1. 群・環・体

Definition (群)

集合 S に対して，演算・が定義されているとする．さらに

(1) $S \ni a, b$ に対して　$a \cdot b \in S$

(2) (結合律) $S \ni a, b, c$

$$(a \cdot b) \cdot c = a \cdot (b \cdot c)$$

(3) (単位元) $S \ni 1$ で $S \ni {}^\forall a$ に対して

$$a \cdot 1 = 1 \cdot a = a$$

(4) (逆元) $S \ni {}^\forall a$ に対して　$S \ni {}^\exists a'$

s.t.　$a \cdot a' = a' \cdot a = 1$

をみたすとき　$(S, \cdot)$ は群という．

Example

・$\mathbb{Z} = \{\text{整数}\} = \{0, \pm 1, \pm 2, \cdots\}$

$(\mathbb{Z}, +)$ no法　　$(\mathbb{Z}, \times)$ 乗法

① $\mathbb{Z} \ni 2, 3$　$2+3 = 5 \in \mathbb{Z}$　　① $2 \cdot 3 = 6 \in \mathbb{Z}$

② $\mathbb{Z} \ni a, b, c$.　$(a+b)+c = a+(b+c)$　　② $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

③ $\mathbb{Z} \ni 0$　$a + \boxed{0} = \boxed{0} + a = a$　　③ $\mathbb{Z}$　$a \cdot \boxed{1} = \boxed{1} \cdot a$

④ $\mathbb{Z} \ni 3$　$3 + \boxed{-3} = \boxed{-3} + 3 = 0$　　1が単位元

$\mathbb{Z} \ni {}^\forall a$

$a + \square = \square + a = 0$

$-a$ は a の逆元

$3 \times \square = \square \times 3 = 1$

$\mathbb{Z} \not\ni 1/3$

$(\mathbb{Z}, +)$ は群　　$(\mathbb{Z}, \times)$ は群でない．

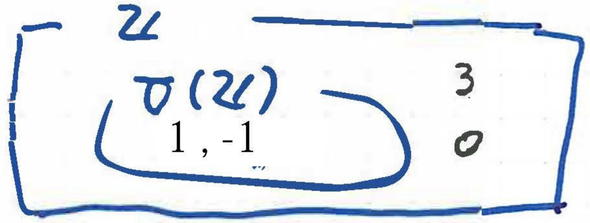
乗法に限定

$$U(\mathbb{Z}) = \{\mathbb{Z} \ni a \mid a \text{ の乗法の逆元} \in \mathbb{Z}\}$$

$$= \{\mathbb{Z} \ni a \mid a \cdot \square = 1,\ \square \in \mathbb{Z}\} = \{1, -1\}$$

注① ① 乗法の逆元 を a に対して a^{-1} とかく

② 加法の単位元 を 零元 という．



$\mathbb{Z} \setminus \{0\} \supsetneq U(\mathbb{Z})$

② 目標　$S \setminus \{0\} = U(S)$ となる S を作る

Def (環)

集合 S に $+, \times$ が定義されていて 下記をみたすとき S を環という．

(1) 加法に関して群

(2) 乗法に関して　(2-1) $S \ni a, b \Rightarrow a \cdot b \in S$

(2-2) $S \ni a, b, c$ に対して　$(a \cdot b) \cdot c = a \cdot (b \cdot c)$

(2-3) $S \ni 1$

(3) $S \to a.b.c$ (分配法則)

$(a+b)\times c = a\cdot c + b\,c$

$a\cdot(b+c) = a\cdot b + a\cdot c$

Example $(\mathbb{Z}, +, \times)$ は環

2. 剰余環

$\mathbb{Z} \to m>0$ に対して

$\mathbb{Z}/m\mathbb{Z} = \{m$で割った余りの集合$\} = \{0, 1, \cdots, m-1\}$

$m=7$ $\mathbb{Z}/7\mathbb{Z} = \{0, 1, 2, 3, 4, 5, 6\}$ ← 代表元

$m=3$

$\mathbb{Z}/m\mathbb{Z}$		
0 -3 3 6	1 4 -2	2 5 -1

$\mathbb{Z} \to a, b$ に対して

$a \equiv b \pmod m$

$\Leftrightarrow$ $a-b$ が m で割れる

$\mathbb{Z}/m\mathbb{Z}$ に演算を定義する

$\mathbb{Z}/m\mathbb{Z} \to a, b$ に対して

$a+b \equiv a+b$ を m で割った余り

$a\cdot b \equiv a\cdot b$ を m で割った余り

Example $\mathbb{Z}/3\mathbb{Z} = \{0, 1, 2\}$

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

×	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$2 + \square = 0$

$2 \times \square = 1$ $2\times 2 = 1$

$U(\mathbb{Z}/3\mathbb{Z}) = \{1, 2\} = \mathbb{Z}/3\mathbb{Z} \setminus \{0\}$

$\mathbb{Z}/3\mathbb{Z} \to \forall a \neq 0$ に逆元がある.

