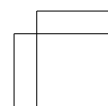
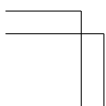


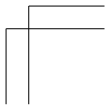
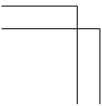


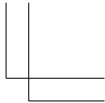
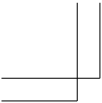
演算と代数系

Yasuhide NUMATA

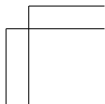
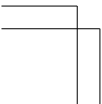
2025 年 1 月 4 日

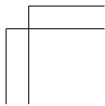
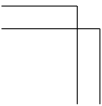






この原稿はまだ書きかけである．近いうちに改訂する．





第 1 章

演算

1.1 演算について

集合 X と集合 Y が与えられているとする. 以下の条件を満たすとき f を演算と呼ぶ:

1. X の各元 x に対して, f による像 $f(x)$ が定まっている.
2. どの $x \in X$ の像 $f(x)$ も Y の元である.
3. 各 $x \in X$ に対し $f(x)$ はただ一つ定まっていなければならない. つまり, $x, x' \in X$ に対し,

$$x = x' \implies f(x) = f(x').$$

このように定義される演算 f は, 集合 X から集合 Y への写像そのものである. つまり, 演算の定義は以下のように言い換えることができる.

Definition 1.1.1. 集合 X から集合 Y への写像 f のことを演算と呼ぶ. 集合 X として, $X_1 \times \cdots \times X_n$ という n 個の集合の直積を考える場合には, n 項演算と呼ぶ. $n = 1$ のときには単項演算と呼ぶ.

X の元に Y を対応させる ‘対応’ としての側面を意識しているとき ‘写像’ という述語を用いることが多く, X の元から Y を作る ‘操作’ としての側面を意識しているとき ‘演算’ という述語を用いることが多いように思うが, 数学的には差はない.

等式が与えられたときに, その両辺に同じ演算を行っても等式は保たれるという原則が, 演算に求められている条件 item 3 により導かれる. この原則は, これから計算をする上で, 頻繁にかつ無意識に使われる重要なものである. item 3 は一見いつでも満たされるように思うかもしれないが, 表記は異なるが等しくなる可能性がある元を X が含むときには, item 3 が満たされない可能性がある. 新しく演算を定義する際には, 注意する必要がある.

以下で, 単項演算と二項演算の例をいくつか挙げる.

Example 1.1.2. 実数 θ から, 各 θ に対する正弦 $\sin(\theta)$ を得ることを考える.

$$\begin{array}{ccc} \sin & : & \mathbb{R} \longrightarrow \mathbb{R} \\ & & \Downarrow \\ & & x \longmapsto \sin(x) \end{array}$$

という写像を考えるととってもいい. このとき, $\sin$ は単項演算である.

これらの例や定義では、演算を表す記号を、関数を表す際に通常行われるように、先頭に書いているが、このような表記を用いる必要はない。

Example 1.1.3. 正の実数 x に対し、その逆数を対応させる

$$\begin{array}{ccc} \frac{1}{\bullet} : \mathbb{R} & \longrightarrow & \mathbb{R} \\ \Downarrow & & \Downarrow \\ x & \longmapsto & \frac{1}{x} \end{array}$$

も単項演算である。 $\frac{1}{\bullet}$ だけでは、どこに実数 x を代入すればよいかわかりにくいので、代入する部分をはっきりさせるため、 $\frac{1}{\bullet}$ とここでは書いている。このように、先頭以外に演算を表す記号を書くこともある。ここでは、代入する部分を $\bullet$ で表したが、このような記号をプレースホルダと呼ぶことがある。プレースホルダとして、 $\bullet$, $-$, $()$ などの記号が使われることがある。

Example 1.1.4. 2次正則実行列全体のなす集合を $GL_2(\mathbb{R})$ とおく。正則行列 A に対し、その逆行列 A^{-1} を対応させる

$$\begin{array}{ccc} \bullet^{-1} : GL_2(\mathbb{R}) & \longrightarrow & GL_2(\mathbb{R}) \\ \Downarrow & & \Downarrow \\ A & \longmapsto & A^{-1} \end{array}$$

も単項演算である。

Example 1.1.5. 実数 x に対し、その絶対値を対応させる

$$\begin{array}{ccc} |\bullet| : \mathbb{R} & \longrightarrow & \mathbb{R} \\ \Downarrow & & \Downarrow \\ x & \longmapsto & \begin{cases} x & (x \geq 0) \\ -x & (x < 0) \end{cases} \end{array}$$

も単項演算である。このように、‘カッコ’を使って演算を表すこともある。

Example 1.1.6. 非負整数 x に対し、その階乗を対応させる

$$\begin{array}{ccc} \bullet! : \mathbb{N} & \longrightarrow & \mathbb{N} \\ \Downarrow & & \Downarrow \\ x & \longmapsto & x(x-1)(x-2)\cdots 1 \end{array}$$

も単項演算である。このように、演算を表す記号を後ろに書くような場合もある。

Example 1.1.7. 複素数 x に対し、その複素共軛を対応させる

$$\begin{array}{ccc} \bar{\bullet} : \mathbb{C} & \longrightarrow & \mathbb{C} \\ \Downarrow & & \Downarrow \\ x & \longmapsto & \bar{x} \end{array}$$

も単項演算である。

Example 1.1.8. 非負実数 x に対し、その平方根を対応させる

$$\begin{array}{ccc} \sqrt{\bullet} : \mathbb{R}_{>0} & \longrightarrow & \mathbb{R}_{>0} \\ \Downarrow & & \Downarrow \\ x & \longmapsto & \sqrt{x} \end{array}$$

も単項演算である。

1.2 0 項演算

Example 1.1.9. 整数 x, y に対し, その和を対応させる

$$\begin{array}{ccc} \bullet + \bullet & : & \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z} \\ \Downarrow & & \Downarrow \\ (x, y) & \longmapsto & x + y \end{array}$$

は二項演算である.

Example 1.1.10. 実ベクトル x, y に対し, その内積を対応させる

$$\begin{array}{ccc} \langle \bullet, \bullet \rangle & : & \mathbb{R}^n \times \mathbb{R}^n \longrightarrow \mathbb{R} \\ \Downarrow & & \Downarrow \\ (x, y) & \longmapsto & \langle x, y \rangle \end{array}$$

も二項演算である. 二項演算でも, ‘カッコ’ を使って演算を表すこともある.

Example 1.1.11. 実数 x と非負整数 n に対し, 二項係数を対応させる

$$\begin{array}{ccc} \binom{\bullet}{\bullet} & : & \mathbb{R} \times \mathbb{N} \longrightarrow \mathbb{R} \\ \Downarrow & & \Downarrow \\ (x, n) & \longmapsto & \frac{x(x-1)\cdots(x-n+1)}{n!} \end{array}$$

も二項演算である.

1.2 0 項演算

n 個の集合の直積 $X_1 \times \cdots \times X_n$ から Y への写像を n 項演算と呼んだ. 0 個の集合の直積は一点集合であると約束し, 一点集合 $\{\star\}$ から Y への写像を 0 項演算と呼ぶことがある. 一点集合 $\{\star\}$ から Y への写像は, $\star$ の像となる Y の元を一つ指定することに他ならないから, これは定数を定めていると思うこともできる. つまり, 0 項演算とは定数のことであるので, 定数のことを 0 項演算と呼ぶこともある. 定数を与えるという言い回しのほうが平易であるため, 通常は 0 項演算という用語はあまり用いられないように思う.

1.3 単項演算

集合 X から集合 Y への写像を単項演算と呼んだ. 特に, X から X への写像を X 上の単項演算と呼ぶ. 例えば, X 上の恒等写像 id_X は, X 上の単項演算である.

Definition 1.3.1. 次の条件を満たすとき, X 上の単項演算 f と g は可換であるという:

$$1. \ x \in X \implies f(g(x)) = g(f(x)).$$

Example 1.3.2. 実数を成分とする n 次正則行列全体からなる集合を $GL(n, \mathbb{R})$ とおく. $X \in GL(n, \mathbb{R})$ に対し, その逆行列を対応させる

$$\begin{array}{ccc} \bullet^{-1} & : & GL(n, \mathbb{R}) \longrightarrow GL(n, \mathbb{R}) \\ \Downarrow & & \Downarrow \\ X & \longmapsto & X^{-1} \end{array}$$

は $GL(n, \mathbb{R})$ 上の単項演算である. $X \in GL(n, \mathbb{R})$ に対し, その転置を対応させる

$$\begin{array}{ccc} {}^t\bullet & : & GL(n, \mathbb{R}) \longrightarrow GL(n, \mathbb{R}) \\ \Downarrow & & \Downarrow \\ X & \longmapsto & {}^tX \end{array}$$

は $GL(n, \mathbb{R})$ 上の単項演算である. $X \in GL(n, \mathbb{R})$ に対し,

$$({}^tX)^{-1} = {}^t(X^{-1})$$

であるので, この2つの単項演算は可換である.

Definition 1.3.3. 次の条件を満たす X 上の単項演算 f を involution と呼ぶ: 全ての $x \in X$ に対し,

$$f(f(x)) = x.$$

Example 1.3.4. 実数 x に対し, その -1 倍を対応させる

$$\begin{array}{ccc} -\bullet & : & \mathbb{R} \longrightarrow \mathbb{R} \\ \Downarrow & & \Downarrow \\ x & \longmapsto & -x \end{array}$$

は $\mathbb{R}$ 上の単項演算である. $-(-x) = x$ であるので, involution である.

Example 1.3.5. 正の実数 x に対し, その逆数を対応させる

$$\begin{array}{ccc} \bullet^{-1} & : & \mathbb{R}_{>0} \longrightarrow \mathbb{R}_{>0} \\ \Downarrow & & \Downarrow \\ x & \longmapsto & x^{-1} \end{array}$$

は $\mathbb{R}_{>0}$ 上の単項演算である. $(x^{-1})^{-1} = x$ であるので, involution である.

Nonexample 1.3.6. 正の実数 x に対し, その平方根を対応させる

$$\begin{array}{ccc} \sqrt{\bullet} & : & \mathbb{R}_{>0} \longrightarrow \mathbb{R}_{>0} \\ \Downarrow & & \Downarrow \\ x & \longmapsto & \sqrt{x} \end{array}$$

は $\mathbb{R}_{>0}$ 上の単項演算である. $16 \in \mathbb{R}_{>0}$ に対し, $\sqrt{\sqrt{16}} = \sqrt{4} = 2 \neq 16$ であるので, involution ではない.

Proposition 1.3.7. f が X 上の involution であるとき,

$$\begin{array}{ccc} \varphi & : & X \longrightarrow X \\ \Downarrow & & \Downarrow \\ x & \longmapsto & f(x) \end{array}$$

は全単射である.

Proof. f が involution であるので, $\varphi \circ \varphi = \text{id}_X$ である. これは, φ が φ 自身の逆写像であることを意味する. $\square$

Definition 1.3.8. f を X 上の単項演算とし, $X' \subset X$ とする. つぎの条件をみたすとき, X' は f について閉じているという:

$$1. \ x \in X' \implies f(x) \in X',$$

Remark 1.3.9. f を X 上の単項演算とし, $X' \subset X$ とする. X' は f について閉じているというのは, f (の制限) は X' 上の単項演算でもあるということである,

1.3 単項演算

Example 1.3.10. $\mathbb{R}^\times = \mathbb{Q} \setminus \{0\}$ とする. このとき, $x \in \mathbb{R}^\times$ に対しその逆数を対応させる

$$\begin{array}{ccc} \bullet^{-1} : \mathbb{R}^\times & \longrightarrow & \mathbb{R}^\times \\ \Downarrow & & \Downarrow \\ x & \longmapsto & x^{-1} \end{array}$$

は $\mathbb{R}^\times$ 上の単項演算である.

$x > 0$ に対し, $x^{-1} > 0$ であるので, $\mathbb{R}_{>0}$ は $\bullet^{-1}$ に関して閉じている. つまり $\bullet^{-1}$ は $\mathbb{R}_{>0}$ 上の単項演算でもある.

