$$(f(\boldsymbol{v}_1), \ldots, f(v_n)) = (\boldsymbol{u}_1, \ldots, \boldsymbol{u}_m)B$$

である. よって, 題意が成り立つ. □

定理 8.1.5. R を単項イデアル整域, M を R 上の階数 m の (有限生成) 自由加群とする. M の任意の部分 R-加群 N は, やはり、自由加群であって, その階数は $\leq m$ である.

証明. m に関する数学的帰納法で証明する. $m=0$ のときは自明である. $m\geq 1$ として, 階数が $m-1$ 以下の R-加群に関しては定理が成り立つと仮定する. M の基底を $(\boldsymbol{x}_1,\dots,\boldsymbol{x}_m)$ として, N を M の R-部分加群とする. $N=\{\boldsymbol{0}\}$ ならば定理は明らかなので, $N\neq\{\boldsymbol{0}\}$ とする. $y\in N$ は

$$y=a_1\boldsymbol{x}_1+\cdots+a_m\boldsymbol{x}_m \tag{8.1.1}$$

と一意的に書き表される. このとき, $f:N\to R,\ y\mapsto a_1$ は R-加群としての準同型写像であるから $f(N)$ は R のイデアルである. R は単項イデアル整域だから $f(N)=(b_1)$ となる $^\exists b_1\in R$ が存在する. また, $f(y_1)=b_1$ となる $^\exists\boldsymbol{y}_1\in N$ が存在する. このとき

$$\boldsymbol{y}_1=b_1\boldsymbol{x}_1+\cdots+b_m\boldsymbol{x}_m$$

としておく. また

$$M'=R\boldsymbol{x}_2+\cdots+R\boldsymbol{x}_m$$

とおくと, M' は階数 $m-1$ の自由 R-加群だから, 帰納法の仮定により, その部分加群 $N'=N\cap M'$ は, 階数が $\leq m-1$ の自由 R-加群である. よって N' の基底 $(\boldsymbol{y}_2,\dots,\boldsymbol{y}_l)$ $(l\leq m)$ を取ることができる.

まず $(\boldsymbol{y}_1,\boldsymbol{y}_2,\dots,\boldsymbol{y}_l)$ が N を生成することを示す.

$\therefore$ 任意の $^\forall\boldsymbol{y}=a_1\boldsymbol{x}_1+\cdots+a_m\boldsymbol{x}_m\in N$ に対して, $f(\boldsymbol{y})=a_1\in(b_1)$ だから $a_1=cb_1$ となる $^\exists c\in N$ が存在する. このとき,

$$\boldsymbol{y}-c\boldsymbol{y}_1=(a_2-cb_2)\boldsymbol{x}_2+\cdots+(a_m-cb_m)\boldsymbol{x}_m\in N'$$

だから $c_2,\dots,c_l\in R$ が存在して

$$\boldsymbol{y}-c\boldsymbol{y}_1=c_2\boldsymbol{y}_2+\cdots+c_l\boldsymbol{y}_l$$

と書ける.

$b_1=0$ のときは, $N=N'$ なので $(\boldsymbol{y}_2,\dots,\boldsymbol{y}_l)$ が自由加群 N の基底であり, 階数は $l-1\leq m-1$ である. よって $b_1\neq 0$ としてよい. このとき, $(\boldsymbol{y}_1,\boldsymbol{y}_2,\dots,\boldsymbol{y}_l)$ が線型独立であることを示す. もし,

$$c_1\boldsymbol{y}_1+c_2\boldsymbol{y}_2+\cdots+c_l\boldsymbol{y}_l=\boldsymbol{0}$$

が成り立つと仮定する. $c_2\boldsymbol{y}_2+\cdots+c_l\boldsymbol{y}_l\in N'$ だから $f(c_2\boldsymbol{y}_2+\cdots+c_l\boldsymbol{y}_l)=0$ なので, 上式に f を作用させると

$$c_1b_1=0$$

となる. R は整域で $b_1\neq 0$ より $c_1=0$ となる. したがって, $c_2\boldsymbol{y}_2+\cdots+c_l\boldsymbol{y}_l=\boldsymbol{0}$ となり, $(\boldsymbol{y}_2,\dots,\boldsymbol{y}_l)$ が基底であることから $c_2=\cdots=c_l=0$ が示される. したがって, N は自由加群で, その階数は $l\leq m$ であることが示された. □

系 8.1.6. 単項イデアル整域 R 上の自由 R-加群 M の階数は一意に決まる.

