代数序論（第4回・2011/06/02）

集合 X とは，ものの集まりのことであった．例えば，

$$\mathbb{N},\quad \mathbb{Z},\quad \mathbb{Q},\quad \mathbb{R},\quad \mathbb{C}$$

は集合の例である．しかし，実数全体の集合 $\mathbb{R}$ と言われると，単に集合 (数を集めたもの) というだけでは，何かが足らない気がする．

2つの実数 $a,b\in\mathbb{R}$ には，順序 $a\leq b$ や距離 $|a-b|$ が定められていて，単なるものの集まりよりは，はるかに豊富な構造を持っている (← 実数直線を想像できるのは，この理由からである)．さらに，2つの実数 $a,b\in\mathbb{R}$ には加法 (和) $a+b\in\mathbb{R}$ と乗法 (積) $a\cdot b\in\mathbb{R}$ が定められている．このように，**演算 (二項演算) が定められた集合を学ぶ**のが今日の (そして今後の！) 目的である．

• 二項演算とは，以下のような写像 (対応) のことであった．

定義 (二項演算)． 集合 X に対して，写像 $f:X\times X\to X,\ (a,b)\mapsto a\circ b:=f(a,b)$ を X 上の**二項演算** (または**演算**) といい，$a\circ b:=f(a,b)$ を a と b の**積**という．この $\circ$ を単に二項演算と呼ぶこともある．集合 X 上に二項演算 $\circ$ が与えられている (=定義されている) ことを $(X,\circ)$ と表す．

• この定義によれば，二項演算とは集合 X の2つの元 $a,b\in X$ に，ある1つの元 $a\circ b\in X$ を対応させる規則 (=写像) のことである．逆にいえば，積 $\circ$ は $2\circ 3=100$ でもよいし，$2\circ(-5)=1$ でもよいわけである．(← 積 $\circ$ は，一般には**結合法則** $(a\circ b)\circ c=a\circ(b\circ c)$ を満たさないことに注意)

例1 (二項演算)． 2つの元からなる集合 $X=\{a,b\}$ に二項演算 $\circ$ を定義して $(X,\circ)$ とみなす方法について考える．積の定め方は，

$$a\circ a=\boxed{?},\quad a\circ b=\boxed{?},\quad b\circ a=\boxed{?},\quad b\circ b=\boxed{?}$$

のそれぞれの $\boxed{?}$ を a または b として定義すればよいので，$2^4=16$ 通りある．同様にして，$X=\{a,b,c\}$ に積を定義して $(X,\circ)$ を考えると，その積の定め方は $3^9=19683$ 通り，$X=\{a,b,c,d\}$ に至っては，$4^{16}=4294967296$ 通りもある (!)．

例2 (二項演算)． 全ての積 $\circ$ を考えるのではなく，ある特定の積を考える事にする．集合 $X=\{0,1\}$ に対して，二項演算 $\circ$ を "$\circ$" = "$+$"(和) あるいは $\circ$ = "$\cdot$"(通常の積) として定義するには，

$$\begin{array}{llll} 0+0=0, & 0+1=1, & 1+0=1, & 1+1=0,\\ 0\cdot 0=0, & 0\cdot 1=0, & 1\cdot 0=0, & 1\cdot 1=1 \end{array}$$

とするのが自然であろう．これを表で表してみると以下の様になる：

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

定義 (演算表)． 二項演算 $\circ$ が与えられた有限集合 $X=\{a_1,a_2,\dots,a_n\}$ に対し，その二項演算の対応を以下の様に表にしたものを，$(X,\circ)$ の演算表という (← $a\circ a$ を a^2 と書く)：

$\circ$	a_1	a_2	$\cdots$	a_j	$\cdots$	a_n
a_1	a_1^2	$a_1\circ a_2$		$\vdots$		$a_1\circ a_n$
a_2	$a_2\circ a_1$	a_2^2		$\vdots$		$a_2\circ a_n$
$\vdots$				$\vdots$		$\vdots$
a_i	$\cdots$	$\cdots$	$\cdots$	$a_i\circ a_j$		$\vdots$
$\vdots$						$\vdots$
a_n	$a_n\circ a_1$	$a_n\circ a_2$	$\cdots$	$\cdots$	$\cdots$	a_n^2

- **群について**

「**群** (ぐん, group)」が現代の数学において非常に重要な概念であることは既に授業の中で述べた．しかし，群とは何なのか (?) その定義は，第 9 回の講義にならないと勉強しない．

その理由の 1 つは，群の定義は非常に抽象的 (一般的) であり，また群の理論は抽象代数学とも呼ばれる，現代における抽象的な数学の一部であることにある (← よって，定義だけ聞いても理解しづらい (イメージが湧かなく，分かりづらい))．