2 に対し, $0 < 2^{-1} < 1$ であり整数ではない. したがって, $\mathbb{Z}_{>0} \subset \mathbb{R}^\times$ であるが, $\mathbb{Z}_{>0}$ は $\bullet^{-1}$ に関して閉じていない.

f と g が可換であるとか, f が *involution* であるといったものは, 演算の性質であり, その演算に関して閉じた部分集合でも自然にその性質は成り立つ.

Proposition 1.3.11. f と g を可換な X 上の単項演算とする. $X' \subset X$ は, f と g に関して閉じているとする. このとき, X' 上の単項演算として, f と g は可換である.

Proposition 1.3.12. f を X 上の単項演算とする. f は *involution* であり, $X' \subset X$ は, f に関して閉じているとする. このとき, X' 上の単項演算として, f は *involution* である.

Definition 1.3.13. f を X 上の単項演算, g を Y 上の単項演算とし, φ を X から Y への写像とする. 次を満たすとき, φ は f を g にうつすということがある:

$$x \in X \implies \varphi(f(x)) = g(\varphi(y)).$$

特に, X 上の単項演算と Y 上の単項演算が同じ記号で表されていたり, 同じ名前と呼ばれていたたり, 同じ‘種類’のものだと考えている場合には, φ は演算を保つということがある.

Example 1.3.14. 次の $\mathbb{R}$ 上の単項演算 $-\bullet$ と $\mathbb{R}_{>0}$ 上の単項演算 $\bullet^{-1}$ について考える:

$$\begin{array}{ccc} -\bullet : \mathbb{R} & \longrightarrow & \mathbb{R} \\ \Downarrow & & \Downarrow \\ t & \longmapsto & -t \end{array},$$

$$\begin{array}{ccc} \bullet^{-1} : \mathbb{R}_{>0} & \longrightarrow & \mathbb{R}_{>0} \\ \Downarrow & & \Downarrow \\ t & \longmapsto & \frac{1}{t} \end{array}.$$

φ を次で定義する:

$$\begin{array}{ccc} \varphi : \mathbb{R} & \longrightarrow & \mathbb{R}_{>0} \\ \Downarrow & & \Downarrow \\ t & \longmapsto & e^t \end{array}$$

このとき,

$$\begin{aligned} \varphi(-t) &= e^{-t} \\ \varphi(t)^{-1} &= (e^t)^{-1} = e^{-t} \end{aligned}$$

であるので, φ は $-\bullet$ を $\bullet^{-1}$ にうつす.

Example 1.3.15. X と Y を次で定義する:

$$\begin{aligned} X &= \left\{ \begin{pmatrix} x & -y \\ y & x \end{pmatrix} \mid x, y \in \mathbb{R} \right\}, \\ Y &= \mathbb{C}. \end{aligned}$$

φ を次で定義する:

$$\begin{aligned} \varphi : \quad & \begin{array}{ccc} X & \longrightarrow & Y \\ \Downarrow & & \Downarrow \\ \begin{pmatrix} x & -y \\ y & x \end{pmatrix} & \longmapsto & x + y\sqrt{-1} \end{array} \end{aligned}$$

次の X 上の単項演算 $- \bullet$ と Y 上の単項演算 $- \bullet$ について考える:

$$\begin{aligned} - \bullet : \quad & \begin{array}{ccc} X & \longrightarrow & X \\ \Downarrow & & \Downarrow \\ A & \longmapsto & -A \end{array}, \\ - \bullet : \quad & \begin{array}{ccc} Y & \longrightarrow & Y \\ \Downarrow & & \Downarrow \\ z & \longmapsto & -z \end{array}. \end{aligned}$$

このとき,

$$\begin{aligned} \varphi(-\begin{pmatrix} x & -y \\ y & x \end{pmatrix}) &= \varphi(\begin{pmatrix} -x & y \\ -y & -x \end{pmatrix}) = -x - y\sqrt{-1} \\ -\varphi(\begin{pmatrix} x & -y \\ y & x \end{pmatrix}) &= -(x + y\sqrt{-1}) = -x - y\sqrt{-1} \end{aligned}$$

であるので, φ は X 上の単項演算 $- \bullet$ を Y 上の単項演算 $- \bullet$ にうつす. φ は $- \bullet$ を保つと言ってもいい.

1.4 二項演算

集合 $X \times X'$ から集合 Y への写像を二項演算と呼んだ. 特に, $X \times X$ から X への写像を X 上の二項演算と呼ぶ. また, $X \times Y$ から Y への写像や, $Y \times X$ から Y への写像を X の Y への作用と呼ぶ. X の Y への作用を考える際には, X や Y が代数系であることが多く, その場合にはそれらの演算と作用の整合性に関する条件が要請されることが多い. また, $X \times X$ から Y への写像を X 上の Y -形式と呼ぶことがある. この場合にもそれらの演算と作用の整合性に関する条件が要請されることが多い. また, この定義では, X 上の二項演算は, X の X への作用でもあり, X 上の X -形式でもある.

Example 1.4.1. 実ベクトル x, y に対し, その和を対応させる

$$\begin{aligned} \bullet + \bullet : \quad & \begin{array}{ccc} \mathbb{R}^n \times \mathbb{R}^n & \longrightarrow & \mathbb{R}^n \\ \Downarrow & & \Downarrow \\ (x, y) & \longmapsto & x + y \end{array} \end{aligned}$$

は $\mathbb{R}^n$ 上の二項演算である. 二項演算では, 演算を表す記号を中央に書く場合もある. このような記法を中置記法と呼ぶ.

Example 1.4.2. ベクトルのスカラー倍

$$\begin{aligned} \bullet \cdot \bullet : \quad & \begin{array}{ccc} \mathbb{R} \times \mathbb{R}^n & \longrightarrow & \mathbb{R}^n \\ \Downarrow & & \Downarrow \\ (a, x) & \longmapsto & ax \end{array} \end{aligned}$$

は二項演算である. これは $\mathbb{R}$ の $\mathbb{R}^n$ への作用である.

1.4 二項演算

Example 1.4.3. 実ベクトル x, y に対し, その内積を対応させる

$$\begin{array}{ccc} \langle \bullet, \bullet \rangle & : & \mathbb{R}^n \times \mathbb{R}^n \longrightarrow \mathbb{R} \\ \Downarrow & & \Downarrow \\ (x, y) & \longmapsto & \langle x, y \rangle \end{array}$$

も二項演算である. これは $\mathbb{R}^n$ 上の $\mathbb{R}$ -形式である.

Definition 1.4.4. X 上の二項演算

$$\begin{array}{ccc} f & : & X \times X \longrightarrow X \\ \Downarrow & & \Downarrow \\ (x, y) & \longmapsto & f(x, y) \end{array}$$

について考える. $X' \subset X$ が次の条件を満たすとき, X' は f に関して閉じているという:

$$1. \ x', y' \in X' \implies f(x', y') \in X'.$$

Remark 1.4.5. f を X 上の二項演算とし, $X' \subset X$ とする. X' は f について閉じているというのは, f (の制限) は X' 上の二項演算でもあるということである,

Definition 1.4.6. X の Y 上の作用

$$\begin{array}{ccc} f & : & X \times Y \longrightarrow Y \\ \Downarrow & & \Downarrow \\ (x, y) & \longmapsto & f(x, y) \end{array}$$

について考える. $Y' \subset Y$ が次の条件を満たすとき, Y' は f に関して閉じているという:

$$1. \ x \in X, y \in Y' \implies f(x, y) \in Y'.$$

Remark 1.4.7. f を X の Y 上の作用とし, $Y' \subset Y$ とする. Y' が f について閉じているというのは, f (の制限) は X の Y' 上の作用でもあるということである,

Definition 1.4.8. X 上の形式

$$\begin{array}{ccc} f & : & X \times X \longrightarrow Y \\ \Downarrow & & \Downarrow \\ (x, y) & \longmapsto & f(x, y) \end{array}$$

について考える. $X' \subset X$ に対し, その制限,

$$\begin{array}{ccc} f|_{X' \times X'} & : & X' \times X' \longrightarrow Y \\ \Downarrow & & \Downarrow \\ (x, y) & \longmapsto & f(x, y) \end{array}$$

を f の X' への制限と呼ぶ. 文脈上問題ない場合には, f の X' への制限も同じ記号 f を使って表す.

Remark 1.4.9. f を X 上の Y -形式とし, $X' \subset X$ とする. f の X' への制限は, X' 上の Y -形式である.

Definition 1.4.10. $\bullet \circ \bullet$ を X 上の二項演算, $\bullet * \bullet$ を Y 上の二項演算とし, φ を X から Y への写像とする. 次を満たすとき, φ は $\circ$ を $*$ にうつすということがある:

$$x, y \in X \implies \varphi(x \circ y) = \varphi(y) * \varphi(x).$$

特に, X 上の二項演算と Y 上の二項演算が同じ記号で表されていたり, 同じ名前と呼ばれていて, 同じ‘種類’のものだと考えている場合には, φ は演算を保つということがある.

Example 1.4.11. $\mathbb{R}$ 上の演算 $+$ と $\mathbb{R}_{>0}$ 上の演算 $\cdot$ を考える. φ を次で定義する:

$$\begin{array}{ccc} \varphi & : & \mathbb{R} \longrightarrow \mathbb{R}_{>0} \\ \Downarrow & & \Downarrow \\ t & \longmapsto & e^t \end{array}$$

このとき,

$$\begin{aligned} \varphi(s+t) &= e^{s+t} \\ \varphi(s) \cdot \varphi(t) &= e^s \cdot e^t = e^{s+t} \end{aligned}$$

であるので, φ は $+$ を $\cdot$ にうつす.

Example 1.4.12. X と Y を次で定義する:

$$\begin{aligned} X &= \left\{ \begin{pmatrix} x & -y \\ y & x \end{pmatrix} \mid x, y \in \mathbb{R} \right\}, \\ Y &= \mathbb{C}. \end{aligned}$$

φ を次で定義する:

$$\begin{array}{ccc} \varphi & : & X \longrightarrow Y \\ \Downarrow & & \Downarrow \\ \begin{pmatrix} x & -y \\ y & x \end{pmatrix} & \longmapsto & x + y\sqrt{-1} \end{array}.$$

次の X 上の二項演算 $+$ と Y 上の二項演算 $+$ について考える. このとき,

$$\begin{aligned} \varphi\left(\begin{pmatrix} x & -y \\ y & x \end{pmatrix} + \begin{pmatrix} a & -b \\ b & a \end{pmatrix}\right) &= \varphi\left(\begin{pmatrix} x+a & -y-b \\ y+b & x+a \end{pmatrix}\right) = (x+a) + (y+b)\sqrt{-1} \\ \varphi\left(\begin{pmatrix} x & -y \\ y & x \end{pmatrix}\right) + \varphi\left(\begin{pmatrix} a & -b \\ a & b \end{pmatrix}\right) &= (x+y\sqrt{-1}) + (a+b\sqrt{-1}) = (x+a) + (y+b)\sqrt{-1} \end{aligned}$$

であるので, φ は X 上の単項演算 $+$ を Y 上の単項演算 $+$ にうつす. φ は $+$ を保つと言ってもいい.

Definition 1.4.13. $*$ を中置記法の X 上の二項演算とする. $x \in X$ と $S \subset X$ に対し, $x * S$ と $S * x$ を

$$\begin{aligned} x * S &= \{ x * s \mid s \in S \} \\ S * x &= \{ s * x \mid s \in S \} \end{aligned}$$

で定義する.

Example 1.4.14. $3\mathbb{Z}$ は

$$3\mathbb{Z} = \{ 3x \mid x \in \mathbb{Z} \}$$

であり, 3 の倍数の集合である.

第 2 章

X 上の二項演算に関する用語

ここでは, X 上の二項関係に関して用いられる用語についていくつか紹介する.

2.1 可換律

ここでは, $*$ を X 上の中置記法の二項演算とする. つまり

$$\begin{array}{ccc} \bullet * \bullet & : & X \times X \longrightarrow X \\ \Downarrow & & \Downarrow \\ (x, y) & \longmapsto & x * y \end{array}$$

とする.