証明. M 自身を M の R-部分加群とみて定理 8.1.5 を適用せよ.

系 8.1.7. R を単項イデアル整域とする. 階数 m の自由 R-加群 M の R-部分加群 N の階数が r であるとき, M の基底 $B=(\boldsymbol{x}_1,\dots,\boldsymbol{x}_m)$ と $e_1,\dots,e_r\in R$ が存在して, 次が成り立つ.

(i) $e_i|e_{i+1}\quad(1\leq i<r)$
(ii) $(e_1\boldsymbol{x}_1,\dots,e_r\boldsymbol{x}_r)$ は N の基底である.

証明. N は定理 8.1.5 により自由 R-加群である. N の階数を r とする. $f:N\to M$ を $f(x)=x$ で定義すると, $\operatorname{rank}f=\dim N=r$ であるから, 定理 8.1.4 により, N の基底 $(\boldsymbol{y}_1,\dots,\boldsymbol{y}_r)$ と M の基底 $(\boldsymbol{x}_1,\dots,\boldsymbol{x}_m)$ が存在して

$$\boldsymbol{y}_i=e_i\boldsymbol{x}_i\quad(1\leq i\leq r),\qquad\qquad e_i|e_{i+1}\quad(1\leq i<r)$$

が成り立つ. よって, 題意が成り立つ.

問題 8.1.8. 次のベクトルで張られる $\mathbb{Z}^3$ の $\mathbb{Z}$-部分加群 $\mathbb{Z}\boldsymbol{v}_1+\mathbb{Z}\boldsymbol{v}_2+\mathbb{Z}\boldsymbol{v}_3$ を標準形を求めよ.

$$\boldsymbol{v}_1=\begin{pmatrix}1\\2\\3\end{pmatrix},\boldsymbol{v}_2=\begin{pmatrix}1\\1\\1\end{pmatrix},\boldsymbol{v}_3=\begin{pmatrix}-1\\0\\1\end{pmatrix}$$

また, $\mathbb{Z}\boldsymbol{v}_1+\mathbb{Z}\boldsymbol{v}_2+\mathbb{Z}\boldsymbol{v}_3$ の基底を求めよ.

解答 行列

$$\begin{pmatrix}1&1&1\\2&1&0\\3&1&-1\end{pmatrix},$$

のスミス標準形を掃出し法で求めると

1	1	1	1	0	0	1	0	0	
2	1	0	0	1	0	0	1	0	②$+$①$\times(-2)$
3	1	-1	0	0	1	0	0	1	③$+$①$\times(-3)$
1	1	1	1	0	0	1	0	0	
0	-1	-2	-2	1	0	0	1	0	[2]$+$[1]$\times(-1)$
0	-2	-4	-3	0	1	0	0	1	[3]$+$[1]$\times(-1)$
1	0	0	1	0	0	1	-1	-1	
0	-1	-2	-2	1	0	0	1	0	②$\times(-1)$
0	-2	-4	-3	0	1	0	0	1	
1	0	0	1	0	0	1	-1	-1	
0	1	2	2	-1	0	0	1	0	
0	-2	-4	-3	0	1	0	0	1	③$+$②$\times 2$
1	0	0	1	0	0	1	-1	-1	
0	1	2	2	-1	0	0	1	0	
0	0	0	1	-2	1	0	0	1	[3]$+$[2]$\times(-2)$
1	0	0	1	0	0	1	-1	-1	
0	1	0	2	-1	0	0	1	-2	
0	0	0	1	-2	1	0	0	1	

