有限 Abel 群と Jordan 標準形

黒木玄

2015 年 12 月 17 日 (木)*

1 有限 Abel 群

1.1 準備

読者は巡回群や Lagrange の定理や群の準同型定理などの群論に関する基本的な事柄については知っていると仮定する.

正の整数 n に対して, $n = p_1^{e_1} \cdots p_N^{e_N}$ かつ, p_i たちが互いに異なる素数であり, e_i たちが 0 以上の整数であるとき, $n = p_1^{e_1} \cdots p_N^{e_N}$ を n の素因数分解と呼ぶことにする.

以下の 2 つの補題を証明抜きに利用する.

補題 1.1 (中国式剰余定理)**.** r, s が互いに素な正の整数であるならば, 群の同型写像

$$\mathbb{Z}/rs\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/r\mathbb{Z} \times \mathbb{Z}/s\mathbb{Z}, \quad a \bmod rs \mapsto (a \bmod r, a \bmod s)$$

が得られる. ゆえに正の整数 n の素因数分解が $n = p_1^{e_1} \cdots p_N^{e_N}$ であるとき, 群の同型写像

$$\mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/p_1^{e_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_N^{e_N}\mathbb{Z}, \quad a \bmod n \mapsto (a \bmod p_1^{e_1}, \ldots, a \bmod p_N^{e_N})$$

が得られる. □

群 G とその部分群 $H_1, \ldots, H_N$ について, 写像

$$H_1 \times \cdots \times H_N \to G, \quad (h_1, \ldots, h_N) \mapsto h_1 \cdots h_N$$

が群の同型写像になるとき, 群 G は部分群 $H_1, \cdots, H_N$ の直積に分解するという.

補題 1.2 (直積)**.** 群 G とその部分群 H, K について以下の二条件は互いに同値である:

- 群 G は部分群 H, K の直積に分解する.
- H, K は G の正規部分群であり, $H \cap K = \{1\}$ かつ $HK = G$. □

以上の補題と注意は以下において断り無しに自由に用いられる.

次の補題は後で群 G の剰余群における直積分解の存在から元の群 G 自身の直積分解の存在を導くために使われる.

*2026 年 2 月 9 日: 補題 1.3 の証明中の「$\pi(G')\overline{H} = G$」を「$\pi(G')\overline{H} = \overline{G}$」に訂正した. 最後に良書紹介を追加した.

補題 1.3. G は群であるとし, G' はその正規部分群であるとする. N は G の正規部分群であるとし, $\overline{G} = G/N$ とおき, 自然な射影を $\pi : G \to \overline{G}$, $x \mapsto xN$ と書く. $G' \cap N = \{1\}$ でかつ, $\overline{G}$ が $\pi(G')$ とある部分群 $\overline{H}$ の直積に分解するならば, G は G' と $\pi^{-1}(\overline{H})$ の直積に分解する.

証明. $\overline{H}$ は $\overline{G}$ の正規部分群であり, 一般に正規部分群の準同型写像による逆像も正規部分群になるので, $H = \pi^{-1}(\overline{H})$ とおくと H は G の正規部分群である.

あとは $G' \cap H = \{1\}$ かつ $G'H = G$ となることを示せば十分である.

$G' \cap H = \{1\}$ を示そう. $x \in G' \cap H$ を任意に取る. このとき $\pi(x) \in \pi(G') \cap \overline{H} = \{1\}$ すなわち $\pi(x) = 1$ なので $x \in N$ となる. ゆえに $x \in G' \cap N = \{1\}$ すなわち $x = 1$ となる. これで $G' \cap H = \{1\}$ が示された.

$G'H = G$ を示そう. $x \in G$ を任意に取る. $\pi(G')\pi(H) = \pi(G')\overline{H} = \overline{G}$ より $\pi(x) \in \overline{G}$ は $\pi(x) = \pi(x')\pi(h) = \pi(x'h)$, $x' \in G'$, $h \in H$ と表される. このとき, ある $n \in N$ が存在して $x = x'hn$ となる. $N = \pi^{-1}(1) \subset \pi^{-1}(\overline{H}) = H$ なので $n \in H$ ゆえに $hn \in H$ となる. これで $G'H = G$ が示された. □

注意 1.4. G は Abel 群であるとし, α, β はその有限位数の元であるとし, それぞれの位数 r, s は互いに素であるならば, $\alpha\beta$ の位数は rs になる. その理由は以下の通り.

