2008年4月11日

命題とは、式や文章で表された事柄で、正しい（真）か正しくない（偽）か明確に定まるもの。

文字（x など）を含んだ命題で、x の値によって真偽が変わるものを（x に関する）条件という。

- 条件 p の否定を $\bar{p}$ と書く。明らかに $\bar{\bar{p}} = p$
- $p \wedge q$ （“p and q,” “p かつ q” とも書く）
- $p \vee q$ （“p or q,” “p または q” とも書く）
- $(\bar{p} \vee q)$ を $(p \implies q)$ と書く。
- $((p \implies q) \wedge (q \implies p))$ を $p \iff q$ と書く。
- $p \implies q$ が成り立つとき p を q の十分条件、q を p の必要条件という。
- $\overline{p \wedge q} = \bar{p} \vee \bar{q}$
- $\overline{p \vee q} = \bar{p} \wedge \bar{q}$
- $(p \implies q) = (\bar{q} \implies \bar{p})$ （対偶）
- $p \wedge (q \vee r) = (p \wedge q) \vee (p \wedge r)$

次の命題

すべての実数 x に対し、$x^2 \geq 0$ である

は、無限個の命題を $\wedge$ で結んだものと考えられる。一般に、$p(x)$ を x に関する条件とするとき、

$$\forall x, \quad p(x)$$

によって、想定されるすべての x について $p(x)$ が真である、ということを表す。例えば

$$\forall x : \text{実数}, \quad x^2 - x + 1 > 0$$

は真であるが、

$$\forall x : \text{実数}, \quad x^2 - x - 1 > 0$$

は偽である。一方、

$$\exists x, \quad p(x)$$

によって、想定されるどれかの x について $p(x)$ が真である、ということを表す。「$p(x)$ を満たす x が存在する」または「ある x に対して $p(x)$ が成り立つ」と読む。例えば

$$\exists x : \text{実数}, \quad x^2 - x - 1 > 0$$

は真であり、

$$\exists x : \text{実数}, \quad x^2 - x - 1 \leq 0$$

も真である。

- $\left(\overline{\forall x,\ p(x)}\right) = \left(\exists x,\ \overline{p(x)}\right)$
- $\forall n : \text{正整数},\ \frac{1}{n} \leq 1$
- $\exists n_0 : \text{正整数},\ \left(\forall n : \text{正整数で } n > n_0,\ \frac{1}{n^2+n} \leq \frac{1}{1000}\right)$

極限 $\lim_{n\to\infty} a_n = a$ の定義は

$$\forall \varepsilon > 0,\ (\exists n_0 : \text{正整数},\ (\forall n : \text{正整数で } n > n_0,\ |a_n - a| < \varepsilon))$$

$\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_k$ を $\mathbf{R}^n$ のベクトルとする。これらが一次独立とは

$$\sum_{i=1}^{k} c_i \boldsymbol{a}_i = 0 \text{ となるのは } (c_1, c_2, \ldots, c_k) = (0, 0, \ldots, 0) \text{ のときに限る}$$

が成り立つときをいう。これを論理記号 $\forall, \exists, \wedge, \vee$ などを用いて書き直してみよ。また一次独立でない（一次従属という）という条件をこれらの記号で書き表してみよ。

定理 1. A を $m \times n$ 行列とする。このとき、$\operatorname{rank} A$ は、A の小行列のうちその行列式が 0 でないようなものの最大次数に等しい。

この定理を論理記号を用いて書き表してみよ。

2008年4月11日の講義の補足説明

- $\forall x$: 実数, $x^2 - x + 1 = (x - \frac{1}{2})^2 + \frac{3}{4} \geq \frac{3}{4} > 0$.
- $x = 1$ とすると $x^2 - x - 1 = -1 < 0$
- $(\forall x : p(x),\ q(x))$ と書くことにより、$p(x)$ を満たす x のみに対して $\forall$ を適用する、ということを表す。
- $(\exists x$: 実数, $\quad x^2 - x - 1 > 0)$ であることを確認するためには、例えば $x = 2$ とすればこの不等式が成立する、ということのみ述べれば良い。この命題の否定は $(\exists x$: 実数, $\quad x^2 - x - 1 \leq 0)$ ではない（これもまた $x = 0$ とすれば真になっている）。否定は

  $$\big(\forall x : \text{実数}, \quad x^2 - x - 1 \leq 0\big)$$

  となる。
- 極限 $\lim_{n\to\infty} a_n = a$ の定義は

  $$\forall \varepsilon > 0,\ (\exists n_0 : \text{正整数},\ (\forall n : \text{正整数で } n > n_0,\ |a_n - a| < \varepsilon))$$

  だが、

  $$\forall \varepsilon > 0,\ (\exists n_0 : \text{正整数},\ (\forall n : \text{正整数}, n > n_0 \implies |a_n - a| < \varepsilon))$$

  と書くこともある。実際、一般に次のような書き換えができるので、どちらでも正しい。

  $$\begin{aligned}(\forall n : p(n),\ q(n)) &= \Big(\forall n : p(n),\ \overline{p(n)} \vee q(n)\Big) \wedge \Big(\forall n : \overline{p(n)},\ \overline{p(n)} \vee q(n)\Big) \\ &= \Big(\forall n,\ \overline{p(n)} \vee q(n)\Big) \\ &= (\forall n,\ p(n) \implies q(n))\end{aligned}$$

- **定理** A を $m \times n$ 行列とする。このとき、$\operatorname{rank} A$ は、A の小行列のうちその行列式が 0 でないようなものの最大次数に等しい。

  例えば行列

  $$\begin{bmatrix} 1 & 2 & -1 & 0 \\ 2 & 1 & 3 & 2 \\ 1 & 5 & -6 & -2 \end{bmatrix}$$

  の３次小行列式（４通りある）はすべて 0 であり、２次小行列式は例えば左上隅をとれば

  $$\begin{vmatrix} 1 & 2 \\ 2 & 1 \end{vmatrix} \neq 0$$

なので、階数は 2 ということがわかる、という意味である。一般に、整数 k に関する条件 $p(k)$ を満たす k の最大値が r とは、

$$p(r) \wedge \left(\forall k > r,\ \overline{p(k)} \right)$$

と書ける。$p(k)$ として「ある k 次の小行列 B があってその行列式が 0 でない」（その否定は $(\forall B : k \text{ 次の小行列},\ \det B = 0)$ となる）という条件をとることで、定理を論理記号を用いて書き表すことができる。

番号 _____ 名前 _____　2008 年 4 月 11 日

$$\begin{aligned}
&\operatorname{rank} A = r \\
&\iff \left(\square B : A \text{ の } r \text{ 次小行列}, \ \det B \square 0 \right) \\
&\qquad \square \left(\square k \square r, \left(\square B : A \text{ の } k \text{ 次小行列}, \ \det B \square 0 \right) \right).
\end{aligned}$$

解答

$$\begin{aligned}
&\operatorname{rank} A = r \\
&\iff \left(\boxed{\exists} B : A \text{ の } r \text{ 次小行列}, \ \det B \boxed{\neq} 0 \right) \\
&\qquad \boxed{\wedge} \left(\boxed{\forall} k \boxed{>} r, \left(\boxed{\forall} B : A \text{ の } k \text{ 次小行列}, \ \det B \boxed{=} 0 \right) \right).
\end{aligned}$$

- 今日の授業の難易度について次の５つのうち最も適当なものに○をつけてください。

  （　）かなり難しく、授業時間内に理解できなかった。

  （　）やや難しく、復習をしないと理解できていない箇所がある。

  （　）ほぼ適当で、大体理解できたと思う。

  （　）やや易しいので、もう少しペースを上げるか詳細な説明まで立ち入らなくて良いと思う。

  （　）易すぎるので、これらは仮定してもっと先に進んでほしい。

- 今日の授業の感想、今後の要望などあれば自由に書いてください。

2008年4月18日

集合とは、ものの集まりであり、ここでいう「もの」とは何でも良い。ただ、与えられた「もの」がその集合に属するかどうかは明確に定まっていなければならない。前回の講義では、命題はその真偽が明確に定まっているもの、と定義した。x に関する条件 $p(x)$ は x を定めるごとに真偽が明確に定まる命題となるので、$p(x)$ が真となるような x すべてを集めると集合ができる。これを

$$\{x \mid p(x)\}$$

と表す。$p(x)$ が真となるような x が有限個しかない場合、または無限個あっても列挙して理解しやすい場合は

$$\{x_1, x_2, \dots, x_n\} \text{ または } \{x_1, x_2, \dots\}$$

と表す。

$\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ は自然数の集合、整数の集合、有理数の集合、実数の集合、複素数の集合を表す。

$A = \{x \mid p(x)\}$ とするとき、$p(x)$ が真のとき $x \in A$, $p(x)$ が偽のとき $x \notin A$ と書く。

$A = \{x_1, x_2, \dots, x_n\}$ とするとき、

$$(x = x_1) \vee (x = x_2) \vee \cdots \vee (x = x_n)$$

のとき $x \in A$, そうでないとき $x \notin A$ と書く。$x \in A$ は 「x は A に属す」、「x は A の元である」、「x は A の要素である」、「A は x を含む」、などと読む。

従って逆に、集合 A に対して、$x \in A$ は x に関する条件と言える。他にも、条件について前回導入した記号に対応して、集合について記号を定義する。$A = \{x \mid p(x)\}$, $B = \{x \mid q(x)\}$ とするとき、

条件	集合
$p(x) \implies q(x)$	$A \subset B$
$p(x) \iff q(x)$	$A = B$
$p(x) \wedge q(x)$	$A \cap B$
$p(x) \vee q(x)$	$A \cup B$
$\overline{p(x)}$	$\overline{A}$
$p(x) \wedge \overline{q(x)}$	$A - B$

集合論の教科書でよくある演習問題：$A \cup B = B \iff A \subset B$.

分配法則

$$(p \wedge (q \vee r)) = ((p \wedge q) \vee (p \wedge r))),$$
$$(p \vee (q \wedge r)) = ((p \vee q) \wedge (p \vee r)))$$

が成り立つことから、

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C),$$
$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

がわかる。

空集合とは元をひとつも含まない集合。$\emptyset$ または $\{\,\}$ と書く。したがって、$x \in \emptyset$ は常に偽である。

$A_1, A_2, \ldots$ を集合とするとき、

$$\bigcup_{n=1}^{\infty} A_n = A_1 \cup A_2 \cup \cdots \cup A_n,$$
$$\bigcap_{n=1}^{\infty} A_n = A_1 \cap A_2 \cap \cdots \cap A_n$$

と書く。$A_k = \{x \mid p_k(x)\}$ $(k = 1, 2, \ldots, n)$ の場合

$$x \in \bigcup_{n=1}^{\infty} A_n \iff \exists k \in \{1, 2, \ldots, n\},\ p_k(x),$$
$$x \in \bigcap_{n=1}^{\infty} A_n \iff \forall k \in \{1, 2, \ldots, n\},\ p_k(x).$$

さらに一般に、I を集合とし、I の各元 $i \in I$ に対して x に関する条件 $p(i, x)$ が定まっているとする。$A_i = \{x \mid p(i, x)\}$ とおくと

$$\bigcup_{i \in I} A_i = \{x \mid \exists i \in I,\ p(i, x)\}, \tag{1}$$
$$\bigcap_{i \in I} A_i = \{x \mid \forall i \in I,\ p(i, x)\}. \tag{2}$$

例えば、$p(i, x)$ を条件 “$0 \leq x \leq i$” とすると、上記 (1), (2) はどのような集合になるか。

A, B を 2 つの集合とするとき、その直積 $A \times B$ とは、A の元と B の元の組全体からなる集合である：

$$A \times B = \{(a, b) \mid i \in I,\ b \in B\}.$$

一般に、$A_1, A_2, \ldots, A_n$ を集合とするとき、

$$A_1 \times A_2 \times \cdots \times A_n = \prod_{k=1}^{n} A_k$$

と書く。特に $A_1 = A_2 = \cdots A_n$ のとき

$$A_1 \times A_2 \times \cdots \times A_n = A^n$$

と書く。

さらに一般に、集合 I の各元 i に対して集合 A_i が定まっているとき、

$$\prod_{i\in I} A_i = \{(x_i)_{i\in I} \mid \forall i \in I,\ x_i \in A_i\}.$$

次が成立する。

$$\left(\bigcap_{i\in I} A_i\right) \times B = \bigcap_{i\in I}(A_i \times B)$$
$$\left(\bigcup_{i\in I} A_i\right) \times B = \bigcup_{i\in I}(A_i \times B)$$

もっと一般に、

$$\bigcap_{i\in I}\left(\prod_{j\in J} A_{i,j}\right) = \prod_{j\in J}\left(\bigcap_{i\in I} A_{i,j}\right)$$

が成り立つが、

$$\prod_{j\in J}\left(\bigcup_{i\in I} A_{i,j}\right) = \bigcup_{i\in I}\left(\prod_{j\in J} A_{i,j}\right)$$
$$\bigcap_{j\in J}\left(\bigcup_{i\in I} A_{i,j}\right) = \bigcup_{i\in I}\left(\bigcap_{j\in J} A_{i,j}\right)$$

はいずれも一般には成り立たない。

集合 A のベキ集合 2^A とは、A の部分集合全体からなる集合とする。

$$2^A = \{B \mid B \subset A\}$$

この講義の配布資料すべて、補足説明、小テストの解答、参考文献などは

`http://www.math.is.tohoku.ac.jp/~munemasa/teaching/2008risan.html`

からダウンロードできるようにした。

2008年4月18日

集合論の教科書でよくある演習問題：$A \cup B = B \iff A \subset B$ は次のようにして証明できる。

$$\begin{aligned}
(A \cup B = B) &= \Big(\big(p(x) \vee q(x)\big) \iff q(x) \Big) \\
&= \Big(\big(p(x) \vee q(x)\big) \Longrightarrow q(x) \Big) \wedge \Big(\big(p(x) \vee q(x)\big) \Longleftarrow q(x) \Big) \\
&= \Big(\overline{\big(p(x) \vee q(x)\big)} \vee q(x) \Big) \wedge \Big(\big(p(x) \vee q(x)\big) \vee \overline{q(x)} \Big) \\
&= \Big(\big(\overline{p(x)} \wedge \overline{q(x)}\big) \vee q(x) \Big) \wedge \Big(p(x) \vee \big(q(x) \vee \overline{q(x)}\big) \Big) \\
&= \Big(\big(\overline{p(x)} \wedge \overline{q(x)}\big) \vee q(x) \Big) \\
&= \Big(\overline{p(x)} \vee q(x) \Big) \wedge \Big(\overline{q(x)} \vee q(x) \Big) \\
&= \Big(\overline{p(x)} \vee q(x) \Big) \\
&= \Big(p(x) \Longrightarrow q(x) \Big) \\
&= (A \subset B).
\end{aligned}$$

次が成立する。

$$\left(\bigcap_{i \in I} A_i \right) \times B = \bigcap_{i \in I} (A_i \times B)$$
$$\left(\bigcup_{i \in I} A_i \right) \times B = \bigcup_{i \in I} (A_i \times B)$$

実際、

$$\begin{aligned}
(x, y) \in \left(\bigcap_{i \in I} A_i \right) \times B &\iff \left(x \in \bigcap_{i \in I} A_i \right) \wedge (y \in B) \\
&\iff (\forall i \in I,\ x \in A_i) \wedge (y \in B) \\
&\iff \forall i \in I,\ ((x \in A_i) \wedge (y \in B)) \\
&\iff \forall i \in I,\ (x, y) \in A_i \times B \\
&\iff (x, y) \in \bigcap_{i \in I} (A_i \times B),
\end{aligned}$$

$$
\begin{aligned}
&(x,y) \in \left(\bigcup_{i\in I} A_i\right) \times B \\
&\iff \left(x \in \bigcup_{i\in I} A_i\right) \wedge (y \in B) \\
&\iff (\exists i \in I,\ x \in A_i) \wedge (y \in B) \\
&\iff \exists i \in I,\ ((x \in A_i) \wedge (y \in B)) \qquad \text{（分配法則より）} \\
&\iff \exists i \in I,\ (x,y) \in A_i \times B \\
&\iff (x,y) \in \bigcup_{i\in I} (A_i \times B),
\end{aligned}
$$