なので, スミス標準形は

$$B=\begin{pmatrix}1&0&0\\0&1&0\\0&0&0\end{pmatrix}$$

で

$$\begin{pmatrix}1&0&0\\2&-1&0\\1&-2&1\end{pmatrix}\begin{pmatrix}1&1&1\\2&1&0\\3&1&-1\end{pmatrix}\begin{pmatrix}1&-1&1\\0&1&-2\\0&0&1\end{pmatrix}=\begin{pmatrix}1&0&0\\0&1&0\\0&0&0\end{pmatrix}$$

となる. 左端と右端の行列の逆行列[1]を計算して

$$\begin{pmatrix}1&1&1\\2&1&0\\3&1&-1\end{pmatrix}=\begin{pmatrix}1&0&0\\2&-1&0\\3&-2&1\end{pmatrix}\begin{pmatrix}1&0&0\\0&1&0\\0&0&0\end{pmatrix}\begin{pmatrix}1&1&1\\0&1&2\\0&0&1\end{pmatrix}$$

と書き換えられる. よって

$$\boldsymbol{u}_1=\begin{pmatrix}1\\2\\3\end{pmatrix},\boldsymbol{u}_2=\begin{pmatrix}0\\-1\\-2\end{pmatrix},\boldsymbol{u}_3=\begin{pmatrix}0\\0\\1\end{pmatrix}$$

[1] これらの行列の行列式は単元である.

とおくと

$$a_1\boldsymbol{v}_1+a_2\boldsymbol{v}_2+a_3\boldsymbol{v}_3=\begin{pmatrix}1&1&1\\2&1&0\\3&1&-1\end{pmatrix}\begin{pmatrix}a_1\\a_2\\a_3\end{pmatrix}=\begin{pmatrix}1&0&0\\2&-1&0\\3&-2&1\end{pmatrix}\begin{pmatrix}1&0&0\\0&1&0\\0&0&0\end{pmatrix}\begin{pmatrix}1&1&1\\0&1&2\\0&0&1\end{pmatrix}\begin{pmatrix}a_1\\a_2\\a_3\end{pmatrix}$$
$$=\begin{pmatrix}1&0&0\\2&-1&0\\3&-2&1\end{pmatrix}\begin{pmatrix}a_1+a_2+a_3\\a_2+2\,a_3\\0\end{pmatrix}=(a_1+a_2+a_3)\boldsymbol{u}_1+(a_2+2\,a_3)\boldsymbol{u}_2$$

だから $\boldsymbol{u}_1$, $\boldsymbol{u}_2$ を基底とする自由 $\mathbb{Z}$-加群で, $\mathbb{Z}^2$ に同型である. □

定義 8.1.9. R が単位的可換環, M が R-加群のとき, $\boldsymbol{x}\in M$ に対して

$$A(\boldsymbol{x})=\{\,a\in R\,|\,a\boldsymbol{x}=\boldsymbol{0}\,\}$$

は R のイデアルであり, $A(\boldsymbol{x})$ を $\boldsymbol{x}$ に関する**零化イデアル (anihilator)** という. R が単項イデアル整域ならば $A(\boldsymbol{x})=(a)$ となる ${}^{\forall}a\in R$ が存在する. a を $\boldsymbol{x}$ の**周期**または**位数 (order)** という. $a\neq 0$ のとき $\boldsymbol{x}$ を**ねじれ元**といい, R 加群 V のすべての元がねじれ元であるとき, **ねじれ加群**という. $a=0$ のとき, $\boldsymbol{x}$ を**自由元**という. R 加群 V の 0 以外のすべての元が自由元であるとき, V を**ねじれなし**という. また一つの元から生成される R-加群を**巡回 R-加群**という.

命題 8.1.10. R を単項イデアル整域, M を有限生成な R-加群とするとき, 次が成り立つ.

(1) $\boldsymbol{x}\in M$ から生成される巡回 R-部分加群 $R\boldsymbol{x}$ は, $R/A(\boldsymbol{x})$ と同型である.
(2) 逆に R の任意のイデアル $\mathfrak{a}$ による商加群 $R/\mathfrak{a}$ は, 巡回 R-加群である.
(3) 単項イデアル整域 R 上の巡回 R-加群 N の部分加群はまた巡回 R-加群である.

