

数学の考え方

2007年 秋学期 第8回目の講義
(04月19日 11:43版)

渇野 昌 (Sakaé Fuchino)

これまでの講義の流れ + 前回の講義の復習

数学の特徴としてあげられるキーワードを中心に考察する:

— 記号と式

— 厳密な論証 — 証明

— 証明からのアルゴリズムの抽出

先週からのテーマ: 抽象化と公理的アプローチ

抽象化 (abstraction)

本質的と思えるものを最小限残して、それ以外の要素をすべて消去する

短所:

— “抽象的” で一見分りづらい

長所:

— 本質が何かが、よりよく見える

— 本質的でないことがらにまぎらわされないため効率的に考えられる

— 抽象化することで、全く別だと思っていたものが実は同じ機構を背後に持っていることが分ることがある

数学の考え方

抽象化と公理的アプローチ (その2)

先週の復習

澁野 昌 (Sakaé Fuchino)

抽象化の例： 実数上の演算法則から群の概念を抽出する

実数の足し算の基本性質として、つぎの3つの性質に着目する:

(a1) すべての実数 x, y, z に対し $(x + y) + z = x + (y + z)$ が成り立つ。
(結合法則)

(a2) ある実数 E があって、どんな実数 x に対しても $x + E = x$ が成り立つ。
(単位元の存在) “単位元”のドイツ語: Einzelement

(a3) 上の (a2) でのような E をとるとき、どんな実数 x に対しても $x + y = E$ となるような実数 y が存在する。
(逆元の存在)

($E = 0$ $y = -x$ と見る)

(a4) すべての実数 x, y に対し、 $x + y = y + x$ である。(可換性)

数学の考え方

抽象化と公理的アプローチ (その2)

先週の復習

澁野 昌 (Sakaé Fuchino)

(a1) (結合法則) と (a4) (可換性 (かかんせい)) は、数の計算で頻繁に応用されている。たとえば:

$$3 + 2 + 4 + 5 + 6 + 7 + 5 + 3$$

という計算をするときに、 $\overbrace{(3 + 2 + 5)}^{10} + \overbrace{(4 + 6)}^{10} + \overbrace{(7 + 3)}^{10} + 5 = 35$ とならばなおしたり組合せなおしたりして暗算してよい

のは、結合法則と可換性を何度か組み合わせて使うことで保証されている、と考えることができる。

数学の考え方

抽象化と公理的アプローチ (その2)

先週の復習

澁野 昌 (Sakaé Fuchino)

実数の基本性質 (a1) ~ (a3) と (a4) に対応する演算の性質から、群 (ぐん group) と **アーベル群** (abelian group) という概念が抽出される。

以下で、集合 (しゅうごう) とは、数学的な対象の集まりのこと。

集合 G の上にある演算 \circ が定義されていて、次の3つの性質が成り立つとき、 G と \circ の組 (G, \circ) は **群** (ぐん, group) であるという:

(g1) すべての G の要素 x, y, z に対し $(x \circ y) \circ z = x \circ (y \circ z)$ が成り立つ。
(結合法則)

(g2) ある G の要素 E があって、どんな G の要素 x に対しても $x \circ E = E \circ x = x$ が成り立つ。
(単位元の存在)

(g3) 上の (g2) でのような E をとるとき、どんな G の要素 x に対しても $x \circ y = E$ となる G の要素 y が存在する。
(逆元の存在)

数学の考え方

抽象化と公理的アプローチ (その2)

先週の復習

澁野 昌 (Sakaé Fuchino)

(G, \circ) がさらに次の (g4) を満たすとき, (G, \circ) は アーベル群 (abelian group) であるという

(g4) すべての G の要素 x, y に対し, $x \circ y = y \circ x$ である. (可換性)

上のような E を (G, \circ) の 単位元 といい, (g3) での y を x の ((G, \circ) での) 逆元 (ぎゃくげん) という.

アーベル (Niels Henrik Abel 1802 - 1829)

数学の考え方

抽象化と公理的アプローチ (その2)

先週の復習

湊野 昌 (Sakaé Fuchino)



アーベル (Niels Henrik Abel 1802 - 1829)

<http://turnbull.mcs.st-and.ac.uk/history/Biographies/Abel.html>

集合に関する用語の補足／復習

◎ **集合** (しゅうごう) : (数学的な) 対象の集まりをひとまとめにして新しい対象と考えたもの

◎ x が集合 X で集めてきたもののなかの1つのとき x は X の **要素** である, あるいは x は X の **元** (げん) であるといい, このことを $x \in X$ であらわす. x が X の要素でないことを $x \notin X$ であらわす

