02. 集合→環の復習

代数Ⅱ

群

- 空でない集合Gに対して，ある演算＊が定義

（1）閉鎖律

（2）結合律　$(x*y)*z = x*(y*z)$

（3）単位元 e の存在　$e*x = x*e = x$

（4）逆元 x'の存在　$x'*x = x*x' = e$

（5）可換律　$x*y = y*x$

可換群

群表 → ラテン方陣

- 群表においては，表の各行と各列にその群のすべての元が漏れなく重複無く丁度1回づつ現れる.

$$S = \{e, a, b, c, d\}$$

	e	a	b	c	d
e	e	a	b	c	d
a	a	e	d	b	c
b	b	c	e	d	a
c	c	d	a	e	b
d	d	b	c	a	e

同型

- 演算の記号の違いを除けば完全に等しい構造を持つとき，同型

$$G \cong G'$$

- 位数1,2,3の群は同型を除くと次の場合のみ

$n=1$

	e
e	e

$n=2$

	e	a
e	e	a
a	a	e

$n=3$

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

クラインの4元数

- どの元もその元自身を逆元とし，異なる二つの積は残りの元となる.

$$a^2 = b^2 = c^2 = e$$

$$ab = c,\ bc = a,\ \ ca = b$$

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

合同式

$$a \equiv b \pmod{m}$$

$\Leftrightarrow a-b$がmの倍数である$\Leftrightarrow m \mid a-b$

$\Leftrightarrow a$をmで割った余り$=b$をmで割った余り

$\Leftrightarrow a$とbは法mで合同である

合同式の法則

nを1より大きい整数とする．このとき，任意の整数a,b,c,dについて，次のことが成り立つ

(1)反射律　$a \equiv a \pmod{m}$

(2)対称律　$a \equiv b \pmod{m}$ならば，$b \equiv a \pmod{m}$

(3)推移律　$a \equiv b \pmod{m}$かつ　$b \equiv c \pmod{m}$ならば　$a \equiv c \pmod{m}$

(4)　$a \equiv b \pmod{m}$かつ　$c \equiv d \pmod{m}$ならば

$a \pm c \equiv b \pm d \pmod{m}$,　$a \cdot c \equiv b \cdot d \pmod{m}$

剰余類の定義と定理

aを任意の整数とするとき，

$C_a = \{x \in Z \,|\, x \equiv a \pmod{n}\} = a + nZ = \{a + nt \,|\, t \in Z\}$を

nを法とするaの剰余類という．

また，nを法とする剰余類の集合をZ_nで表す．

すなわち，$Z_n = \{C_a \,|\, a \in Z\}$

nを1より大きい整数，a, bを任意の整数とするとき，

$$a \equiv b \pmod{n} \Leftrightarrow C_a = C_b$$

剰余類の性質

C_aをnを法とするaの剰余類を表すものとする.

このとき，次のことが成り立つ.

(1)$a = C_a$

(2)$C_a \cap C_b \neq \phi \Leftrightarrow C_a = C_b$

(3)Z_nは相異なるn個の元$C_0, C_1, \cdots, C_{n-1}$から構成される.

$Z_n = \{C_0, C_1, \cdots, C_{n-1}\}, C_i \cap C_j = \phi (i \neq j)$

また，このとき$Z = C_0 \cup C_1 \cup \cdots \cup C_{n-1}$となっている

既約剰余類

nを法とするaの剰余類C_aは$(a,n)=1$であるとき，既約剰余類であるという．nを法とする剰余類の集合Z_nにおいて，既約剰余類の集合を$Z_n^{\times}$と表す

剰余類Z_nから0を除外した集合をZ_n^*と表す$(P.70)$

例題

以下の集合に対して，加法と乗法について群となるか考えよう.

- 法7の剰余類
- 法7の既約剰余類

剰余環

剰余類・・・整数をmで割った余りの集合

$$Z_m = \{0,1,2,\cdots,m-1\}$$

環

2つの演算（加法と乗算とすれば）に対して

(1)加法に関して群

(2)乗法に関して結合律

(3)乗法単位元が存在

(4)分配律

体

環に対して除算が成立

すなわち

(1)零元以外が可逆元

→（斜体）

(2)乗法に関して可換

環

- 集合Fが2つの演算（加法と乗法）をもち，
  （１）Fは加法において群
  （２）Fが乗法において半群
- （３）分配律

$$a(b+c)=ab+ac$$

- 乗法において逆元をもつとはいえない

整域

- 零因子：非零の元で演算の結果，零元0となる因子のことをいう

$$ab = 0 (a \neq 0, b \neq 0)$$

- 単位元1を持つ可換環で零因子が存在しないとき整域という

法4の剰余類（剰余環）

$$Z_4 = \{0,1,2,3\}$$

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

加法群
加法単位元　0

加法において逆元が存在
0については0
1については3
2については2
3については1

乗法に関して結合律を満たす

乗法単位元　1

加法と乗法に関して分配律を満たす

$$x(y+z) = xy + xz$$

例)　$1(2+3) = 2+3 = 1$

x	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

零因子
2･2=0から2
整域ではない

法5の剰余類（剰余環，整域，体）

$$Z_5 = \{0,1,2,3,4\}$$

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

加法群
加法単位元　0

加法において逆元が存在

乗法に関して結合律を満たす

乗法単位元　1

加法と乗法に関して分配律を満たす

$$x(y+z) = xy + xz$$

例)　$1(2+3) = 2+3 = 0$

逆元について
　1については1
　2については3
　3については2
　4については4

既約剰余類

$$Z_m = \{0,1,2,\cdots,m-1\}$$

法mの剰余類の中で，mと互いに疎となる元のみの集合

$$Z_m^*$$

素数pを法とする剰余類の場合は0を除いた集合と同じとなる

$$Z_p^* = Z_p^\times = Z_p - \{0\} = \{1,2,\cdots,p-1\}$$

フェルマーの定理

$$a^{p-1} \equiv 1 \pmod{p}$$

$$Z_6^* = \{1,5\}$$

2，3，4に対しては，何乗しても1にはならない