証明. (1), (2) は易しいので自分で. (3) は (1), (2) より明らか. □

問題 8.1.11. 定理 8.1.10 の証明を述べよ.

定理 8.1.12 (有限生成 R-加群の構造定理)**.** R を単項イデアル整域, M を有限生成な R-加群とするとき, 次が成り立つ.

(i) M は有限個の 0 でない巡回 R-部分加群 M_i の直和となる.

$$M=M_1\oplus\cdots\oplus M_s$$

(ii) $M_i\simeq R/(a_i)\quad(1\leq i\leq s)$ であって, $a_i\in R$ は

$$a_i|a_{i+1}\quad(1\leq i<r),\qquad (a_i)\neq R$$

をみたす.

(iii) $a_i\neq 0\ (1\leq i\leq r),\quad a_j=0\ (r<i\leq s)$ とすれば $M_1\oplus\cdots\oplus M_r$ が M のねじれ部分で, $M_{r+1}\oplus\cdots\oplus M_s\simeq R^{s-r}$ は自由 R 加群である.

証明. M の有限個の生成元を $(\boldsymbol{x}_1,\ldots,\boldsymbol{x}_m)$ としよう. 同数の m 個の基底 $(\boldsymbol{v}_1,\ldots,\boldsymbol{v}_m)$ をもつ自由 R-加群 V を取り R-準同型写像 $f:V\to M$ を

$$f(a_1\boldsymbol{v}_1+\cdots+a_m\boldsymbol{v}_m)=a_1\boldsymbol{x}_1+\cdots+a_m\boldsymbol{x}_m$$

によって定義する. このとき, 準同型定理により

$$M\simeq V/\operatorname{Ker}f$$

である. $\operatorname{Ker}f$ は自由 R-加群 V の R-部分加群だから, 系 8.1.7 により, $\operatorname{Ker}f$ の階数を μ とするとき ${}^{\exists}e_1,\ldots,e_\mu\in R$ が存在して

$$(e_1\boldsymbol{v}_1,\ldots,e_\mu\boldsymbol{v}_\mu)$$

が $\operatorname{Ker}f$ の基底になり, $e_i|e_{i+1}\ (1\leq i<\mu)$ をみたす. よって

$$\operatorname{Ker}f=Re_1\boldsymbol{v}_1\oplus Re_2\boldsymbol{v}_2\oplus\cdots\oplus Re_\mu\boldsymbol{v}_\mu$$

とかける. このとき, $0 \le \lambda \le \mu$ が存在して $e_1, \dots, e_\lambda$ は単元, $e_{\lambda+1}, \dots, e_\mu$ は単元でないとしてよい. このとき,

$$M \simeq V/\operatorname{Ker} f \simeq \underbrace{R\boldsymbol{v}_1/Re_1\boldsymbol{v}_1 \oplus \cdots \oplus R\boldsymbol{v}_\lambda/Re_\lambda\boldsymbol{v}_\lambda}_{\lambda} \oplus \underbrace{R\boldsymbol{v}_{\lambda+1}/Re_{\lambda+1}\boldsymbol{v}_{\lambda+1} \oplus \cdots \oplus R\boldsymbol{v}_\mu/Re_\mu\boldsymbol{v}_\mu}_{t-\lambda} \oplus \underbrace{R\boldsymbol{v}_{\mu+1} \oplus \cdots \oplus R\boldsymbol{v}_m}_{m-\mu}$$

である. ここで e_i が単元のときは, $Re_i\boldsymbol{v}_i = R\boldsymbol{v}_i$ で $R\boldsymbol{v}_i/Re_i\boldsymbol{v}_i = 0$ $(1 \le i \le \lambda)$ である. また, $i > \mu$ のとき $e_{\mu+1} = \cdots = e_m = 0$ と定義しておくと $Re_i\boldsymbol{v}_i = \boldsymbol{0}$ で $R\boldsymbol{v}_i/Re_i\boldsymbol{v}_i = R\boldsymbol{v}_i$ $(\mu < i \le m)$ である. ゆえに

$$M \simeq V/\operatorname{Ker} f \simeq \underbrace{R\boldsymbol{v}_{\lambda+1}/Re_{\lambda+1}\boldsymbol{v}_{\lambda+1} \oplus \cdots \oplus R\boldsymbol{v}_\mu/Re_\mu\boldsymbol{v}_\mu}_{\mu-\lambda} \oplus \underbrace{R\boldsymbol{v}_{\mu+1}/Re_{\mu+1}\boldsymbol{v}_{\mu+1} \oplus \cdots \oplus R\boldsymbol{v}_m/Re_m\boldsymbol{v}_m}_{m-\mu}$$

である. よって, $r = \mu - \lambda$, $s = m - \mu$ とおくと (i), (ii) が証明される.