Definition 2.1.1. $x, y \in X$ が次の条件を満たすとき, x と y は可換であるという:

$$x * y = y * x.$$

Definition 2.1.2. 次の条件を満たすとき, $*$ は可換律を満たすという:

$$x, y \in X \implies x * y = y * x.$$

Remark 2.1.3. $*$ が可換律を満たすことを, $*$ が可換であるともいう,

Example 2.1.4. $\mathbb{N}$ 上の二項演算として, 通常和 $+$ を考える. 和 $+$ は可換である.

Example 2.1.5. $\mathbb{N}$ 上の二項演算として, 通常積 $\cdot$ を考える. 積 $\cdot$ は可換である.

Nonexample 2.1.6.

$$\begin{array}{ccc} \bullet \bullet & : & \mathbb{Z}_{>0} \times \mathbb{Z}_{>0} \longrightarrow \mathbb{Z}_{>0} \\ \Downarrow & & \Downarrow \\ (x, y) & \longmapsto & x^y \end{array}$$

は $\mathbb{Z}_{>0}$ 上の二項演算である.

$$\begin{array}{l} 2^3 = 8, \\ 3^2 = 9 \end{array}$$

であるので, この演算は可換ではない.

Nonexample 2.1.7. n 次正方行列同士の積も n 次正方行列である. n 次正方行列上の二項

演算として積を考える.

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

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

であるので, 積は可換ではない.

Noneexample 2.1.8. n 次正方行列 A, B に対し,

$$[A, B] = AB - BA$$

とおくと, $[\bullet, \bullet]$ は, n 次正方行列上の二項演算である. この演算をリー・ブラケットと呼ぶ.

$$\begin{aligned} [A, B] &= AB - BA \\ [B, A] &= BA - AB = -(AB - BA) \end{aligned}$$

であるので $[A, B] = -[B, A]$ である.

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

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

とおくと,

$$\begin{aligned} [E, F] &= EF - FE = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} - \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \\ [F, E] &= -[E, F] = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \end{aligned}$$

となるので, $[\bullet, \bullet]$ は可換ではない.

$*$ が可換であるという演算自身の性質であり, その演算が閉じた部分集合でも自然に成り立つ.

Proposition 2.1.9. $*$ は可換な X 上の二項演算とし, $X' \subset X$ は $*$ に関して閉じているとする. このとき, X' 上の二項演算として, $*$ は可換である.

X 上の二項演算について可換であるということを定義したが, より一般に X 上の Y -形式についても, 定義できる.

Definition 2.1.10. 二項演算

$$\begin{array}{ccc} \bullet * \bullet & : & X \times X \longrightarrow Y \\ & \Psi & \Psi \\ & (x, y) & \longmapsto x * y \end{array}$$

に対し, $x, y \in X$ が次の条件を満たすとき, x と y は可換であるという:

$$x * y = y * x.$$

2.2 結合律

Definition 2.1.11. 二項演算

$$\begin{array}{ccc} \bullet * \bullet & : & X \times X \longrightarrow Y \\ \Downarrow & & \Downarrow \\ (x, y) & \longmapsto & x * y \end{array}$$

に対し, 次の条件を満たすとき, $*$ は可換律を満たすという:

$$x, y \in X \implies x * y = y * x.$$

Remark 2.1.12. $*$ が可換律を満たすことを, $*$ が可換であるともいう, また $*$ が対称であるともいう,

2.2 結合律

ここでは, $*$ を X 上の中置記法の二項演算とする.

Definition 2.2.1. 次の条件を満たすとき, $*$ は結合律を満たすという:

$$x, y, z \in X \implies (x * y) * z = x * (y * z).$$

Remark 2.2.2. $*$ が結合律を満たすことを, $*$ が結合的であるともいう,

Example 2.2.3. $\mathbb{N}$ 上の二項演算として, 通常のと $+$ を考える. 和 $+$ は結合律を満たす.

Nonexample 2.2.4.

$$\begin{array}{ccc} \bullet \bullet & : & \mathbb{Z}_{>0} \times \mathbb{Z}_{>0} \longrightarrow \mathbb{Z}_{>0} \\ \Downarrow & & \Downarrow \\ (x, y) & \longmapsto & x^y \end{array}$$

は $\mathbb{Z}_{>0}$ 上の二項演算である.

$$\begin{aligned} (3^3)^3 &= 9^3 = 729, \\ 3^{(3^3)} &= 3^9 = 19683 \end{aligned}$$

であるので, この演算は結合律を満たさない.

Nonexample 2.2.5. n 次正方形上での二項演算としてリー・ブラケットを考える.

$$[A, A] = AA - AA = O_n$$

である. ただし O_n は零行列を表す.

$$\begin{aligned} E &= \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \\ F &= \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \\ H &= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \end{aligned}$$

とおくと,

$$\begin{aligned} [[E, E], F] &= [O_n, F] = O_n F - F O_n = O_n \\ [E, [E, F]] &= [E, H] = -2E \end{aligned}$$

となるので, リー・ブラケットは結合的ではない.

Nonexample 2.2.6. 2元集合 $X = \{\top, \perp\}$ 上の演算 $\overline{\bullet \vee \bullet}$ を

$$\begin{array}{ll} \overline{\top \vee \top} = \perp & \overline{\top \vee \perp} = \perp \\ \overline{\perp \vee \top} = \perp & \overline{\perp \vee \perp} = \top \end{array}$$

で定める。このとき、

$$\begin{array}{l} \overline{\perp \vee \overline{\perp \vee \top}} = \overline{\perp \vee \perp} = \top \\ \overline{\overline{\perp \vee \perp} \vee \top} = \overline{\top \vee \top} = \perp \end{array}$$

であるので、この演算は結合的でない。

Remark 2.2.7. $*$ が結合律が成り立つ演算ならば、

$$a * b * c$$

を

$$(a * b) * c$$

と解釈しても、

$$a * (b * c)$$

と解釈しても等しい元となる。これは、

$$a_1 * a_2 * \cdots * a_n$$

のような場合でも同様である。そのため、結合の順序を表すカッコを省略することが多い。

Remark 2.2.8. $*$ が X 上の結合的な二項演算であるとき、正の整数 n に対し、

$$\underbrace{a * \cdots * a}_n$$

は $a \in X$ と n のみから決まる。そこで、これを、 a と n のみを使って略記することがある。演算によってその略記法は異なるが、 a^n とか na などと書かれることがある。また複数の演算が扱われているときには a^{*n} などと演算の記号を伴って書かれる記法もある。

a^n や a^{*n} のように‘指数’として略記する場合には、その演算は乗法と呼ばれ、その演算の結果は積と呼ばれることが多い。 na のように‘係数’として略記する場合には、その演算は加法と呼ばれ、その演算の結果は和と呼ばれることが多い。

結合律を満たす演算に関して、いわゆる指数法則が成り立つ。

Proposition 2.2.9. $*$ を X 上の結合律を満たす中置記法の二項演算とする。 $a \in X$ と正の整数 n に対し、

$$a^n = \underbrace{a * \cdots * a}_n$$

という表記を用いる。このとき、 $a \in X$ と正の整数 n, m に対し次が成り立つ：

1. $a^m * a^n = a^{m+n}$.
2. $(a^m)^n = a^{mn}$.

2.3 単位元

Proof.

□

‘係数’として略記する場合には、指数法則は以下のように言い換えられる：

Proposition 2.2.10. $*$ を X 上の結合律を満たす中置記法の二項演算とする． $a \in X$ と正の整数 n に対し、

$$na = \underbrace{a * \cdots * a}_n$$

という表記を用いる．このとき、 $a \in X$ と正の整数 n, m に対し次が成り立つ：

1. $(na) * (ma) = (n + m)a$.
2. $m(na) = (nm)a$.

Proof.

□

$*$ が結合的であるという演算自身の性質であり、その演算が閉じた部分集合でも自然に成り立つ．

Proposition 2.2.11. $*$ は結合的な X 上の二項演算とし、 $X' \subset X$ は $*$ に関して閉じているとする．このとき、 X' 上の二項演算として、 $*$ は結合的である．

Remark 2.2.12. $*$ が結合的な X 上の二項演算であるとき、 $x, y \in X$ と $S \subset X$ に対して、 $x * (S * y) = (x * S) * y$ であるので、 $x * S * y$ と略記する．つまり、

$$x * S * y = \{ x * s * y \mid s \in S \}$$

とする．

2.3 単位元

ここでは、 $*$ を X 上の中置記法の二項演算とする．

Definition 2.3.1. $e \in X$ とする．

1. 次の条件を満たすとき、 e は $*$ に関し左単位的であるという：
 - (a) $x \in X \implies e * x = x$.
2. 次の条件を満たすとき、 e は $*$ に関し右単位的であるという：
 - (a) $x \in X \implies x * e = x$.
3. e が、 $*$ に関し左単位的かつ $*$ に関し右単位的であるとき、 e は $*$ に関し単位的であるという．

Lemma 2.3.2. $e \in X$ が左単位的であり、 $e' \in X$ が右単位的であるなら、 $e = e'$ 、

Proof. $e * e'$ について考える． e は左単位的であるので、 $e * e' = e'$ ． e' は右単位的であるので、 $e * e' = e$ ．したがって、 $e = e'$ ． □

Corollary 2.3.3. $e \in X$ 、 $e' \in X$ が単位的なら、 $e = e'$ ．

Corollary 2.3.4. 右単位元と左単位元が存在するなら、それらは一致し $*$ の単位元である．

Corollary 2.3.5. $*$ の単位元が存在するとする.

1. 左単位的な元は, $*$ の単位元である.
2. 右単位的な元は, $*$ の単位元である.

Corollary 2.3.6. $*$ は可換な二項演算であるとする.

1. 左単位的な元は, $*$ の単位元である.
2. 右単位的な元は, $*$ の単位元である.

Remark 2.3.7. Corollary 2.3.3 により, 単位的な元は存在するなら, ただ一つであることがわかる. 単位的な元を (もし存在するなら) $*$ の単位元と呼ぶ.

$*$ が乗法と呼ばれる演算であるとき, つまり, 結合律を満たし $a \in X$ の n 個の積を a^n と略記するとき, 単位元は, 乗法単位元と呼ばれ e の他に 1 や I にまつわる記号を用いることが多い. また, $a \in X$ に対し, a^0 を単位元として定義する.

$*$ が加法と呼ばれる演算であるとき, つまり, $a \in X$ の n 個の和を na と略記するとき, 単位元は, 加法単位元と呼ばれ 0 や O のような記号を用いることが多い. また, $a \in X$ に対し, $0a$ を単位元として定義する.

この表記においても指数法則は成り立つ:

Proposition 2.3.8. $*$ を X 上の結合律を満たす中置記法の二項演算とする. また, e を $*$ の単位元とし, $a \in X$ と $n \in \mathbb{N}$ に対し,

$$a^n = \begin{cases} \underbrace{a * \cdots * a}_n & (n > 0) \\ e & (n = 0) \end{cases}$$

とする. このとき, このとき, $a \in X$ と $n, m \in \mathbb{N}$ に対し次が成り立つ:

1. $a^m * a^n = a^{m+n}$.
2. $(a^m)^n = a^{mn}$.

Proof.

□

‘係数’として略記する場合には以下のように指数法則は言い換えられる:

Proposition 2.3.9. $*$ を X 上の結合律を満たす中置記法の二項演算とする. また, o を $*$ の単位元とし, $a \in X$ と $n \in \mathbb{N}$ に対し,

$$na = \begin{cases} \underbrace{a * \cdots * a}_n & (n > 0) \\ o & (n = 0) \end{cases}$$

とする. このとき, $a \in X$ と $n, m \in \mathbb{N}$ に対し次が成り立つ:

1. $ma * na = (m+n)a$.
2. $n(ma) = (nm)a$.

Proof.

□

Example 2.3.10. $\mathbb{Z}$ における通常の和 $+$ を考える. 0 は $+$ に関する単位元である.

2.3 単位元

Example 2.3.11. $\mathbb{Z}_{>0}$ における通常の積 $\cdot$ を考える. 1 は $\cdot$ に関する単位元である.