Example $\mathbb{Z}/4\mathbb{Z} = \{0, 1, 2, 3\}$

×	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

$U(\mathbb{Z}/4\mathbb{Z}) = \{1, 3\} \subsetneq_{+} \mathbb{Z}/4\mathbb{Z} \setminus \{0\}$

Def 環 R に対して $R \to \forall a \neq 0$ に対して 逆元 $a^{-1} \in R$ とき、R を体という.

(Theorem) $\mathbb{Z}/m\mathbb{Z}$ が体になる $\Leftrightarrow$ m が素数

Theorem $\mathbb{Z} \ni m > 0$ に対して

$\mathbb{Z}/m\mathbb{Z} \ni a$ に逆元がある $\Leftrightarrow$ a と m が互いに素

Def $\mathbb{Z}/m\mathbb{Z}$, $m > 0$ の整数

$\#U(\mathbb{Z}/m\mathbb{Z}) = \#\{\mathbb{Z}/m\mathbb{Z} \ni a \mid a^{-1} \in \mathbb{Z}/m\mathbb{Z}\}$

$= \varphi(m)$ (オイラー関数)

3. 逆元の求め方

Euclid の互除法

入力：$\mathbb{Z} \ni a, b$　　出力：$gcd(a,b)$

a と b の最大公約数

Example $\mathbb{Z} \ni 3, 5$

$gcd(3,5) = 1$　(互いに素)

$gcd(4,12) = 4$

(アイデア) $a = bq + r$　(q：商)　(r：余り)

$(|b| > r \geq 0)$

$gcd(a,b) = gcd(b,r)$

$a_1 \leftarrow a$,　$a_2 \leftarrow b$,　$q_1 \leftarrow q$,　$a_3 \leftarrow r$

$a_1 = a_2 q_1 + a_3$　$(|a_2| > a_3 \geq 0)$

$a_2 = a_3 q_2 + a_4$　$(|a_3| > a_4 \geq 0)$

$|a_1| > a_2 > a_3 > \cdots > a_{i+1} = 0$

$a_{i-1} = a_i q_i + a_{i+1}$　($a_{i+1} = 0$)

$gcd(a_i, 0) = a_i$

出力：$gcd(a_i, 0) = a_i$

拡張ユークリッドの互除法

入力：$\mathbb{Z} \ni a, b$　　出力：$ax + by = d = gcd(a,b)$

となる $a, b \in \mathbb{Z}$

(アイデア) Euclida 互除法 $\{a_i\}$

$\begin{cases} a_{j-1} = a_j q_j + a_{j+1} \\ a_j = a_j \end{cases}$

$\det(L_j) = -1 \neq 0$

$\Rightarrow \begin{bmatrix} a_{j-1} \\ a_j \end{bmatrix} = \underbrace{\begin{bmatrix} q_j & 1 \\ 1 & 0 \end{bmatrix}}_{L_j\ (2\times2\ 整数行列)} \begin{bmatrix} a_j \\ a_{j+1} \end{bmatrix}$　$L_j^{-1} = M_j$ とする

M_j かける.

$\begin{bmatrix} a_j \\ a_{j+1} \end{bmatrix} = M_j \begin{bmatrix} a_{j-1} \\ a_j \end{bmatrix} = M_j M_{j-1} \begin{bmatrix} a_{j-2} \\ a_{j-1} \end{bmatrix}$

$d \begin{bmatrix} a_i \\ a_{i+1} \end{bmatrix} = M_i \cdot M_{i-1} \cdots M_2 \begin{bmatrix} a_1 \\ a_2 \end{bmatrix} \begin{matrix} a \\ b \end{matrix}$

$$\begin{bmatrix} d \\ 0 \end{bmatrix} = \begin{bmatrix} x & y \\ z & w \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix}$$

$$\begin{bmatrix} d \\ 0 \end{bmatrix} = \begin{bmatrix} ax + by \\ az + bw \end{bmatrix}$$

$\mathbb{Z}/m\mathbb{Z} \ni a$ に対して $\gcd(m, a) = 1$ とすると

拡張 Euclid の互除法より

$$mx + ay = 1 \quad となる \quad x, y \in \mathbb{Z}$$

$$ay = 1 - mx$$

$$\equiv 1 \pmod{m}$$

y は a の $\mathbb{Z}/m\mathbb{Z}$ での逆元

4. 群の特徴

Def 群 (Group) G と $G \ni a$ に対して

$$\underbrace{a \cdots \cdot a}_{k} = 1$$

となる最小の正整数 あるいは ないときは ∞

を a の位数という.

G の元の個数を位数といい, $|G|$, $\#G$ で表す

Example

1) $\mathbb{Z}/3\mathbb{Z} = \{0, 1, 2\}$

2の位数は?

$2, 2 \cdot 2, 2 \cdot 2 \cdot 2, \cdots$

$2^2 = 1 \pmod 3$ より 2の位数は 2

(2) $\mathbb{Z} \ni 2$

$2, \quad 2^2 = 4, \quad 2^3 = 8, \quad$ 2の位数は ∞

5. べき演算

$\mathbb{Z}/m\mathbb{Z} \ni a$ に対して $(m > 0$, 整数)

- $a^k \pmod m$ を求める
- $a^2 \Rightarrow a$ が 100 bits $\rightarrow a^2$ は 200 bits

$$4 = 100$$

↑ 10進数　↑ 2進表記