(iii) は (i), (ii) から簡単に証明される. □

問題 8.1.13. 定理 8.1.12 (iii) の証明を述べよ.

問題 8.1.14. 次で与えられる有限生成アーベル群 G の標準形と, その形の群への同型写像を具体的に構成せよ

$$G = \left\{ \begin{pmatrix} x \\ y \\ z \end{pmatrix} \in \mathbb{Z}^3 \,\middle|\, x - 3\,y - 2\,z = 0 \right\}$$

解答 G を $\mathbb{Z}$-加群と考えて $M = G$ と書く. $\mathbb{Z}$-準同型写像 $f : \mathbb{Z}^3 \to \mathbb{Z}$ を

$$f(x, y, z) = x - 3\,y - 2\,z$$

で定義すると, $\operatorname{Ker} f$ は自由 $\mathbb{Z}$-加群である.

$$\boldsymbol{e}_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \quad \boldsymbol{e}_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \quad \boldsymbol{e}_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$$

f の標準基底 $\boldsymbol{e}_1, \boldsymbol{e}_2, \boldsymbol{e}_3$ に関する表現行列は

$$\begin{pmatrix} f(\boldsymbol{e}_1) & f(\boldsymbol{e}_2) & f(\boldsymbol{e}_3) \end{pmatrix} = 1 \cdot \begin{pmatrix} 1 & -3 & -2 \end{pmatrix}$$

なので $A = \begin{pmatrix} 1 & -3 & -2 \end{pmatrix}$ である. A のスミス標準形を掃出し法で計算すると

1	−3	−2	1	1	0	0	
				0	1	0	[2] + [1] × 3
				0	0	1	[3] + [1] × 2
1	0	0	1	1	3	2	
				0	1	0	
				0	0	1	

なので, スミス標準形は $B = \begin{pmatrix} 1 & 0 & 0 \end{pmatrix}$ で

$$A \begin{pmatrix} 1 & 3 & 2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \end{pmatrix}$$

である. よって

$$\boldsymbol{v}_1 = \boldsymbol{e}_1, \qquad \boldsymbol{v}_2 = 3\,\boldsymbol{e}_1 + \boldsymbol{e}_2, \qquad \boldsymbol{v}_3 = 2\,\boldsymbol{e}_1 + \boldsymbol{e}_3$$

とおくと

$$\begin{pmatrix} f(\boldsymbol{v}_1) & f(\boldsymbol{v}_2) & f(\boldsymbol{v}_3) \end{pmatrix} = 1 \cdot \begin{pmatrix} 1 & 0 & 0 \end{pmatrix}$$

である. すなわち,

$$\operatorname{Ker} f = \mathbb{Z}\boldsymbol{v}_2 + \mathbb{Z}\boldsymbol{v}_3 \simeq \mathbb{Z}^2$$

である □

問題 8.1.15. 次で与えられる有限生成アーベル群 G の標準形と, その形の群への同型写像を具体的に構成せよ

$$G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$$

解答 G を $\mathbb{Z}$-加群と考えて $M = G$ と書く.

$$\boldsymbol{x}_1 = \begin{pmatrix} 1+2\mathbb{Z} \\ 0 \end{pmatrix}, \qquad \boldsymbol{x}_2 = \begin{pmatrix} 0 \\ 1+3\mathbb{Z} \end{pmatrix}$$

から生成される. 自由 $\mathbb{Z}$-加群 $V = \mathbb{Z} \oplus \mathbb{Z}$ の基底を

$$\boldsymbol{e}_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \qquad \boldsymbol{e}_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

