

UEC 代数勉強会 01 回目

bokuroro

December 26, 2020

群の定義

群の定義

- ① 結合法則 $\forall a, b, c \in G$ に対し、 $(a \circ b) \circ c = a \circ (b \circ c)$
- ② 単位元の存在 $\exists e \in G$ s.t. $\forall a \in G$ に対し、 $a \circ e = e \circ a = a$
このような e を **単位元** と呼ぶ.
- ③ 逆元の存在 $\forall a \in G$ に対し、 $\exists b \in G$ s.t. $a \circ b = b \circ a = e$
このような b を a の **逆元** と呼び、 a^{-1} で表す.

二項演算が定義されていることが前提となっている.

また、交換則 $a \circ b = b \circ a$ が成り立つものを **可換群** または **Abel 群** と呼ぶ.

変換群

定義は参考書参照

写像 $f, g, h \in G : X \rightarrow X$ を考えたとき、 $x \in X$ として、

$$\begin{aligned} ((h \circ g) \circ f)(x) &= (h \circ g)(f(x)) \\ &= (h \circ g)(f(x)) \\ &= h(g(f(x))) \\ &= h((g \circ f)(x)) \\ &= (h \circ (g \circ f))(x) \end{aligned}$$

よって結合則成立.

まあこんなの考えなくてもほぼ自明ですが.

恒等写像 $\text{id}(x) = x$ が存在すること、逆元が存在することは、写像が全単射より自明ですね.

対称群

要するに n 個のものの置換の群である.

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

と書いたら、対称群 S_3 の元で $1 \rightarrow 2, 2 \rightarrow 1, 3 \rightarrow 3$ に置き換わることを表す.

巡回置換と**互換**については参考書参照. 任意の置換は互いに素 (交わらない) 巡回置換に分解でき、いくつかの互換に分解できる.

積についてはこの先出てくるので演習問題にしておきます.

定義 1.2

群の元の総数のことを群の**位数** (order) と呼ぶ.

- 位数が有限 → **有限群**
- 位数が無限 → **無限群**

また、

- 連続パラメータで依存する → **連続群**
- それ以外 → **離散群**

と呼ぶ.

問 1.1

S_3 において $p = (1, 2, 3), q = (1, 2)$ とおく時、 $px = q, yp = q$ となる元 x, y をそれぞれ求めよ.

環の定義

環の定義

集合 A に 2 つの二項演算 $(+, \cdot)$ が定義されていて、次の性質を持つ.

- ① $(A, +)$ は可換群をなす.
- ② 乗法 \cdot は結合法則 $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ を満たす.
- ③ 2 つの演算は分配法則を満たす.

$\forall a, b, c \in A$ に対し、 $a \cdot (b + c) = a \cdot b + a \cdot c$, $(a + b) \cdot c = a \cdot c + b \cdot c$

勘違いしやすいが、必ずしも乗法の単位元を持つ必要はない.

行列環

n 次正方行列の全体が行列の和と積を演算として成り立つ環、行列環 $M(n, \mathbb{R})$ がある. 加法の単位元はゼロ行列 O 、乗法の単位元は単位行列 E である.

成分を任意の環としても、再び環となる.

零因子

零元と異なる2つの元 x, y で掛けたもの $xy = 0$ となってしまうものを**零因子**と呼ぶ。例えば、二次正方行列の環では

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \quad (1)$$

となり、零因子がたくさん存在する。

零因子を持つとややこしいので、零因子を持たない環を**整域**と呼び、重宝される。

問 1.8

D を平方因子を持たない整数とする. $a + b\frac{1+\sqrt{D}}{2}, a, b \in \mathbb{Z}$ の形の複素数の全体が複素数の通常の演算で環となるのは D がどのような場合か?

