一意分解整域のノート

箱（@o_ccah）

2019 年 5 月 18 日

本稿の議論の主要なアイデアは，立腹層（@rippukusou）による．

1　可換モノイド

定義 1.1（モノイド）　集合に単位的かつ結合的な 2 項演算を与えたものを，**モノイド**という．モノイドは，その 2 項演算が可換であるとき，**可換**であるという．

特に断らない限り，モノイドの演算は乗法的に書き，その単位元は 1 と書く．モノイドの演算を加法的に書く場合には，その単位元は 0 と書く．

定義 1.2（モノイドの準同型・同型）　モノイドの間の写像は，それがモノイドの演算と単位元を保つとき，（モノイドの）**準同型**という．全単射なモノイドの準同型を，（モノイドの）**同型**という．モノイド M, N について，M から N への同型が存在するとき，M と N は**同型**であるといい，$M \cong N$ と書く．

以下，モノイドは可換なものしか考えない．可換モノイドの準同型・同型とは，可換モノイドの間のモノイドの準同型・同型のことである．

定義 1.3（消約可能性）　M を可換モノイドとする．任意の $a, b, c \in M$ に対して $ca = cb$ ならば $a = b$ が成り立つとき，M は**消約可能**であるという．

集合 Λ に対して

$$\mathbb{N}^{\oplus\Lambda} = \{(n_\lambda)_{\lambda\in\Lambda} \mid n_\lambda \in \mathbb{N},\ \text{有限個の } \lambda \in \Lambda \text{ を除いて } n_\lambda = 0\}$$

と定め，$\mathbb{N}^{\oplus\Lambda}$ に成分ごとの加法による 2 項演算を与えると，これは可換モノイドとなる．容易にわかるように，$\mathbb{N}^{\oplus\Lambda}$ は可換モノイドの圏における自由対象である．

定義 1.4（自由・生成・基底）　M を可換モノイド，$\{a_\lambda\}_{\lambda\in\Lambda}$ を M の元の族とする．

(1) 対応 $\lambda \mapsto a_\lambda$ から自然に定まる可換モノイドの準同型 $\mathbb{N}^{\oplus\Lambda} \to M$ が単射であるとき，$\{a_\lambda\}_{\lambda\in\Lambda}$ は（M において）**自由**であるという．
(2) 対応 $\lambda \mapsto a_\lambda$ から自然に定まる可換モノイドの準同型 $\mathbb{N}^{\oplus\Lambda} \to M$ が全射であるとき，$\{a_\lambda\}_{\lambda\in\Lambda}$ は M を**生成する**という．
(3) $\{a_\lambda\}_{\lambda\in\Lambda}$ が自由かつ M を生成するとき，$\{a_\lambda\}_{\lambda\in\Lambda}$ は M の**基底**であるという．

可換モノイド M の部分集合 S について「S は M において自由である」などといった場合，それは「M の元の族 $\{s\}_{s\in S}$ が M において自由である」という意味であるとする．

定義 1.5（自由可換モノイド） 基底をもつ可換モノイドは，（可換モノイドとして）**自由**であるという．

容易にわかるように，可換モノイド M が自由であるための必要十分条件は，ある Λ が存在して M が $\mathbb{N}^{\oplus\Lambda}$ と可換モノイドとして同型であることである．

2 順序型可換モノイド

定義 2.1（可換モノイド上の前順序） M を可換モノイドとする．M 上の関係 $\leq$ を，$a, b \in M$ に対して

$$a \leq b \iff \text{ある } c \in M \text{ が存在して } ca = b$$

と定めると，これは M 上の前順序（反射律と推移律を満たす関係）となる．この前順序 $\leq$ を，M の**代数的前順序**あるいは**整除関係**という．

定義 2.2（順序型可換モノイド） 可換モノイドは，その代数的前順序が順序（反射律，推移律，反対称律を満たす関係）であるとき，**順序型**であるという*[1]．

定義より，可換モノイド M が順序型であるための必要十分条件は，任意の $a, c, c' \in M$ に対して，$c'ca = a$ ならば $ca = a$ であることである．

順序型可換モノイド M において，$1 \in M$ は整除関係に関する最小限である．

可換モノイド M が順序型ならば，M の単元は 1 のみである．消約可能な可換モノイド M に対しては，M の単元が 1 のみならば，M は順序型である．また明らかに，自由可換モノイドは消約可能かつ順序型である．

3 順序型可換モノイドの既約元と素元

定義 3.1（順序型可換モノイドの既約元・素元） M を順序型可換モノイドとする．

(1) $M \setminus \{1\}$ の整除関係に関する極小元を，M の**既約元**という．M の既約元全体の集合を I_M と書く．
(2) $p \in M$ であって，任意の $a_0, \ldots, a_{n-1} \in M$ に対して，$p \leq a_0 \cdots a_{n-1}$ ならばある i が存在して $p \leq a_i$ であるものを，M の**素元**という．M の素元全体の集合を P_M と書く．

順序構造の一般論より，異なる既約元は整除関係に関して比較不能である．

命題 3.2 M を順序型可換モノイドとする．$S \subseteq M$ が M を生成するならば，S は I_M を含む．

証明 $S \subseteq M$ が M を生成するとする．任意の $a \in I_M$ は $s_0, \ldots, s_{k-1} \in S$ を用いて $a = s_0 \cdots s_{k-1}$ と書けるが，既約元の定義より，この $s_0, \ldots, s_{k-1}$ のうち 1 つ以外は 1，残りの 1 つは a でなければならない．よって，$a \in S$ である． □