もっと一般に、

$$
\bigcap_{i\in I}\left(\prod_{j\in J} A_{i,j}\right) = \prod_{j\in J}\left(\bigcap_{i\in I} A_{i,j}\right)
$$

が成り立つ。実際、

$$
\begin{aligned}
(x_j)_{j\in J} \in \prod_{j\in J}\left(\bigcap_{i\in I} A_{i,j}\right) &\iff \forall j \in J,\ x_j \in \bigcap_{i\in I} A_{i,j} \\
&\iff \forall j \in J,\ (\forall i \in I,\ x_j \in A_{i,j}) \\
&\iff \forall (i,j) \in I \times J,\ x_j \in A_{i,j} \\
&\iff \forall i \in I,\ (\forall j \in J,\ x_j \in A_{i,j}) \\
&\iff \forall i \in I,\ (x_j)_{j\in J} \in \prod_{i\in I} A_{i,j} \\
&\iff (x_j)_{j\in J} \in \bigcap_{i\in I}\Big(\prod_{i\in I} A_{i,j}\Big).
\end{aligned}
$$

集合 A のベキ集合 2^A とは、A の部分集合全体からなる集合とする。

$$
2^A = \{B \mid B \subset A\}
$$

例えば、$A = \{1,2,3\}$ のとき、

$$
2^A = \{\{1,2,3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1\}, \{2\}, \{3\}, \emptyset\}
$$

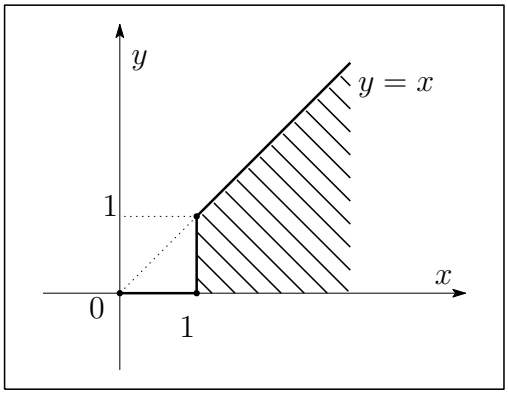
である。$\{1,2\} \subset A$, $\{1,2\} \in 2^A$, $\{\{1,2\}\} \subset 2^A$, $\{\{1\},\{2\}\} \subset 2^A$ は真であるが $\{1,2\} \subset 2^A$ は偽である。

番号 _____ 名前 _____ 2008 年 4 月 18 日

$A_n = \{(x, y) \mid 0 \le x \text{ and } 0 \le y \le x^n\}$ とすると

$$
\begin{aligned}
&\left((x,y) \in \bigcap_{n=1}^{\infty} A_n\right) \\
&= (\forall n \in \{1,2,\dots\},\ ((0 \le x) \wedge (0 \le y \le x^n))) \\
&= \big((0 \le x) \boxed{\wedge} (\forall n \in \{1,2,\dots\},\ 0 \le y \le x^n)\big) \\
&= \big(((0 \le x < 1) \boxed{\vee} (1 \le x)) \boxed{\wedge} (0 \le y \le \inf\{x^n \mid n \in \{1,2,\dots\}\})\big) \\
&= \boxed{\Big(\big((0 \le x < 1) \wedge (0 \le y \le \inf\{x^n \mid n \in \{1,2,\dots\}\})\big)} \\
&\quad \boxed{\vee \big((1 \le x) \wedge (0 \le y \le \inf\{x^n \mid n \in \{1,2,\dots\}\})\big)\Big)} \\
&= \Big((0 \le x < 1) \boxed{\wedge} (\boxed{y = 0})\Big) \boxed{\vee} \Big((1 \le x) \boxed{\wedge} (\boxed{0 \le y \le x})\Big).
\end{aligned}
$$

この集合を平面 $\mathbf{R}^2$ 上に図示せよ。



2008年4月25日

一般に集合 A, B に対し、B^A を、

$$B^A = \prod_{a \in A} B$$

と定義し、B^A の元を A から B への写像という。B^A の元は $(b_a)_{a \in A}$ と書くが、これは A の各元 a に対して B の元 b_a が定まっている、ということになる。このよう

に書くかわりに、$b_a = f(a)$ と書いて、$f : A \to B$ を A から B への写像というのが普通である。

写像 $f : A \to B$ に対して、A を f の定義域といい、

$$\{(a, f(a)) \mid a \in A\} \subset A \times B$$

を f のグラフという。

一般に、

$$\exists x,\ p(x)$$

は条件 $p(x)$ を満たす x が少なくとも一つ存在すること、

$$\exists! x,\ p(x)$$

は条件 $p(x)$ を満たす x がただ一つ存在することを表す。

2^A と $\{0,1\}^A$ とは自然に対応がある。$B \in 2^A$ に対して、次で定義される $\chi_B \in \{0,1\}^A$ を B の特性関数という：

$$\chi_B : A \to \{0,1\}, \quad \chi_B(a) = \begin{cases} 1 & \text{if } a \in B, \\ 0 & \text{if } a \notin B. \end{cases}$$

「対応」とはどういう意味か。これを説明するために

- $f : A \to B$ が全射とは $\forall b \in B,\ \exists a \in A,\ f(a) = b$.
- $f : A \to B$ が単射とは $\forall a \in A,\ \forall a' \in A,\ (f(a) = f(a') \implies a = a')$.
- $f : A \to B$ が全単射とは f が全射かつ単射のときをいう。

$f : 2^A \to \{0,1\}^A,\ f(B) = \chi_B$ は全単射。

$f : A \to B,\ g : B \to C$ に対して、合成写像 $g \circ f : A \to C$ が定義できる。

- $g \circ f$ が単射ならば f は単射、
- $g \circ f$ が全射ならば g は全射。

$X \subset A,\ f : A \to B$ とするとき、

$$\bigcup_{x \in X} \{f(x)\}$$

を $\{f(x) \mid x \in X\}$ または $f(X)$ と書き、f による X の像という。したがって

$$b \in \{f(x) \mid x \in X\} \iff \exists x \in X,\ b = f(x).$$

また、$Y \subset B$ に対し、$f^{-1}(Y) = \{a \mid a \in A,\ f(a) \in Y\}$ を f による Y の逆像という。

- $f(\bigcup_{i\in I} X_i) = \bigcup_{i\in I} f(X_i)$,
- $f^{-1}(\bigcup_{j\in J} Y_j) = \bigcup_{j\in J} f(Y_j)$,
- $f^{-1}(\bigcap_{j\in J} Y_j) = \bigcap_{j\in J} f(Y_j)$,
- $X \subset f^{-1}(f(X))$,
- $Y \cap f(A) = f(f^{-1}(Y))$.

恒等写像 $\mathrm{id}_A : A \to A$ とは、$\forall a \in A$, $\mathrm{id}_A(a) = a$ を満たす写像。$f : A \to B$ に対して、$g \circ f = \mathrm{id}_A$ かつ $f \circ g = \mathrm{id}_B$ を満たす $g : B \to A$ を f の逆写像といい、$g = f^{-1}$ と書く。f が逆写像をもつとき、$Y \subset B$ に対して $f^{-1}(Y)$ は2通りに定義されていることに注意。実は2つの定義は同じになる。

$$\prod_{i\in I}\sum_{j\in J} a_{i,j} = \sum_{f\in J^I}\prod_{i\in I} a_{i,f(i)}.$$

$$\bigcap_{i\in I}\bigcup_{j\in J} A_{i,j} = \bigcup_{f\in J^I}\bigcap_{i\in I} A_{i,f(i)}.$$

$$\bigcup_{i\in I}\bigcap_{j\in J} A_{i,j} = \bigcap_{f\in J^I}\bigcup_{i\in I} A_{i,f(i)}.$$

有限集合 A の元の個数を $|A|$ と書く。

- $|A \cup B| = |A| + |B| - |A \cap B|$
- $|A \times B| = |A||B|$, $|A^B| = |A|^{|B|}$
- $|\bigcup_{i=1}^n A_i| = \sum_{i=1}^n |A_i|$ if $A_i \cap A_j = \emptyset$ whenever $i \neq j$.

2008年4月25日

前回の小テストの解き方：

$$\inf\{x^n \mid n \in \{1,2,\dots\}\} = \begin{cases} 0 & \text{if } 0 \le x < 1, \\ x & \text{if } 1 \le x. \end{cases}$$

B^A は A から B への写像全体の集合である。

べき集合 2^A は A の部分集合全体からなる集合。2^A と書くには理由がある。

写像はそのグラフを定めることによって定めることもできる。写像のグラフ $G \subset A \times B$ は条件

$$\forall a \in A,\ G \cap (\{a\} \times B) \text{ はちょうどひとつの元からなる} \tag{3}$$

を満たし、逆にこの条件を満たす $G \subset A \times B$ はある写像のグラフである。上の条件 (3) を略記するために、$\exists!$ という記号を用いる：

$$\forall a \in A,\ \exists! b \in B,\ (a,b) \in G. \tag{4}$$

$$\begin{aligned} f^{-1}\Big(\bigcap_{j\in J} Y_j\Big) &= \{a \mid a \in A,\ f(a) \in \bigcap_{j\in J} Y_j\} \\ &= \{a \mid a \in A,\ \forall j \in J,\ f(a) \in Y_j\} \\ &= \{a \mid \forall j \in J,\ (a \in A,\ f(a) \in Y_j)\} \\ &= \{a \mid \forall j \in J,\ a \in f^{-1}(Y_j)\} \\ &= \bigcap_{j\in J} f^{-1}(Y_j). \end{aligned}$$

$$\begin{aligned} b \in f\big(f^{-1}(y)\big) &\iff \exists a,\ \Big(\big(a \in f^{-1}(y)\big) \wedge \big(b = f(a)\big)\Big) \\ &\iff \exists a,\ \Big(\big(a \in A\big) \wedge \big(f(a) \in Y\big) \wedge \big(b = f(a)\big)\Big) \\ &\iff \exists a,\ \Big(\big(a \in A\big) \wedge \big(b \in Y\big) \wedge \big(b = f(a)\big)\Big) \\ &\iff \big(b \in Y\big) \wedge \Big(\exists a,\ \big(a \in A\big) \wedge \big(b = f(a)\big)\Big) \\ &\iff \big(b \in Y\big) \wedge \big(b \in f(A)\big) \\ &\iff b \in Y \cap f(A). \end{aligned}$$

番号 _____ 名前 _____　　2008 年 4 月 25 日

$f : A \to B$ を写像とし、$Y \subset B$ とするとき、

$$f(f^{-1}(Y)) = f(A) \cap Y$$

を証明せよ。

$$\begin{aligned}
b \in f(f^{-1}(Y)) &\iff b \in \{f(a) \mid a \in f^{-1}(Y)\} \\
&\iff \boxed{}, \quad (a \in f^{-1}(Y))\boxed{}(b = f(a)) \\
&\iff \\
&\iff \\
&\iff \left(\boxed{}\right) \wedge (b \in Y) \\
&\iff (b \in \{f(a) \mid a \in A\}) \wedge (b \in Y) \\
&\iff b \in f(A) \cap Y.
\end{aligned}$$

2008 年 5 月 2 日

有限集合 A の元の個数を $|A|$ と書く。

- $|A \cup B| = |A| + |B| - |A \cap B|$
- $|A \times B| = |A||B|$
- $|A^B| = |A|^{|B|}$
- $|\bigcup_{i=1}^n A_i| = \sum_{i=1}^n |A_i|$ if $A_i \cap A_j = \emptyset$ whenever $i \neq j$ (disjoint と言う)

$f : A \to B$ を有限集合 A から B への写像とする。このとき、f が全射ならば $|A| \geq |B|$ であり、f が単射ならば $|A| \leq |B|$ である。特に、f が全単射ならば $|A| = |B|$ である。

有限集合とは、

$$\exists n \in \mathbf{N},\ \exists f : \{1, 2, \ldots, n\} \to X,\ f \text{ は全単射}$$

を満たす集合 X のこと。これを否定したのが無限集合の定義となる。$\mathbf{N}$ は無限。$\mathbf{N}$ を含む集合は無限。

X, Y を無限集合とするとき、

$$\begin{aligned}
&\exists f : X \to Y,\ f \text{ は全射} \quad \text{のとき } |X| \geq |Y|, \\
&\exists f : X \to Y,\ f \text{ は単射} \quad \text{のとき } |X| \leq |Y|, \\
&\exists f : X \to Y,\ f \text{ は全単射} \quad \text{のとき } |X| = |Y|
\end{aligned}$$

と書く。

- シュレーダー・ベルンシュタインの定理：$|X| \geq |Y|$ かつ $|X| \leq |Y|$ ならば $|X| = |Y|$.
- カントールの定理：$|X| < 2^{|X|}$.

$S \subset A \times B$ のとき、

$$\begin{aligned} |S| &= \sum_{a \in A} |\{b \mid b \in B,\ (a,b) \in S\}| \\ &= \sum_{b \in B} |\{a \mid a \in A,\ (a,b) \in S\}| \end{aligned}$$

2008年5月2日

$f : A \to B$ を有限集合 A から B への写像とする。このとき、f が全射ならば $|A| \geq |B|$ であり、f が単射ならば $|A| \leq |B|$ である。このことの証明をよく見ると、次の事実もわかる。

- f が全射でかつ $|A| = |B|$ ならば、f は全単射。
- f が単射でかつ $|A| = |B|$ ならば、f は全単射。

$f : X \to Y$, $g : Y \to Z$ をそれぞれ集合 X から Y, Y から Z への写像とする。f, g がともに全射であれば合成写像 $g \circ f : X \to Z$ も全射、f, g がともに単射であれば $g \circ f$ も単射となる。したがって、

- $|X| \geq |Y|$ かつ $|Y| \geq |Z| \implies |X| \geq |Z|$
- $|X| \leq |Y|$ かつ $|Y| \leq |Z| \implies |X| \leq |Z|$

例えば、A を正二十面体の面の集合、B を正二十面体の頂点の集合、とし、$S \subset A \times B$ を、$a \in b$ を満たす組 (a, b) 全体とする。各面は正三角形なので、$|S| = 3|A| = 60$ である。一方、各頂点には5つの正三角形が集まっているので、$|S| = 5|B|$ である。よって $|B| = 12$ となる。

番号 _____ 名前 _____ 2008 年 5 月 2 日

X を 6 人からなる集合とし、X に属するどの 2 人についても、彼らが互いに知人であるかそうでないか明確に定まっているとする。このとき、次のいずれかが成り立つことを示せ。

(1) X の中に、互いに知人どうしの 3 人が存在する。

(2) X の中に、互いに知人でない 3 人が存在する。

2008 年 5 月 9 日

A, B を有限集合とし、$|A| = k$, $|B| = n$ とする。A から B への単射全体の集合を X とすると、

$$|X| = n(n-1)\cdots(n-k+1)$$

となる。これは n 個から k 個とる順列のことである。特に、$k = n$ のとき、単射は必ず全単射となり、その個数は $n!$ となる。一般に有限集合 A から A への全単射を置換という。

k を $0 \leq k \leq n$ を満たす整数とするとき、

$$\binom{B}{k} = \{X \mid X \subset B,\ |X| = k\}.$$

と定義する。このとき、

$$\left|\binom{B}{k}\right| = \frac{n!}{k!(n-k)!} = \frac{n(n-1)\cdots(n-k+1)}{k(k-1)\cdots 1}$$

であり、これを

$$\binom{n}{k}$$

と書く。

X を n 人からなる集合とし、X に属するどの 2 人についても、彼らが互いに知人であるかそうでないか明確に定まっているとする。

$$F = \{T \mid T \in \tbinom{X}{3},\ (\forall x \in T,\ \forall y \in T, (x \neq y \implies x \text{ と } y \text{ は知人}))\},$$
$$F' = \{T \mid T \in \tbinom{X}{3},\ (\forall x \in T,\ \forall y \in T, (x \neq y \implies x \text{ と } y \text{ は知人でない}))\},$$
$$G = \{T \mid T \in \tbinom{X}{3},\ T \notin F \cup F'\}.$$