Example 2.3.12. 二点集合 $\{0, 1\}$ 上の演算 $\triangleright$ を

$$\begin{array}{ll} 0 \triangleright 0 = 0 & 0 \triangleright 1 = 1 \\ 1 \triangleright 0 = 0 & 1 \triangleright 1 = 1 \end{array}$$

で定義する. このとき, 0 は左単位的である. また 1 も左単位的である.

Nonexample 2.3.13. $\mathbb{Z}_{>0}$ 上の和 $+$ について考える. $x \in \mathbb{Z}_{>0}$ とする. このとき, $x+1 > 1$ となるので $x+1 = 1$ となることはない. したがって, $+$ の単位元は存在しない.

$*$ に関して閉じている部分集合を考えると, 二項演算が単位元を持つかどうかは, 考えている集合による. $*$ が単位元をもっていたとしても, $*$ に関して部分集合に単位元が存在しているかはわからない. しかし, 単位元が満たしている条件自体は演算の性質であり, $*$ の単位元が $*$ に関して部分集合に含まれているなら, その元は単位元となる.

Proposition 2.3.14. $*$ は X 上の二項演算とし, $X' \subset X$ は $*$ に関して閉じているとする. $e \in X$ は左単位的であるとし, $e \in X'$ とする. このとき, e は, X' 上の二項演算 $*$ でも, 左単位的である.

Proposition 2.3.15. $*$ は X 上の二項演算とし, $X' \subset X$ は $*$ に関して閉じているとする. $e \in X$ は右単位的であるとし, $e \in X'$ とする. このとき, e は, X' 上の二項演算 $*$ でも, 右単位的である.

Proposition 2.3.16. $*$ は X 上の二項演算とし, $e \in X$ は $*$ の単位元であるとする. $X' \subset X$ は $*$ に関して閉じているとする. $e \in X'$ ならば, e は, X' 上の二項演算としての $*$ の単位元である.

Remark 2.3.17. X 上の二項演算 $*$ が単位元をもつとし, その単位元を e とする. $X' \subset X$ は $*$ に関して閉じているとする. $e \in X'$ ならば, Proposition 2.3.16 より, X' 上の二項演算 $*$ も単位元をもち, その単位元は e である. 一方, $e \notin X'$ であっても, X' 上の二項演算 $*$ も単位元をもつことはある. この場合, その単位元を e' とすると $e \neq e'$ であり, e' は X 上の演算 $*$ の単位元ではない.

Example 2.3.18. 2 元集合 $X = \{\top, \perp\}$ 上の演算 $\bullet \vee \bullet$ を

$$\begin{array}{ll} \top \vee \top = \top & \top \vee \perp = \top \\ \perp \vee \top = \top & \perp \vee \perp = \perp \end{array}$$

で定める. このとき, $\perp$ は $\vee$ の単位元である. $X' = \{\perp\}$ とおくと, X' は $\vee$ に関して閉じている. $\perp \in X'$ であり, $\perp$ は X 上の演算 $\vee$ の単位元であったから, X' 上の演算としての $\vee$ の単位元でもある. $X'' = \{\top\}$ とおくと, X'' は $\vee$ に関して閉じている. $\perp \notin X''$ であるが, $\top$ は X'' 上の演算としての $\vee$ の単位元である.

X 上の二項演算に関して単位的な元というものを定義したが, これは, X の Y 上の作用でも定義できる.

Definition 2.3.19. 二項演算

$$\begin{array}{ccc} \bullet * \bullet & : & X \times Y \longrightarrow Y \\ \Downarrow & & \Downarrow \\ (x, y) & \longmapsto & x * y \end{array}$$

に対し, $e \in X$ が次の条件を満たすとき, e は $*$ に関し左単位的であるという:

$$1. x \in X \implies e * x = x.$$

2.4 逆元

ここでは, $*$ を X 上の中置記法の二項演算とし, $*$ が単位元 e を持つとする.

Definition 2.4.1. $e \in X$ は $*$ の単位元であるとする. $x \in X$ とする.

1. 次の条件を満たす y を x の左逆元と呼ぶ:
 - (a) $y * x = e$.
2. 次の条件を満たす y を x の右逆元と呼ぶ:
 - (a) $x * y = e$.
3. 次の条件を満たす y を x の逆元と呼ぶ:
 - (a) $y * x = e$.
 - (b) $x * y = e$.

逆元をもつ $x \in X$ を可逆元と呼ぶことがある.

Lemma 2.4.2. $*$ は結合的であるとし, $x \in X$ とする. $y \in X$ が x の左逆元であり, $y' \in X$ が x の右逆元であり, $y = y'$.

Proof. $*$ の単位元を e とする. y は x の左単位元であるので, $(y * x) * y' = e * y' = y'$. y は x の右単位元であるので, $y * (x * y') = y * e = y$. $*$ は結合的なので, $(y * x) * y' = y * (x * y')$. したがって, $y = y'$. $\square$

Corollary 2.4.3. $*$ は結合的であるとし, $x \in X$ とする. $y \in X, y' \in X$ が x の逆元なら, $y = y'$.

Corollary 2.4.4. $*$ は結合的であるとする. $x \in X$ の右逆元と左逆元が存在するなら, それらは一致し x の逆元である.

Corollary 2.4.5. $*$ は結合的であるとし, $x \in X$ とする. x の逆元が存在するとする.

1. x の左逆元は, x の逆元である.
2. x の右逆元は, x の逆元である.

Corollary 2.4.6. $*$ は結合的かつ可換律を満たす二項演算であるとし, $x \in X$ とする.

1. x の右逆元は, x の逆元である.
2. x の右逆元は, x の逆元である.

Lemma 2.4.7. $*$ は結合的であるとし, $x, x' \in X$ とする. $y \in X$ が x の左逆元であり, $y' \in X$ が x' の左逆元なら, $y' * y$ は $x * x'$ の左逆元である.

Proof. e を $*$ の単位元とする. $y * x = e, y' * x' = e$ とすると,

$$(y' * y) * (x * x') = y' * (y * x) * x' = y' * e * x' = y' * x' = e.$$

2.4 逆元

□

Lemma 2.4.8. $*$ は結合的であるとし, $x, x' \in X$ とする. $y \in X$ が x の右逆元であり, $y' \in X$ が x' の右逆元なら, $y * y'$ は $x' * x$ の右逆元である.

Proof. e を $*$ の単位元とする. $x * y = e, x' * y' = e$ とすると,

$$(x' * x) * (y * y') = x' * (x * y) * y' = x' * e * y' = x' * y' = e.$$

□

Lemma 2.4.9. $*$ は結合的であるとし, $x, x' \in X$ とする. $y \in X$ が x の逆元であり, $y' \in X$ が x' の逆元なら, $y * y'$ は $x' * x$ の逆元である.

Proof. Lemmas 2.4.7 and 2.4.8 から従う. □

Remark 2.4.10. $*$ が結合的であるとき, Corollary 2.4.3 により, $x \in X$ の逆元は, 存在するなら, $x \in X$ に対して, ただ一つであることがわかる. そこで, $x \in X$ の逆元を x を用いて表すことが多い.

$*$ が乗法と呼ばれる演算であるとき, つまり, 結合律を満たし $a \in X$ の n 個の積を a^n と略記するとき, x の逆元は, x の乗法逆元とも呼ばれ, x^{-1} のような記号が用いられる. Section 2.4 より, $n \in \mathbb{N}$ に対し, $(x^{-1})^n = (x^n)^{-1}$ である. そこで, $x^{-n} = (x^{-1})^n$ と略記する.

$*$ が加法と呼ばれる演算であるとき, つまり, $a \in X$ の n 個の和を na と略記するとき, x の逆元は, x の加法逆元とも呼ばれ, $-x$ のような記号が用いられる. Section 2.4 より, $n \in \mathbb{N}$ に対し, $n(-x) = -(nx)$ である. そこで, $-nx = n(-x)$ と略記する.

この表記においても指数法則は成り立つ:

Proposition 2.4.11. $*$ を X 上の結合律を満たす中置記法の二項演算とする. また, e を $*$ の単位元とし, 可逆元 $a \in X$ と $n \in \mathbb{N}$ に対し,

$$a^n = \begin{cases} \underbrace{a * \cdots * a}_n & (n > 0) \\ e & (n = 0) \\ \underbrace{a^{-1} * \cdots * a^{-1}}_{|n|} & (n < 0) \end{cases}$$

とする. このとき, 可逆元 $a \in X$ と $n, m \in \mathbb{Z}$ に対し次が成り立つ:

1. $a^m * a^n = a^{m+n}.$
2. $(a^m)^n = a^{mn}.$

Proof. □

‘係数’として略記する場合には以下のように指数法則は言い換えられる:

Proposition 2.4.12. $*$ を X 上の結合律を満たす中置記法の二項演算とする. また, o

を $*$ の単位元とし, 可逆元 $a \in X$ と $n \in \mathbb{N}$ に対し,

$$na = \begin{cases} \underbrace{a * \cdots * a}_n & (n > 0) \\ o & (n = 0) \\ \underbrace{-a * \cdots * -a}_{|n|} & (n < 0) \end{cases}$$

とする. このとき, 可逆元 $a \in X$ と $n, m \in \mathbb{Z}$ に対し次が成り立つ:

1. $ma * na = (m + n)a$.
2. $n(ma) = (nm)a$.

Proof.

□

Example 2.4.13. $\mathbb{Z}$ 上の通常の和を考える. このとき, 0 は $+$ の単位元である. どの $x \in \mathbb{Z}$ も逆元を持ち, x の逆元はその -1 倍の $-x$ である.

Example 2.4.14. $\mathbb{Q}$ 上の通常の積を考える. このとき, 1 は $\cdot$ の単位元である. どの $x \in \mathbb{Q}$ に対しても $0x = 0$ であり, $0x = 1$ となることはない. したがって 0 の逆元はない. 0 以外の $x \in \mathbb{Q}$ は逆元を持ち, x の逆元はその逆数 $\frac{1}{x}$ である.

Example 2.4.15. $\mathbb{Z}$ 上の通常の積を考える. このとき, 1 は $\cdot$ の単位元である. $0 \in \mathbb{Z}$ は逆元を持たない. また, $x > 1$ に対して, $0 < \frac{1}{x} < 1$ であるので, $\frac{1}{x} \notin \mathbb{Z}$ である. したがって, $x > 1$ ならば $x \in \mathbb{Z}$ は逆元を持たない. 同様に, $x < -1$ ならば $x \in \mathbb{Z}$ は逆元を持たない. 1 の逆元は 1 であり, -1 の逆元は -1 である.

$*$ に関して閉じている部分集合を考えると x が逆元を持つかどうかは考えている集合による. x^{-1} がもとの集合に存在していても, 部分集合に存在しているかどうかはわからない. しかし, 逆元が満たしている条件自体は演算の性質であり, もとの集合の単位元が含まれており, 逆元が部分集合に含まれているなら, その元は逆元となる.

Proposition 2.4.16. $*$ は X 上の二項演算とし, $e \in X$ は $*$ の単位元であるとする. $X' \subset X$ は $*$ に関して閉じており, $e \in X'$ とする. $x \in X$ の逆元 $y \in X$ が $y \in X'$ をみたすなら, y は, X' 上の二項演算としての x の逆元である.

Proposition 2.4.17. $*$ は X 上の二項演算とし, $e \in X$ は $*$ の単位元であるとする. $X' \subset X$ は $*$ に関して閉じており, $e \in X'$ とする. $x \in X$ の左逆元 $y \in X$ が $y \in X'$ をみたすなら, y は, X' 上の二項演算としての x の左逆元である.

Proposition 2.4.18. $*$ は X 上の二項演算とし, $e \in X$ は $*$ の単位元であるとする. $X' \subset X$ は $*$ に関して閉じており, $e \in X'$ とする. $x \in X$ の右逆元 $y \in X$ が $y \in X'$ をみたすなら, y は, X' 上の二項演算としての x の右逆元である.

2.5 分配律

ここでは, $*$, $\diamond$ を X 上の中置記法の二項演算とする.

Definition 2.5.1. $*$, $\diamond$ を X 上の中置記法の二項演算とする.

