群　論

群の定義

スター

空集合でない集合Gに演算＊が定義され、次の条件を満たすとき、
Gは＊に関して群である。

演算＊が定義されるとは、集合Gのどんな要素にも、$a*b \in G$が成り立つこと

1　結合法則が成立

$$(a*b)*c = a*(b*c)$$

2　単位元の存在

$a*e = e*a = a$をみたす e が存在する。

3　すべての元に逆元が存在

Gの任意の元 a に対して、$a*b = b*a = e$ をみたす b が存在する。

b を逆元とよび、a^{-1}であらわす。

練　習

1　整数全体の集合は、加法に関して群になっているか。

2　整数全体の集合は、乗法に関して群になっているか。

アーベル群

４　交換法則が成立。Gの任意の元a,bに対して

$$a * b = b * a$$

１，２，３に加えて４も満たすならば、

Gは＊に関して可換群(アーベル群)という。

補足；　条件１を満たす集合が、　半群

条件１と２を満たす集合が、モノイド

群の元の個数：　位数

演算表

元：集合の要素

横に並んでいる演算を先にする

縦に並んでいる演算を後でやる

	[1 2 3]	[1 3 2]	[2 1 3]	[2 3 1]	[3 1 2]	[3 2 1]
[1 2 3]	[1 2 3]	[1 3 2]	[2 1 3]	[2 3 1]	[3 1 2]	[3 2 1]
[1 3 2]	[1 3 2]	[1 2 3]	[3 1 2]	[3 2 1]	[2 1 3]	[2 3 1]
[2 1 3]	[2 1 3]	[2 3 1]	[1 2 3]	[1 3 2]	[3 2 1]	[3 1 2]
[2 3 1]	[2 3 1]	[2 1 3]	[3 2 1]	[3 1 2]	[1 2 3]	[1 3 2]
[3 1 2]	[3 1 2]	[3 2 1]	[1 3 2]	[1 2 3]	[2 3 1]	[2 1 3]
[3 2 1]	[3 2 1]	[3 1 2]	[2 3 1]	[2 1 3]	[1 3 2]	[1 2 3]

1 2 3
1 3 2
2 1 3

$a * [1\ 2\ 3] = [1\ 2\ 3] * a = a$

$a * b = b * a = e$　bをaの逆元という

$[2\ 3\ 1] * b = [1\ 2\ 3]$

$b = [3\ 1\ 2]$

「縦棒３本のあみだくじ全体の集合 S_3は群をなす。」

群(GROUP)の用語

n個の要素を並び替えてできた「群」を、n次対称群 S_nという。

n次対称群 S_nはn!個の要素からなる。すなわち、$|S_n| = n!$

$|X|$で要素の個数（位数）と表す。

例）　3本の縦線からなるあみだくじは、3次の対称群をなしている。

$$\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}\quad\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\quad\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}\quad\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\quad\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\quad\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$$

可能な並び替えは６通り。

剰余類

$A \mod B = C$

「AとBは法Cに関して合同である」

$A \equiv B \pmod{C}$

6 mod 3 = 0　　9 mod 3 = 0

7 mod 3 = 1　　10 mod 3 = 1

8 mod 3 = 2　　11 mod 3 = 2

…

左の集合を剰余類といい、

この場合、$\boldsymbol{Z}/3\boldsymbol{Z}$と表す。

整数を３で割ると、余りの種類は

0,1,2である。整数は３で割った余り

によって、３つに分類される。

剰余類は群をなす

3で割った余りが0となる類を$\bar{0}$、余りが1となる類を$\bar{1}$、余りが2となる類を$\bar{2}$と書く。

3の剰余類の集合を$\boldsymbol{Z}/3\boldsymbol{Z}$と書く。

$\bar{0}+\bar{0}=\bar{0}, \bar{0}+\bar{1}=\bar{1}, \bar{0}+\bar{2}=\bar{2}$
$\bar{1}+\bar{0}=\bar{1}, \bar{1}+\bar{1}=\bar{2}, \bar{1}+\bar{2}=\bar{0}$
$\bar{2}+\bar{0}=\bar{2}, \bar{2}+\bar{1}=\bar{0}, \bar{2}+\bar{2}=\bar{1}$

