Grillet, *Abstract Algebra* 第 1 章（群）のまとめ

鴎海

最終更新日：2026 年 1 月 30 日

概要

これは，Grillet, P.A. (2007). *Abstract Algebra* (2 ed.). Springer. の I をベースとしたまとめノートである．かなりの部分を書き直したり，意味の変わらない範囲で再定式化し直したりしている場合があるので，必ずしもオリジナルの記述に忠実ではない．

目次

第 1 章

詳細

1.1　半群

演算

A 上の 2 項演算を，単に**演算**（operation）という．

$f(a,b)$ を $a*b$ や $a\bullet b$ などとも書く．さらに，$a\cdot b$ または省略して ab（**乗法的記法**（multiplicative notation）)，または $a+b$（**加法的記法**（additive notation））などとも書く[*1]．演算に添え字をつけることもある．

$a*b$ を，$*$ による a と b の**結合**（composition）という．

一般的記法	乗法的記法	加法的記法
$a*b$	$a\cdot b$ または ab	$a+b$
結合	**積**（product）	**和**（sum）

結合

有限列

n_bv9W3

定義 1.1.1（有限列）　A の元の族 $(a_i)_{i\in I}$ は，I が有限線形順序集合であるとき，A の元の**有限列**（finite sequence）であるという．

x_5bq0c

例 1.1.2　整数 m,n に対して，$(a_i)_{i\in[m,n]}$ は有限列である．

$(a_i)_{i\in[m,n]}$ を $(a_i)_{m\leq i\leq n}$ とも書く．

n_bH27G

定義 1.1.3（同形な有限列）　$(a_i)_{i\in I}$ と $(b_j)_{j\in J}$ を A の元の有限列とする．

$$\forall i\in I,\ a_i=b_{\phi(i)}$$

なる順序同型写像 $\phi\colon I\to J$ があるとき，$(a_i)_{i\in I}$ と $(b_j)_{j\in J}$ は**同形**であるといい，$(a_i)_{i\in I}\sim(b_j)_{j\in J}$ と書く．

m_5Uqp2

補題 1.1.4　$\sim$ は同値関係である．つまり，

(1) **反射性**：$(a_i)_{i\in I}\sim(a_i)_{i\in I}$
(2) **対称性**：$(a_i)_{i\in I}\sim(b_j)_{j\in J}$ ならば，$(b_j)_{j\in J}\sim(a_i)_{i\in I}$
(3) **推移性**：$(a_i)_{i\in I}\sim(b_j)_{j\in J}\sim(c_k)_{k\in K}$ ならば，$(a_i)_{i\in I}\sim(c_k)_{k\in K}$

[*1] 加法的記法は，演算が可換であるときしか使わない．

証明　同形の定義より，

$$\forall i \in I,\ a_i = b_{\phi(i)}$$
$$\forall j \in J,\ b_j = c_{\psi(j)}$$

なる順序同型写像 $\phi\colon I \to J$ と $\psi\colon J \to K$ を取れる．

(反射性)： $\mathrm{id}_I\colon I \to I$ が所望の順序同型写像を与える．

(対称性)： 仮定のもとで，$\phi^{-1}\colon J \to I$ が所望の順序同型写像を与える．

(推移性)： 仮定のもとで，$\psi \circ \phi\colon I \to K$ が所望の順序同型写像を与える．

m_J3dq9

補題 1.1.5　$(a_i)_{i\in I}$ を A の元の有限列とし，$n := \# I$ とする．$[1,n]$ を添え字集合とする A の元の有限列のうち，$(a_i)_{i\in I}$ と同形であるものがただ 1 つ存在する．

