情報数学Ⅰ

第 14 回「巡回群、多項式環」

§巡回群

① 乗法群

群Gの記法として、$(G;\cdot)$ もしくは $(G;\times)$を用いる群

$$a^n = \overbrace{a\cdot a\cdot\cdots\cdot a}^{n個} \quad (n\in\mathbb{N})$$

$$a^0 = e \ (\text{乗法単位元})$$

$$a^{-n} = (a^n)^{-1} \quad (n\in\mathbb{N})$$

[定理]$\forall m,n\in\mathbb{Z}$に対し、次の性質が成立する。

$$(a^n)^{-1} = (a^{-1})^n$$

$$a^m\cdot a^n = a^{m+n}$$

$$(a^m)^n = a^{mn}$$

② 加法群

群Gの記法として、$(G;+)$を用いる群

$$na = \overbrace{a+a+\cdots+a}^{n個} \quad (n\in\mathbb{N})$$

$$0a = o \ (\text{加法単位元})$$

$$(-n)a = -(na) \quad (n\in\mathbb{N})$$

[定理] $\forall m,n\in\mathbb{Z}$に対し、次の性質が成立する。

$$-(na) = n(-a)$$

$$ma+na = (m+n)a$$

$$m(na) = (mn)a$$

③ 巡回群

n個の元をもつ有限乗法群$(G;\cdot)$がGのある元aを使って

$$G = \{e, a, a^2, \cdots, a^{n-1}\}$$

と表せるとき、Gを巡回群といい、aをその生成元という。

n個の元をもつ有限加法群$(G;+)$がGのある元aを使って、

$$G = \{o, a, 2a, \cdots, (n-1)a\}$$

と表せるとき、Gを巡回群といい、aをその生成元という。

§多項式環

$(F;\ +,\cdot\ )$を体とし、Fの要素を係数とする全ての多項式

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \quad (\text{ただし、} a_i \in F, i = 0, 1, \cdots n)$$

の集合Pを考える。Pの要素の和+、積$\cdot$を、多項式としての和、積とする。ただし、係数の計算は体F上で行うこととする。$(P;\ +,\ \cdot\ )$は単位的可換環となり、このような環を多項式環という。