$x \in X$ をとり、

$$\{(x,T) \mid (x,T) \in X \times G,\ x \in T,$$
$$T - \{x\} \text{ は } x \text{ の知人と } x \text{ の知人でない人からなる } \} \subset X \times G$$

の元の個数を数える。

　このような問題を定式化するために、「関係」という概念を導入する。X を集合とし、$X \times X$ の部分集合を X の上の関係という。

　関係を図で表したものがグラフ（または、関係そのものをグラフということもある）。

以下の３つの条件を満たす関係 $R \subset X \times X$ を X 上の同値関係という。

反射律 $\forall a \in X,\ (a,a) \in R$

対称律 $\forall a,b \in X,\ (a,b) \in R \implies (b,a) \in R$

推移律 $\forall a,b,c \in X,\ (a,b) \in R,\ (b,c) \in R \implies (a,c) \in R$

$(a,b) \in R$ のとき、$a \sim b$ などと書くこともある。

同値関係の例：通常の等号、元の個数が同じ集合、グラフの連結成分、図形の合同、図形の相似、整数の合同。

反射律、推移律に加えて以下の条件を満たす関係 $R \subset X \times X$ を X 上の順序関係といい、(X,R) を半順序集合という。

反対称律 $\forall a,b \in X,\ (a,b) \in R,\ (b,a) \in R \implies a = b$

$(a,b) \in R$ のとき、$a \preceq b$ などと書くこともある。

順序関係の例：通常の不等式、元の個数の大小、集合の包含、部分列、自然数の整除。

さらに、

$$\forall a,b \in X,\ ((a,b) \in R \text{ or } (b,a) \in R)$$

が成り立つとき、(X,R) を全順序集合という。

(X,R) を有限な半順序集合とし、$(x,y) \in R$ のとき $x \preceq y$ と書くことにする。X が最小元を持つ、すなわち

$$\exists x_0 \in X,\ \forall x \in X,\ x_0 \preceq x$$

が成り立つとする。このとき X 上の Möbius 関数 μ とは写像 $\mu : X \to \mathbf{Z}$ で

- $\mu(x_0) = 1$,
- $\forall y \in X,\ y \neq x_0$,

$$\sum_{\substack{x \in X \\ x \preceq y}} \mu(x) = 0$$

を満たすもの。

A を有限集合、$X = 2^A$,

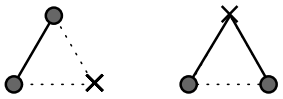
$$R = \{(x,y) \mid (x,y) \in X \times X,\ x \subset y\}$$

とすると、$x_0 = \emptyset$ は最小元であり、$\mu(x) = (-1)^{|x|}$ となる。

2008年5月9日

$|A| = k \leq |B| = n$ とする。

$$\begin{aligned}
\left|\binom{B}{k}\right| &= |\{X \mid X \subset B,\ |X| = k\}| \\
&= \sum_{\substack{X \subset B \\ |X|=k}} 1 \\
&= \frac{1}{k!} \sum_{\substack{X \subset B \\ |X|=k}} k! \\
&= \frac{1}{k!} \sum_{\substack{X \subset B \\ |X|=k}} |\{f \mid f : A \to X \text{ (全単射)}\}| \\
&= \frac{1}{k!} \, |\{(X, f) \mid X \subset B,\ |X| = k,\ f : A \to X \text{ (全単射)}\}| \\
&= \frac{1}{k!} \, |\{(X, f) \mid X \subset B,\ f : A \to B \text{ (単射)},\ f(A) = X\}| \\
&= \frac{1}{k!} \sum_{\substack{f : A \to B \\ \text{単射}}} |\{X \mid X \subset B,\ f(A) = X\}| \\
&= \frac{1}{k!} \sum_{\substack{f : A \to B \\ \text{単射}}} 1 \\
&= \frac{1}{k!} \, n(n-1) \cdots (n-k+1) \\
&= \frac{n!}{k!(n-k)!} \, .
\end{aligned}$$



$$
\begin{aligned}
2|G| &= \sum_{T\in G} 2 \\
&= \sum_{T\in G} |\{x \mid x\in T,\ \overset{\alpha(T-\{x\},x)}{\boxed{T-\{x\} \text{ は } x \text{ の知人と } x \text{ の知人でない人からなる}}}\}| \\
&= |\{(x,T) \mid (x,T)\in X\times G,\ x\in T,\ \alpha(T-\{x\},x)\}| \\
&= \sum_{x\in X} |\{T \mid T\in S,\ x\in T,\ \alpha(T-\{x\},x)\}| \\
&= \sum_{x\in X} |\{T \mid T\in \tbinom{X}{3},\ x\in T,\ \alpha(T-\{x\},x)\}| \\
&= \sum_{x\in X} |\{P \mid P\in \tbinom{X-\{x\}}{2},\ \alpha(P,x)\}| \\
&= \sum_{x\in X} |\{x \text{ の知人 }\}\times\{x \text{ と知人でない人 }\}| \\
&= \sum_{x\in X} r_x(n-1-r_x) \\
&= -\sum_{x\in X} (r_x^2-(n-1)r_x) \\
&= -\sum_{x\in X} \left((r_x-\tfrac{n-1}{2})^2-\tfrac{(n-1)^2}{4}\right) \\
&\le \begin{cases} n\frac{(n-1)^2}{4} & n:\text{odd} \\ n\frac{n^2-2n}{4} & n:\text{even} \end{cases}
\end{aligned}
$$

特に、$n=6$ のとき、

$$|S| \le 6\tfrac{6^2-2\cdot 6}{8} = 18 < 20 = \binom{6}{3}$$

番号 _____ 名前 _____　2008 年 5 月 9 日

集合 X 上の関係 $R \subset X \times X$ に対して、

$$R^{-1} = \{(x,y) \mid (x,y) \in X \times X,\ (y,x) \in R\},$$
$$\bar{R} = \{(x,y) \mid (x,y) \in X \times X,\ (x,y) \notin R\}$$

とする。このとき、次の 2 つの命題は正しいか？

(1) R が集合 X 上の推移的な関係ならば R^{-1} も推移的である。

(2) R が集合 X 上の推移的な関係ならば $\bar{R}$ も推移的である。

2008 年 5 月 16 日

(X,R) を半順序集合とし、$(x,y) \in R$ のとき $x \leq y$ と書くことにする。次を仮定する。

$$\forall x \in X,\ \forall y \in X,\ (x \leq y \implies \{z \mid z \in X,\ x \leq z, z \leq y\}) \text{ は有限}$$

例えば、$\mathbf{Z}$ における大小関係、$\mathbf{N}$ における整除など。このような (X,R) に対し、Möbius 関数 $\mu : X \times X \to \mathbf{Z}$ を、次を満たす関数として定義する。

$$\mu(x,y) = \begin{cases} 1 & \text{if } x = y, \\ 0 & \text{if } x \not\leq y, \\ -\sum_{x \leq z < y} \mu(x,z) & \text{if } x < y \end{cases}$$

例えば $X = 2^A$ を包含関係に関して半順序集合とみたとき、

$$\mu(B,C) = \begin{cases} (-1)^{|C|-|B|} & \text{if } B \subset C, \\ 0 & \text{otherwise.} \end{cases}$$

また、$X = \mathbf{N}$ を整除に関して半順序集合とみたとき、$\mu(1,n)$ $(n \in \mathbf{N})$ を $\mu(n)$ と略記し、これを単に Möbius 関数ということもある。

再び一般に、(X,R) を半順序集合とする。ゼータ関数 $\zeta : X \times X \to \mathbf{Z}$ を

$$\zeta(x,y) = \begin{cases} 1 & \text{if } x \leq y, \\ 0 & \text{otherwise.} \end{cases}$$

とする。μ, ζ をともに行列と考えて、積を計算すると

$$(\mu\zeta)_{x,y} = \sum_{z \in X} \mu(x,z)\zeta(z,y) = \sum_{x \leq z \leq y} \mu(x,z) = \delta_{x,y}$$

従って $\mu\zeta = \zeta\mu = I$ (単位行列)。

定理 2. $f, g : X \to \mathbf{Z}$ が

$$\forall x \in X,\ g(x) = \sum_{y \le x} f(y)$$

を満たすとすると

$$\forall x \in X,\ f(x) = \sum_{y \le x} \mu(y, x) g(y)$$

が成り立つ。

$A_i\ (i \in I)$ を A の部分集合とする。$f : 2^I \to \mathbf{Z}$ を

$$f(J) = |\{a \mid a \in A,\ J = \{j \mid j \in I,\ a \notin A_j\}\}|$$

により定義し、

$$g(J) = \sum_{K \subset J} f(K)$$

とおくと

$$\forall J \in 2^I,\ g(J) = \left| \bigcap_{j \in \bar{J}} A_j \right|$$

となる。これより

$$\left| X - \bigcup_{i \in I} A_i \right| = f(I) = \sum_{J \subset I} (-1)^{|J|} \left| \bigcap_{j \in J} A_j \right|.$$

$|A| = m \ge |B| = n$ とし、$F_b = \{f \mid f : A \to B,\ b \notin f(A)\}$ とおく。すると

$$\begin{aligned}
&|\{f \mid f : A \to B,\ f \text{ は全射 }\}| \\
&= \left| B^A - \bigcup_{b \in B} F_b \right| \\
&= \sum_{i=0}^{n} \sum_{C \in \binom{B}{i}} (-1)^i |\{f \mid f : A \to B,\ C \cap f(A) = \emptyset\}| \\
&= \sum_{i=0}^{n} \binom{n}{i} (-1)^i (n-i)^m.
\end{aligned}$$

A を有限集合、$X = 2^A$,

$$R = \{(x, y) \mid (x, y) \in X \times X,\ x \subset y\}$$

とすると、$x_0 = \emptyset$ は最小元であり、$\mu(x) = (-1)^{|x|}$ となる。

$R \subset X \times X$ を同値関係とし、$x \in X$ とするとき、

$$[x] = \{y \mid y \in X,\ (x, y) \in R\}$$

を、（関係 R に関する、）x を含む同値類という。同値類全体の集合

$$\{[x] \mid x \in X\}$$

を関係 R による商集合といい、X/R と書く。$\pi : X \to X/R$, $\pi(x) = [x]$ を自然な写像という。

2008年5月16日

推移律 $\forall a,b,c \in X,\ (a,b) \in R,\ (b,c) \in R \implies (a,c) \in R$

であったが、これは $(a,b) \in R,\ (b,c) \in R$ を満たすような a,b,c が存在することを意味してはいない。$\implies$ の意味を思い出すと、

$$\forall a,b,c \in X,\ \overline{((a,b) \in R) \wedge ((b,c) \in R)} \vee ((a,c) \in R)$$

したがって、$R = \emptyset \subset X \times X$ は推移律を満たす。

$B \subset C \subset A$ のとき、2^A における Möbius 関数 μ の (B,C) での値は、帰納的に

$$\begin{aligned}
\mu(B,C) &= -\sum_{B \subset D \subsetneq C} (-1)^{|D|-|B|} \\
&= -\sum_{\substack{E \in 2^{C-B} \\ E \neq C-B}} (-1)^{|E|} \\
&= -\sum_{i=0}^{|C-B|-1} \sum_{E \in \binom{C-B}{i}} (-1)^{|}E| \\
&= -\sum_{i=0}^{|C-B|-1} \binom{|C-B|}{i} (-1)^i \\
&= -((1-1)^{|C-B|} - (-1)^{|C-B|}) \\
&= (-1)^{|C-B|}
\end{aligned}$$

写像 $f,g : X \to \mathbf{Z}$ をベクトル $(f(x))_{x \in X},\ (g(x))_{x \in X}$ と考えると、$g = f\zeta$ から $g\mu = f$ が得られる。これは

$$\forall x \in X,\ g(x) = \sum_{y \leq x} f(y)$$

から

$$\forall x \in X,\ f(x) = \sum_{y \leq x} \mu(y,x) g(y)$$

が導かれることを意味している。

番号 _____ 名前 _____　2008 年 5 月 16 日

$\mu : \mathbf{N} \to \mathbf{Z}$ を、$\mathbf{N}$ の整除に関する順序関係の Möbius 関数とするとき、$\mu(12)$, $\mu(24)$, $\mu(30)$ を求めよ。

2008年5月30日

(X, R) を半順序集合とし、$(x, y) \in R$ のとき $x \leq y$ と書くことにする。次を仮定する。

$$\forall x \in X,\ \forall y \in X,\ (x \leq y \implies \{z \mid z \in X,\ x \leq z, z \leq y\}) \text{ は有限}$$

このような (X, R) に対し、Möbius 関数 $\mu : X \times X \to \mathbf{Z}$ を、次を満たす関数として定義する。

$$\mu(x, y) = \begin{cases} 1 & \text{if } x = y, \\ 0 & \text{if } x \not\leq y, \\ -\sum_{x \leq z < y} \mu(x, z) & \text{if } x < y \end{cases}$$

例えば $X = 2^A$ を包含関係に関して半順序集合とみたとき、

$$\mu(B, C) = \begin{cases} (-1)^{|C|-|B|} & \text{if } B \subset C, \\ 0 & \text{otherwise.} \end{cases}$$

定理 3. $f, g : X \to \mathbf{Z}$ が

$$\forall x \in X,\ g(x) = \sum_{y \leq x} f(y)$$

を満たすとすると

$$\forall x \in X,\ f(x) = \sum_{y \leq x} \mu(y, x) g(y)$$

が成り立つ。

A_i $(i \in I)$ を A の部分集合とする。$f : 2^I \to \mathbf{Z}$ を

$$f(J) = |\{a \mid a \in A,\ J = \{j \mid j \in I,\ a \notin A_j\}\}|$$

により定義し、

$$g(J) = \sum_{K \subset J} f(K)$$

とおくと

$$\forall J \in 2^I,\ g(J) = \left| \bigcap_{j \in \bar{J}} A_j \right|$$

となる。これより

$$\left| A - \bigcup_{i \in I} A_i \right| = f(I) = \sum_{J \subset I} (-1)^{|J|} \left| \bigcap_{j \in J} A_j \right|.$$

$|A| = m \geq |B| = n$ とし、$F_b = \{f \mid f : A \to B,\ b \notin f(A)\}$ とおく。すると

$$\begin{aligned}
&|\{f \mid f : A \to B,\ f \text{ は全射 }\}| \\
&= \left| B^A - \bigcup_{b \in B} F_b \right| \\
&= \sum_{i=0}^{n} \sum_{C \in \binom{B}{i}} (-1)^i |\{f \mid f : A \to B,\ C \cap f(A) = \emptyset\}| \\
&= \sum_{i=0}^{n} \binom{n}{i} (-1)^i (n-i)^m.
\end{aligned}$$