◎ $\{x_1, \dots, x_n\}$ で x_1, \dots, x_n を要素として持つ集合をあらわす

例 : $\{1, 2, 64\}$ は 1 と 2 と 64 を要素として持つ集合である

◎ $\{x : x \text{ は } \dots \text{ を満たす}\}$ で, 条件 \dots を満たすすべての x からなる集合をあらわす 例 : $\mathbb{R} = \{x : x \text{ は実数}\}$, $\mathbb{N} = \{x : x \text{ は自然数}\}$

◎ 例 : $3 \in \mathbb{N}$, $\pi \notin \mathbb{N}$, $2 \in \mathbb{R}$, $\pi \in \mathbb{R}$, $(1, 2) \notin \mathbb{R}$, $2 \in \{1, 2, 64\}$, $3 \notin \{1, 2, 64\}$

群の定義 (集合の記号を使った書きなおし)

ある集合 G の上に演算 \circ が定義されていて、次の3つの性質が成り立つとき、 G と \circ の組 (G, \circ) は **群** (ぐん) であるという:

(g1) すべての $x, y, z \in G$ に対し $(x \circ y) \circ z = x \circ (y \circ z)$ が成り立つ.

(結合法則)

(g2) $E \in G$ で、どんな $x \in G$ に対しても $x \circ E = E \circ x = x$ が成り立つようなものが存在する.

(単位元の存在)

(g3) 上の (g2) でのような E をとるとき、どんな $x \in G$ に対しても $x \circ y = E$ となる $y \in G$ が存在する.

(逆元の存在)

(g2) でのような E のことを群 (G, \circ) の**単位元**という.

$x \in G$ に対して (g3) でのような y を x の**逆元**という.

定理 (G, \circ) を群とするととき (G, \circ) の単位元はただ1つしか存在しない.

証明. E と E' を (G, \circ) の単位元とするととき, 単位元の定義から,
 $E = E \circ E' = E'$ である. □

(G, \circ) を群として E を (上の定理によって一意に決まるところの)
 G の単位元とする.

(g4) すべての $x, y \in G$ に対し, $x \circ y = y \circ x$ となる (可換性)

が成り立つとき (G, \circ) は **アーベル群** である, という.

定理 (G, \circ) を群として E を (G, \circ) の単位元とする. このとき次が成り立つ:

- (1) $y \in G$ を $x \in G$ の逆元とするとき, $y \circ x = E$ が成り立つ.
- (2) $y \in G$ を $x \in G$ の逆元とするとき, x は y の逆元である.
- (3) $x \in G$ の逆元はただ1つしかない.

証明. (1): $y \circ x = (y \circ E) \circ x = (y \circ (x \circ y)) \circ x \stackrel{(g1)}{=} (y \circ x) \circ (y \circ x)$ である.
 $y \circ x$ の逆元 z をとる. z を上の等式の各辺に右から \circ で演算すると,
 $E = (y \circ x) \circ z = (y \circ x) \circ \underbrace{(y \circ x) \circ z}_{=E} = y \circ x$ となる.

(2): y が x の逆元なら (1) により $y \circ x = E$ だから x は y の逆元である.

(3): y と y' を x の逆元とすると, $y = y \circ \underbrace{(x \circ y')}_{=E} = \underbrace{(y \circ x)}_{=E} \circ y' = y'$ □

群の例

(1) $(\mathbb{R}, +)$ はアーベル群である.

$(\mathbb{R}, +)$ の単位元は 0 で, $x \in \mathbb{R}$ の逆元は $-x$ である.

(2) $\mathbb{R}^\times = \{x : x \text{ は実数で } x \neq 0\}$ とするとき, $(\mathbb{R}^\times, \times)$ はアーベル群である.

$x, y, z \in \mathbb{R}^\times$ に対し, $(x \times y) \times z = x \times (y \times z)$

すべての $x \in \mathbb{R}^\times$ に対し, $x \times 1 = 1 \times x = x$

すべての $x \in \mathbb{R}^\times$ に対し, $x \times \frac{1}{x} = 1$

すべての $x, y \in \mathbb{R}$ に対し, $x \times y = y \times x$

(3) $\mathbb{R}^+ = \{x : x \text{ は実数で } x > 0\}$ とするとき, (\mathbb{R}^+, \times) はアーベル群である.

(2) と同様.

群の歴史

群の概念を最初が最初に用いられたのは、**アーベル** (Niels Henrik Abel 1802 - 1829 ノルウエー) や **ガロア** (Evariste Galois 1811 - 1832 フランス) による (5次以上の) 方程式の解の研究においてだった.



E. ガロア

1920年代, ゲッティンゲン (Göttingen) 大学での **ネーター** (Emmy Amalie Noether 1882 - 1935 ドイツ — アメリカ) を中心とする数学者たちによって, 群を含む代数の諸概念が, この講義で述べたような形に整理された.



E. ネーター