代数系の基礎要綱 #1

2002–4–11　　河野

この講義は情報数学基礎 I 及び II の内容の理解を前提にしている。あやふやな人は復習をしておく事。以下の問題に全問正確に答えられれば一応の理解はされていると考えてよい。

演習問題 0.1

(1) 以下の用語の定義を述べよ; 集合，元 (要素)，部分集合，共通部分，和集合，直積集合，関係，同値関係，写像。

(2) $A = \{1, 2, 3, 4\}, B = \{a, b, c\}$ とする。次の性質を持つ写像は全部でいくつあるか答えよ。

(1) A から B への写像全体

(2) A から B への全射

(3) B から A への単射

(4) A から A への全単射

(3) 次の命題の否定命題をつくれ。

(1) A かつ B

(2) A ならば B

(3) このクラスの人はすべて『代数系の基礎』に合格する。

(4) $\forall \varepsilon > 0\ \exists \delta > 0\ \forall x \in I\ ;\ 0 < |x - a| < \varepsilon \Longrightarrow |f(x) - f(a)| < \varepsilon$

この講義の目標を**有限体**の理解におく。この概念を理解するためには，演算，群，環，体等の理解が前提となる。

成績は，試験の成績・レポート・演習の 3 つにより判定する。試験が十分できていればレポート・演習点がなくても合格点になる様な基準を採用する。

参考書を幾つかあげておく。

廣瀬健『情報数学』コロナ社

細井勉『情報科学のための代数系入門』産業図書

寺田文行『数理・情報系のための代数系の基礎』サイエンス社

コルビッツ『暗号の代数理論』シュプリンガー・フェアラーク (訳が悪い)

コルビッツ『数論アルゴリズムと楕円暗号理論入門』シュプリンガー・フェアラーク (訳がちょっと悪い)

平松豊一『応用代数学』裳華房

なおこれから講義で配るプリントは http://math.cs.kitami-it.ac.jp/~kouno/ に置く予定である。

1　演算

一般的に演算を定義する前にいくつか例を見よう。

例 1.1　(1) 以下数の集合の記号 $\boldsymbol{N}$(自然数), $\boldsymbol{Z}$(整数), $\boldsymbol{Q}$(有理数), $\boldsymbol{R}$(実数), $\boldsymbol{C}$(複素数) は一々

断らずに用いる事にする。数の集合 $X = \boldsymbol{N}, \boldsymbol{Z}, \boldsymbol{Q}, \boldsymbol{R}, \boldsymbol{C}$ には和・足し算 $[+]$ と積・掛け算 $[\,\cdot\,]$ が定義されている。例えば数 a と b の和は $a+b$, 積は $a\cdot b$ と通常書かれる。ポーランド記法で表すと $+(a,b)$, $\cdot(a,b)$ となる。$+, \cdot$ を写像と考えると，これらは $X \times X$ から X への写像と見る事ができる。

(2) $\boldsymbol{B} = \{0,1\}$ を 2 進数を構成する数字の集合とする。bit 演算としての和・積を考える。和を $[+]$，積を $[\,\cdot\,]$ で書くと，

$$0+0=0, 0+1=1, 1+0=1, 1+1=0, 0\cdot 0=0, 0\cdot 1=0, 1\cdot 0=0, 1\cdot 1=1$$

となる (ここで桁上がりは考えてない)。$+, \cdot$ は $\boldsymbol{B}\times\boldsymbol{B}$ から $\boldsymbol{B}$ への写像と見る事ができる。

(3) $\boldsymbol{H} = \{0,1,2,\ldots,9,A,B,C,D,E,F\}$ を16 進数 (を構成する数字) の集合とする。$Y = \boldsymbol{H}\times\boldsymbol{H}$ を 2 桁の 16 進数の集まりと考える (byte と呼ぶ事もある)。これにも和・積が定義できるが，桁上がりの考慮の方法により 2 通りの定義が考えられる。全く桁上がりを考慮しない和を $\bigoplus$ で表し, 2 桁目への桁上がりは考慮するが，3 桁目への桁上がりを考慮しない和を $+$ で表す。例でいうと

$$67 + AB = 12, \quad 67 \bigoplus AB = 02$$

同様に全く桁上がりを考慮しない積 $\bigodot$ と 2 桁目への桁上がりは考慮するが，3 桁目への桁上がりを考慮しない積を $\cdot$ で表す。例は

$$55\cdot 55 = A9, \quad 55 \bigodot 55 = 99$$

となる。

2 種類の和・積とも $Y\times Y$ から Y への写像になっている。

(4) S を集合とする S から S への写像の全体を $M(S)$ と書く。$M(S)$ の 2 元 f, g に対しその合成写像 $f\circ g$ を考えることができる。この $\circ$ も $M(S)\times M(S)$ から $M(S)$ への写像になっている。