→ ＋という演算について、閉じている。

$(\bar{1}+\bar{1})+\bar{2}=\bar{1}+(\bar{1}+\bar{2})=\bar{1}$

→ 結合法則が成り立つ。

$\bar{0}+\bar{0}=\bar{0}+\bar{0}=\bar{0}$
$\bar{1}+\bar{0}=\bar{0}+\bar{1}=\bar{1}$
$\bar{2}+\bar{0}=\bar{0}+\bar{2}=\bar{2}$

→ $\bar{0}$という単位元がある。

$\bar{0}+\bar{0}=\bar{0}, \bar{1}+\bar{2}=\bar{0}, \bar{2}+\bar{1}=\bar{0}$

→ すべての元$\bar{0}, \bar{1}, \bar{2}$に逆元がある。

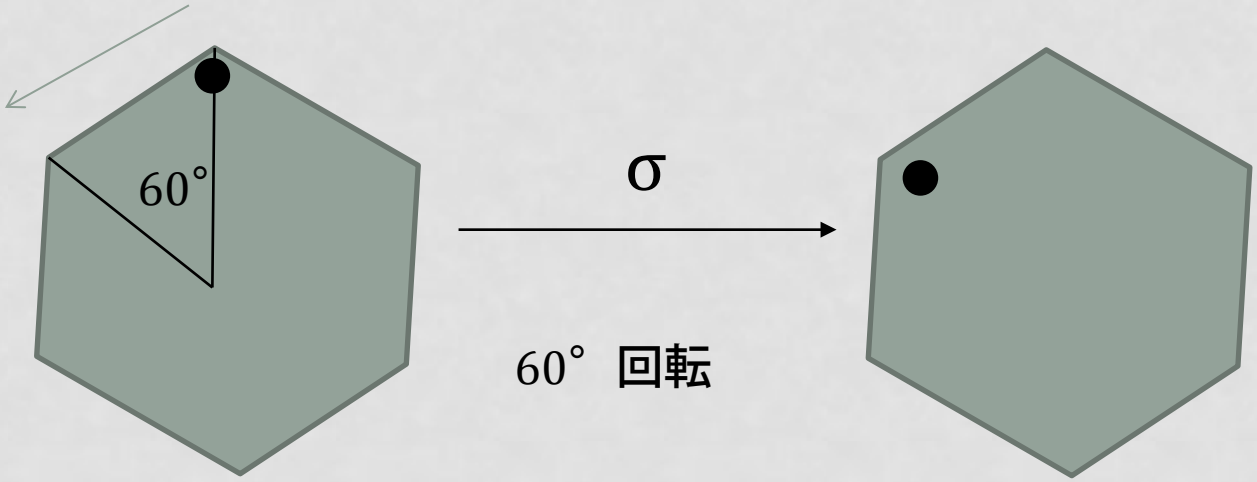
演　習

６の剰余類　$Z/6Z$の足し算の表を作れ。

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$						
$\bar{1}$						
$\bar{2}$						
$\bar{3}$						
$\bar{4}$						
$\bar{5}$						

正六角形を回転させる

１つの頂点に印をつけた正六角形が、その頂点を上にして置かれている。
正六角形の対角線の交点を中心にして、$0°$ 回転することをe、左回りに
$60°$ 回転することをσ、$120°$ 回転することをσ^2、$180°$ 回転することを
σ^3、$240°$ 回転することをσ^4、$300°$ 回転することをσ^5と表す。