証明　順序同型写像 $I \to [1,n]$ はただ 1 つだけ存在するので，それを ϕ と書く．

(存在)： A の元の有限列 $(s_i)_{i\in[1,n]}$ を，以下のように定義する．

$$s_j = a_{\phi^{-1}(j)} \quad (j \in [1,n])$$

すると，任意の $i \in I$ に対して，

$$a_i = a_{\phi^{-1}(\phi(i))} = s_{\phi(i)}$$

であるから，$(a_i)_{i\in I}$ と $(s_i)_{i\in[1,n]}$ は同形である．

(一意性)： 有限列 $(t_j)_{j\in[1,n]}$ も $(a_i)_{i\in I}$ と同形であるとする．

// $\forall j \in [1,n],\ s_j = t_j$ を示せばよい．

同形の定義より，

$$\forall i \in I,\ a_i = t_{\psi(i)}$$

なる順序同型写像 $\psi\colon I \to [1,n]$ が存在する．しかし，順序同型写像 $I \to [1,n]$ はただ 1 つしか存在しないので，$\psi = \phi$. ゆえに，任意の $j \in [1,n]$ に対して，

$$s_j = a_{\phi^{-1}(j)} = a_{\psi^{-1}(j)} = t_j$$

補題 1.1.5 で一意存在性が示された有限列を，**$(a_i)_{i\in I}$ の標準化列**という．

結合

以下，$*$ は A 上の演算とする．

n_n23Xb

定義 1.1.6（結合）　$n \geq 1$ とし，$(a_i)_{1\leq i\leq n}$ を A の元の族とする．$(a_i)_{1\leq i\leq n}$ の $*$ による**結合**（composition）$\mathop{\Large\ast}\limits_{i=1}^{n} a_i$ を，以下のように再帰的に定義する．

1. $\mathop{\Large\ast}\limits_{i=1}^{1} a_i = a_1$
2. $\mathop{\Large\ast}\limits_{i=1}^{n+1} a_i = \left(\mathop{\Large\ast}\limits_{i=1}^{n} a_i\right) * a_n$　$(n \geq 1)$

n_Ppb2y

定義 1.1.7（一般の結合）　一般に，A の元の空でない有限列 $(a_i)_{i\in I}$ の**結合** $\mathop{\Large\ast}\limits_{i\in I} a_i$ を以下のように定義する：

$(a_i)_{i\in I}$ の標準化列を $(b_j)_{1\leq j\leq n}$ とすると，

$$\mathop{\Large\ast}\limits_{i\in I} a_i := \mathop{\Large\ast}\limits_{j=1}^{n} b_j$$

特に，有限列 $(a_i)_{i\in I}$ が

$$a_i = \tau \quad (i \in I)$$

によって定義されているとき，$\mathop{\ast}\limits_{i\in I} a_i$ を，単に $\mathop{\ast}\limits_{i\in I}^{n} \tau$ と書く．

整数 $m \leq n$ に対して，$\mathop{\ast}\limits_{i\in[m,n]} \tau(i)$ を，$\mathop{\ast}\limits_{i=m}^{n} \tau(i)$，または $\tau(m) \ast \cdots \ast \tau(n)$ と書く．

一般的記法	乗法的記法	加法的記法
$\mathop{\ast}\limits_{i=m}^{n} a_i$	$\prod\limits_{i=m}^{n} a_i$	$\sum\limits_{i=m}^{n} a_i$
$\tau(m) \ast \cdots \ast \tau(n)$	$\tau(m) \cdots \tau(n)$	$\tau(m) + \cdots + \tau(n)$

m_Os2yy

補題 1.1.8　有限列 $(a_i)_{i\in I}$ と $(b_j)_{j\in J}$ が同形であれば，

$$\mathop{\ast}\limits_{i\in I} a_i = \mathop{\ast}\limits_{j\in J} b_j$$

特に，任意の整数 k に対して，

$$\mathop{\ast}\limits_{i=m}^{n} a_i = \mathop{\ast}\limits_{i=m+k}^{n+k} a_{i-k}$$