以上の例から次の定義を与える。

定義 1.2 集合 X で定義された**演算** (*operation*) φ とは $X\times X$ から X への写像 φ のことである。正確にはこれを 2 項演算というが通常演算と呼ぶ。X から X への写像 ψ を 1 項演算と呼ぶことがある。

各演算について成立する性質や，(2 つ以上の演算が定義される場合には) 演算間の関係等を**代数的構造** (*algebraic structure*) と呼び, ある代数的構造を満たす体系，即ち，その代数的構造を満たす演算とそれが定義されている集合を**代数系** (*algebraic system*) という。

集合 X に演算 $\varphi_1,\ldots,\varphi_n$ が定義されている場合この代数系を $(\,X\,;\,\varphi_1,\ldots,\varphi_n\,)$ と書く。考えている演算が明らかな場合は演算を省略して X と略記する場合もある。数の集合で言うと $(\,\boldsymbol{R}\,;\,+,\cdot\,)$ 等表す事ができる。和と積について考えているのが明らかな場合 (数の場合ほとんどがそうである)$\boldsymbol{R}$ 等表す。

定義 1.3 2 つの代数系 $(\,S\,;\,\varphi_1,\ldots,\varphi_n\,)$, $(\,M\,;\,\psi_1,\ldots,\psi_n\,)$ に対して S から M への写像 F が存在して任意の $a,b\in S$ に対し

$$F(\varphi_i(a,b)) = \psi_i(F(a),F(b))$$

が成立するとき F を**準同型写像** (*homomorphism*) と呼ぶ。

準同型写像 F が特に S から M への全単射のとき**同型写像** (*isomorphism*) といい，S と M は**同型** (*isomorphic*) であるといい，$S \cong M$ と書く。

演習問題 1.1　2 つの代数系 $S = (\, S\,;\, \varphi_1, \ldots, \varphi_n\,)$ と $(\, M\,;\, \psi_1, \ldots, \psi_n\,)$ の間に準同型写像 F が存在している。このとき $M' = F(S)$, $\psi_i' = \psi_i|_{M' \times M'}$ とおくとき，$(\, M'\,;\, \psi_1', \ldots, \psi_n'\,)$ も代数系である事を示せ。この M' を S の F のよる準同型像といい，S と M' とは**準同型** (*homomorphic*) であるという事もある。

例 1.4 $\varphi : \boldsymbol{R}^2 \to \boldsymbol{R}$ を実数の加法とする。$\boldsymbol{R}^+ = \{\, x \in \boldsymbol{R} \mid\ x > 0\,\}$ とし，
$\psi : \boldsymbol{R}^+ \times \boldsymbol{R}^+ \to \boldsymbol{R}^+$ を実数の乗法とする。$\boldsymbol{R}$ から $\boldsymbol{R}^+$ への写像 F を $F(x) = e^x$ で定義すると，任意の実数 x, y に対し

$$F(\varphi(x, y)) = \psi(F(x), F(y)) \qquad \text{(指数法則)}$$

が成立するので，$(\, \boldsymbol{R}\,;\, +\,)$ と $(\, \boldsymbol{R}^+\,;\, \cdot\,)$ は同型である。抽象的には $\boldsymbol{R}$ 上の和と $\boldsymbol{R}^+$ 上の積は同じ構造をしているという事ができる。

実数の和・積などは $a + b = b + a$ の様な性質をもっている。ここで一般の演算に関して幾つかの性質に名前をつけておく。$(\, S\,;\, \varphi\,)$ を代数系とする。

(1) 任意の $x, y, z \in S$ に対し $\varphi(\varphi(x, y), z) = \varphi(x, \varphi(y, z))$ を満たすとき，**結合法則** (*assosiative low*) が成立するという。

(2) 任意の $x, y \in S$ に対し $\varphi(x, y) = \varphi(y, x)$ を満たすとき，**交換法則** (*commutative low*) が成立するという。

(3) ある S の元 e が次の性質を持つとき，演算 φ に関する**単位元** (*unit*) という; 任意の元 $a \in S$ に対し $\varphi(a, e) = \varphi(e, a) = a$ が成立する。

(4) 単位元の存在を仮定する。ある元 x に対し $\varphi(x, y) = \varphi(y, x) = e$ となる元が存在するとき，この元を演算 φ に関する**逆元** (*inverse element*) といい x^{-1} で表す。