2.5 分配律

1. 次の条件を満たすとき, $*$ は $\diamond$ に対し左分配的であるという:

$$(a) \ x, y, z \in X \implies x * (y \diamond z) = (x * y) \diamond (x * z).$$

2. 次の条件を満たすとき, $*$ は $\diamond$ に対し右分配的であるという:

$$(a) \ x, y, z \in X \implies (y \diamond z) * x = (y * x) \diamond (z * x).$$

3. $*$ が $\diamond$ に対し左分配的かつ右分配的であるとき, $*$ は $\diamond$ に対し分配的であるという.

Corollary 2.5.2. $*$, $\diamond$ を X 上の中置記法の二項演算とする. $*$ が可換であり, $*$ は $\diamond$ に対し左分配的なら, $*$ は $\diamond$ に対し分配的である.

Corollary 2.5.3. $*$, $\diamond$ を X 上の中置記法の二項演算とする. $*$ が可換であり, $*$ は $\diamond$ に対し右分配的なら, $*$ は $\diamond$ に対し分配的である.

Example 2.5.4. $\mathbb{Z}$ 上の通常のと積 $\cdot$ を考える. このとき, 和は積に対して分配的である. 一方

$$\begin{aligned} (1 \cdot 1) + 1 &= 2, \\ (1 + 1) \cdot (1 + 1) &= 4 \end{aligned}$$

であるので, 積は和に対して分配的ではない.

Example 2.5.5. Ω を集合とし, Ω の冪集合を X とする. このとき, $\cup$ と $\cap$ は X 上の二項演算である. このとき, $\cap$ は $\cup$ に対して分配的である. また, $\cup$ は $\cap$ に対して分配的である.

$*$ が $\diamond$ に対して分配的であるかどうかは, 演算自身の性質であり, その演算が閉じた部分集合でも自然に成り立つ.

Proposition 2.5.6. $*$, $\diamond$ を X 上の二項演算で, $*$ は $\diamond$ に対し左分配的であるとする. $X' \subset X$ は $*$, $\diamond$ に関し閉じているとする. このとき, X' 上の二項演算として, $*$ は $\diamond$ に対し左分配的である.

Proposition 2.5.7. $*$, $\diamond$ を X 上の二項演算で, $*$ は $\diamond$ に対し右分配的であるとする. $X' \subset X$ は $*$, $\diamond$ に関し閉じているとする. このとき, X' 上の二項演算として, $*$ は $\diamond$ に対し右分配的である.

Proposition 2.5.8. $*$, $\diamond$ を X 上の二項演算で, $*$ は $\diamond$ に対し分配的であるとする. $X' \subset X$ は $*$, $\diamond$ に関し閉じているとする. このとき, X' 上の二項演算として, $*$ は $\diamond$ に対し分配的である.

X 上の二項演算について分配的であるということを定義したが, より一般に X の Y 上の作用についても, 定義できる.

Definition 2.5.9. 二項演算

$$\begin{array}{lll} & X \times Y & \longrightarrow Y \\ \bullet * \bullet : & \Downarrow & \Downarrow \\ & (x, y) & \longmapsto x * y \\ & Y \times Y & \longrightarrow Y \\ \bullet \diamond \bullet : & \Downarrow & \Downarrow \\ & (y, y') & \longmapsto y \diamond y' \end{array}$$

に対し, 次の条件を満たすとき, $*$ は $\diamond$ に対し左分配的であるという:

$$1. x \in X, y, y' \in Y \implies x * (y \diamond y') = (x * y) \diamond (x * y').$$

Definition 2.5.10. 二項演算

$$\begin{array}{ccc} & X \times X & \longrightarrow X \\ \bullet * \bullet: & \Downarrow & \Downarrow \\ & (x, x') & \longmapsto x * x' \\ & X \times Y & \longrightarrow Y \\ \bullet \diamond \bullet: & \Downarrow & \Downarrow \\ & (x, y) & \longmapsto x \diamond y \end{array}$$

に対し, 次の条件を満たすとき, $\diamond$ は $*$ に対し右分配的であるという:

$$1. x, x' \in X, y \in Y \implies (x * x') \diamond y = (x * y) \diamond (x' * y).$$

Definition 2.5.11. 二項演算

$$\begin{array}{ccc} & X \times Y & \longrightarrow X \\ \bullet * \bullet: & \Downarrow & \Downarrow \\ & (x, y) & \longmapsto x * y \\ & Y \times Y & \longrightarrow Y \\ \bullet \diamond \bullet: & \Downarrow & \Downarrow \\ & (y, y') & \longmapsto y \diamond y' \end{array}$$

に対し, 次の条件を満たすとき, $*$ は $\diamond$ に対し左分配的であるという:

$$1. x \in X, y, y' \in Y \implies x * (y \diamond y') = (x * y) \diamond (x * y').$$

Definition 2.5.12. 二項演算

$$\begin{array}{ccc} & X \times X & \longrightarrow X \\ \bullet * \bullet: & \Downarrow & \Downarrow \\ & (x, x') & \longmapsto x * x' \\ & X \times Y & \longrightarrow X \\ \bullet \diamond \bullet: & \Downarrow & \Downarrow \\ & (x, y) & \longmapsto x \diamond y \end{array}$$

に対し, 次の条件を満たすとき, $\diamond$ は $*$ に対し右分配的であるという:

$$1. x, x' \in X, y \in Y \implies (x * x') \diamond y = (x * y) \diamond (x' * y).$$

第3章

代表的な代数系の定義

演算を伴った集合を代数系と呼ぶ。演算が複数与えられることもある。ここでは、代表的な代数系について定義と例を紹介する。

3.1 半群とモノイド

Definition 3.1.1. X を集合とし、 $*$ を X 上の二項演算とする。次の条件を満たすとき、 $(X, *)$ を半群 (semi-group) と呼ぶ:

$$1. x, y, z \in X \implies (x * y) * z = x * (y * z).$$

つまり、 $*$ が結合律をみたす二項演算であるとき、 $(X, *)$ を半群 (semi-group) と呼ぶ。

Remark 3.1.2. $(X, *)$ が半群であることを、 X は $*$ で半群であると言い表すことがある。また、文脈上 $*$ が明らかなき際には、 X が半群であるということもある。

Definition 3.1.3. X を集合とし、 $*$ を X 上の二項演算とする。 $e \in X$ とする。以下の条件を満たすとき、 $(X, *, e)$ をモノイド (monoid) と呼ぶ:

$$1. x, y, z \in X \implies (x * y) * z = x * (y * z).$$

$$2. x \in X \implies e * x = x * e = x.$$

つまり、 $(X, *)$ が半群であり e が $*$ の単位元であるとき、 $(X, *, e)$ をモノイド (monoid) と呼ぶ。

Remark 3.1.4. $(X, *, e)$ がモノイドであることを、 X は $*$ で e を単位元とするモノイドであるという。また、文脈上問題ないときには X がモノイドであるということもある。 $*$ の単位元 e のことをモノイド X の単位元と呼ぶ。

Remark 2.3.7 で見たように、単位元は、存在するならただ一つである。したがって、 $(X, *, e)$ も $(X, *, e')$ もモノイドなら、 $e = e'$ である。そこで、単位元を明示せず $(X, *)$ がモノイドであるということもある。つまり、次の様に定義することもある:

Definition 3.1.5. X 上の二項演算 $*$ が以下の条件をみたすとき、 $(X, *)$ がモノイドと呼ぶ:

$$1. x, y, z \in X \implies (x * y) * z = x * (y * z).$$

2. 次の条件をみたす $e \in X$ が存在する:

$$(a) \ x \in X \implies e * x = x * e = x.$$

Remark 3.1.6. Definition 3.1.5 を言い換えると, 単位元をもつ半群をモノイドと呼ぶということである.

Example 3.1.7. $(\mathbb{Z}_{>0}, \cdot)$ は, 半群である. また, 1 が $\cdot$ の単位元であるので, $(\mathbb{Z}_{>0}, \cdot, 1)$ はモノイドである. 同様に, $(\mathbb{N}, \cdot, 1)$ もモノイドである.

Example 3.1.8. $(\mathbb{N}, +)$ は, 半群である. また, 0 が $+$ の単位元であるので, $(\mathbb{N}, +, 0)$ はモノイドである.

Nonexample 3.1.9. $(\mathbb{Z}_{>0}, +)$ も半群である. しかし, $0 \notin \mathbb{Z}_{>0}$ であり単位元が存在しないので, モノイドではない.

Nonexample 3.1.10. 整数 x, y に対し, その差を対応させる

$$\begin{array}{ccc} \bullet - \bullet & : & \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z} \\ & \Psi & \Psi \\ & (x, y) & \longmapsto x - y \end{array}$$

は二項演算である. このとき,

$$\begin{aligned} 0 - (0 - 1) &= 0 - (-1) = 1 \\ (0 - 0) - 1 &= 0 - 1 = -1 \end{aligned}$$

となり結合律が成り立たない. したがって, $(\mathbb{Z}, -)$ は半群ではない.

Nonexample 3.1.11. 2 元集合 $X = \{\top, \perp\}$ 上の演算 $\bullet \oplus \bullet$ を

$$\begin{array}{ll} \top \oplus \top = \perp & \top \oplus \perp = \top \\ \perp \oplus \top = \top & \perp \oplus \perp = \perp \end{array}$$

で定める. このとき, $(X, \oplus, \perp)$ はモノイドである. $\oplus$ は排他的論理和と呼ばれる.

Example 3.1.12. X を集合とする. X の元の列 $w_1 w_2 \cdots w_l$ を, X をアルファベットとする長さ l のワードと呼ぶ. 長さ 0 のワードを空列と呼び, ここでは λ で表す. X^* で X をアルファベットとするワードをすべて集めた集合とする. $w = w_1 w_2 \cdots w_l, v = v_1 v_2 \cdots v_m \in X^*$ に対し, w と v の連結 $w \cdot v$ を,

$$w \cdot v = w_1 w_2 \cdots w_l v_1 v_2 \cdots v_m$$

で与えられる長さ $l + m$ のワードとする. このとき, $(X^*, \cdot, \lambda)$ はモノイドである.

3.2 群

Definition 3.2.1. $*$ を G 上の二項演算とする. $e \in G$ とし, $\bullet^{-1}$ を G 上の単項演算とする. 以下の条件を満たすとき, $(G, *, e, \bullet^{-1})$ を群と呼ぶ:

1. $x, y, z \in G \implies (x * y) * z = x * (y * z).$
2. $x \in G \implies x * e = e * x = x.$
3. $x \in G \implies x * x^{-1} = x^{-1} * x = e.$

3.3 環

Remark 3.2.2. $(G, *, e, \bullet^{-1})$ が群であることを, X は $*$ で, e を単位元とし, x^{-1} が x の逆元である群であるという. また, 文脈上問題ないときには G が群であるということもある. $*$ の単位元 e のことを群 G の単位元と呼ぶ.

Remarks 2.3.7 and 2.4.10 で見たように, G の単位元や x の逆元は, $*$ に対し一意的に定まる. 単位元や逆元与え方を明示せず $(G, *)$ が群であるということもある. つまり, 次の様に定義することもある:

Definition 3.2.3. G 上の二項演算 $*$ が以下の条件をみたすとき, $(G, *)$ を群と呼ぶ:

1. $x, y, z \in G \implies (x * y) * z = x * (y * z)$.
2. 次の条件をみたす $e \in G$ が存在する:
 - (a) $x \in G \implies e * x = x * e = x$.
3. Item 2 の e と任意の $x \in G$ に対し, 次の条件を満たす $y \in G$ が存在する:
 - (a) $x * y = y * x = e$.

Remark 3.2.4. Definition 3.2.3 を言い換えると, すべての元に対し逆元が存在するモノイドを群と呼ぶということである.

Definition 3.2.5. 群 $(G, *, e, \bullet^{-1})$ が次の条件を満たすとき, $(G, *, e, \bullet^{-1})$ をアーベル群と呼ぶ.

1. $x, y \in G \implies x * y = y * x$.

Remark 3.2.6. 可換演算による群のことをアーベル群と呼ぶ. アーベル群のことを可換群と呼ぶこともある.