とする. $\mathbb{Z}$-加群としての準同型写像 $f : V \to M$ を

$$f(\boldsymbol{e}_1) = \boldsymbol{x}_1, \qquad f(\boldsymbol{e}_2) = \boldsymbol{x}_2$$

によって定義すると, $N = \operatorname{Ker} f$ は

$$\boldsymbol{y}_1 = 2\boldsymbol{e}_1 = \begin{pmatrix} 2 \\ 0 \end{pmatrix}, \qquad \boldsymbol{y}_2 = 3\boldsymbol{e}_2 = \begin{pmatrix} 0 \\ 3 \end{pmatrix}$$

を基底とする自由 $\mathbb{Z}$-加群である. 系 8.1.7 の証明の中で述べたように自由 R-加群 N から自由 R-加群 M への R-準同型写像 $f : N \to M$, $x \mapsto x$ を N の基底 $(\boldsymbol{y}_1, \boldsymbol{y}_2)$ と M の基底 $(\boldsymbol{x}_1, \boldsymbol{x}_2, \boldsymbol{x}_3)$ に関する表現行列は

$$A = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}$$

である. A のスミス標準形を掃出し法で計算すると

2	0	1	0	1	0	① + ② × 1
0	3	0	1	0	1	
2	3	1	1	1	0	2 + 1 × (−1)
0	3	0	1	0	1	
2	1	1	1	1	−1	1 ↔ 2
0	3	0	1	0	1	
1	2	1	1	−1	1	
3	0	0	1	1	0	② + ① × (−3)
1	2	1	1	−1	1	
0	−6	−3	−2	1	0	② × (−1)
1	2	1	1	−1	1	2 + 1 × (−2)
0	6	3	2	1	0	
1	0	1	1	−1	3	
0	6	3	2	1	−2	

なので, スミス標準形は $B = \begin{pmatrix} 1 & 0 \\ 0 & 6 \end{pmatrix}$ で

$$\begin{pmatrix} 1 & 1 \\ 3 & 2 \end{pmatrix} A \begin{pmatrix} -1 & 3 \\ 1 & -2 \end{pmatrix} = B$$

である. $\begin{pmatrix} 1 & 1 \\ 3 & 2 \end{pmatrix}^{-1} = \begin{pmatrix} -2 & 1 \\ 3 & -1 \end{pmatrix}$ なので

$$A \begin{pmatrix} -1 & 3 \\ 1 & -2 \end{pmatrix} = \begin{pmatrix} -2 & 1 \\ 3 & -1 \end{pmatrix} B$$

と書き直すことができる. すなわち

$$\boldsymbol{y}_1' = -\boldsymbol{y}_1 + \boldsymbol{y}_2 = \begin{pmatrix} -2 \\ 3 \end{pmatrix}, \quad \boldsymbol{y}_2' = 3\boldsymbol{y}_1 - 2\boldsymbol{y}_2 = \begin{pmatrix} 6 \\ -6 \end{pmatrix}$$

は N の基底で,

$$M = V/\operatorname{Ker} f \simeq \mathbb{Z}/\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z} \simeq \mathbb{Z}/6\mathbb{Z}$$

である. 実際

$$\boldsymbol{x}_1' = -2\boldsymbol{x}_1 + 3\boldsymbol{x}_2 = \begin{pmatrix} 2\mathbb{Z} \\ 3\mathbb{Z} \end{pmatrix} = \boldsymbol{0}, \quad \boldsymbol{x}_2' = \boldsymbol{x}_1 - \boldsymbol{x}_2 = \begin{pmatrix} 1 + 2\mathbb{Z} \\ -1 + 3\mathbb{Z} \end{pmatrix}$$

なので, M は $\boldsymbol{x}_2'$ によって生成される位数 6 の巡回群である. □

問題 8.1.16. 次の連立 1 次方程式のすべての整数解を求めよ.

$$\begin{cases} 14\boldsymbol{x} - 4\,y - 8\,z = 18 & \cdots \quad ① \\ 32\boldsymbol{x} - 10\,y - 20\,z = 24 & \cdots \quad ② \\ 4\boldsymbol{x} - 2\,y - 4\,z = -12 & \cdots \quad ③ \end{cases}$$