$R \subset X \times X$ を同値関係とし、$x \in X$ とするとき、

$$[x] = \{y \mid y \in X,\ (x, y) \in R\}$$

を、（関係 R に関する、）x を含む同値類という。同値類全体の集合

$$\{[x] \mid x \in X\}$$

を関係 R による商集合といい、X/R と書く。$\pi : X \to X/R$, $\pi(x) = [x]$ を自然な写像という。

m を正の整数とし、$\mathbf{Z}$ の関係 R を

$$R = \{(a, b) \mid (a, b) \in \mathbf{Z} \times \mathbf{Z},\ m|(a - b)\}$$

とおき、$(a, b) \in R$ のとき $a \equiv b \pmod{m}$ と書く。これは同値関係になる。

$$X = \{(a, b) \mid a \in \mathbf{Z},\ b \in \mathbf{Z},\ b \neq 0\}$$

とおき、

$$R = \{((a, b), (c, d)) \mid ((a, b), (c, d)) \in X \times X,\ ad = bc\}$$

とおくと、R は X 上の同値関係になる。

2008年5月30日

$$f(J) = \left|\left\{a \mid \{j \in I \mid a \notin A_j\} = J\right\}\right|$$

$$\begin{aligned} g(J) &= \sum_{\substack{K \in 2^I \\ K \subset J}} f(K) \\ &= \Big|\bigcup_{\substack{K \in 2^I \\ K \subset J}} \left\{a \mid a \in A,\ \{j \in I \mid a \notin A_j\} = K\right\}\Big| \\ &= \left|\left\{a \mid a \in A,\ \{j \in I \mid a \notin A_j\} \subset J\right\}\right| \\ &= \Big|\bigcap_{j \in \overline{J}} A_j\Big|. \end{aligned}$$

$$\begin{aligned} \Big|A - \bigcup_{i \in I} A_i\Big| &= f(I) \\ &= \sum_J \mu(J, I) g(J) \\ &= \sum_J \mu(\overline{J}, I) g(\overline{J}) \\ &= \sum (-1)^{|I| - |\overline{J}|} \Big|\bigcap_{j \in J} A_j\Big| \\ &= \sum (-1)^{|J|} \Big|\bigcap_{j \in J} A_j\Big|. \end{aligned}$$

$$\begin{aligned} &|\{f \mid f : A \to B,\ f \text{ は全射 }\}| \\ &= \Big|B^A - \bigcup_{b \in B} F_b\Big| \\ &= \sum_{C \subset B} (-1)^{|C|} \cdot \Big|\bigcap_{b \in C} F_b\Big| \\ &= \sum_{i=0}^{n} \sum_{C \in \binom{B}{i}} (-1)^i |\{f \mid f : A \to B,\ C \cap f(A) = \varnothing\}| \\ &= \sum_{i=0}^{n} \sum_{C \in \binom{B}{i}} (-1)^i |(B - C)^A| \\ &= \sum_{i=0}^{n} \tbinom{n}{i} (-1)^i (n - i)^m. \end{aligned}$$

番号 _____ 名前 _____　2008 年 5 月 30 日

関係 $R \subset X \times X$ を X に関する性質。

反射律 $\forall a \in X,\ (a,a) \in R$

対称律 $\forall a,b \in X,\ (a,b) \in R \implies (b,a) \in R$

推移律 $\forall a,b,c \in X,\ (a,b) \in R,\ (b,c) \in R \implies (a,c) \in R$

$\mathbf{Z}$ 上の以下の関係 R が上の性質を持つかどうか決定せよ。

R	反射律	対称律	推移律
$\{(a,b) \mid a < b\}$			
$\{(a,b) \mid a+b$ は奇数 $\}$			
$\{(a,b) \mid a+b$ は偶数 $\}$			
$\{(a,b) \mid ab = 1\}$			
$\{(a,b) \mid \sqrt{ab}$ は整数 $\}$			

解説

R	反射律	対称律	推移律
$\{(a,b) \mid a < b\}$	×	×	○
$\{(a,b) \mid a+b$ は奇数 $\}$	×	○	×
$\{(a,b) \mid a+b$ は偶数 $\}$	○	○	○
$\{(a,b) \mid ab = 1\}$	×	○	○
$\{(a,b) \mid \sqrt{ab}$ は整数 $\}$	○	○	×

- $(0,0) \notin \{(a,b) \mid ab = 1\}$ であるから、反射律は成り立たない。
- $(x,y),(y,z) \in \{(a,b) \mid ab = 1\}$ とすると、$xy = yz = 1$ である。$x,y,z \in \mathbf{Z}$ であるから、$x,y,z \in \{1,-1\}$ となり、特に $y^2 = 1$ である。従って $xz = xzy^2 = (xy)(yz) = 1$ である。よって推移律は成り立つ。
- $(2,0),(0,3) \in \{(a,b) \mid \sqrt{ab}$ は整数 $\}$ だが、$(2,3) \notin \{(a,b) \mid \sqrt{ab}$ は整数 $\}$ となり、推移律は成り立たない。ただし、$\mathbf{Z}$ ではなく、$\mathbf{Z} - \{0\}$ 上の関係と考えると推移律は成り立つ。実際 $(x,y),(y,z) \in \{(a,b) \mid \sqrt{ab}$ は整数 $\}$ とすると、$\mathbf{Z} \ni \sqrt{xy}\sqrt{yz} = |y|\sqrt{xz}$ となり、$y \in \mathbf{Z} - \{0\}$ より $\sqrt{xz}$ は有理数、したがって整数となる。

2008年6月6日

定義の復習

$R \subset X \times X$ を同値関係とし、$x \in X$ とするとき、

$$[x] = \{y \mid y \in X,\ (x, y) \in R\}$$

を、(関係 R に関する、) x を含む同値類という。同値類全体の集合 $\{[x] \mid x \in X\}$ を関係 R による商集合といい、X/R と書く。

Z の構成

$$\mathbf{N} = \{1, 2, 3, \dots\},$$
$$\mathbf{N}_0 = \{0, 1, 2, 3, \dots\}$$

とし、$\mathbf{N}_0^2 = \mathbf{N}_0 \times \mathbf{N}_0$ 上の関係 R を次で定める。

$$R = \{((a, b), (c, d)) \in \mathbf{N}_0^2 \mid a + d = b + c\}$$

すると R は同値関係になる。R による商集合

$$\mathbf{N}_0^2/R = \{[a, b] \mid (a, b) \in \mathbf{N}_0^2\}$$

から $\mathbf{Z}$ への写像　f を

$$f([a, b]) = a - b$$

によって定める。f の定義は見かけ上同値類 $[a, b]$ の代表元 (a, b) の取り方に依存しているように見えるので、$[a, b] = [c, d]$ のとき $f([a, b]) = f([c, d])$ が示されないと f は写像になっていると言えない。実際、

$$[a, b] = [c, d] \implies ((a, b), (c, d)) \in R \implies a + d = b + c \implies a - b = c - d$$

なので、$f([a, b]) = f([c, d])$ が成り立つ。

このように、商集合を定義域とする写像の定義が見かけ上同値類の代表元の取り方に依存しているとき、その写像の値が実際には同値類の代表元の取り方に依存しないことを示すことを、「写像が well-defined である」ことを示す、という。上の写像 f は全単射でもある。

集合 X における演算とは、$X \times X$ から X への写像のことである。例えば、$\mathbf{N}_0^2/R$ に演算 $+$ を次のように定義することができる。

$$+ : (\mathbf{N}_0^2/R) \times (\mathbf{N}_0^2/R) \to \mathbf{N}_0^2/R,\ +([a, b], [c, d]) = [a + c, b + d].$$

以後 $+([a,b],[c,d])$ を $[a,b]+[c,d]$ と書くことにする。この写像 $+$ は well-defined である。実際、$[a,b]=[a',b']$, $[c,d]=[c',d']$ とすると、$\alpha=a'-a=b'-b$, $\beta=c'-c=d'-d$ とおくことにより、$[a+c,b+d]=[a'+c',b'+d']$ が確かめられる。さらに、

$$f([a,b]+[c,d])=f([a,b])+f([c,d])$$

が成り立つ。ただし、右辺における $+$ は $\mathbf{Z}$ における通常の和である。

Q の構成

$$X=\{(a,b)\mid a\in\mathbf{Z},\ b\in\mathbf{Z},\ b\neq 0\}$$

とおき、

$$R=\{((a,b),(c,d))\mid((a,b),(c,d))\in X\times X,\ ad=bc\}$$

とおくと、R は X 上の同値関係になる。R による商集合

$$X/R=\{[a,b]\mid(a,b)\in X\}$$

から $\mathbf{Q}$ への写像　f を

$$f([a,b])=\frac{a}{b}$$

によって定める。f は well-defined であることがわかり、また f は全単射でもある。

X/R に演算 $\times$ を次のように定義することができる。

$$\times:(X/R)\times(X/R)\to X/R,\ \times([a,b],[c,d])=[ac,bd].$$

この写像 $\times$ は well-defined である。さらに、

$$f(\times([a,b],[c,d]))=f([a,b])f([c,d])$$

が成り立つ。ただし、右辺は $\mathbf{Q}$ における通常の積である。

X/R に演算 $+$ を次のように定義することができる。

$$+:(X/R)\times(X/R)\to X/R,\ +([a,b],[c,d])=[ad+bc,bd].$$

この写像 $+$ は well-defined である。さらに、

$$f(+([a,b],[c,d]))=f([a,b])+f([c,d])$$

が成り立つ。ただし、右辺の $+$ は $\mathbf{Q}$ における通常の和である。

$\mathbf{Z}/m\mathbf{Z}$ の構成

m を正の整数とし、

$$R = \{(a, b) \mid (a, b) \in \mathbf{Z} \times \mathbf{Z},\ m|(a - b)\}$$

とおくと、R は $\mathbf{Z}$ 上の同値関係になる。R による商集合

$$\mathbf{Z}/R = \{[a] \mid a \in \mathbf{Z}\}$$

を $\mathbf{Z}/m\mathbf{Z}$ とも書く。$\mathbf{Z}/m\mathbf{Z}$ に演算 $+$ を次のように定義することができる。

$$+ : \mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/m\mathbf{Z} \to \mathbf{Z}/m\mathbf{Z},\ +([a], [b]) = [a + b].$$

この写像 $+$ は well-defined である。また、$\mathbf{Z}/m\mathbf{Z}$ に演算 $\times$ を次のように定義することができる。

$$\times : \mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/m\mathbf{Z} \to \mathbf{Z}/m\mathbf{Z},\ \times([a], [b]) = [ab].$$

この写像 $\times$ は well-defined である。

環

集合 A に 2 つの演算 $+$（加法）, $\times$（乗法）が定義されていて、下記の性質が成り立つとき、X は環であるという。

(1) $\forall a, b, c \in A,\ (a + b) + c = a + (b + c)$ （結合法則）

(2) $\forall a, b \in A,\ a + b = b + a$ （交換法則）

(3) $\exists 0 \in A,\ \forall a \in A,\ a + 0 = a$ （零元の存在）

(4) $\forall a \in A,\ \exists b \in A,\ a + b = 0$ （加法に関する逆元の存在）

(5) $\forall a, b, c \in A,\ (a \times b) \times c = a \times (b \times c)$ （結合法則）

(6) $\exists 1 \in A,\ \forall a \in A,\ a \times 1 = 1 \times a = a$ （単位元の存在）

(7) $\forall a, b, c \in A,\ a \times (b + c) = (a \times b) + (a \times c),\ (b + c) \times a = (b \times a) + (c \times a)$ （分配法則）

例えば、$\mathbf{Z}, \mathbf{Q}, \mathbf{R}, \mathbf{C}$ などがそうである。$\mathbf{R}$ を成分とする n 次正方行列全体の集合も環になる。さらに、$\mathbf{Z}/m\mathbf{Z}$ も環になる。

2008年6月6日

$$\mathbf{N} = \{1, 2, 3, \dots\},$$
$$\mathbf{N}_0 = \{0, 1, 2, 3, \dots\}$$

とし、$\mathbf{N}_0^2 = \mathbf{N}_0 \times \mathbf{N}_0$ 上の関係 R を次で定める。

$$R = \{((a, b), (c, d)) \in \mathbf{N}_0^2 \mid a + d = b + c\}$$

すると R は同値関係になる。これは、R を定義している条件は $a - b = c - d$ ということなので、差が同じ非負整数の組を同値類にまとめたものになっている。したがって、

$$((a, b), (c, d)) \in R \iff \exists \alpha \in \mathbf{Z},\ c = a + \alpha,\ d = b + \alpha.$$

$\mathbf{N}_0^2/R$ と $\mathbf{Z}$ の間の全単射を構成したことで、$\mathbf{N}_0$ を使って $\mathbf{Z}$ を「定義」したことになっている。

$$X = \{(a, b) \mid a \in \mathbf{Z},\ b \in \mathbf{Z},\ b \neq 0\}$$

とおき、

$$R = \{((a, b), (c, d)) \mid ((a, b), (c, d)) \in X \times X,\ ad = bc\}$$

とおくと、R は X 上の同値関係になる。X/R と $\mathbf{Q}$ の間の全単射を構成したことで、X を使って $\mathbf{Q}$ を「定義」したことになっている。

$\mathbf{Q}$ から $\mathbf{R}$ を構成する方法は、「Dedekind の切断」を用いる方法と、コーシー列を用いる方法がある。

番号 _____ 名前 _____　2008 年 6 月 6 日

$\mathbf{N}_0^2 = \mathbf{N}_0 \times \mathbf{N}_0$ 上の同値関係 R を次で定める。

$$R = \{((a,b),(c,d)) \in \mathbf{N}_0^2 \mid a+d = b+c\}.$$

商集合 $\mathbf{N}_0^2/R$ から $\mathbf{Z}$ への写像　f を

$$f([a,b]) = a - b$$

によって定める。

このとき、$\mathbf{N}_0^2/R$ に演算 $\times$ を定義し、それが well-defined であることを確認し、さらに

$$f(\times([a,b],[c,d])) = f([a,b])f([c,d])$$

が成り立つようにせよ。ただし、右辺は $\mathbf{Z}$ における通常の積である。

解答

写像　$\times : (\mathbf{N}_0^2/R)^2 \to \mathbf{N}_0^2/R$ を $\times([a,b],[c,d]) = [ac+bd, ad+bc]$ によって定める。

Well-defined については、$\big([a,b],[c,d]\big), \big([a',b'],[c',d']\big) \in (\mathbf{N}_0^2/R)^2$ に対して

$$\begin{aligned}[a,b] = [a',b'],\ [c,d] = [c',d'] &\Longrightarrow a+b' = b+a',\ c+d' = d+c' \\ &\Longrightarrow a-b = a'-b',\ c-d = c'-d' \qquad (\text{in } \mathbf{Z})\end{aligned}$$

であるから

$$\begin{aligned}a'c' + b'd' - (b'c' + a'd') &= (a'-b')(c'-d') \\ &= (a-b)(c-d) \\ &= ac + bd - (bc+ad).\end{aligned}$$

よって

$$(ac+bd) + (b'c' + a'd') = (a'c' + b'd') + (bc+ad),$$

つまり $[ac+bd, bc+ad] = [a'c'+b'd', b'c'+a'd']$ なので $\times$ は well-defined.