Example 3.2.7. $(\mathbb{Z}, +, 0, -\bullet)$ はアーベル群である.

Example 3.2.8. 集合 X に対し, $\text{Sym}(X)$ を

$$\text{Sym}(X) = \{ f: X \rightarrow X: \text{全単射} \}$$

と定義する. 写像の合成 $\circ$ は $\text{Sym}(X)$ 上の二項演算である. $(\text{Sym}(X), \circ, \text{id}_X, \bullet^{-1})$ は群である. また, $S_n = \text{Sym}(\{1, \dots, n\})$ とおき, n 次対称群と呼ぶ. S_1, S_2 はアーベル群であるが, $n \geq 3$ に対し, S_n はアーベル群ではない

3.3 環

Definition 3.3.1. 次を満たすとき, $(R, +, \cdot, 0_R, 1_R)$ は環であるという:

1. $(R, +, 0_R)$ はアーベル群である.
2. $(R, \cdot, 1_R)$ はモノイドである.
3. $a, b, c \in R$ に対し, 次が成り立つ:

$$\begin{aligned} a(b + c) &= ab + ac \\ (b + c)a &= ba + ca \end{aligned}$$

Definition 3.3.2. 次を満たすとき, $(R, +, \cdot, 0_R, 1_R)$ は可換環であるという:

1. $(R, +, \cdot, 0_R, 1_R)$ は環.

2. $a, b \in R$ に対し, 次が成り立つ:

$$ab = ba$$

Example 3.3.3. $(\mathbb{Z}, +, \cdot)$ は可換環. この環を, 有理整数環と呼ぶ.

Definition 3.3.4. 環 R の元 a が乗法に関する逆元をもつとき, つまり $ab = ba = 1$ を満たす元 $b \in R$ が存在するとき, a を可逆元と予備, a の逆元 b を b^{-1} で表す.

Proposition 3.3.5. R の可逆元全体のなす集合は, 乗法で群になる.

Proof. □

Definition 3.3.6. R の可逆元全体のなす集合を $R^\times$ や R^* で表す.

Proof. □

Definition 3.3.7. a を環 R の元とする. $ab = 0_R$ を満たす $b \in R \setminus \{0_R\}$ が存在するとき, a を左零因子と呼ぶ. $ba = 0_R$ を満たす $b \in R \setminus \{0_R\}$ が存在するとき, a を右零因子と呼ぶ. 左零因子や右零因子を零因子と呼ぶ. 0_R 以外の零因子がない可換環を整域とよぶ.

Example 3.3.8. 有理整数環 $(\mathbb{Z}, +, \cdot)$ は整域.

Nonexample 3.3.9. $\mathbb{Z}/6\mathbb{Z}$ は整域ではない.

3.4 体

Definition 3.4.1. 次を満たすとき, $(K, +, \cdot, 0_R, 1_R)$ は体であるという:

1. $(K, +, \cdot, 0_R, 1_R)$ は可換環.
2. どの $a \in R \setminus \{0\}$ も可逆元である.

Example 3.4.2. $\mathbb{Q}$ は体である. これを有理数体と呼ぶ.

Nonexample 3.4.3. 有理整数環 $\mathbb{Z}$ は体ではない.

Example 3.4.4. $\mathbb{Z}/5\mathbb{Z}$ は体.

Nonexample 3.4.5. $\mathbb{Z}/6\mathbb{Z}$ は体ではない.

Proposition 3.4.6. F が体ならば, F は整域.

Proof. □

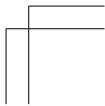
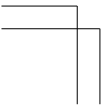
以下はあとでやる.

Proposition 3.4.7. $\mathbb{Z}/n\mathbb{Z}$ は n が素数のとき体となる. n が合成数のときには, 体ではない.

Proof. □

Proposition 3.4.8. 有限体の位数は素数の冪である. また逆に p を素数として n を正の整数とすると, p^n を位数とする有限体が同型を除いてただ一つ存在する.

Proof. □



第 4 章

群

4.1 群の構造

4.1.1 準同型写像と同型写像

Definition 4.1.1 (再掲). $*$ を G 上の二項演算とする. $e \in G$ とし, $\bullet^{-1}$ を G 上の単項演算とする. 以下の条件を満たすとき, $(G, *, e, \bullet^{-1})$ を群と呼ぶ:

1. $x, y, z \in G \implies (x * y) * z = x * (y * z).$
2. $x \in G \implies x * e = e * x = x.$
3. $x \in G \implies x * x^{-1} = x^{-1} * x = e.$

Remark 4.1.2. 通常は, 群の演算を乗法と呼び, x の逆元を与える単項演算は x^{-1} のような形で与え, 単位元を 1 や e などのような記号で与えることが多い. アーベル群の際には, 演算に $+$ のような記号を用い, x の逆元を与える単項演算を $-x$ のような形で与え, また単位元を 0 のような記号で与えることがある. この様な表記を用いたアーベル群を加法群と呼び, その演算を加法と呼ぶ.

Definition 4.1.3. $(G_1, *_1, e_1, \bullet^{-1}), (G_2, *_2, e_2, \bullet^{-1})$ を群とする. G_1 から G_2 への写像 f が次の条件を満たすとき, f は $(G_1, *_1, e_1, \bullet^{-1})$ から $(G_2, *_2, e_2, \bullet^{-1})$ への群準同型写像であるという:

1. $a, b \in G_1 \implies f(a *_1 b) = f(a) *_2 f(b).$

Example 4.1.4. $(\mathbb{Z}, +)$ は群であった. $(\{1, -1\}, \cdot)$ も群であった.

$$\begin{array}{ccc} \varphi : \mathbb{Z} & \longrightarrow & \{1, -1\} \\ \Downarrow & & \Downarrow \\ i & \longmapsto & (-1)^i \end{array}$$

は準同型写像である.

Example 4.1.5. $(\mathbb{R}, +)$ は群であった. $(\mathbb{R}_{>0}, \cdot)$ も群であった.

$$\begin{array}{ccc} \varphi : \mathbb{R}_{>0} & \longrightarrow & \mathbb{R} \\ \Downarrow & & \Downarrow \\ t & \longmapsto & e^t \end{array}$$

は準同型写像である.

$$\begin{array}{ccc} \psi & : & \mathbb{R} \longrightarrow \mathbb{R}_{>0} \\ \Psi & & \Psi \\ t & \longmapsto & \log(t) \end{array}$$

も準同型写像である.

Example 4.1.6.

$$\begin{aligned} G &= \left\{ \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix} \mid \theta \in \mathbb{R} \right\} \\ G' &= \{ \cos(\theta) + \sin(\theta)\sqrt{-1} \mid \theta \in \mathbb{R} \} \end{aligned}$$

とおくと, G は行列としての積で, G' は複素数としての積で群である.

$$\begin{array}{ccc} \varphi & : & G \longrightarrow G' \\ \Psi & & \Psi \\ \begin{pmatrix} x & -y \\ y & x \end{pmatrix} & \longmapsto & x + \sqrt{-1}y \end{array}$$

は準同型写像である.

$$\begin{array}{ccc} \varphi & : & G' \longrightarrow G \\ \Psi & & \Psi \\ x + \sqrt{-1}y & \longmapsto & \begin{pmatrix} x & -y \\ y & x \end{pmatrix} \end{array}$$

も準同型写像である.

Proposition 4.1.7. $(G_1, *_1, e_1, \bullet^{-1})$, $(G_2, *_2, e_2, \bullet^{-1})$ を群とし, f を $(G_1, *_1, e_1, \bullet^{-1})$ から $(G_2, *_2, e_2, \bullet^{-1})$ への準同型写像であるとする. このとき, $f(e_1) = e_2$.

Proof.

□

Proposition 4.1.8. $(G_1, *_1, e_1, \bullet^{-1})$, $(G_2, *_2, e_2, \bullet^{-1})$ を群とし, f を $(G_1, *_1, e_1, \bullet^{-1})$ から $(G_2, *_2, e_2, \bullet^{-1})$ への準同型写像であるとする. このとき, $x \in G_1$ に対し, $f(x^{-1}) = f(x)^{-1}$.

Proof.

□

Definition 4.1.9. f を $(G_1, *_1, e_1, \bullet^{-1})$ から $(G_2, *_2, e_2, \bullet^{-1})$ への群準同型写像とする.

$$\begin{aligned} \text{Ker}(f) &= \{ x \in G_1 \mid f(x) = e_2 \} \\ \text{Img}(f) &= \{ f(x) \mid x \in G_1 \} \end{aligned}$$

とし, f の核, f の像と呼ぶ.

Example 4.1.10. $(\mathbb{Z}, +)$ は群であった. $(\{1, -1\}, \cdot)$ も群であった.

$$\begin{array}{ccc} \varphi & : & \mathbb{Z} \longrightarrow \{1, -1\} \\ \Psi & & \Psi \\ i & \longmapsto & (-1)^i \end{array}$$

は準同型写像であった.

$$\begin{aligned} \text{Ker}(\varphi) &= \{ 2n \mid n \in \mathbb{Z} \} \\ \text{Img}(\varphi) &= \{ 1, -1 \} \end{aligned}$$

である.

4.1 群の構造

Example 4.1.11. $(\mathbb{R}, +)$ は群であった. $(\mathbb{R} \setminus \{0\}, \cdot)$ も群であった.

$$\begin{array}{ccc} \varphi : \mathbb{R} & \longrightarrow & \mathbb{R} \setminus \{0\} \\ \Downarrow & & \Downarrow \\ t & \longmapsto & e^t \end{array}$$

は準同型写像である.

$$\begin{aligned} \text{Ker}(\varphi) &= \{0\} \\ \text{Img}(\varphi) &= \mathbb{R}_{>0} \end{aligned}$$

である.

Proposition 4.1.12. $(G_1, *_1, e_1, \bullet^{-1})$, $(G_2, *_2, e_2, \bullet^{-1})$ を群とし, f を $(G_1, *_1, e_1, \bullet^{-1})$ から $(G_2, *_2, e_2, \bullet^{-1})$ への準同型写像であるとする. このとき, 以下が成り立つ:

1. f が全射 $\iff \text{Img}(f) = G_2$.
2. f が単射 $\iff \text{Ker}(f) = \{e_1\}$.

Proof.

□

Definition 4.1.13. $(G_1, *_1, e_1, \bullet^{-1})$, $(G_2, *_2, e_2, \bullet^{-1})$ を群とする. 次の条件を満たすとき, f は $(G_1, *_1, e_1, \bullet^{-1})$ から $(G_2, *_2, e_2, \bullet^{-1})$ への同型写像であるという:

1. f は $(G_1, *_1, e_1, \bullet^{-1})$ から $(G_2, *_2, e_2, \bullet^{-1})$ への群準同型写像である.
2. 次の条件を満たす g が存在する:
 - (a) g は $(G_2, *_2, e_2, \bullet^{-1})$ から $(G_1, *_1, e_1, \bullet^{-1})$ の群準同型写像である.
 - (b) $g \circ f = \text{id}_{G_1}$.
 - (c) $f \circ g = \text{id}_{G_2}$.

Definition 4.1.14. $(G_1, *_1, e_1, \bullet^{-1})$, $(G_2, *_2, e_2, \bullet^{-1})$ を群とする. $(G_1, *_1, e_1, \bullet^{-1})$ から $(G_2, *_2, e_2, \bullet^{-1})$ への同型写像 f が存在するとき, $(G_1, *_1, e_1, \bullet^{-1})$ と $(G_2, *_2, e_2, \bullet^{-1})$ は同型であるという. また, $(G_1, *_1, e_1, \bullet^{-1})$ と $(G_2, *_2, e_2, \bullet^{-1})$ は同型であることを, $(G_1, *_1, e_1, \bullet^{-1}) \simeq (G_2, *_2, e_2, \bullet^{-1})$ で表す.