$x \in \langle\alpha\rangle \cap \langle\beta\rangle$ の位数は α の位数 r と β の位数 s の公約数になるので 1 になる. つまり $x = 1$ となる. これで $\langle\alpha\rangle \cap \langle\beta\rangle = \{1\}$ となることがわかった.

ゆえに G の部分群 $\langle\alpha, \beta\rangle = \langle\alpha\rangle\langle\beta\rangle$ はその部分群 $\langle\alpha\rangle$, $\langle\beta\rangle$ の直積に分解する.

中国式剰余定理は $\mathbb{Z}/r\mathbb{Z} \times \mathbb{Z}/s\mathbb{Z}$ が $(1 \bmod r, 1 \bmod s)$ から生成される位数 rs の巡回群になることを意味している. そのことから $\langle\alpha, \beta\rangle$ が $\alpha\beta$ から生成されることと $\alpha\beta$ の位数が rs になることがただちに導かれる. □

1.2 有限 Abel 群の構造

補題 1.5. Abel 群 G の有限位数を持つ元 a, b の位数はそれぞれ r, s であるとし, それらの最小公倍数を m と書く. このとき位数 m の G の元が存在する.

証明. r, s の素因数分解を

$$r = p_1^{e_1} \cdots p_N^{e_N}, \quad s = p_1^{f_1} \cdots p_N^{f_N}$$

と書く. 必要があれば番号を付け変えて

$$e_1 \geqq f_1, \ \ldots, \ e_n \geqq f_n, \ e_{n+1} \leqq f_{n+1}, \ \ldots, \ e_N \leqq f_N$$

が成立していると仮定してよい. 正の整数 r', r'', s', s'' を

$$r' = p_1^{e_1} \cdots p_n^{e_n}, \quad r'' = p_{n+1}^{e_{n+1}} \cdots p_N^{e_N}, \quad s' = p_1^{f_1} \cdots p_n^{f_n}, \quad s'' = p_{n+1}^{f_{n+1}} \cdots p_N^{f_N}$$

と定める. このとき $r = r'r''$, $s = s's''$, $r's'' = m$ が成立し, r' と s'' は互いに素になる.

$\alpha = a^{r''}$, $\beta = b^{s'}$ とおく. このとき α, β それぞれの位数は $r' = r/r''$, $s'' = s/s'$ になる. ゆえに注意 1.4 より $\alpha\beta$ の位数は $r's'' = m$ になる. □

この補題から次の補題がただちに導かれる.

補題 1.6. G は有限 Abel 群であるとし, G の元の位数の最大値を r と書く. このとき G の任意の元の位数は r の約数になる.

証明. G の最大位数 r の元 a を取る. G の元 b を任意に取ってその位数を s と書き, r, s の最小公倍数を m と書く. 補題 1.5 より G の中に位数 m の元が存在する. しかし r の最大性から $m \leqq r$ でなければいけない. ゆえに s は r の約数でなければいけない. (もしも s が r の約数でなければ $m > r$ となってしまう.) □

次の補題を証明できれば, 補題 1.3 を用いた群の位数に関する帰納法で有限 Abel 群が巡回群の直積になることを容易に証明できる.

補題 1.7. G は有限 Abel 群であるとし, a はその位数最大の元であるとし, $G \neq \langle a \rangle$ であると仮定する. このとき G の部分群 $N \neq \{1\}$ で $\langle a \rangle \cap N = \{1\}$ をみたすものが存在する.

証明. $\overline{G} = G/\langle a \rangle$ とおき, 自然な射影を $\pi : G \to \overline{G}$, $x \mapsto \pi(x) = x\langle a \rangle$ と書く. 仮定 $G \neq \langle a \rangle$ より, ある $b \in G$ で $b \notin \langle a \rangle$ となるものが存在する. a, b の位数をそれぞれ r, s と書く. 補題 1.6 より s は r の約数である.