解答 まず

$$\begin{cases} 14\boldsymbol{x} - 4\,y - 8\,z = 0 \\ 32\boldsymbol{x} - 10\,y - 20\,z = 0 \\ 4\boldsymbol{x} - 2\,y - 4\,z = 0 \end{cases}$$

の一般解を求める. 行列

$$A = \begin{pmatrix} 14 & -4 & -8 \\ 32 & -10 & -20 \\ 4 & -2 & -4 \end{pmatrix},$$

のスミス標準形を求めると

$$\begin{pmatrix} 1 & 0 & -3 \\ -1 & 0 & 2 \\ -2 & 1 & -1 \end{pmatrix} A \begin{pmatrix} 0 & -1 & 0 \\ 1 & 1 & -2 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 6 & 0 \\ 0 & 0 & 0 \end{pmatrix} = B$$

である. ここで $\begin{pmatrix} 1 & 0 & -3 \\ -1 & 0 & 2 \\ -2 & 1 & -1 \end{pmatrix}^{-1} = \begin{pmatrix} -2 & -3 & 0 \\ -5 & -7 & 1 \\ -1 & -1 & 0 \end{pmatrix}$ を使って, この式を

$$A \begin{pmatrix} 0 & -1 & 0 \\ 1 & 1 & -2 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} -2 & -3 & 0 \\ -5 & -7 & 1 \\ -1 & -1 & 0 \end{pmatrix} B$$

と書き換えることができる. よって, $\operatorname{Ker} f$ は階数 1 の自由 $\mathbb{Z}$-加群で

$$\operatorname{Ker} f = \mathbb{Z} \begin{pmatrix} 0 \\ -2 \\ 1 \end{pmatrix}$$

である.

一方, ① ② ③ の特殊解の 1 つを求める. ② + ③ × (−5) を行うと $12x = 84$ なので

$$x = 7 \quad \cdots \quad ④$$

である. よって, これを① ② ③ のいずれかに代入すると

$$y + 2\,z = 20 \quad \cdots \quad ⑤$$

をえる. ④ ⑤ をみたす特殊解の 1 つとして, 例えば

$$x = 7, \quad y = 0, \quad z = 10$$

が挙げられる. ゆえに① ② ③ の一般解は

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 7 \\ 0 \\ 10 \end{pmatrix} + \mathbb{Z} \begin{pmatrix} 0 \\ -2 \\ 1 \end{pmatrix}$$

である. □

関連図書

[1] 藤崎 源二郎, **体と** *Galois* **理論** *I*, 岩波講座 基礎数学, 岩波書店, 1977.

[2] I. Kaplansky, "Elementary divisors and modules", *Trans. Amer. Math. Soc.* **66** (1949), 464–491.

[3] 近藤 武, **群論** *I*, 岩波講座 基礎数学, 岩波書店, 1976.

[4] M.D. Larsen, W. J. Lewis, and T. S. Shores, "Elementary divisor rings and finitely presented modules", *Trans. Amer. Math. Soc.* **187** (1974), 231–248.

[5] L. Levine and J. Propp, "WHAT IS a sandpile?", *Notices Amer. Math. Soc.* **57** (2010), 976–979.

[6] 杉浦 光夫, *Jordan* **標準形と単因子論** *I*, 岩波講座 基礎数学, 岩波書店, 1977.

[7] 杉浦 光夫, *Jordan* **標準形と単因子論** *II*, 岩波講座 基礎数学, 岩波書店, 1977.

[8] Richard Stanley, "Smith Normal Form in Combinatorics" arXiv:1602.00166 [math.CO].

[9] Richard Stanley, *Enumerative Combinatorics*, vol. 1, second edition, Cambridge Studies in Advanced Mathematics, vol. 49, Cambridge University Press, Cambridge, 2012.

[10] Richard Stanley, *Enumerative Combinatorics*, vol. 2, Cambridge Studies in Advanced Mathematics, vol. 62, Cambridge University Press, Cambridge, 1999.