証明　$(b_j)_{j\in J}$ の標準化列を $(s_k)_{1\leq k\leq n}$ とする．いま，$(a_i)_{i\in I} \sim (b_j)_{j\in J} \sim (s_k)_{1\leq k\leq n}$ だから，$\sim$ の推移律 (→ 補題 1.1.4) より，$(a_i)_{i\in I} \sim (s_k)_{1\leq k\leq n}$．よって，

$$\mathop{\ast}\limits_{i\in I} a_i = \mathop{\ast}\limits_{k=1}^{n} s_k = \mathop{\ast}\limits_{j\in J} b_i$$

n_4ThGn

定義 1.1.9（n 乗）　$a \in A$ とする．$n \geq 1$ に対して，a の **n 乗**（nth power）$\mathop{\ast}\limits^{n} a$ を，以下のように定義する．

$$\mathop{\ast}\limits^{n} a := \mathop{\ast}\limits_{i=1}^{n} a$$

一般的記法	乗法的記法	加法的記法
$\mathop{\ast}\limits^{n} a$	a^n	na
n 乗	n 乗	n 倍

演算の性質

n_4xjRn

定義 1.1.10（結合的）　A 上の演算 $\ast$ は，

$$\forall x, y, z \in A,\ (x \ast y) \ast z = x \ast (y \ast z)$$

を満たすとき，**結合的**（associative）であるという．

n_ojY5Q

定義 1.1.11（可換）　A 上の演算 $\ast$ は，

$$\forall x, y \in A,\ x \ast y = y \ast x$$

を満たすとき，**可換**（commutative）であるという．

半群

n_hKVA1

定義 1.1.12（半群，可換半群）

(1) A 上の演算 $*$ が結合的なら，組 $(A,*)$ を**半群**（semigroup）という．

(2) 半群は，その演算が可換であるとき，**可換**（commutative）であるという．

一般結合法則・一般可換法則

TODO：任意の $n \geq m \geq 1$ に対して，

$$\left(\mathop{\Large *}\limits_{i=m}^{n} a_i\right) * a_{n+1} = \mathop{\Large *}\limits_{i=m}^{n+1} a_i$$

が成り立つ．

m_mGv2j

定理 1.1.13（一般結合法則）　半群 $(A,*)$ では，以下が成り立つ．

$$\mathop{\Large *}\limits_{i=1}^{n} a_i = \mathop{\Large *}\limits_{i=1}^{k-1} a_i * \mathop{\Large *}\limits_{i=k}^{n} a_i$$

ここで，n は 2 以上の自然数，k は $2 \leq k \leq n$ なる自然数である．

証明　n についての帰納法で示す．

$(n=2)$：$\mathop{\Large *}\limits_{i=1}^{2} a_i = a_1 * a_2 = \mathop{\Large *}\limits_{i=1}^{1} a_i * \mathop{\Large *}\limits_{i=2}^{2} a_i$

(Step)：n の場合に成り立つと仮定する．$n+1$ の場合にも成り立つことを示すために，k の値で場合分けをする．

$(2 \leq k \leq n$ の場合$)$：

$$\begin{aligned}
\mathop{\Large *}\limits_{i=1}^{n+1} a_i &= \left(\mathop{\Large *}\limits_{i=1}^{n} a_i\right) * a_{n+1} \\
&= \left(\mathop{\Large *}\limits_{i=1}^{k-1} a_i * \mathop{\Large *}\limits_{i=k}^{n} a_i\right) * a_{n+1} \\
&= \mathop{\Large *}\limits_{i=1}^{k-1} a_i * \left(\left(\mathop{\Large *}\limits_{i=k}^{n} a_i\right) * a_{n+1}\right) \\
&= \mathop{\Large *}\limits_{i=1}^{k-1} a_i * \mathop{\Large *}\limits_{i=k}^{n+1} a_i
\end{aligned}$$

よって，$n+1$ の場合も成り立つ．

$(k = n+1$ の場合$)$：

$$\mathop{\Large *}\limits_{i=1}^{n+1} a_i = \left(\mathop{\Large *}\limits_{i=1}^{n} a_i\right) * a_{n+1} = \mathop{\Large *}\limits_{i=1}^{n} a_i * \mathop{\Large *}\limits_{i=n+1}^{n+1} a_i$$