$b \notin \langle a \rangle$ なので $\pi(b) \neq 1$ である. $\pi(b)$ の位数 t は s の約数になり, $\pi(b) \neq 1$ より $t > 1$ となる. $\pi(b^t) = 1$ なので $b^t \in \langle a \rangle$ となる. ゆえにある整数 k で $b^t = a^k$ を満たすものが存在する. このとき

$$1 = b^s = b^{t \cdot s/t} = a^{k \cdot s/t}$$

なのである整数 l が存在して $ks/t = lr$ となる. このとき $k/t = l \cdot r/s$ は整数になる. ゆえに G の元 c を次のように定めることができる:

$$c = a^{-k/t} b.$$

$N = \langle c \rangle$ が構成したい G の部分群であることを示そう. まず, $\pi(c) = \pi(b)$ の位数は $t > 1$ なので c の位数も 1 より大きいので $N = \langle c \rangle \neq \{1\}$ である. 次に, $x \in \langle a \rangle \cap N = \langle a \rangle \cap \langle c \rangle$ とすると, $x = a^i = c^j$, $i, j \in \mathbb{Z}$ と書ける. $1 = \pi(a^i) = \pi(x) = \pi(c^j) = \pi(c)^j$ より, j は t の倍数になる. しかし $c^t = a^{-k} b^t = 1$ なので $x = c^j = c^{t \cdot j/t} = 1$ となる. これで $\langle a \rangle \cap N = \langle a \rangle \cap \langle c \rangle = \{1\}$ となることもわかった. □

補題 1.8. 有限 Abel 群 G の最大位数の元を a と書くと, G は $\langle a \rangle$ とある部分群 H の直積に分解する.

証明. G の位数に関する帰納法で証明する.

$|G| = 1$ のときに定理の結論は自明に成立している.

$|G| > 1$ のとき. 位数が $|G|$ より小さな Abel 群について定理の結論が成立していると仮定する. $G = \langle a \rangle$ の場合には定理の結論は自明に成立しているので, $G \neq \langle a \rangle$ と仮定してよい補題 1.7 より, G の部分群 $N \neq \{1\}$ で $\langle a \rangle \cap N = \{1\}$ をみたすものが存在する. $\overline{G} = G/N$ とおき, 自然な射影を $\pi : G \to \overline{G}$, $x \mapsto xN$ と書く. $N \neq \{1\}$ より $\overline{G}$ の位数は G の位数より小さいので, 帰納法の仮定より, $\overline{G}$ は $\pi(\langle a \rangle)$ とある部分群 $\overline{H}$ の直積に分解する. ゆえに, 補題 1.3 より, G は $\langle a \rangle$ と $H = \pi^{-1}(\overline{H})$ の直積に分解する. □

定理 1.9. 有限 Abel 群 G に対して, 単位元以外の $a_1, a_2, \ldots, a_N \in G$ で以下の条件を満たすものが存在する ($G = \{1\}$ の場合には $N = 0$ だとみなす):

- G は巡回部分群 $\langle a_1 \rangle, \ldots, \langle a_N \rangle$ の直積に分解する.
- a_i の位数を r_i と書くと, $r_N | \cdots | r_2 | r_1$.

ここで整数 r, s に対する $s | r$ は s が r を割り切ることを意味する.

証明. G の位数 $|G|$ に関する帰納法で証明する.

$|G| = 1$ のとき, 定理の結論は自明に成立している.

$|G| > 1$ のとき. 位数が $|G|$ より小さな Abel 群について定理の結論が成立していると仮定する. G の位数最大の元を a_1 とし, その位数を r_1 と書く. 補題 1.8 より, G は $\langle a_1 \rangle$ とある部分群 H の直積に分解する. H の位数は G の位数より小さいので, 帰納法の仮定より, 単位元以外のある $a_2, \ldots, a_N \in H$ が存在して, H は $\langle a_2 \rangle, \ldots, \langle a_N \rangle$ の直積に分解し, a_i の位数を r_i と書くと $r_N | \cdots | r_3 | r_2$ が成立する. ゆえに G は $\langle a_1 \rangle, \langle a_2 \rangle, \ldots, \langle a_N \rangle$ の直積に分解する. 補題 1.6 より a_i の位数 r_i たちはすべて a_1 の位数 r_1 の約数になる. これで示すべきことがすべて示された. □

系 1.10. 有限 Abel 群は素数べき位数の巡回部分群たちの直積に分解する.

