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.

群の例

変換群

定義は参考書参照
写像 $f, g, h \in G : X \to X$ 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.
まぁこんなの考えなくてもほぼ自明ですが.
恒等写像 $\mathrm{id}(x) = x$ 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.

群の例

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 $1 \to 2, 2 \to 1, 3 \to 3$ に置き換わることを表す.
巡回置換、$(1, 2, 3)$ 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.

いろいろ定義

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 $\rightarrow$ **有限群**
- 位数が無限 $\rightarrow$ **無限群**

また、

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

と呼ぶ.

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

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \tag{1}$$

となり、零因子がたくさん存在する.

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 $K^\times := K \backslash \{0\}$ 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.
   $\forall a, b, c \in K$ 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 F_p

p は素数である.
集合としては、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.