次に

$$\begin{aligned}f\big(\times([a,b],[c,d])\big) &= f\big([ac+bd, bc+ad]\big) \\ &= ac+bd-(bc+ad) \\ &= (a-b)(c-d) \\ &= f([a,b])f([c,d]).\end{aligned}$$

2008年6月13日

集合 A に2つの演算 $+$（加法）, $\times$（乗法）が定義されていて、下記の性質が成り立つとき、A は環であるという。

(1) $\forall a, b, c \in A,\ (a+b)+c = a+(b+c)$ （結合法則）

(2) $\forall a, b \in A,\ a+b = b+a$ （交換法則）

(3) $\exists 0 \in A,\ \forall a \in A,\ a+0 = a$ （零元の存在）

(4) $\forall a \in A,\ \exists b \in A,\ a+b = 0$ （加法に関する逆元の存在）

(5) $\forall a, b, c \in A,\ (a \times b) \times c = a \times (b \times c)$ （結合法則）

(6) $\exists 1 \in A,\ \forall a \in A,\ a \times 1 = 1 \times a = a$ （単位元の存在）

(7) $\forall a, b, c \in A,\ a \times (b+c) = (a \times b) + (a \times c),\ (b+c) \times a = (b \times a) + (c \times a)$ （分配法則）

通常、「$\times$」は省略して書かない。また、a の加法に関する逆元（上記 (4) 参照）を $-a$ と書き、$a+(-b)$ を $a-b$ と書く（これで減法が定義されたことになる）。例えば、$\mathbf{Z}, \mathbf{Q}, \mathbf{R}, \mathbf{C}$ などがそうである。$\mathbf{R}$ を成分とする n 次正方行列全体の集合も環になる。さらに、$\mathbf{Z}/m\mathbf{Z}$ も環になる。

A を環とし、

$$\mathbf{N}_0 = \{0, 1, 2, \dots\}$$

とすると、$A^{\mathbf{N}_0}$ に和と積を定義することができる。

$$(f+g)(n) = f(n) + g(n),$$
$$(fg)(n) = \sum_{k=0}^{n} f(k)g(n-k).$$

これらの演算により $A^{\mathbf{N}_0}$ は環になり、これを A 係数1変数形式的べき級数環という。通常 f のかわりに変数（ただの記号）x を用いて

$$\sum_{n=0}^{\infty} f(n)x^n$$

と書き、そのとき $A^{\mathbf{N}_0}$ を $A[[x]]$ と書く。

$f \in A^{\mathbf{N}_0}$ であって

$$\text{有限個の } n \in \mathbf{N}_0 \text{ を除いて } f(n) = 0$$

を満たすものを A 係数1変数多項式という。A 係数1変数多項式全体のつくる $A^{\mathbf{N}_0}$ の部分集合はそれ自身、$A^{\mathbf{N}_0}$ の演算に関して環になり、これを A 係数1変数多項式環という。変数に x を使うとき、A 係数1変数多項式環を $A[x]$ と書く。

$\mathbf{Z}$ から $\mathbf{Q}$ を作る構成法を、「商体」の構成という。同じ構成法は次に定義する整域にも適用できる。

整域とその商体

環 A が次の条件を満たすとき、整域という。

(1) $\forall a, b \in A,\ a \times b = b \times a$ （乗法に関する交換法則）

(2) $\forall a, b \in A - \{0\},\ a \times b \neq 0$

$\mathbf{Z}, \mathbf{Q}, \mathbf{R}, \mathbf{C}$ は整域である。p が素数のとき $\mathbf{Z}/p\mathbf{Z}$ は整域だが、$m > 1$ が素数でない自然数のとき、$\mathbf{Z}/m\mathbf{Z}$ は整域ではない。環 A が整域ならば、$A[[x]], A[x]$ も整域である。

A を整域とするとき、

$$X = \{(a, b) \mid a \in A,\ b \in A,\ b \neq 0\}$$

とおき、

$$R = \{((a, b), (c, d)) \mid ((a, b), (c, d)) \in X \times X,\ ad = bc\}$$

とおくと、R は X 上の同値関係になる。R による商集合

$$X/R = \{[a, b] \mid (a, b) \in X\}$$

に演算 $+, \times$ を次のように定義することができる。

$$+ : (X/R) \times (X/R) \to X/R, \quad + ([a, b], [c, d]) = [ad + bc, bd]$$
$$\times : (X/R) \times (X/R) \to X/R, \quad \times ([a, b], [c, d]) = [ac, bd].$$

これらの写像 $+, \times$ は well-defined であり、これらの演算により X/R は環になる。X/R を整域 A の商体という。

$\mathbf{Z}$ の商体が $\mathbf{Q}$ であることは先週示した。$\mathbf{R}[x]$ の商体は有理関数体（x の有理式＝分数式の全体で、$\mathbf{R}(x)$ と書く）ができる。$\mathbf{R}[[x]]$ の商体はどんなものになるだろうか？

剰余環の構成

$\mathbf{Z}$ から $\mathbf{Z}/m\mathbf{Z}$ を作る方法を、一般化する。A を、乗法に関する交換法則を満たす（整域でなくてもよい）環とする。A の空でない部分集合 I がイデアルとは、

(1) $\forall a \in I, \forall b \in I,\ a - b \in I$

(2) $\forall a \in A, \forall b \in I,\ ab \in I$

が成り立つときをいう。$A = \mathbf{Z}$ とし、$m \in \mathbf{Z}$ とすると

$$I = m\mathbf{Z} = (m) = \{am \mid a \in \mathbf{Z}\}$$

はイデアルになる。一般に、I が A のイデアルならば

$$R = \{(a, b) \mid a \in A,\ b \in A,\ a - b \in I\}.$$

は A 上の同値関係になる。商集合 A/R を A/I と書く。A/I に演算 $+, \times$ を次のように定義することができる。

$$\begin{aligned} + &: A/I \times A/I \to A/I, \quad + ([a], [b]) = [a + b], \\ \times &: A/I \times A/I \to A/I, \quad \times ([a], [b]) = [ab]. \end{aligned}$$

これらの写像 $+, \times$ は well-defined であり、これらの演算により A/I は環になる。

$A = \mathbf{R}[x]$ のイデアル

$$(x^2 + 1) = \{f(x)(x^2 + 1) \mid f(x) \in \mathbf{R}[x]\}$$

を考えると、写像 $g : \mathbf{R}[x]/(x^2 + 1) \to \mathbf{C}$, $g([f(x)]) = f(\sqrt{-1})$ が定義できて、これは全単射であり、しかも $[f_1(x)], [f_2(x)] \in \mathbf{R}[x]/(x^2 + 1)$ に対して

$$\begin{aligned} g([f_1(x)] + [f_2(x)]) &= g([f_1(x)]) + g([f_2(x)]), \\ g([f_1(x)] \times [f_2(x)]) &= g([f_1(x)])g([f_2(x)]) \end{aligned}$$

ただし右辺は $\mathbf{C}$ における和と積である。

一般に A, B を 2 つの環とするとき、ある全単射 $g : A \to B$ が存在して、$\forall a, b \in A$,

$$\begin{aligned} g(a + b) &= g(a) + g(b), \\ g(ab) &= g(a)g(b) \end{aligned}$$

となるとき、A と B は同型であるといい、$A \cong B$ と書く。上のことは $\mathbf{R}[x]/(x^2+1) \cong \mathbf{C}$ となることを示している。また、$\mathbf{Q} \cong$ ($\mathbf{Z}$ の商体) である。

番号 _____ 名前 _____ 2008 年 6 月 13 日

以下の剰余環のうち、$\mathbf{C}$ と同型になるものはどれか。

$\mathbf{R}[x]/(x^2-1)$	
$\mathbf{R}[x]/(x^2+x+1)$	
$\mathbf{R}[x]/(x^3+1)$	
$\mathbf{R}[x]/(x^4+1)$	

解答

- $\mathbf{R}[x]/(x^2-1)$ は整域ではない。実際 $[x+1] \in \mathbf{R}[x]/(x^2-1)$, $[x-1] \in \mathbf{R}[x]/(x^2-1)$, $[x+1] \neq [0]$, $[x-1] \neq [0]$ だが $[x+1][x-1] = [x^2-1] = [0]$ となる。

- $g : \mathbf{R}[x]/(x^2+x+1) \to \mathbf{C}$, $g([f(x)]) = f(\frac{-1+\sqrt{-3}}{2})$ が定義できて、これは全単射であり、しかも $[f_1(x)], [f_2(x)] \in \mathbf{R}[x]/(x^2+x+1)$ に対して

$$g([f_1(x)] + [f_2(x)]) = g([f_1(x)]) + g([f_2(x)]),$$
$$g([f_1(x)] \times [f_2(x)]) = g([f_1(x)])g([f_2(x)])$$

  ただし右辺は $\mathbf{C}$ における和と積である。よって $\mathbf{R}[x]/(x^2+x+1)$ は $\mathbf{C}$ と同型である。

- $\mathbf{R}[x]/(x^3+1)$ は整域ではない。実際 $[x+1] \in \mathbf{R}[x]/(x^3+1)$, $[x^2-x+1] \in \mathbf{R}[x]/(x^3+1)$, $[x+1] \neq [0]$, $[x^2-x+1] \neq [0]$ だが $[x+1][x^2-x+1] = [x^3+1] = [0]$ となる。

- $\mathbf{R}[x]/(x^4+1)$ は整域ではない。実際 $[x^2+\sqrt{2}x+1] \in \mathbf{R}[x]/(x^4+1)$, $[x^2-\sqrt{2}x+1] \in \mathbf{R}[x]/(x^4+1)$, $[x^2+\sqrt{2}x+1] \neq [0]$, $[x^2-\sqrt{2}x+1] \neq [0]$ だが $[x^2+\sqrt{2}x+1][x^2-\sqrt{2}x+1] = [x^4+1] = [0]$ となる。

2008年6月20日

$A = \mathbf{R}[x]$ のイデアル $I = (x^2+1)$ を考え、同値関係

$$R = \{(a,b) \mid a \in A,\ b \in A,\ a-b \in I\}.$$

による商集合 A/R (A/I とも書く) に演算

$$+ : A/I \times A/I \to A/I, \quad + ([a],[b]) = [a+b],$$
$$\times : A/I \times A/I \to A/I, \quad \times ([a],[b]) = [ab].$$

を入れることにより、$\mathbf{R}[x]/I \cong \mathbf{C}$ となる。

同様のことを $\mathbf{R}$ の代わりに $\mathbf{Z}/3\mathbf{Z}$ でやってみる。$A = \mathbf{Z}/3\mathbf{Z}[x]$ のイデアル $I = (x^2+1)$ を考え、同値関係

$$R = \{(a,b) \mid a \in A,\ b \in A,\ a-b \in I\}.$$

による商集合 A/R (A/I とも書く) に演算

$$+ : A/I \times A/I \to A/I, \quad + ([a],[b]) = [a+b],$$
$$\times : A/I \times A/I \to A/I, \quad \times ([a],[b]) = [ab].$$

を入れる。$\mathbf{Z}/3\mathbf{Z}$ は3個の同値類 $[0],[1],[2]$ からなるので、A/I は以下の9個の同値類からなる：

$$[[0]],[[1]],[[2]],[[1]x],[[1]x+[1]],[[1]x+[2]],[[2]x],[[2]x+[1]],[[2]x+[2]]$$

これらを簡単に

$$0,1,2,x,x+1,x+2,2x,2x+1,2x+2$$

と書くことにする。加法は例えば、A において

$$(x+2)+(2x+2) = ([1]x+[2])+([2]x+[2]) = ([1]+[2])x+([2]+[2])$$
$$= [1+2]x+[2+2] = [0]x+[1] = [1] = 1$$

というように計算するので、A/I においては $[x+2]+[2x+2] = [1]$ となる。

乗法は例えば、A において

$$(x+2)(2x+2) = ([1]x+[2]) \times ([2]x+[2]) = [1][2]x^2+([1][2]+[2][2])x+[2][2]$$
$$= [2]x^2+[2+4]x+[4] = [2]x^2+[1] = 2x^2+1$$

というように計算するので、A/I においては $[x+2] \times [2x+2] = [2x^2+1] = [2(x^2+1)+2] = [2]$ となる。

体の定義

集合 A に 2 つの演算 $+$（加法）と $\times$（乗法）が定義されていて、下記の性質が成り立つとき、A は環であるという。

(1) $\forall a, b, c \in A,\ (a+b)+c = a+(b+c)$ （結合法則）

(2) $\forall a, b \in A,\ a+b = b+a$ （交換法則）

(3) $\exists 0 \in A,\ \forall a \in A,\ a+0 = a$ （零元の存在）

(4) $\forall a \in A,\ \exists b \in A,\ a+b = 0$ （加法に関する逆元の存在）

(5) $\forall a, b, c \in A,\ (a \times b) \times c = a \times (b \times c)$ （結合法則）

(6) $\exists 1 \in A,\ \forall a \in A,\ a \times 1 = 1 \times a = a$ （単位元の存在）

(7) $\forall a, b, c \in A,\ a \times (b+c) = (a \times b) + (a \times c),\ (b+c) \times a = (b \times a) + (c \times a)$ （分配法則）

環 A が次の条件を満たすとき、体という。

(1) $\forall a, b \in A,\ a \times b = b \times a$ （乗法に関する交換法則）

(2) $\forall a \in A - \{0\},\ \exists b \in A,\ ab = 1$ （乗法に関する逆元の存在）

例えば、$\mathbf{Q}, \mathbf{R}, \mathbf{C}$ は体である。$\mathbf{Z}$ は体ではない。また、一般に整域の商体は体であり、体は必ず整域である。

代数学の基本定理（定数でない複素数係数の 1 変数多項式は複素数の零点を必ず持つ）から、$\mathbf{R}[x]/(3\text{次以上の多項式})$ は整域にならない。ただし、$\mathbf{Q}[x]/(3\text{次以上の多項式})$ は体になることもある。因数分解できない多項式を既約という。

ユークリッドの互除法

以下 $A = \mathbf{Z}$ または $A = K[x]$ (ただし K は体) とする。

- $A = \mathbf{Z}$ のとき、$a \in A,\ b \in A,\ b > 0$ とすると、a を b で割った商と余りを求めることができる。すなわち、$a = bq + r,\ 0 \leq r < b$ となる $q, r \in A$ がただひとつ定まる。

- $A = K[x]$ のとき、$a(x) \in A,\ b(x) \in A,\ b(x) \neq 0$ とすると、$a(x)$ を $b(x)$ で割った商と余りを求めることができる。すなわち、$a(x) = b(x)q(x) + r(x),\ 0 \leq \deg r(x) < \deg b(x)$ または $r(x) = 0$ となる $q(x), r(x) \in A$ がただひとつ定まる。

以後、$a(x), b(x)$ の代わりに、a, b と書く。$A = \mathbf{Z}$, $A = K[x]$ いずれの場合にも、$r = 0$ となるとき、$b|a$ と書き、a は b で割り切れる、という。

$a, b \in A$ とし、a と b の少なくとも一方は 0 でないとする。a と b の最大公約数（最大公約元） d とは、以下の条件を満たすものである。

(1) $d > 0$ ($A = \mathbf{Z}$ の場合), d は最高次の係数が 1 ($A = K[x]$ の場合)

(2) $(d|a) \wedge (d|b)$

(3) $\forall e \in A,\ ((e|a) \wedge (e|b)) \implies e|d$

a と b の最大公約元を $\gcd(a, b)$ と書く。

$a, b \in A$ とし、a と b の少なくとも一方は 0 でないとする。今、0 でない方を b とし、$A = \mathbf{Z}$ の場合は $b' = |b|$ とする。$r_0 = a$, $r_1 = b'$ とおき、$k = 0, 1, \ldots$ に対して、r_k を r_{k+1} で割った商を q_{k+2}, 余りを r_{k+2} とおく。このとき

$$\begin{array}{ll} r_k > r_{k+1} & (A = \mathbf{Z}) \\ \deg r_k > \deg r_{k+1} & (A = K[x]) \end{array}$$

なので、$\exists n,\ r_n \neq 0,\ r_{n+1} = 0$ となる。すると r_{n+2} 以降は定義できない。

このとき、

$$\begin{aligned} r_n &= r_{n-2} - r_{n-1}q_n \\ &= r_{n-2} - (r_{n-3} - r_{n-2}q_{n-1})q_n \\ &= -r_{n-3}q_n + r_{n-2}(1 + q_{n-1}q_n) \\ &= \cdots \\ &= m_0 r_0 + m_1 r_1 \\ &= m_0 a + m_1 b' \\ &= m_0 a \pm m_1 b. \end{aligned}$$

これより、

$$\gcd(a, b) = \begin{cases} r_n & (A = \mathbf{Z}), \\ r_n \text{ をその最高次の係数で割ったもの} & (A = K[x]) \end{cases}$$

であり、しかも $\exists s, t \in A,\ sa + tb = \gcd(a, b)$ となる。

2008年6月20日

$g : A \to B$ を環の同型写像、すなわち、g は全単射でかつ、任意の $a, b \in A$ に対して、

$$g(a+b) = g(a) + g(b),$$
$$g(ab) = g(a)g(b)$$

を満たすとする。このとき、

$$g(0) = 0$$

が成り立つ。ただし、左辺の 0 は環 A の零元であり、右辺の 0 は環 B の零元である。実際、

$$\begin{aligned} g(0) &= 0 + g(0) \\ &= (g(0) + (-g(0))) + g(0) \\ &= (-g(0)) + (g(0) + g(0)) \\ &= (-g(0)) + g(0+0) \\ &= (-g(0)) + g(0) \\ &= 0. \end{aligned}$$