体の定義

体は環の特別なもので、単位可換環 $(K, +, \cdot)$ において、零元を除いたもの $K^\times := K \setminus \{0\}$ が乗法に関して群をなすものを言う。

性質を改めて書けば

体の定義

- ① $(K, +)$ は可換群をなす.
- ② (K^\times, \cdot) は可換群をなす.
- ③ $+$ と \cdot は分配法則で関連する.

$$\forall a, b, c \in K \text{ に対し、 } a(b + c) = ab + ac, (a + b)c = ac + bc$$

有限体

無限体 有限体

体に含まれる元の個数が有限個であるものを**有限群**、多くの元を含む体を**無限体**と言う。

無限体の例としては、有理数体 \mathbb{Q} 、実数体 \mathbb{R} 、複素数体 \mathbb{C} 、実係数の有理関数体 $\mathbb{R}(x)$ 、複素係数の有理関数体 $\mathbb{C}(x)$ が存在する。

また、有限体の例としては次である。

有限体 \mathbb{F}_p

p は素数である。

集合としては、 \mathbb{Z}_p と同じもので、 p で割ったあまりを並べてある。

p が素数の時、0 以外の元に乗法の逆元が存在することを次ページで証明しておく。

ここでは、下を用いて証明を行います。直感的には鳩で置き換えた方がわかりやすいですが、適用するときは、こちらの表現を使った方が良いと思います。

鳩の巣原理

元の個数が等しい二つの有限集合の間に写像があるとき

- ① 全射なら単射
- ② 単射なら全射

$1 \leq \forall x \leq p-1$ に対して、乗法の逆元が存在することを証明する。

まず、 p が素数より、 x による乗法は $\mathbb{F}_p^\times = \{1, 2, \dots, p-1\}$ から、一対一写像を引き起こす。(つまり単射)

なぜなら、 $a, b \in \{1, 2, \dots, p-1\}$ について $xa = xb$ が言えるとき、 $p|x(a-b)$ で、 $|a-b| < p$ より、 $a=b$ が言えるからである。

よって、鳩の巣原理より、この写像は全射であり、 $xy=1$ となるような y が存在する。

有限体 \mathbb{F}_p と、有理数体 \mathbb{Q} は、これ以上小さな部分体が取れない素体 (1.6 で詳しくやる) というものです.

全ての素体は \mathbb{Q} か \mathbb{F}_p と同型 (全く同じ代数構造を持つこと) であることが言えます.

参考: <http://hooktail.sub.jp/algebra/PrimeFiled/>

公理を用いた推論

全部書いてると冗長になってしまうので、どれも重要ですが、2 つだけ書いておきます。

命題 1.2 環の公理の系

$\forall a \in A$ に対し、 $a \cdot 0 = 0 \cdot a = 0$ 、よって 0 は乗法の逆元を持ち得ない。また、零因子も乗法の逆元を持ち得ない。

分配法則より、 $a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$ であり、両辺に $a \cdot 0$ の加法の逆元 $-a \cdot 0$ を加えると、結合法則より

$$\begin{aligned} 0 &= a \cdot 0 + (-a \cdot 0) = (a \cdot 0 + a \cdot 0) + (-a \cdot 0) = a \cdot 0 + (a \cdot 0 + (-a \cdot 0)) \\ &= a \cdot 0 + 0 = a \cdot 0 \end{aligned}$$

また、 0 に逆元 x があるとすれば、 $0 = x \cdot 0 = 1$ で矛盾。 $x, y \neq 0$ で、 $x \cdot y = 0$ とし、 x に乗法の逆元 x^{-1} があるとする

$$0 = x^{-1} \cdot 0 = x^{-1} \cdot (x \cdot y) = (x^{-1} \cdot x) \cdot y = 1 \cdot y = y$$

となって矛盾。

命題 1.5

体には零因子は存在しない. また、これより体の元を係数とする一変数代数方程式 $f(x) := a_n x^n + a_1 x^{n-1} + \dots + a_0 = 0 (a_0 \neq 0)$ は次数 n より多くの根を持たない.

$xy = 0$ で $x \neq 0$ なら、体の公理により、 x^{-1} が存在し、これを両辺にかけると

$$0 = x^{-1}(xy) = (x^{-1}x)y = 1 \cdot y = y$$

となる. また、 $f(\alpha) = 0$ とすると、因数定理

$$f(x) = (x - \alpha)q(x)$$

という式が得られ、 $q(x)$ は $n - 1$ 次だから、数学的帰納法により、主張が証明できる.

では、いくつか演習問題を解いてみましょう.

問 1.12

群 G において、任意の元が $x^2 = e$ を満たしていれば G は可換群であることを示せ.

問 1.13

群 G において、二つの元 x, y が可換であるためには $(xy)^2 = x^2y^2$ が成立することが必要かつ十分であること証明せよ.