よって，$n+1$ の場合も成り立つ．

m_4V1BW

定理 1.1.14（一般可換法則）　半群 $(A,*)$ が可換なら，以下が成り立つ．

$$\mathop{\Large *}\limits_{i=1}^{n} a_i = \mathop{\Large *}\limits_{i=1}^{n} a_{\sigma(i)}$$

ここで，n は 1 以上の自然数，σ は $[1,n]$ の任意の置換である．

証明　n についての帰納法で示す．

$(n=1)$：$\mathop{\Large\ast}\limits_{i=1}^{1} a_i = a_1 = a_{\sigma(1)} = \mathop{\Large\ast}\limits_{i=1}^{1} a_{\sigma(i)}$

(Step)：n の場合に成り立つと仮定する．$[1, n+1]$ の置換 σ を任意に取る．k を，$\sigma(k) = n+1$ なる自然数とする．

$$
\begin{aligned}
\mathop{\Large\ast}\limits_{i=1}^{n+1} a_{\sigma(i)} &= \mathop{\Large\ast}\limits_{i=1}^{k} a_{\sigma(i)} * \mathop{\Large\ast}\limits_{i=k+1}^{n+1} a_{\sigma(i)} && \because \text{一般結合法則} \\
&= \mathop{\Large\ast}\limits_{i=1}^{k-1} a_{\sigma(i)} * a_{\sigma(k)} * \mathop{\Large\ast}\limits_{i=k+1}^{n+1} a_{\sigma(i)} \\
&= \mathop{\Large\ast}\limits_{i=1}^{k-1} a_{\sigma(i)} * \mathop{\Large\ast}\limits_{i=k+1}^{n+1} a_{\sigma(i)} * a_{\sigma(k)} && \because \text{一般可換法則・可換性}
\end{aligned}
$$

ここで，$[1, n]$ の置換 ρ を以下のように定義する：

$$
\rho(i) = \begin{cases} \sigma(i) & \text{if } 1 \leq i \leq k-1 \\ \sigma(i+1) & \text{if } k \leq i \leq n \end{cases}
$$

すると，

$$
\begin{aligned}
\mathop{\Large\ast}\limits_{i=1}^{k-1} a_{\sigma(i)} * \mathop{\Large\ast}\limits_{i=k+1}^{n+1} a_{\sigma(i)} * a_{\sigma(k)} &= \mathop{\Large\ast}\limits_{i=1}^{k-1} a_{\rho(i)} * \mathop{\Large\ast}\limits_{i=k}^{n} a_{\rho(i)} * a_{n+1} \\
&= \mathop{\Large\ast}\limits_{i=1}^{n} a_{\rho(i)} * a_{n+1} \\
&= \mathop{\Large\ast}\limits_{i=1}^{n} a_i * a_{n+1} && \because \text{帰納法の仮定} \\
&= \mathop{\Large\ast}\limits_{i=1}^{n+1} a_i
\end{aligned}
$$

よって，$n+1$ の場合も成り立つ．

m_e3gHj **定理 1.1.15（指数法則）**　$(A, *)$ を半群とする．整数 $m, n \geq 1$ に対し，以下が成り立つ．

(1) $\mathop{\Large\ast}\limits^{m} a * \mathop{\Large\ast}\limits^{n} a = \mathop{\Large\ast}\limits^{m+n} a$

(2) $\mathop{\Large\ast}\limits^{n} \mathop{\Large\ast}\limits^{m} a = \mathop{\Large\ast}\limits^{mn} a$

さらに可換であれば，以下が成り立つ．

(3) $\mathop{\Large\ast}\limits^{n} (ab) = \mathop{\Large\ast}\limits^{n} a * \mathop{\Large\ast}\limits^{n} b$

証明

(1) TODO

(2) TODO

(3) TODO