また、B が整域ならば A も整域である。実際、$a \in A$, $b \in A$, $a \neq 0$, $b \neq 0$ とすると g は単射なので $g(a) \neq g(0) = 0$, $g(b) \neq g(0) = 0$ となる。B は整域なので $g(a)g(b) \neq 0$ となるが、$g(ab) = g(a)g(b)$ より、$g(ab) \neq 0$ となる。これは $ab \neq 0$ を意味している。

番号 _____ 名前 _____　　2008 年 6 月 20 日

$A = \mathbf{Z}/5\mathbf{Z}[x]$ の元 $a = x^4 + 2x^2 + 4x + 1$ と $b = x^2 + 2x + 1$ に対して $d = \gcd(a, b)$ を求め、$sa + tb = d$ となる $s, t \in A$ を一組求めなさい。

解答

a を b で割ると

$$a = (x^2 + 3x)b + x + 1.$$

次に、b を $x + 1$ で割ると

$$b = (x + 1)(x + 1)$$

となるので、$\gcd(a, b) = x + 1$ であり、

$$x + 1 = a - (x^2 + 3x)b = a + (4x^2 + 2x)b.$$

番号＿＿＿＿＿＿＿＿名前＿＿＿＿＿＿＿＿　2008年6月20日（2008年6月27日提出）

$(\mathbf{Z}/3\mathbf{Z}[x])/(x^2+1)$ における乗積表を完成させなさい。

$\times$	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
1	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
2	2	1	$2x$	$2x+2$	$2x+1$	x	$x+2$	$x+1$
x	x	$2x$	2	$x+2$	$2x+2$	1	$x+1$	$2x+1$
$x+1$	$x+1$	$2x+2$	$x+2$	$2x$	1	$2x+1$	2	x
$x+2$	$x+2$	$2x+1$	$2x+2$	1	x	$x+1$	$2x$	2
$2x$	$2x$	x	1	$2x+1$	$x+1$	2	$2x+2$	$x+2$
$2x+1$	$2x+1$	$x+2$	$x+1$	2	$2x$	$2x+2$	x	1
$2x+2$	$2x+2$	$x+1$	$2x+1$	x	2	$x+2$	1	$2x$

また、上の乗積表が次の形になるように、$\alpha_1, \alpha_2, \ldots, \alpha_7$ を定めなさい。

$\times$	1	α_1	α_2	α_3	α_4	α_5	α_6	α_7
1	1	α_1	α_2	α_3	α_4	α_5	α_6	α_7
α_1	α_1	α_2	α_3	α_4	α_5	α_6	α_7	1
α_2	α_2	α_3	α_4	α_5	α_6	α_7	1	α_1
α_3	α_3	α_4	α_5	α_6	α_7	1	α_1	α_2
α_4	α_4	α_5	α_6	α_7	1	α_1	α_2	α_3
α_5	α_5	α_6	α_7	1	α_1	α_2	α_3	α_4
α_6	α_6	α_7	1	α_1	α_2	α_3	α_4	α_5
α_7	α_7	1	α_1	α_2	α_3	α_4	α_5	α_6

$\alpha_1 =$	$2x+1$	$2x+2$	$x+1$	$x+2$
$\alpha_2 =$	x	$2x$	$2x$	x
$\alpha_3 =$	$x+1$	$x+2$	$2x+1$	$2x+2$
$\alpha_4 =$	2	2	2	2
$\alpha_5 =$	$x+2$	$x+1$	$2x+2$	$2x+1$
$\alpha_6 =$	$2x$	x	x	$2x$
$\alpha_7 =$	$2x+2$	$2x+1$	$x+2$	$x+1$

2008年6月27日

体の定義

環 A が次の条件を満たすとき、体という。

(1) $\forall a, b \in A,\ a \times b = b \times a$ （乗法に関する交換法則）

(2) $\forall a \in A - \{0\},\ \exists b \in A,\ ab = 1$ （乗法に関する逆元の存在）

ユークリッドの互除法

$A = \mathbf{Z}$ または $A = K[x]$ (ただし K は体) とする。$a, b \in A$ とし、a と b の少なくとも一方は 0 でないとする。今、0 でない方を b とし、$A = \mathbf{Z}$ の場合は $b' = |b|$ とする。$r_0 = a,\ r_1 = b'$ とおき、$k = 0, 1, \ldots$ に対して、r_k を r_{k+1} で割った商を q_{k+2}, 余りを r_{k+2} とおく。このとき

$$\begin{array}{ll} r_k > r_{k+1} \geq 0 & (A = \mathbf{Z}) \\ \deg r_k > \deg r_{k+1} & (A = K[x]) \end{array}$$

なので、$\exists n,\ r_n \neq 0,\ r_{n+1} = 0$ となる。このとき、

$$\gcd(a, b) = \begin{cases} r_n & (A = \mathbf{Z}), \\ r_n \text{ をその最高次の係数で割ったもの} & (A = K[x]) \end{cases}$$

であり、しかも $\exists s, t \in A,\ sa + tb = \gcd(a, b)$ となる。

体の例

p を素数とすると、$\mathbf{Z}/p\mathbf{Z}$ は体である。また、K を体とし、$f(x) \in K[x]$ を既約多項式とすると、$K[x]/(f(x))$ は体である。

体の元の位数

K を体とし、$0 \neq x \in K$ とする。

$$\exists n \in \mathbf{N},\ x^n = 1$$

が成り立つとき、このような最小の n を x の位数という。このような $n \in \mathbf{N}$ が存在しないときは、x の位数は無限であるという。$1 \in K$ の位数は 1 である。$-1 \in \mathbf{Q}$ の位数は 2 である。

$n \in \mathbf{N}$ とすると、

$$\zeta = e^{2\pi i/n} = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n} \in \mathbf{C}$$

の位数は n である。$\mathbf{C}$ における位数 n の元全体の集合は

$$\{\zeta^k \mid k \in \{1, \ldots, n\},\ \gcd(k, n) = 1\}$$

である。この集合の元の個数、すなわち

$$|\{k \mid k \in \{1, \ldots, n\},\ \gcd(k, n) = 1\}|$$

を $\varphi(n)$ で表し、φ をオイラーの関数という。例えば、$\varphi(1) = 1$ である。また、p が素数ならば

$$\varphi(p) = |\{1, 2, \ldots, p-1\}| = p - 1$$

であり、一般には $\varphi(n) \leq n - 1$ である。例えば $\varphi(12) = |\{1, 5, 7, 9\}| = 4$ である。

有限体

K が体であり、しかも有限集合のとき、K を有限体という。例えば $\mathbf{Z}/p\mathbf{Z}$ は有限体である。また、$f(x) \in \mathbf{Z}/p\mathbf{Z}[x]$ が既約なら、$(\mathbf{Z}/p\mathbf{Z}[x])/(f(x))$ は有限体である。特に $(\mathbf{Z}/3\mathbf{Z}[x])/(x^2+1)$ は有限体である。

K を有限体とし、$0 \neq x \in K$ とすると、x の位数は有限でしかもそれは $|K| - 1$ の約数である。例えば、$(\mathbf{Z}/3\mathbf{Z}[x])/(x^2+1)$ の 8 個の非零元の位数は、$1, 2, 4, 8$ のいずれかである。実は、この逆も成り立つ。K を有限体とし、d を $|K| - 1$ の約数とすると、K には位数 d の元が存在する。この事実の証明は次回の講義で行う。

2008年6月27日

ユークリッドの互除法

$A = \mathbf{Z}$ または $A = K[x]$ (ただし K は体) とする。$a, b \in A$ とし、a と b の少なくとも一方は 0 でないとする。今、0 でない方を b とし、$A = \mathbf{Z}$ の場合は $b' = |b|$ とする。$r_0 = a$, $r_1 = b'$ とおき、$k = 0, 1, \ldots$ に対して、r_k を r_{k+1} で割った商を q_{k+2}, 余りを r_{k+2} とおく。このとき

$$\begin{array}{ll} r_k > r_{k+1} \geq 0 & (A = \mathbf{Z}) \\ \deg r_k > \deg r_{k+1} & (A = K[x]) \end{array}$$

なので、$\exists n,\ r_n \neq 0,\ r_{n+1} = 0$ となる。このとき、

$$\gcd(a, b) = \begin{cases} r_n & (A = \mathbf{Z}), \\ r_n \text{ をその最高次の係数で割ったもの} & (A = K[x]) \end{cases}$$

であり、しかも $\exists s, t \in A,\ sa + tb = \gcd(a, b)$ となる。

実際、a と b の最大公約数（最大公約元）d とは、以下の条件を満たすものである。

(1) $d > 0$ ($A = \mathbf{Z}$ の場合), d は最高次の係数が 1 ($A = K[x]$ の場合)

(2) $(d|a) \wedge (d|b)$

(3) $\forall e \in A,\ ((e|a) \wedge (e|b)) \implies e|d$

a と b の最大公約元を $\gcd(a, b)$ と書く。

r_n の作り方から $r_{n+1} = 0$ より、r_{n-1} は r_n で割り切れている。r_{n-2} を r_{n-1} で割った余りが r_n であるということから r_{n-2} も r_n で割り切れている。同様に r_{n-3} も r_n で割り切れている。続けていくと r_1, r_0 も r_n で割り切れている。したがって r_n は a, b 両方を割り切っている。

$$d = \begin{cases} r_n & (A = \mathbf{Z}), \\ r_n \text{ をその最高次の係数で割ったもの} & (A = K[x]) \end{cases}$$

とおくと、上で示したように、d は a, b 両方を割り切っている。

また、$e|a$ かつ $e|b$ とすると、$e|r_0$ かつ $e|r_1$ である。r_2 は r_0 を r_1 で割った余りなので $e|r_2$ となる。r_3 は r_1 を r_2 で割った余りなので $e|r_1$, $e|r_2$ より $e|r_3$ となる。同様に続けていくと $e|r_n$ がわかる。よって $e|d$ となる。

以上より、$d = \gcd(a, b)$ が言えた。

番号 _____ 名前 _____ 2008 年 6 月 27 日

$(\mathbf{Z}/3\mathbf{Z}[x])/(x^2+1)$ における 0 以外の各元の位数を求めよ。

元	位数
1	
2	
x	
$x+1$	
$x+2$	
$2x$	
$2x+1$	
$2x+2$	

$\mathbf{Z}/13\mathbf{Z}$ における位数 3 の元をすべて求めよ。また、位数 4 の元をすべて求めよ。

2008年7月4日

有限体

K が体であり、しかも有限集合のとき、K を有限体という。以下、K を有限体とし、$q = |K|$ とする。$K^\times = K - \{0\}$ と書く。$x \in K^\times$ とすると、x の位数は有限でしかもそれは $q-1$ の約数である。実際、x の位数を n とすると、

$$\{1, x, x^2, \ldots, x^{n-1}\} \subseteq K^\times.$$

である。ここで等号が成り立てば $n = q-1$ だが、等号が成り立たなければ $\exists y \in K^\times$, $y \notin \{1, x, x^2, \ldots, x^{n-1}\}$ となる。このとき

$$\{1, x, x^2, \ldots, x^{n-1}\} \cup \{y, xy, x^2y, \ldots, x^{n-1}y\} \subseteq K^\times.$$

この操作を繰り返すと、$\exists y_1, \ldots, y_m \in K^\times$,

$$\bigcup_{j=1}^{m} \{y_j, xy_j, x^2y_j, \ldots, x^{n-1}y_j\} = K^\times \quad \text{(disjoint)}$$

となるので $q-1 = mn$ となって n は $q-1$ の約数であることがわかる。

実は、この逆も成り立つ。n を $q-1$ の約数とすると、K には位数 n の元が存在する。これを示すために補題を準備する。

補題 1. $x \in K^\times$ の位数が n とすると、$m \in \mathbf{N}$ に対して、$x^m = 1 \iff n|m$ である。

証明. 明らかに、$n|m$ ならば $x^m = 1$ である。逆に $x^m = 1$ とすると、m を n で割って $m = ns + r$, $0 \le r < n$ とすると、$1 = x^m = (x^n)^q x^r = x^r$ となる。n の最小性より $r = 0$ を得る。 □

補題 2. $\forall n \in \mathbf{N}$, $n|q-1 \implies |\{x \mid x \in K^\times,\ x^n = 1\}| = n$.

証明. $f(X) = X^n - 1 \in K[X]$ とおくと、$n|q-1$ より $\exists g(X) \in K[X]$, $X^{q-1} - 1 = f(X)g(X)$ となる。補題1 より、

$$X^{q-1} - 1 = \prod_{x \in K^\times} (X - x)$$

となるので、

$$\begin{aligned} q-1 = |K^\times| &= |\{x \mid x \in K^\times,\ x^{q-1} - 1 = 0\}| \\ &= |\{x \mid x \in K^\times,\ f(x) = 0 \text{ or } g(x) = 0\}| \\ &\le |\{x \mid x \in K^\times,\ f(x) = 0\}| + |\{x \mid x \in K^\times,\ g(x) = 0\}| \\ &\le \deg f(X) + \deg g(X) \\ &= n + (q - 1 - n) = q - 1. \end{aligned}$$

したがって、$f(X) = 0$ は n 個の相異なる解を $K^\times$ に持つ。 □

補題 3. $\forall n \in \mathbf{N}$

$$n = \sum_{\substack{d \in \mathbf{N} \\ d|n}} \varphi(d).$$

証明. $N = \{1, 2, \ldots, n\}$, $D = \{d \mid d \in \mathbf{N},\ d|n\}$ とし、

$$S = \{(k, d) \mid (k, d) \in N \times D,\ d = \gcd(k, n)\}$$

とおく。すると

$$\begin{aligned} n = |N| &= \sum_{k \in N} 1 = \sum_{k \in N} |\{d \mid d \in D,\ d = \gcd(k, n)\}| \\ &= |S| = \sum_{d \in D} |\{k \mid k \in N,\ d = \gcd(k, n)\}| \\ &= \sum_{d \in D} |\{k' \mid k' \in \{1, \ldots, \frac{n}{d}\},\ 1 = \gcd(k', \frac{n}{d})\}| \\ &= \sum_{d \in D} \varphi(\frac{n}{d}) = \sum_{e \in D} \varphi(e). \end{aligned}$$

□

定理 4. K を有限体、$n \in \mathbf{N}$ を $|K| - 1$ の約数とすると、

$$|\{x \mid x \in K^\times,\ x \text{ の位数は } n\}| = \varphi(n).$$

証明. 左辺を $\alpha(n)$ とおくと、$\alpha(1) = \varphi(1)$ は明らか。ある n より小さい d について $\alpha(d) = \varphi(d)$ が成立すると仮定すると、

$$\begin{aligned} \sum_{\substack{d \in \mathbf{N} \\ d|n}} \varphi(d) &= n && \text{(補題 4 より)} \\ &= |\{x \mid x \in K^\times,\ x^n = 1\}| && \text{(補題 2 より)} \\ &= \sum_{\substack{d \in \mathbf{N} \\ d|n}} \alpha(d) && \text{(補題 1 より)} \\ &= \sum_{\substack{d \in \mathbf{N} \\ d|n \\ d \neq n}} \alpha(d) + \alpha(n) \\ &= \sum_{\substack{d \in \mathbf{N} \\ d|n \\ d \neq n}} \varphi(d) + \alpha(n) && \text{(帰納法の仮定より).} \end{aligned}$$

よって $\varphi(n) = \alpha(n)$ を得る。 □

例えば、$\mathbf{Z}/13\mathbf{Z}$ は体であり、位数 12 の元は $2, 6, 7, 11$ である。

一般に、$|K| = q$ である体 K には、位数 $q - 1$ の元の存在が保証されているので、そのような元のひとつを α とすると、$K^\times$ の乗積表は、次のようになる。

$\times$	1	α	α^2	$\cdots$	α^{q-1}
1	1	α	α^2	$\cdots$	α^{q-1}
α	α	α^2	α^3	$\cdots$	1
α^2	α^2	α^3	α^4	$\cdots$	α
$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\vdots$
α^{q-2}	α^{q-2}	1	α	$\cdots$	α^{q-3}