そこで，定義を紹介する代わりに，なぜ抽象的な定義 (概念) が必要なのかについて考えてみたい．**群とは** (誤解を恐れずに) そのイメージだけを伝えれば，

群 "=" 集合 + 二項演算 + いくつかの条件　　(← 数学的な等式ではなくイメージ)

である．すなわち，群とは二項演算が定義された集合 $(X, \circ)$ であって，いくつかの条件を満たすものの総称である．ただ単に，二項演算が定義された集合 $(X, \circ)$ を考えるだけでは，上の例 1 でみたように膨大に多くの例が存在してしまう．そこで，しかるべき「いくつかの条件」を満たす $(X, \circ)$ のみを考える，それが**群**を考えるという事である (← どうしても今すぐ定義が知りたい (!) という場合には，教科書 p.92 を参照)．二項演算 $\circ$ が明らかな場合は群 $(X, \circ)$ を単に群 X とも書く．

実は,「いくつかの条件」の中には，積 $\circ$ が**結合法則**を満たすという条件が入っている．(← 結合法則が満たされない積 $\circ$ を考えると，困った事になるのは既に述べた通り) よって，結合法則を満たすような $(X, \circ)$ であり，さらにいくつかの条件を満たすもの，と思ってよい．

例 (群の例)． 群の定義を述べる代わりに，その例を紹介する．以下は全て群の例である：

$$(\mathbb{Z}, +),\ (\mathbb{Q}, +),\ (\mathbb{R}, +),\ (\mathbb{C}, +),\ (\mathbb{Q}^\times, \times),\ (\mathbb{R}^\times, \times),\ (\mathbb{C}^\times, \times),\ (S_n, \circ),$$

但し, $\mathbb{Q}^\times := \mathbb{Q} \setminus \{0\}$, $\mathbb{R}^\times := \mathbb{R} \setminus \{0\}$, $\mathbb{C}^\times := \mathbb{C} \setminus \{0\}$ (← $\{0\}$ を除いた集合 (差集合)) とする．

> 上の例からも分かるように，群とは，新しくて難しい概念ではなく，実は既にこれまでも群に触れながら数学をしてきた事になる．(← ただ，群であるという認識がなかっただけのことである) 群の理論はこれらを抽象化 (一般化) した「仕組み」である．
> なぜ，一つ一つの場合を考えるのではなく，**群**として抽象化して勉強するのだろうか (?) その答えは，群の公理 (定義) のみを使って，一度 (抽象的，一般的に) 定理 (命題，系，補題) が得られると，その理論が (世の中の) **全ての群**に適用できるからである (!!)．

• 以下，n 次対称群 S_n を考える．(← ここでは，S_n が群である事は一時的に認めることにする)

$(S_n, \circ)$ とは，置換 $\sigma, \tau \in S_n$ に対して，置換の合成 (積) $\sigma \circ \tau \in S_n$ が定義された集合のことである．

定理 (n 次対称群 S_n の性質)． $(S_n, \circ)$ に対して，次が成り立つ：

(i) 積 $\circ$ は結合法則を満たす：

任意の $\sigma, \tau, \rho \in S_n$ に対して，$(\sigma \circ \tau) \circ \rho = \sigma \circ (\tau \circ \rho)$ が成り立つ．

(ii) 置換 $(1) = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix} \in S_n$ は，いかなる置換 $\sigma \in S_n$ にかけても相手を変化させない：

任意の $\sigma \in S_n$ に対して，$(1) \circ \sigma = \sigma \circ (1) = \sigma$ が成り立つ．

置換 (1) のことを**恒等置換**と呼ぶ．(← 恒等写像に対応している!)

(iii) 任意の置換 $\sigma \in S_n$ に対して，

$\sigma \circ \sigma' = \sigma' \circ \sigma = (1)$ を満たす置換 $\sigma' \in S_n$ が存在する．

この σ' を σ **の逆置換**とよび，σ^{-1} と表す．(← 定義から $\sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma = (1)$ である)

定義 (部分群)．群 $(X,\circ)$ に対して，部分集合 $X'\subset X$ が再び同じ積 $\circ$ に関して群をなすとき，X' は X の**部分群** (subgroup) であるという．($\leftarrow$ しかし，群の定義はまだ勉強していないことに注意)

例 (部分群)．S_3 は S_4 の部分群，S_4 は S_5 の部分群であり，S_3 は S_5 の部分群でもある．より一般に，$1\le k\le n$ に対して，S_k は S_n の部分群である．