命題 3.3 M を消約可能な順序型可換モノイドとする．$P_M \subseteq I_M$ である．

証明 $p \in P_M$ とし，$a, b \in M$ が $p = ab$ を満たすとする．すると特に $p \leq ab$ だから，素元の定義より $p \leq a$ または $p \leq b$ である．一般性を失わず，$p \leq a$ と仮定する．すると，$c \in M$ が存在して $a = cp$ と書ける．これ

---

*[1] 「順序型」は，本稿だけの用語である（あまりよい語だとは思わないが）．もしかすると，すでに別の名前がついているか，あるいは簡単な同値条件があるかもしれない．

を $p = ab$ に代入して $p = cbp$ を得るが，M は消約可能だから $cb = 1$ であり，さらに M は順序型，したがって 1 以外の単元をもたないから $b = 1$ である．よって，$a = p$ である．これは，$p \in I_M$ を示している． $\square$

命題 3.4 M を消約可能な順序型可換モノイドとする．P_M は M において自由である．

証明 $p_0, \ldots, p_{k-1} \in P_M$ を異なる素元，$m_0, \ldots, m_{k-1}, n_0, \ldots, n_{k-1} \in \mathbb{N}$ とする．$p_0^{m_0} \cdots p_{k-1}^{m_{k-1}} = p_0^{n_0} \cdots p_{k-1}^{n_{k-1}}$ ならば $i = 0, \ldots, k-1$ に対して $m_i = n_i$ であることを，$m_0 + \cdots + m_{k-1}$ に関する帰納法で示す．$m_0 + \cdots + m_{k-1} = 0$ のときは明らかである．$m_0 + \cdots + m_{k-1} \geq 1$ のとき，一般性を失わず，$m_0 \geq 1$ と仮定できる．すると，$p_0 \leq p_0^{m_0} \cdots p_{k-1}^{m_{k-1}} = p_0^{n_0} \cdots p_{k-1}^{n_{k-1}}$ だから，p_0 が素元であることより，ある i が存在して $n_i \geq 1$ かつ $p_0 \leq p_i$ となる．ところが，$p_0, \ldots, p_{k-1}$ は既約元だから（命題 3.3），$p_0 \leq p_i$ となるためには $p_0 = p_i$，すなわち $i = 0$ でなければならない．よって，$n_0 \geq 1$ である．ここから，消約可能性より $p_0^{m_0-1} \cdots p_{k-1}^{m_{k-1}} = p_0^{n_0-1} \cdots p_{k-1}^{n_{k-1}}$ が得られ，帰納法の仮定に帰着できる． $\square$

4 順序型可換モノイドの基底

定理 4.1 M を順序型可換モノイドとする．$S \subseteq M$ が M の基底ならば，$S = I_M = P_M$ が成り立つ．

証明 $S \subseteq M$ が M の基底であるとする．すると M は自由可換モノイドだから，消約可能であることに注意する．命題 3.3 より $P_M \subseteq I_M$ であり，命題 3.2 より $I_M \subseteq S$ である．また，基底 S により可換モノイドの同型 $\mathbb{N}^{\oplus S} \cong M$ を得るが，$s \in S$ に対応する $\mathbb{N}^{\oplus S}$ の元 $e_s = (\delta_{st})_{t \in S}$（ただし，$\delta_{st}$ は $s = t$ ならば 1，$s \neq t$ ならば 0 と定める）は $\mathbb{N}^{\oplus S}$ の素元だから，$S \subseteq P_M$ である．よって，$S = I_M = P_M$ が成り立つ． $\square$

系 4.2 自由可換モノイド M に対して，$I_M = P_M$ である． $\square$

定理 4.3 M を順序型可換モノイドとする．次の条件 (a)–(c) は同値である．さらに，M が消約可能ならば，これらは条件 (d) とも同値である．

(a) M は自由可換モノイドである．
(b) I_M は M の基底である．
(c) P_M は M の基底である．
(d) P_M は M を生成する．

証明 定理 4.1 と命題 3.4 から従う． $\square$

5 整域の乗法が定める順序型可換モノイド，一意分解整域

定義 5.1（整域） 可換環 A は，$A \setminus \{0\}$ が A の乗法に関して可換モノイドをなすとき，**整域**という．

可換環 A が整域であるための必要十分条件は，任意の $a_0, \ldots, a_{k-1} \in A$ に対して，$a_0 \cdots a_{k-1} = 0$ ならばある i が存在して $a_i = 0$ であることである．零環は整域ではないことに注意する．

定義 5.2（整域の乗法が定める順序型可換モノイド） A を整域とする．A の乗法に関する可換モノイド $A \setminus \{0\}$ を同伴関係で割った商集合は，自然な演算によってふたたび可換モノイドをなす．これを **A の乗法が定める**

順序型可換モノイドといい，M_A と書く．

容易にわかるように，整域 A に対して，M_A は消約可能な順序型可換モノイドである．

定義 5.3（整域の既約元・素元） A を整域とする．M_A の既約元・素元を A の既約元・素元といい，I_{M_A}, P_{M_A} をそれぞれ I_A, P_A と書く．

命題 5.4 A を整域とする．$P_A \subseteq I_A$ である．

証明 命題 3.3 の特別な場合である． □

定義 5.5（一意分解整域） 整域 A は，M_A が自由可換モノイドであるとき，**一意分解整域**であるという．

命題 5.6 一意分解整域 A に対して，$I_A = P_A$ である．

証明 系 4.2 の特別な場合である． □

定理 5.7 A を整域とする．次の 4 条件は同値である．

(a) A は一意分解整域である．
(b) I_A は M_A の基底である．
(c) P_A は M_A の基底である．
(d) P_A は M_A を生成する．

証明 定理 4.3 の特別な場合である． □

参考文献

[1] Wikipedia「モノイド」．https://ja.wikipedia.org/wiki/モノイド