指数だけ書けば

$+$	0	1	2	$\cdots$	$q-1$
0	0	1	2	$\cdots$	$q-1$
1	1	2	3	$\cdots$	0
2	2	3	4	$\cdots$	1
$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\vdots$
$q-2$	$q-2$	0	1	$\cdots$	$q-3$

群

集合 G に演算 $*: G \times G \to G$ が定義されていて、次の性質を満たすとき、$(G, *)$ は群であるという。

(1) $\forall a, b, c \in G,\ (a * b) * c = a * (b * c)$ （結合法則）

(2) $\exists e \in G,\ \forall a \in G,\ a * e = e * a = a$ （単位元の存在）

(3) $\forall a \in G,\ \exists b \in G,\ a * b = b * a = e$ （逆元の存在）

もし $*$ を指定しなくても他の演算と混乱することがないときは、単に G は群であるという。e を 1 または 0 と書くこともある。上の b は a^{-1} または $-a$ と書くことがある。

任意の環 A は、その加法 $+$ に関して群になる。体 K に対して、$K^\times$ は乗法に関して群になる。実数を成分とする n 次正則行列全体は行列の積に関して群になる。

二つの群 $(G_1, *_1)$, $(G_2, *_2)$ に対して、全単射 $f: G_1 \to G_2$ が存在して $\forall x, y \in G_1$, $f(x *_1 y) = f(x) *_2 f(y)$ が成り立つとき、G_1 と G_2 は同型であるといい、$G_1 \cong G_2$ と書く。例えば $(\mathbf{Z}/3\mathbf{Z}[x])/(x^2+1), \times) \cong (\mathbf{Z}/8\mathbf{Z}, +)$, $(\mathbf{R}_{>0}, \times) \cong (\mathbf{R}, +)$ である。

群 G に対して、$\exists a \in G,\ G = \{a^n \mid n \in \mathbf{Z}\}$ が成り立つとき、G は巡回群であるという。ここで、

$$a^n = \begin{cases} a * a * \cdots * a \quad (n \text{ 個}) & (n \in \mathbf{N}) \\ e & (n = 0) \\ a^{-1} * a^{-1} * \cdots * a^{-1} \quad (n \text{ 個}) & (-n \in \mathbf{N}) \end{cases}$$

このとき指数法則が成り立つ。定理 4 より、任意の有限体 K に対して $K^\times$ は巡回群である。任意の $m \in \mathbf{N}$ に対して、$(\mathbf{Z}/m\mathbf{Z}, +)$ は巡回群である。有限巡回群の乗積表は上図のようになる。$(\mathbf{Z}, +)$ は巡回群であるが、$(\mathbf{Q}, +)$ は巡回群ではない。任意の無限巡回群は $(\mathbf{Z}, +)$ と同型である。

前回までに講義済みの内容

体の定義

環 A が次の条件を満たすとき、体という。

(1) $\forall a, b \in A,\ a \times b = b \times a$ （乗法に関する交換法則）

(2) $\forall a \in A - \{0\},\ \exists b \in A,\ ab = 1$ （乗法に関する逆元の存在）

体の元の位数

K を体とし、$0 \neq x \in K$ とする。

$$\exists n \in \mathbf{N},\ x^n = 1$$

が成り立つとき、このような最小の n を x の位数という。オイラーの関数とは

$$\varphi(n) = |\{k \mid k \in \{1, \ldots, n\},\ \gcd(k, n) = 1\}|$$

で定義される関数 $\varphi : \mathbf{N} \to \mathbf{N}$ のことである。

2008年7月4日

$n = 12$ とすると $D = \{1, 2, 3, 4, 6, 12\}$ であり、

$$
\begin{aligned}
|S| = |\{&(1,1),(5,1),(7,1),(11,1)\}| && (d = 1)\\
&+ |\{(2,2),(10,2))\}| && (d = 2)\\
&+ |\{(3,3),(9,3)\}| && (d = 3)\\
&+ |\{(4,4),(8,4)\}| && (d = 3)\\
&+ |\{(6,6)\}| && (d = 6)\\
&+ |\{(12,12)\}| && (d = 12)
\end{aligned}
$$

番号 _____ 名前 _____　　2008 年 7 月 4 日

次の命題の証明を完成せよ。

$$a, b, c \in \mathbf{N} \implies \gcd(ca, cb) = c \gcd(a, b).$$

証明 $d = \gcd(a, b)$, $d' = \gcd(ca, cb)$ とおくと、gcd の定義より、

$$d|a,\ d|b \tag{5}$$
$$\forall e \in \mathbf{N},\ e|a,\ e|b \implies e|d \tag{6}$$
$$d'|ca,\ d'|cb \tag{7}$$
$$\forall f \in \mathbf{N},\ f|ca,\ f|cb \implies f|d' \tag{8}$$

が成り立つ。(5) より、$cd|ca$, $cd|cb$ であるから、(8) で $f = cd$ とおくことにより、

$$cd|d' \tag{9}$$

を得る。

明らかに

$$\boxed{c|ca},\ \boxed{c|cb}$$

だから $\boxed{(4)}$ で $f = \boxed{c}$ とおくと、$c|d'$ を得る。

そこで

$$g = \frac{d'}{c}$$

とおくと、$\boxed{(3)}$ より $g|a$, $g|b$ を得る。

よって $\boxed{(2)}$ において $\boxed{e} = \boxed{g}$ とおくと、$g|d$ を得る。したがって

$$d'|cd \tag{10}$$

となる。(9), (10) より $d' = cd$ が成立する。

2008年7月11日

群

集合 G に演算 $*: G \times G \to G$ が定義されていて、次の性質を満たすとき、$(G, *)$ は群であるという。

(1) $\forall a, b, c \in G,\ (a * b) * c = a * (b * c)$ （結合法則）

(2) $\exists e \in G,\ \forall a \in G,\ a * e = e * a = a$ （単位元の存在）

(3) $\forall a \in G,\ \exists b \in G,\ a * b = b * a = e$ （逆元の存在）

上の b は a^{-1} または $-a$ と書くことがある。

二つの群 $(G_1, *_1)$, $(G_2, *_2)$ に対して、全単射 $f: G_1 \to G_2$ が存在して $\forall x, y \in G_1$, $f(x *_1 y) = f(x) *_2 f(y)$ が成り立つとき、G_1 と G_2 は同型であるといい、$G_1 \cong G_2$ と書く。

群 G に対して、$\exists a \in G,\ G = \{a^n \mid n \in \mathbf{Z}\}$ が成り立つとき、G は巡回群であるという。無限巡回群は $\mathbf{Z}$ と同型である。位数 m の巡回群は $\mathbf{Z}/m\mathbf{Z}$ と同型である。

G を群とし、その単位元を 1 と書くことにする。$x \in G$ に対し、

$$\min\{n \mid n \in \mathbf{N},\ x^n = 1\}$$

を、元 x の位数という。ただし $\{n \mid n \in \mathbf{N},\ x^n = 1\} = \emptyset$ のときは位数無限という。K が体ならば、$K^\times$ は群になるので、すでに定義済みの $x \in K^\times$ の位数と上の定義は一致する。

群 G が有限集合のとき有限群という。$K^\times$ の場合と全く同様にして、$x \in G$ の位数は $|G|$ の約数であることがわかる。

$n \in \mathbf{N}$ とし、n 個の元からなる集合（例えば $X = \{1, 2, \ldots, n\}$）からそれ自身への全単射全体のなす集合を n 次対称群といい、S_n で表す。S_n は写像の合成に関して群をなす。単位元は恒等写像、逆元は逆写像である。恒等写像というのは、

$$\mathrm{id}(1) = 1, \quad \mathrm{id}(2) = 2, \ldots, \mathrm{id}(n) = n$$

で定義される X から X への写像である。一般には $|S_n| = n!$ である。例えば、$n = 3$, $X = \{1, 2, 3\}$ とすると、

$$f(1) = 2, \quad f(2) = 3, \quad f(3) = 1,$$
$$g(1) = 2, \quad g(2) = 1, \quad g(3) = 3$$

などが S_3 の元である。これらは順列と考えても良く、省略してそれぞれ 231, 213 と書くこともできる。写像の合成 $f \circ g$ とは $f \circ g(x) = f(g(x))$ によって定義される写像である。上記の f, g に対しては

$$f \circ g(1) = 3, \quad f \circ g(2) = 2, \quad f \circ g(3) = 1$$

となる。一般に、f, g が全単射ならば、$f \circ g$ も全単射である。したがって $\circ$ は S_n における演算となり、この演算に関して S_n は群になる。

S_n は線形代数学で習ったはず：$A = (a_{ij})$ を n 次正方行列とすると

$$\det A = \sum_{f \in S_n} \mathrm{sgn}(f) \prod_{i=1}^{n} a_{i,f(i)}$$

と表される。ここで

$$\mathrm{sgn}(f) = (-1)^{|\{(i,j)|i\in X,\, j\in X,\, i<j,\, f(i)>f(j)\}|}.$$

K を体とすると、K の元を成分とする n 次正方行列に、通常の行列の積を定義することができる。K が体であることから、K の元を成分とする行列の積は結合法則をみたし、K の単位元、零元から単位行列を作ることができる。また、K が体であることから、行列式の定義、それによる逆行列の公式が成り立つ。逆行列を持つ行列を正則行列といい、K の元を成分とする n 次正則行列全体の集合を $GL(n, K)$ と書く。$GL(n, K)$ は行列の積に関して群になる。

例えば、$n = 2$, $K = \mathbf{Z}/2\mathbf{Z}$ とすると

$$GL(2, \mathbf{Z}/2\mathbf{Z}) = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \right\}.$$

S_3 も $GL(2, \mathbf{Z}/2\mathbf{Z})$ も位数 6 の元を持たないので、$\mathbf{Z}/6\mathbf{Z}$ とは同型でない。

前回までに講義済みの内容

一般に、$|K| = q$ である体 K には、位数 $q-1$ の元の存在が保証されているので、そのような元のひとつを α とすると、$K^\times$ の乗積表は、次のようになる。

$\times$	1	α	α^2	$\cdots$	α^{q-1}
1	1	α	α^2	$\cdots$	α^{q-1}
α	α	α^2	α^3	$\cdots$	1
α^2	α^2	α^3	α^4	$\cdots$	α
$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\vdots$
α^{q-2}	α^{q-2}	1	α	$\cdots$	α^{q-3}

指数だけ書けば

$+$	0	1	2	$\cdots$	$q-1$
0	0	1	2	$\cdots$	$q-1$
1	1	2	3	$\cdots$	0
2	2	3	4	$\cdots$	1
$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\vdots$
$q-2$	$q-2$	0	1	$\cdots$	$q-3$

番号＿＿＿＿＿＿＿名前＿＿＿＿＿＿＿　2008年7月11日（2008年7月18日提出）

3次対称群 S_3 と一般線形群 $GL(2, \mathbf{Z}/2\mathbf{Z})$ の間の同型写像をひとつ挙げなさい。また、同型写像は全部でいくつあるか。

123	•	•	$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$
132	•	•	$\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$
213	•	•	$\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$
231	•	•	$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
312	•	•	$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$
321	•	•	$\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$

2008年7月18日

$GL(2, \mathbf{Z}/2\mathbf{Z})$ と S_3 の同型写像の作り方

$$\left\{ \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \end{bmatrix} \right\} = \{v_1, v_2, v_3\}$$

とする（v_1, v_2, v_3 の定め方は $3! = 6$ 通りある）。$A \in GL(2, \mathbf{Z}/2\mathbf{Z})$ に対し、$f(A) \in S_3$ を

$$Av_i = v_{f(A)(i)}$$

で定めると、$f : GL(2, \mathbf{Z}/2\mathbf{Z}) \to S_3$ は同型写像になる。このようにして、6個の同型写像が得られる。

$$A = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad B = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

とすれば、A, B の位数はともに 2 である。従って、$f : GL(2, \mathbf{Z}/2\mathbf{Z}) \to S_3$ が同型写像ならば、$f(A), f(B)$ も位数が 2 でなければならない。S_3 には位数 2 の元が3つ（213, 321, 132）存在するので、$(f(A), f(B))$ の取り得る値は高々 6 通りしかない。

$$GL(2, \mathbf{Z}/2\mathbf{Z}) = \{I, A, B, AB, BA, ABA\}$$

が確かめられるので、同型写像 f は $f(A), f(B)$ のみで定まり、従って同型写像の個数は高々 6 個しかない。一方、実際に 6 個の同型写像があることはすでに示したので、答えは 6 個である。

記号的な群の構成法

$(\mathbf{Z}/6\mathbf{Z}, +) \cong ((\mathbf{Z}/7\mathbf{Z})^\times, \times) = \{[3]^n \mid n \in \mathbf{Z}\}$ である。

$\mathbf{Z}$ から $\mathbf{Z}/6\mathbf{Z}$ を構成するには、合同式で定義された同値関係を用いた。これを一般的、かつ乗法的に書くと、無限巡回群 $G = \{a^n \mid n \in \mathbf{Z}\}$ に同値関係

$$a^{n_1} \sim a^{n_2} \iff n_1 \equiv n_2 \pmod{m}$$

を定義して、商集合に演算を定義したものと考えることができる。これは、a または a^{-1} が n 個続けて並んだら単位元なのでそこを消して良い、という規則であると解釈できる。

$GL(2, \mathbf{Z}/2\mathbf{Z})$ は巡回群ではない（位数 6 の元を持たない）ので、$(\mathbf{Z}/7\mathbf{Z})^\times$ のように表すことはできない。しかし、$A, B \in GL(2, \mathbf{Z}/2\mathbf{Z})$ を上記のように定めると、他の全ての元は A, B で表すことができる。A, B, AB の位数はそれぞれ、$2, 2, 3$ であるから、

$$A^2 = B^2 = (AB)^3 = 1$$

が成り立つ。実はこの式だけから、$\{I, A, B, AB, BA, ABA\}$ が群になることが導かれるのである。

同値関係の作り方

X を集合、$D \subset X \times X$ とするとき、$\hat{D} \subset X \times X$ を次で定義する。

$$\begin{aligned}\hat{D} = &\{(x,x) \mid x \in X\} \\ &\cup \{(x,y) \mid x \in X,\ y \in X, \\ &\quad \exists x_0, x_1, \ldots, x_n \in X,\ x_0 = x,\ x_n = y, \\ &\quad\quad \forall i \in \{1,\ldots,n\},\ (x_{i-1}, x_i) \in D \text{ or } (x_i, x_{i-1}) \in D\}.\end{aligned}$$

このとき、$\hat{D}$ は同値関係になる。

基本関係を用いた群の構成

a, b を無意味な記号とし、X を a, b からなる有限列全体の集合とする。長さ 0 の列を 1 で表し、これも X の元とする。X には自明な演算が定義されている。

$$\begin{aligned}D = &\{(w_1w_2, w_1aaw_2) \mid w_1 \in X,\ w_2 \in X\} \\ &\cup \{(w_1w_2, w_1bbw_2) \mid w_1 \in X,\ w_2 \in X\} \\ &\cup \{(w_1w_2, w_1ababaw_2) \mid w_1 \in X,\ w_2 \in X\}\end{aligned}$$

とおき、D の推移閉包 $\hat{D}$ による商集合 $X/\hat{D}$ に演算 $[w][w'] = [ww']$ を定義することができる（well-defined になる）。この演算により、$X/\hat{D}$ は群になり、しかも

$$X/\hat{D} = \{[1], [a], [b], [ab], [ba], [aba]\}$$

である。

同様にして、無意味な記号の集合

$$A = \{a_1, a_2, \ldots, a_n, a_1^{-1}, a_2^{-1}, \ldots, a_n^{-1}\}$$

に対し、A の元の有限列全体の集合 X を考えて、

$$X \supset R \supset \{a_i a_i^{-1} \mid i \in \{1,\ldots,n\}\} \cup \{a_i^{-1} a_i \mid i \in \{1,\ldots,n\}\}$$