定義 (有限群)．有限集合 X からなる群 $(X,\circ)$ を**有限群** (finite group) という．

例 (有限群)．$S_2=\{(1),(12)\}$, $S_3=\{(1),(12),(1\ 3),(2\ 3),(1\ 2\ 3),(1\ 3\ 2)\}$，より一般に S_n は有限群の例である．($\leftarrow$ S_n の位数 (元の個数) は n の階乗 $n!$ であったことを思い出す)

定義 (可換群, アーベル群)．$(X,\circ)$ を群とする．任意の $a,b\in X$ に対して，$a\circ b=b\circ a$ が成り立つとき，X を**可換群** (commutative group) または**アーベル群** (abelian group) という．

定義 (有限群の同型)．2 つの有限群 $(X,\circ)$ と $(X',\star)$ は，それぞれの演算表が，元の名前を変更し，順番も適当に入れ替えて全く同じ形にできるとき，**同型** (isomorphic) であるといい，$(X,\circ)\cong(X',\star)$ または $X\cong X'$ とかく．($\leftarrow$ X と X' は集合としては異なっていて構わない．X と X' の集合の位数 (元の個数) が等しく，かつ積 $\circ$ と積 $\star$ は構造 (=二項演算の対応) が同じという意味である)

• 群 $(X,\circ)$ のことをよく知るには，実際に積 $\circ$ がどのように定義されているかを知る必要がある．それを自分の目で見て確かめる為に，実際に $(X,\circ)$ の演算表を書いてみよう!

$(X,\circ)$ が群である限り，そこには「美しい」演算表が現われる!

演習問題 (小テスト・中間テストの予想問題)

[1] 以下の問題を解きながら，群 (部分群) の演算表にはどんな特徴があるか，できるだけ多く予想すること．また，その証明も考えること．さらに，同型な群はどれとどれかを答えよ.

[2] 次の集合は群 (S_n とその部分群 $X'\subset S_n$) の例である．演算表はどのようになるか？
各元の名前を (1), a, b, c, d, e とし，実際に演算表を次の形で書け.
但し，二項演算 $\circ$ は全て置換の合成 (積) $(\sigma\circ\tau)(i)=\sigma(\tau(i))$, $i\in I_n:=\{1,\dots,n\}$ とする.

$\circ$	(1)	a	b	$\cdots$
(1)	(1)	a	b	$\cdots$
a	a	?	?	
$\vdots$				

? の中には (1), a, b, c, d, e **のどれかが入る**

(i) $S_2=\{(1),a\}$, $a=(1\ 2)$,
(ii) $S_3=\{(1),a,b,c,d,e\}$, $a=(1\ 2\ 3)$, $b=(1\ 3\ 2)$, $c=(1\ 2)$, $d=(1\ 3)$, $e=(2\ 3)$,
(iii) $X_3=\{(1),a,b\}$, $a=(1\ 2\ 3)$, $b=(1\ 3\ 2)$,
(iv) $X_4=\{(1),a,b\}$, $a=(1\ 4\ 3)$, $b=(1\ 3\ 4)$,
(v) $X_5=\{(1),a,b,c\}$, $a=(1\ 2\ 3\ 4)$, $b=(1\ 3)(2\ 4)$, $c=(1\ 4\ 3\ 2)$,
(vi) $X_6=\{(1),a,b,c\}$, $a=(1\ 2)(3\ 4)$, $b=(1\ 3)(2\ 4)$, $c=(1\ 4)(2\ 3)$,
(vii) $X_7=\{(1),a,b,c\}$, $a=(1\ 5\ 2\ 3)$, $b=(1\ 2)(5\ 3)$, $c=(1\ 3\ 2\ 5)$,
(viii) $X_8=\{(1),a,b,c\}$, $a=(1\ 2)$, $b=(3\ 4)$, $c=(1\ 2)(3\ 4)$,
(ix) $X_9=\{(1),a,b,c,d\}$, $a=(1\ 2\ 3\ 4\ 5)$, $b=(1\ 3\ 5\ 2\ 4)$, $c=(1\ 4\ 2\ 5\ 3)$, $d=(1\ 5\ 4\ 3\ 2)$.

[3] 次の集合は有限群の例である．演算表はどのようになるか？演算表を 1, a, b, c を使って，[2] と同じように書け．但し，二項演算 $\circ$ は $\mathbb{C}$ 内 (複素数) での通常の積とする.
(i) $Y_1=\{1,a\}$, $a=-1$,
(ii) $Y_2=\{1,a,b\}$, $a=(-1+\sqrt{-3})/2$, $b=(-1-\sqrt{-3})/2$,
(iii) $Y_3=\{1,a,b,c\}$, $a=\sqrt{-1}$, $b=-1$, $c=-\sqrt{-1}$.