巡回群

σのあと、σ^2することを$\sigma^2 \cdot \sigma$と表す（右側が先、左側があと）。

$60°$ 回転して、$120°$ 回転すれば、$180°$ 回転と同じになる。

それを$\sigma^2 \cdot \sigma = \sigma^3$と表す。

$\sigma^3 \cdot \sigma^4$は、$240°$ 回転させたあと、$180°$ 回転させることなので、

$420°$ 回転になる。$360°$ で一回りなので、$60°$ 回転と同じ。

これを$\sigma^3 \cdot \sigma^4 = \sigma$と書く。

すべての元がひとつの元 σ で表せる群を巡回群という。

位数６の巡回群を、 C_6と書く。

この例では、すべての元が σ^n (n=1,2, ..., n)となっている。

演習：巡回群

一度回転したあと、二度目の回転をすると、どの回転に等しいか。

表を埋め、この集合が群をなしていることを示しなさい。

先に行う回転

あとで行う回転

↓ →→→	e	σ	σ^2	σ^3	σ^4	σ^5
e						
σ						
σ^2						
σ^3						
σ^4						
σ^5						

演算表が似ている、ということは…

６の剰余類$\boldsymbol{Z}/6\boldsymbol{Z}$と、位数６の巡回群$C_6$の作る群は

対応している　＝　同型

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$

	e	σ	σ^2	σ^3	σ^4	σ^5
e	e	σ	σ^2	σ^3	σ^4	σ^5
σ	σ	σ^2	σ^3	σ^4	σ^5	e
σ^2	σ^2	σ^3	σ^4	σ^5	e	σ
σ^3	σ^3	σ^4	σ^5	e	σ	σ^2
σ^4	σ^4	σ^5	e	σ	σ^2	σ^3
σ^5	σ^5	e	σ	σ^2	σ^3	σ^4

群GとG'が同型　：　$G \cong G'$

部分群

群Gの元の一部（全部）からできた集合Hが、群の定義を満たすとき、HはGの**部分群**である。

C_6の部分群は、{e}, $\{e, \sigma^2, \sigma^4\}$, $\{e, \sigma^3\}$, C_6の４つだけ。

$\{e, \sigma^3\}$は部分群になる。

後＼先	e	σ^3
e	e	σ^3
σ^3	σ^3	e

$\{e, \sigma^2, \sigma^4\}$は部分群になる。

後＼先	e	σ^2	σ^4
e	e	σ^2	σ^4
σ^2	σ^2	σ^4	e
σ^4	σ^4	e	σ^2

定理：　Hを巡回群C_mの部分群とする。Hの位数はmの約数であり、巡回群の部分群は巡回群である。

群の直積

２つの剰余群$Z/3Z$、$Z/5Z$を組み合わせる

$$(\bar{2}+\bar{4})+(\bar{1}+\bar{2})=(\bar{0}+\bar{1})$$

$$\bar{0}+\bar{0}=\bar{0}+\bar{0}=\bar{0}$$
$$\bar{1}+\bar{0}=\bar{0}+\bar{1}=\bar{1}$$
$$\bar{2}+\bar{0}=\bar{0}+\bar{2}=\bar{2}$$

→　$\bar{0}$という単位元がある。

環(RING)の定義

環では、２種類の演算を考える

以下の条件を満たす集合を環とよぶ

1　和に関して、可換群をなす

2　積に関して、結合法則が成り立つ

$$(a * b) * c = a * (b * c)$$

3　積に関して、単位元を持つ(整数環の時)

4　和と積に対して、分配法則が成り立つ

$$(a + b)\, c = a\, c + b\, c \qquad a\,(b + c) = a\, b + a\, c$$

環では、乗法について逆元が存在するとは限らない。つまり、除法ができるとは限らない。

積について可換である時、「可換環」

例）　整数全体の集合$\mathbb{Z}$は、加法＋と乗法Ｘに関して、環をなす。

体(FIELD)の定義

以下の条件を満たす集合を体とよぶ。

1　和に関して、可換群をなす

2　積に関して、結合法則・交換法則が成り立つ

3　積に関して、単位元を持つ

4　積に関して、０以外のすべての要素について逆元を持つ

5　和と積に対して、分配法則が成り立つ

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

例）　法mが素数のとき、剰余環$\mathbb{Z}/m\mathbb{Z}$は、体をなす。