を満たす R から

$$D = \{(w_1w_2, w_1rw_2) \mid w_1 \in X,\ w_2 \in X\}$$

を作ると、$X/\hat{D}$ は群になる。例えば、$A = \{a, b, c, a^{-1}, b^{-1}, c^{-1}\}$,

$$R = \{a^2, b^2, c^2, (ab)^3, (bc)^3, aa^{-1}, a^{-1}a, bb^{-1}, b^{-1}b, cc^{-1}, c^{-1}c, \}$$

とすると、$X/\hat{D} \cong S_4$ となる。

第２学期火曜日２講時藤原教授による「情報基礎数理学 IVb」ではこのようにして得られた群に関してさらに進んだ内容を講義する予定。

前回までに講義済みの内容

群

集合 G に演算 $*: G \times G \to G$ が定義されていて、次の性質を満たすとき、$(G, *)$ は群であるという。

(1) $\forall a, b, c \in G,\ (a * b) * c = a * (b * c)$ （結合法則）

(2) $\exists e \in G,\ \forall a \in G,\ a * e = e * a = a$ （単位元の存在）

(3) $\forall a \in G,\ \exists b \in G,\ a * b = b * a = e$ （逆元の存在）

上の b は a^{-1} または $-a$ と書くことがある。

二つの群 $(G_1, *_1)$, $(G_2, *_2)$ に対して、全単射 $f: G_1 \to G_2$ が存在して $\forall x, y \in G_1$, $f(x *_1 y) = f(x) *_2 f(y)$ が成り立つとき、G_1 と G_2 は同型であるといい、$G_1 \cong G_2$ と書く。

$n \in \mathbf{N}$ とし、n 個の元からなる集合（例えば $X = \{1, 2, \ldots, n\}$）からそれ自身への全単射全体のなす集合を n 次対称群といい、S_n で表す。S_n は写像の合成に関して群をなす。単位元は恒等写像、逆元は逆写像である。

K を体とし、K の元を成分とする n 次正則行列全体の集合を $GL(n, K)$ と書く。$GL(n, K)$ は行列の積に関して群になる。例えば、$n = 2$, $K = \mathbf{Z}/2\mathbf{Z}$ とすると

$$GL(2, \mathbf{Z}/2\mathbf{Z}) = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \right\}.$$

S_3 も $GL(2, \mathbf{Z}/2\mathbf{Z})$ も位数 6 の元を持たないので、$\mathbf{Z}/6\mathbf{Z}$ とは同型でない。

2008年7月18日

$$\begin{aligned} v_{f(AB)(i)} &= ABv_i \\ &= A(Bv_i) \\ &= Av_{f(B)(i)} \\ &= v_{f(A)(f(B)(i))} \\ &= v_{f(A)\circ f(B)(i)} \end{aligned}$$

よって $f(AB)(i) = f(A) \circ f(B)(i)$ が成り立つ。$i \in \{1,2,3\}$ は任意なので $f(AB) = f(A) \circ f(B)$ が成り立つ。

$a^2 = b^2 = (ab)^3 = 1$ という規則の下で、a, b を次々とかけることで得られる元は

$$1, a, b, ab, ba, aba$$

のみである。実際、$(ab)^3 = 1$ から、$ababab = 1$ となるが、$a^2 = b^2 = 1$ より、移項することでこれは $aba = bab$ を意味していることになる。長い列でも、a または b が続けばキャンセルすることができ、a, b が交互にあらわれるときは $aba = bab$ を使って a または b を続くようにすることができる。したがって、どんなにたくさん a と b をかけたとしても、この規則の下で書き換えると上の6元のうちのどれかに等しくなってしまう。このことを厳密に議論するために、用語を準備する。

$D \subset X \times X$ から $\hat{D} \subset X \times X$ を作る方法は、推移閉包、 またはグラフの連結成分とも呼ばれる。

例えば、$X = \{1,2,3,4,5\}$, $D = \{(1,2),(3,4),(5,4)\}$ とすると、

$$\hat{D} = \{(x,x) \mid x \in X\} \cup \{(1,2),(2,1),(3,4),(4,3),(3,5),(5,3),(4,5),(5,4)\}.$$

来週の期末試験には、本、ノート他、何を持ち込んでも良い。

番号 _____ 名前 _____　2008 年 7 月 18 日

a, b を無意味な記号とし、X を a, b からなる有限列全体の集合とする。

$$\begin{aligned} D = &\{(w_1w_2, w_1aaw_2) \mid w_1 \in X,\ w_2 \in X\} \\ &\cup \{(w_1w_2, w_1bbw_2) \mid w_1 \in X,\ w_2 \in X\} \\ &\cup \{(w_1w_2, w_1ababaw_2) \mid w_1 \in X,\ w_2 \in X\} \end{aligned}$$

とおく。$x = abab \in X$, $y = ba \in X$ に対し、次を満たす $x_0, x_1, \ldots, x_n \in X$ を見つけなさい。

$$\begin{aligned} &x = x_0,\ y = x_n, \\ &\forall i \in \{1, \ldots, n\},\ (x_{i-1}, x_i) \in D \text{ or } (x_i, x_{i-1}) \in D. \end{aligned}$$

また、$x = bab$, $y = aba$ についても上の条件を満たす $x_0, x_1, \ldots, x_n \in X$ を見つけなさい。

解答

$$\begin{aligned} x_0 &= abab = x, \\ x_1 &= b^2(abab) = b(babab), && (x_0, x_1) \in D \\ x_2 &= ba^2(babab) = (ba)(ababab), && (x_1, x_2) \in D \\ x_3 &= ba = y, && (x_3, x_2) \in D. \end{aligned}$$

$$\begin{aligned} x_0 &= bab = x, \\ x_1 &= a^2(bab) = a(abab), && (x_0, x_1) \in D \\ x_2 &= ab^2(abab) = (ab)(babab), && (x_1, x_2) \in D \\ x_3 &= (ab)a^2(babab) = (aba)(ababab), && (x_2, x_3) \in D \\ x_4 &= aba = y, && (x_4, x_3) \in D. \end{aligned}$$

期末試験　2008 年 7 月 25 日

1. A, B を集合とし、f, g を A から B への単射とする。写像 $h : A \times A \to B \times B$ を $h(a_1, a_2) = (f(a_1), g(a_2))$ $((a_1, a_2) \in A \times A)$ によって定義するとき、h は単射であることを示せ。

2. (1) $x^3 + x + 1 \in \mathbf{Z}/2\mathbf{Z}[x]$ は既約であることを示せ。

(2) 体 $K = (\mathbf{Z}/2\mathbf{Z}[x])/(x^3 + x + 1)$ において、x の属する同値類もまた x と表すことにするとき、$K^\times$ における x の位数を求めよ。

3. a, b を無意味な記号とし、X を a, b からなる有限列全体の集合とする。長さ 0 の列を 1 と書き、これも X の元とみなす。

$$\begin{aligned} D = &\{(w_1w_2, w_1a^4w_2) \mid w_1 \in X,\ w_2 \in X\} \\ &\cup \{(w_1w_2, w_1b^4w_2) \mid w_1 \in X,\ w_2 \in X\} \\ &\cup \{(w_1w_2, w_1a^2b^2w_2) \mid w_1 \in X,\ w_2 \in X\} \\ &\cup \{(w_1w_2, w_1abab^3w_2) \mid w_1 \in X,\ w_2 \in X\} \end{aligned}$$

とおく。D の推移閉包を $\hat{D}$ とし、$\hat{D}$ によって定義された同値関係を $\sim$ で表す。

(1) $x \in X$, $y \in X$, $z \in X$, $x \sim y \implies xz \sim yz$, $zx \sim zy$ を示せ。

(2) $b^2a^2 \sim 1$ を示せ。

(3) $ab^3 \sim ba$ を示せ。

(4) 商集合 $X/\hat{D}$ の元をできるだけ多く、相異なるように列挙せよ。

- 写像 $f : A \to B$ が単射であるとは、

$$\forall a \in A,\ \forall a' \in A,\ f(a) = f(a') \implies a = a'$$

が成り立つときを言う。

- 定数でない多項式 $f(x)$ が既約とは、定数でない 2 つの多項式の積に因数分解できないときを言う。

- A を環とし、$f(x) \in A[x]$ を定数でない多項式とするとき、$A[x]/(f(x))$ は $A[x]$ を同値関係

$$g_1(x) \sim g_2(x) \iff g_1(x) - g_2(x) \text{ は } f(x) \text{ で割り切れる}$$

による商集合に和 $[g_1(x)]+[g_2(x)] = [g_1(x)+g_2(x)]$, 積 $[g_1(x)][g_2(x)] = [g_1(x)g_2(x)]$ を定義して環の構造を定義したものである。

- 体 K に対し、$y \in K^\times$ の位数とは

$$\min\{n \mid n \in \mathbf{N},\ y^n = 1\}$$

である。

- X を集合、$D \subset X \times X$ とするとき、$\hat{D} \subset X \times X$ を次で定義する。

$$\begin{aligned}\hat{D} = &\{(x,x) \mid x \in X\} \\ &\cup \{(x,y) \mid x \in X,\ y \in X, \\ &\quad \exists x_0, x_1, \ldots, x_n \in X,\ x_0 = x,\ x_n = y, \\ &\quad\quad \forall i \in \{1, \ldots, n\},\ (x_{i-1}, x_i) \in D \text{ or } (x_i, x_{i-1}) \in D\}.\end{aligned}$$

このとき、$\hat{D}$ は同値関係になり、$\hat{D}$ を D の推移閉包と言う。

解答例

1. $(a,b),(c,d) \in A \times A$ とする。

$$\begin{aligned} h(a,b) = h(c,d) &\Longrightarrow \big((f(a),g(b)\big) = \big(f(c),g(d)\big) && (h \text{ の定義}) \\ &\Longrightarrow (f(a)=f(c)) \wedge (g(b)=g(d)) && (\text{直積集合における等号の定義}) \\ &\Longrightarrow (a=c) \wedge (b=d) && (f,g \text{ はともに単射}) \\ &\Longrightarrow (a,b)=(c,d) && (\text{直積集合における等号の定義}) \end{aligned}$$

より、 h も単射である。

2. (1) $f(x) = x^3 + x + 1 \in \mathbf{Z}/2\mathbf{Z}[x]$ は、既約でなければ 1 次式を因子にもつが、

$$f(0) = 1,\ f(1) = 1$$

だから 1 次式を因子にもたないので、対偶により $f(x)$ は既約である。

(2) $|K| = 2^{\deg(f)} = 8$ より、x の位数は $8-1=7$ の約数でなければならない。x の位数は明らかに 1 ではないので、従って 7 である。

以下のように直接計算しても良い。

$$\begin{aligned} x \to x^2 \to x^3 &= x+1 \\ &\to x^4 = x(x+1) = x^2 + x \\ &\to x^5 = x(x^2+x) = x^3 + x^2 = x^2 + x + 1 \\ &\to x^6 = x(x^2+x+1) = x^3 + x^2 + x = x^2 + 1 \\ &\to x^7 = x(x^2+1) = x^3 + x = 1 \end{aligned}$$

3. (1) 示したいことのひとつは

$$\forall x,y,z \in X,\ x \sim y \Longrightarrow xz \sim yz \tag{3.11}$$

であるが、これを示すためには

$$\forall x,y,z \in X,\ (x,y) \in D \Longrightarrow (xz,yz) \in D \tag{3.12}$$

を示せば十分である。なぜなら、$x=y$ のときは $xz=yz$ より $(xz,yz) \in \hat{D}$ で (3.11) が成り立ち、$x \neq y$ のときは、『$\hat{D}$ によって定義された同値関係』の定義から

$$\begin{aligned} &\exists n \in \mathbf{N},\ \exists x_0,x_1,\ldots,x_n \in X, \\ &x_0 = x,\ x_n = y,\ \forall i \in \{1,\ldots,n\},\ (x_{i-1},x_i) \in D \text{ or } (x_i,x_{i-1}) \in D \end{aligned} \tag{3.13}$$

である。X の元の列 $x_0z, x_1z, \ldots, x_nz$ を作れば、列 x_i の仮定により

$$(x_{i-1},x_i) \in D \text{ or } (x_i,x_{i-1}) \in D$$

であるから、(3.12) が正しければ

$$(x_{i-1}z, x_iz) \in D \text{ or } (x_iz, x_{i-1}z) \in D$$

となり、$xz = x_0z$ と $yz = x_nz$ について $xz \sim yz$ が成り立つから、である。

(3.12) について、たとえば $(w_1w_2, w_1a^4w_2)$ という D の元をとってくると、$w_3 = w_2z$ によって D の元 w_3 を定義すれば $(w_1w_2z, w_1a^4w_2z) = (w_1w_3, w_1a^4w_3)$ となるのでこれも D の元である。その他の場合も同様に (3.12) が示せる。したがって (3.11) が示せた。もう一方の主張 $zx \sim zy$ は、$w_3 = zw_1$ とすることで同様に示せる。

(2)

$$b^2a^2 \sim a^2b^2(b^2a^2) = a^2b^4a^2 \sim a^2a^2 = a^4 \sim 1.$$

(3)

$$\begin{aligned}
ab^3 &\sim (a^2b^2)ab^3 && (1 \sim a^2b^2 \text{ より}) \\
&= (a^2b)(bab^3) \\
&\sim a^2b(a^4)bab^3 && (1 \sim a^4 \text{ より}) \\
&= a^2ba^3(abab^3) \\
&\sim a^2ba^3 && (abab^3 \sim 1 \text{ より}) \\
&\sim a^2b(b^4)a^3 && (1 \sim b^4 \text{ より}) \\
&= (a^2b^2)b^3a^3 \\
&\sim b^3a^3 && (a^2b^2 \sim 1 \text{ より}) \\
&= b(b^2a^2)a \\
&\sim ba && ((2) \text{ より } b^2a^2 \sim 1 \text{ であるから}).
\end{aligned}$$

(4) 長さ 4 以下の語を同値類に分けると表のようになる。

同値類	含まれる長さ 4 以下の語
$[1]$	$1, a^4, b^4, a^2b^2, ab^2a, ba^2b, b^2a^2$
$[a]$	a, bab
$[b]$	b, aba
$[a^2]$	$a^2, b^2, abab, baba$
$[ab]$	$ab, a^2ba, ba^3, bab^2, b^3a$
$[ba]$	$ba, a^3b, aba^2, ab^3, b^2ab$
$[a^3]$	a^3, ab^2, b^2a
$[a^2b]$	a^2b, ba^2, b^3

長さ 4 以下の任意の語は、長さ 3 以下のいずれかの語と同値になるので、帰納法により、長さ 5 以上の語でも表のいずれかの同値類に含まれることがわかる。

注意. これは、商集合 $X/\hat{D}$ の元をできるだけ多く、相異なるように列挙させる問題であるので、上の 8 個より少なければ減点となり、また相異ならない同値類を列挙した場合も減点となる。

この講義の範囲外であるが、表の 8 個の同値類が本当に相異なるものであることは、以下のようにしてわかる。

$$A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \quad B = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}$$

とおく。$f : X \to GL(2, \mathbf{C})$ を $f(a) = A$, $f(b) = B$ を満たす写像とする（このような写像はただ一つに定まる）。行列 A, B は

$$A^4 = B^4 = ABAB^3 = I$$

を満たすことが容易に確かめられるので、

$$\bar{f} : X/\hat{D} \to GL(2, \mathbf{C}), \quad \bar{f}[w] = f(w)$$

によって well-defined な写像 $\bar{f}$ が定義できる。このとき、

$$I, A, B, A^2, AB, BA, A^3, A^2B$$

は相異なる行列であることが容易に確かめられる。

$$I = \bar{f}([1]),\ A = \bar{f}([a]),\ B = \bar{f}([b]),\ A^2 = \bar{f}([a^2]),$$
$$AB = \bar{f}([ab]),\ BA = \bar{f}([ba]),\ A^3 = \bar{f}([a^3]),\ A^2B = \bar{f}([a^2b])$$

であるから、表の 8 個の同値類

$$[1], [a], [b], [a^2], [ab], [ba], [a^3], [a^2b]$$

は相異ならなければならない。