Example 4.1.15. $(\mathbb{R}, +)$, $(\mathbb{R}_{>0}, \cdot)$ は群であり,

$$\begin{array}{ccc} \varphi : \mathbb{R}_{>0} & \longrightarrow & \mathbb{R} \\ \Downarrow & & \Downarrow \\ t & \longmapsto & e^t \end{array}$$

$$\begin{array}{ccc} \psi : \mathbb{R} & \longrightarrow & \mathbb{R}_{>0} \\ \Downarrow & & \Downarrow \\ t & \longmapsto & \log(t) \end{array}$$

は準同型写像である.

$$\begin{aligned} \varphi \circ \psi &= \text{id}_{\mathbb{R}} \\ \psi \circ \varphi &= \text{id}_{\mathbb{R}_{>0}} \end{aligned}$$

であるので, これらは同型写像であり, $\mathbb{R}_{>0}$ と $\mathbb{R}$ は同型である.

Example 4.1.16.

$$G = \left\{ \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix} \mid \theta \in \mathbb{R} \right\}$$

$$G' = \{ \cos(\theta) + \sin(\theta)\sqrt{-1} \mid \theta \in \mathbb{R} \}$$

とおくと, G は行列としての積で, G' は複素数としての積で群であり,

$$\begin{aligned} \varphi : G &\longrightarrow G' \\ \Psi &\quad \quad \quad \Psi \\ \begin{pmatrix} x & -y \\ y & x \end{pmatrix} &\longmapsto x + \sqrt{-1}y \\ \psi : G' &\longrightarrow G \\ \Psi &\quad \quad \quad \Psi \\ x + \sqrt{-1}y &\longmapsto \begin{pmatrix} x & -y \\ y & x \end{pmatrix} \end{aligned}$$

は準同型写像である.

$$\begin{aligned} \varphi \circ \psi &= \text{id}_{G'} \\ \psi \circ \varphi &= \text{id}_G \end{aligned}$$

であるので, これらは同型写像であり, G と G' は同型である.

Remark 4.1.17. $(G, *, e, \bullet^{-1})$ を群とする. $(G, *, e, \bullet^{-1})$ から $(G, *, e, \bullet^{-1})$ への群準同型写像を自己準同型写像, $(G, *, e, \bullet^{-1})$ から $(G, *, e, \bullet^{-1})$ への同型写像を自己同型写像と呼ぶ.

Lemma 4.1.18. $(G_1, *_1, e_1, \bullet^{-1})$, $(G_2, *_2, e_2, \bullet^{-1})$ を群とする. f は $(G_1, *_1, e_1, \bullet^{-1})$ から $(G_2, *_2, e_2, \bullet^{-1})$ への準同型写像とする. f が全単射であるとき, 逆写像 f^{-1} は, $(G_2, *_2, e_2, \bullet^{-1})$ から $(G_1, *_1, e_1, \bullet^{-1})$ への準同型写像である.

Proof. □

Proposition 4.1.19. $(G_1, *_1, e_1, \bullet^{-1})$, $(G_2, *_2, e_2, \bullet^{-1})$ を群とする. 写像 $f: G_1 \rightarrow G_2$ に対し以下は同値:

1. f は同型写像.
2. f は全単射かつ $(G_1, *_1, e_1, \bullet^{-1})$ から $(G_2, *_2, e_2, \bullet^{-1})$ への準同型写像.

Proof. □

4.1.2 準同型定理

TODO: 正規部分群を定義する. 例を挙げる. 剰余群を定義する. 例を挙げる. 準同型定理. 例を挙げる. normal iff Ker

Definition 4.1.20. $(G, *, e, \bullet^{-1})$ を群とする. $H \subset G$ とする. $(H, *, e, \bullet^{-1})$ が群であるとき, H は $(G, *, e, \bullet^{-1})$ の部分群であるという.

4.1 群の構造

Remark 4.1.21. $(G, *, e, \bullet^{-1})$ を群とし, $H \subset G$ とする. $(H, *, e, \bullet^{-1})$ が群であるためには, $*$ が H 上の二項演算でないといけない. つまり,

$$x, y \in H \implies x * y \in H$$

でないといけない. また, $e \in H$ でないといけない. また, $\bullet^{-1}$ は H 上の単項演算でないといけない. つまり,

$$x \in H \implies x^{-1} \in H$$

でないといけない. 一方, これらの演算が H で閉じていることがわかれば, $*$ が結合律を満たすこと, e が単位元であること, x^{-1} が x の逆元であることは, 演算の性質であるので, G が群であることから自動的に成り立つ.

Proposition 4.1.22. $(G, *, e, \bullet^{-1})$ を群とし, $H \subset G$ とする. このとき, 以下は同値:

1. H が G の部分群である.
2. 以下が成り立つ:
 - (a) $x, y \in H \implies x * y \in H$.
 - (b) $e \in H$.
 - (c) $x \in H \implies x^{-1} \in H$.
3. 以下が成り立つ:
 - (a) $H \neq \emptyset$.
 - (b) $x, y \in H \implies x * y^{-1} \in H$.
4. 以下が成り立つ:
 - (a) $H \neq \emptyset$.
 - (b) $x, y \in H \implies x^{-1} * y \in H$.

Example 4.1.23.

$$\zeta = e^{\frac{2\pi\sqrt{-1}}{6}} = \cos\left(\frac{2\pi}{6}\right) + \sin\left(\frac{2\pi}{6}\right)\sqrt{-1}$$

とし,

$$G = \{1, \zeta, \zeta^2, \zeta^3, \zeta^4, \zeta^5\}$$

とすると, $(G, \cdot)$ は群である. G の部分集合のうち,

$$H_6 = \{1, \zeta, \zeta^2, \zeta^3, \zeta^4, \zeta^5\}$$

$$H_3 = \{1, \zeta^2, \zeta^4\}$$

$$H_2 = \{1, \zeta^3\}$$

$$H_1 = \{1\}$$

は G の部分群である.

Example 4.1.24. $(G, *, e, \bullet^{-1})$ を群とする. G と $\{e\}$ は G の部分群となる.

Definition 4.1.25. $(G, *, e, \bullet^{-1})$ を群とする. G と $\{e\}$ を G の自明な部分群と呼ぶ. G でも $\{e\}$ でもない G の部分群を G の非自明な部分群と呼ぶ. G とは等しくはない G の部分群を G の真の部分群と呼ぶ.

Example 4.1.26. Example 4.1.23 で挙げた例を再び考える. H_1, H_6 が G の自明な部分群. H_2, H_3 が G の非自明な部分群. H_1, H_2, H_3 が G の真の部分群.

Definition 4.1.27. $(G, *, e, \bullet^{-1})$ を群とする. 次の条件を満たすとき N を G の正規部分群と呼ぶ:

1. N は, G の部分群.
2. $x \in N, g \in G \implies g * x * g^{-1} \in N$.

Example 4.1.28. 自明な部分群は正規部分群.

Example 4.1.29. アーベル群の部分群は正規部分群.

Proposition 4.1.30. f を $(G_1, *_1, e_1, \bullet^{-1})$ から $(G_2, *_2, e_2, \bullet^{-1})$ への群準同型写像とする. このとき, 以下が成り立つ:

1. $\text{Img}(f)$ は G_2 の部分群.
2. $\text{Ker}(f)$ は G_1 の正規部分群.

Proof. □

Definition 4.1.31. $(G, *, e, \bullet^{-1})$ を群とし, H を G の部分群とする. このとき, $x \in G$ に対し, $x * H = \{ x * h \mid h \in H \}$ とし,

$$G/H = \{ x * H \mid x \in G \}$$

と定義する.

Lemma 4.1.32. $(G, *, e, \bullet^{-1})$ を群とし, N を G の正規部分群とする. $x * N = x' * N$ かつ $y * N = y' * N$ ならば, $(x * y) * N = (x' * y') * N$

Proof. □

Theorem 4.1.33. $(G, *, e, \bullet^{-1})$ を群とし, N を G の正規部分群とする. $x * N, y * N \in G/N$ に対し,

$$(x * N) \cdot (y * N) = (x * y) * N$$

G/N はこの演算で群となる. G/N の単位元は $e * N = N$ であり, $x * N$ の逆元は $x^{-1} * N$ である.

Proof. □

Definition 4.1.34. $(G, *, e, \bullet^{-1})$ を群とし, N を G の正規部分群とする. Theorem 4.1.33 の群 G/N を G の N による剰余群と呼ぶ. 通常は G/N の演算も G の演算と同じ記号を用いる. つまり $x * N$ と $y * N$ の積を $(x * N) * (y * N)$ と書く.

Theorem 4.1.35. 群準同型写像 $f: G \rightarrow G'$ に対し, $G/\text{Ker}(f) \simeq \text{Img}(f)$.

Proof. $x, y \in G$ かつ $x * \text{Ker}(f) = y * \text{Ker}(f)$ であるとき, $x = y * k$ を $k \in \text{Ker}(f)$ みたす k がとれるので, $f(x) = f(y * k) = f(y) * f(k) = f(y) * e_{G'} = f(y)$ となる. したがって

4.2 群に関する用語

て, 次の写像が定義できる.

$$\begin{array}{ccc} g & : & G/\text{Ker}(f) \longrightarrow \text{Img}(f) \\ & \Downarrow & \Downarrow \\ & & x * \text{Ker}(f) \longmapsto f(x) \end{array}$$

また,

$$\begin{aligned} g(x * \text{Ker}(f)) *_2 g(y * \text{Ker}(f)) &= f(x) *_2 f(y) \\ g(x * \text{Ker}(f) * y * \text{Ker}(f)) &= f(x * y * \text{Ker}(f)) = f(x * y) = f(x) *_2 f(y). \end{aligned}$$

であるので, g は準同型写像.

$f(x) \in \text{Img}(f)$ に対し, $x * \text{Ker}(f) \in G/\text{Ker}(f)$ をとれば, $f(x) = g(x * \text{Ker}(f))$ であることから, 全射であることがわかる.

また, $g(x * H) = e'$ とすると, $f(x) = e'$ であるので, $x \in \text{Ker}(f)$ である. したがって, $\text{Ker}(g) = \{e * \text{Ker}(f)\}$ である. $\square$

4.2 群に関する用語

Definition 4.2.1. 集合 G が有限集合であるとき, 群 $(G, *, e, \bullet^{-1})$ を有限群と呼ぶ. 集合 G に含まれる元の個数を群 $(G, *, e, \bullet^{-1})$ の位数と呼び, $|G|$ で表す.

集合 G が無限集合であるとき, 群 $(G, *, e, \bullet^{-1})$ を無限群と呼ぶ. また, 位数は無限であるといい $|G| = \infty$ と書く.

Definition 4.2.2. $(G, *, e, \bullet^{-1})$ を群とし, $x \in G$ とする. $x^k = e$ となる正の整数がないとき, x の位数は無限であるといい, そうでないとき, x の位数は有限であるという. x の位数が有限であるとき, $x^k = e$ となる正の整数で最小のものを, 元 x の位数と呼ぶ.

Example 4.2.3. $(\mathbb{Z}, +, 0, -\bullet)$ はアーベル群である. 0 の位数は 1 , それ以外の元の位数は無限.

Example 4.2.4. $\{0, 1, 2, \dots, 6\}$ は通常の $+$ では群にならない. $(\text{mod } 6)$ では群. 各元の位数は $1, 6, 3, 2, 2, 3, 6$.

Definition 4.2.5. 自明な部分群以外に正規部分群がない群を単純群と呼ぶ.

Remark 4.2.6. アーベル群の部分群は正規部分群.

Definition 4.2.7. $S \subset G$ に対し,

$$\langle S \rangle = \{ a_1^{m_1} * \dots * a_k^{m_k} \mid k \in \mathbb{N}, a_i \in G, m_i \in \mathbb{Z} \}$$

とすると G の部分群となる. S で生成された G の部分群と呼び, S をこの部分群の生成系とよぶ.

Definition 4.2.8. $a \in G$ に対し,

$$\langle a \rangle = \{ a^n \mid n \in \mathbb{Z} \}$$

とおく. a で生成された巡回群と呼ぶ.

Example 4.2.9. $(\mathbb{Z}, 0, +, -\bullet)$ は 1 で生成されている.