証明. 定理 1.9 より, 有限 Abel 群は巡回部分群たちの直積に分解する. 中国式剰余定理より, 巡回群は素数べき位数の巡回部分群の直積に分解する. ゆえに有限 Abel 群は素数べき位数の巡回群たちの直積に分解する. □

Abel 群 A と整数 k に対して, $A^k = \{ a^k \mid a \in A \}$ と定める. そのとき A^k は A の部分群になる. Abel 群 A が部分群 B, C の直積に分解しているとき, A^k は B^k, C^k の直積に分解する. 群 G, H とそれぞれの正規部分群 M, N に対して, $M \times N$ は $G \times H$ の正規部分群になり, 自然な群の同型 $(G \times H)/(M \times N) \cong (G/M) \times (H/N)$ が成立している.

補題 1.11. 位数 r の有限巡回群 C と正の整数 k に対して, r と k の最大公約数を g と書くと, $C^k = \langle a^k \rangle$ は位数 r/g の巡回部分群になる. ゆえに剰余群 C/C^k は位数 g の巡回群になる.

証明. C の生成元の 1 つを a と書く. ある整数 l, m で $lr + mk = g$ を満たすものが存在する. ゆえに $a^g = a^{lr+mk} = a^{mk} \in C^k$. 任意の整数 i に対して $(a^i)^k = (a^g)^{ki/g} \in \langle a^g \rangle$. ゆえに $C^k = \langle a^g \rangle$. したがって C^k は a^g から生成される位数 r/g の巡回部分群になり, C/C^k は a の像から生成される位数 g の巡回群になる. □

定理 1.12. 定理 1.9 の $r_1, r_2, \ldots, r_N$ は G から一意的に決まる. ($(r_1, r_2, \ldots, r_N)$ を G の **単因子 (elementary divisors)** と呼ぶ.)

証明. この定理を証明するためには正の整数 k に対する $|G/G^k|$ たちから r_i たちが一意に決まることを示せばよい. (以下のように実際には素数べき $k = p^e$ に対する $|G/G^k|$ たちから r_i たちが一意に決まることを示せる.)

G の元の位数の最大値を r と書くと, 補題 1.6 より, G の元の位数はすべて r の約数になる. 定理 1.9 の状況を仮定し, $r_{N+1} = 1$ とおく. そのとき $r_1 = r$ となる[1].

各 r_i の素因数分解を $r_i = p_1^{e_1(i)} \cdots p_N^{e_N(i)}$ と書いておく. $r_N | \cdots | r_2 | r_1$ より, 各素数 p_t ごとに $e_t(N) \leqq \cdots \leqq e_t(2) \leqq e_t(1)$ が成立している. $e_t(i)$ たちが $|G/G^k|$ たちから一意に決まることを示せばよい.

補題 1.11 より, 位数 r_i の巡回群 C_i に対して, $\left| C_i / C_i^{p_t^e} \right| = p_t^{\min\{e, e_t(i)\}}$ となる. ゆえに

$$e_t(i+1) \leqq e \leqq e_t(i) \text{ のとき} \quad \left| G/G^{p_t^e} \right| = p_t^{e_t(N) + \cdots + e_t(i+2) + e_t(i+1) + ie}.$$

これより $e_t(1), e_t(2), \ldots$ が数列 $\left| G/G^{p_t^e} \right|$ $(e = 0, 1, 2, \ldots)$ から一意的に決まってしまうことがわかる[2]. □

[1] 理由を考えよ.

[2] それはなぜかを自分で考えてみよ.