Proposition 4.2.10. $(G_1, *_1, e_1, \bullet^{-1})$, $(G_2, *_2, e_2, \bullet^{-1})$ を群とする. $G_1 \times G_2 = \{(x_1, x_2) \mid x_1 \in G_1, x_2 \in G_2\}$ 上の演算 $*$ を,

$$(x_1, x_2) * (y_1, y_2) = (x_1 *_1 y_1, x_2 *_2 y_2)$$

で定めると, $(G_1 \times G_2, *)$ は群になる. これを G_1 と G_2 の直積群と呼ぶ.

Proof.

□

Example 4.2.11. $\mathbb{Z}/6\mathbb{Z}$ の自己同型すべて.

Example 4.2.12. $\mathbb{R} \times \mathbb{R}$ と $\mathbb{C}$ は同型.

4.2.1 剰余類

群 G とその部分群 H について考える, G 上の二項関係 $\sim$ を次で定義する:

$$x \sim y \iff x^{-1} * y \in H.$$

このとき, $\sim$ は, 以下を満たす:

1. $x \in G \implies x \sim x$
2. $x \sim y, y \sim z \implies x \sim z$
3. $x \sim y \implies y \sim x$

つまり, $\sim$ は G 上の同値関係である. $\sim$ による剰余類は

$$x * H = \{x * h \mid h \in H\}$$

とかける. G/H で, 剰余類を全て集めた集合 $\{x * H \mid x \in G\}$ を表す.

Theorem 4.2.13. G を有限群とし, H を G の部分群とする. このとき, H の位数は G の位数を割り切る.

Definition 4.2.14. $\frac{|G|}{|H|}$ を G における H の指数と呼ぶ.

4.2.2 有限アーベル群

$\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ 上の演算を,

$$(a, b) + (a', b') = (a + a', b + b')$$

で定義する. この演算によりアーベル群になる.

Theorem 4.2.15. m, n が互いに素のとき, $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/mn\mathbb{Z}$.

Example 4.2.16. $\mathbb{Z}/6\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$

Theorem 4.2.17 (有限生成アーベル群の基本定理). 有限生成アーベル群 G に対し,

$$G \simeq \mathbb{Z}^n \times \mathbb{Z}/p_1^{a_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k^{a_k}\mathbb{Z}$$

を満たす素数 p_i と整数 n, a_i が存在する.

4.2.3 一般線形群

$$GL(n, \mathbb{R}) = \{ A \} SL(n, \mathbb{R})$$

Example 4.2.18. $\det$ は準同型写像

Example 4.2.19. $SL(n, \mathbb{R})$ は $GL(n, \mathbb{R})$ の正規部分群.

4.2.4 対称群

$n > 2$ で, S_n はアーベル群ではない.

Theorem 4.2.20. 任意の置換はいくつかの巡回置換の積で表せる.

Proof. □

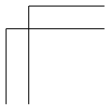
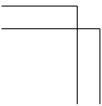
Theorem 4.2.21. 任意の置換はいくつかの互換の積で表せる.

Proof. □

Definition 4.2.22. σ の符号. 偶置換, 奇置換.

Proof. □

符号は, 準同型写像. 交代群.



第5章

環

5.1

環を定義する. 準同型写像を定義する. 同型写像を定義する. 同型写像の定義を言い換える. 同型な環の例をあげる. ($\mathbb{C}$ の行列による実現)

部分環を定義する. イデアルを定義する. 例を挙げる. 剰余環を定義する. 例を挙げる. 準同型定理. 例を挙げる. $\text{ideal} \iff \text{Ker}$

5.2

Definition 5.2.1. 右イデアル, 左イデアル, 両側イデアル.

Example 5.2.2. 自明なイデアル.

Example 5.2.3. $\{0, 3, 6, 9\} \subset \mathbb{Z}/12\mathbb{Z}$ はイデアル.

Definition 5.2.4. 単項イデアル, 単項イデアル整域.

Example 5.2.5. $\mathbb{Z}$ は PID.

Definition 5.2.6. 剰余環.

Example 5.2.7. 2×2 行列環.

$$\left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \mid a, b \in \mathbb{Q} \right\} \qquad \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \mid a, b \in \mathbb{Q} \right\}$$

は片側イデアル.

$$\left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \mid a, b \in \mathbb{Q} \right\}$$

は両側イデアル.

Definition 5.2.8. 極大イデアル. 素イデアル.

5.2.1

Theorem 5.2.9. 可換環 R のイデアル I に対し以下は同値:

1. I が素イデアルである
2. R/I が整域である

Proof.

■Item 1 $\implies$ Item 2

■Item 2 $\implies$ Item 1

□

Theorem 5.2.10. 可換環 R のイデアル I に対し以下は同値:

1. I が極大イデアルである
2. R/I が体である

Proof.

■Item 1 $\implies$ Item 2

■Item 2 $\implies$ Item 1

□

Theorem 5.2.11. 可換環の極大イデアルは素イデアルである.

Proof. I を可換環 R の極大イデアルであるとする. このとき, Theorem 5.2.10 より, R/I は体. よって, R/I は整域. Theorem 5.2.9 より, I は素イデアル. □

Definition 5.2.12. 環 $(R_1, +_1, *_1, 1_1)$, $(R_2, +_2, *_2, 1_2)$ 以下の条件を満たすとき写像 $\varphi: R_1 \rightarrow R_2$ は, $(R_1, +_1, *_1, 1_1)$ から $(R_2, +_2, *_2, 1_2)$ への環準同型写像であるという.

1. $a, b \in R_1 \implies \varphi(a + b) = \varphi(a) + \varphi(b)$.
2. $a, b \in R_1 \implies \varphi(a * b) = \varphi(a) * \varphi(b)$.
3. $\varphi(1_1) = 1_2$.

Definition 5.2.13. 同型写像, 同型

Proposition 5.2.14. 1. φ が同型である
2. φ 全単射な準同型である

Proof.

□

Definition 5.2.15. Ker, Img

Theorem 5.2.16. $R_1 / \text{Ker}(\varphi) \simeq \text{Img}(\varphi)$

Proof.

□

5.3 整数

Definition 5.3.1. $a \mid b$ $a \nmid b$

Theorem 5.3.2. $a, b \in \mathbb{Z}$, $b > 0$ とする. このとき, $a = qb + r$, $0 \leq r < b$ を満たす, $q, r \in \mathbb{Z}$ が存在する.

Proof. □

Definition 5.3.3. a, b の公約数. 最大公約数.

Proposition 5.3.4. 最大公約数は公約数のうち $<$ で最大のもの.

Proof. □

Definition 5.3.5. a, b の公倍数. 最小公倍数.

Proposition 5.3.6. 最小公倍数は正の公倍数のうち $<$ で最小のもの.

Proof. □

Proposition 5.3.7. $a, b \in \mathbb{Z}$ とする. 最小公倍数 m , 最大公約数 d は, $ab = md$ を満たす.

Proof. □

Proposition 5.3.8. $a, b \in \mathbb{Z} \setminus \{0\}$ とし, $A = \{ax + by \mid x, y \in \mathbb{Z}\}$ とする. $\min \{a \in A \mid a > 0\}$ は a, b の最大公約数.

Proof. □

Definition 5.3.9. 素数, 合成数.

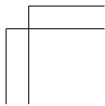
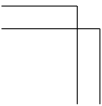
Proposition 5.3.10. 一意的に素因数分解できる.

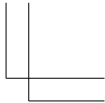
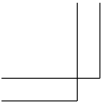
Proof. □

Definition 5.3.11. n 進数表示. 桁数.

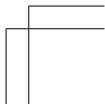
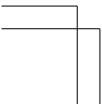
Proposition 5.3.12. n 進数表示の一意性.

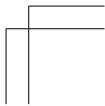
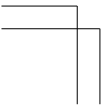
Proof. □





第 6 章
体





第 7 章

アルゴリズム関係

n 進数表示を得るアルゴリズム.

章末問題

- 1. 可換かつ結合的な二項演算の例を挙げよ.
- 2. 非可換かつ結合的な二項演算の例を挙げよ.
- 3. 可換かつ非結合的な二項演算の例を挙げよ.

付録 A

二項演算

A.1 二項演算の用語の図式による表記

A.2 二項演算の用語について

ここでは, X 上の二項関係に関して用いられる用語についていくつか紹介する. 以下では, $*$ を X 上の中置記法の二項演算とする. つまり

$$\begin{array}{ccc} \bullet * \bullet & : & X \times X \longrightarrow X \\ \Downarrow & & \Downarrow \\ (x, y) & \longmapsto & x * y \end{array}$$

とする.

A.2.1 吸収元

Definition A.2.1. $e \in X$ とする.

- 次の条件を満たすとき, z は $*$ に関し左吸収的であるという:
 - $x \in X \implies z * x = z$.
- 次の条件を満たすとき, e は $*$ に関し右吸収的であるという:
 - $x \in X \implies x * z = x$.
- z が, $*$ に関し左吸収的かつ $*$ に関し右吸収的であるとき, z は $*$ に関し吸収的であるという.

Lemma A.2.2. $z \in X$ が左吸収的であり, $z' \in X$ が右吸収的であるなら, $z = z'$,

Proof. $z * z'$ について考える. z は左吸収的であるので, $z * z' = z$. z' は右吸収的であるので, $z * z' = z'$. したがって, $z = z'$. $\square$

Corollary A.2.3. $e \in X, e' \in X$ が単位的なら, $e = e'$.

Remark A.2.4. Corollary A.2.3 により, 吸収的な元は存在するなら, ただ一つであることがわかる. 吸収的な元を (もし存在するなら) $*$ の吸収元 (absorbing element) と呼ぶ.

代数系によっては, 吸収元のことを零元と呼ぶもあるが, 加法単位元のことを零元と呼ぶ代数系のほうが多いように思う.

Corollary A.2.5. 右吸収元と左吸収元が存在するなら, それらは一致し $*$ の吸収元で

ある.

Corollary A.2.6. $*$ の吸収元が存在するとする.

1. 左吸収的な元は, $*$ の吸収元である.
2. 右吸収的な元は, $*$ の吸収元である.

Corollary A.2.7. $*$ は可換な二項演算であるとする.

1. 左吸収的な元は, $*$ の吸収元である.
2. 右吸収的な元は, $*$ の吸収元である.

Example A.2.8. $\mathbb{Z}_{\geq 0}$ における通常の積 $\cdot$ を考える. 0 は $\cdot$ に関する吸収元である.

Example A.2.9. $x, y \in \mathbb{R}_{\geq 0}$ に対し, $\min(x, y)$ を x と y の小さい方とする. このとき, $\min$ は $\mathbb{R}_{\geq 0}$ 上の二項演算である. 0 は $\min$ に関する吸収元である.

Example A.2.10. 二点集合 $\{0, 1\}$ 上の演算 $\triangleright$ を

$$\begin{array}{ll} 0 \triangleright 0 = 0 & 0 \triangleright 1 = 1 \\ 1 \triangleright 0 = 0 & 1 \triangleright 1 = 1 \end{array}$$

で定義する. このとき, 0 は右吸収的である. また 1 も右吸収的である.

Nonexample A.2.11. $\mathbb{Z}_{> 0}$ 上の積 $\cdot$ について考える. $x \in \mathbb{Z}_{> 0}$ とする. このとき, $2 \cdot x > x$ であるので, $2 \cdot x = x$ となることはない. したがって, $\cdot$ の吸収元は存在しない.

A.2.2 冪等元

Definition A.2.12. 次の条件を満たすとき, $c \in X$ を冪等元と呼ぶ:

1. $c * c = c$.

すべての元が冪等元であるとき, マグマ $(X, *)$ は冪等であるという.

Example A.2.13. $*$ の単位元 e は冪等元である.

Example A.2.14. 吸収的な元 z は冪等元である.

Example A.2.15. X を実数を成分とする二次正方行列全体からなる集合とする. 行列の積 $\cdot$ は X 上の二項演算である.

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

は冪等元である.

A.2.3 単位的

記号表

- $\mathbb{Z}$: 整数全体のなす集合.
- $\mathbb{R}$: 実数全体のなす集合.

- $\mathbb{R}_{>0}$: 正の実数全体のなす集合.
- $\mathbb{R}_{\geq 0}$: 非負実数全体のなす集合.
- S_n : n 次対称群.

111 2 34 511