注意 1.13. 上の証明中の記号のもとで系 1.10 の結果は

$$G \cong \prod_{t,i} \left(\mathbb{Z}/p_t^{e_t(i)}\mathbb{Z} \right)$$

と書ける. この素数べき位数の巡回群への直積分解も G から本質的に一意的に決まる. このようにして有限 Abel 群の同型類と素数べきの組は一対一に対応している. □

例 1.14. p は素数であり, n は 0 以上の整数であるとする. 位数が素数べき p^n の有限 Abel 群の同型類全体と n の分割全体は一対一に対応している. n の分割とは整数の列 $e_1 \geqq e_2 \geqq \cdots \geqq e_N \geqq 1$ で $n_1 + n_2 + \cdots + n_N = n$ をみたすもののことである. n の分割に対して $\mathbb{Z}/p^{n_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p^{n_N}\mathbb{Z}$ の同型類を対応させることによって, n の分割と位数 p^e の有限 Abel 群の同型類の一対一対応が定まる. n の分割全体の個数を $p(n)$ と書き, n の**分割数 (partition number)** と呼ぶ[3]. 例えば $p(0) = 1$, $p(1) = 1$, $p(2) = 2$, $p(3) = 3$, $p(4) = 5$, $p(5) = 7$ である. □

例 1.15. 位数 $540000 = 2^5 3^3 5^4$ の有限 Abel 群の同型類全体の個数は $p(5)p(3)p(4) = 7 \cdot 3 \cdot 5 = 105$ 個である. □

2 Jordan 標準形

2.1 有限 Abel 群の場合との類似

実は前節と全く同様にして Jordan 標準形の存在と一意性を証明できる. 有限 Abel 群と Jordan 標準形の理論は主イデアル整域 (PID) 上の有限生成加群の一般論に吸収されてしまうのだが, このノートでは一般論に頼らずに有限 Abel 群の場合の証明との類似を追及することによって Jordan 標準形の存在と一意性の証明を見付ける方法を解説する. ただし, 可換環上の加群に関する基礎的な事柄は既知であると仮定する.

以下, K は任意の代数閉体であると仮定する. (代数閉体の定義を知らない人は $K = \mathbb{C}$ と仮定してよい.)

以下のような類似を考えることになる.

- 有理整数環 $\mathbb{Z} \longleftrightarrow$ 多項式環 $K[x]$
- Abel 群の元の整数乗 $\longleftrightarrow$ $K[x]$ 加群の元の多項式倍
- 有限 Abel 群 $\longleftrightarrow$ K 上有限次元の $K[x]$ 加群
- Abel 群の位数 $\longleftrightarrow$ $K[x]$ 加群の K 上のベクトル空間としての次元
- 巡回群 $Z/n\mathbb{Z} \longleftrightarrow$ 巡回 $K[x]$ 加群 $K[x]/f(x)K[x]$
- 素数べき $p^e \longleftrightarrow \alpha \in K$ に対する $(x-\alpha)^e$
- 素数べき位数の巡回群 $\mathbb{Z}/p^e\mathbb{Z} \longleftrightarrow$ 点 α に台を持つ巡回 $K[x]$ 加群 $K[x]/(x-\alpha)^e K[x]$

[3] 分割数の母函数表示 $\sum_{n=0}^{\infty} p(n)q^n = \prod_{k=1}^{\infty}(1-q^k)^{-1}$ が成立している. $q = e^{2\pi i\tau}$ とおく. $\eta(q) = q^{1/24}\prod_{k=1}^{\infty}(1-q^k)$ は Dedekind の eta 函数と呼ばれる数論的に特別な函数である.

$K[x]$ 加群の世界における行列の対応物は $K[x]$ 加群への x 倍の作用である. 有限 Abel 群の世界には行列の類似物は存在しない. 完全な類似が不可能になっているおかげで話が面白くなっているとも考えられる.

A は K の元を成分とする $n \times n$ 行列であるとする. A は行列の積によって列ベクトルの空間 K^n に左から作用している. だから x の作用を行列 A の作用で定めることによって, $M = K^n$ を $K[x]$ 加群とみなせる:

$$f(x)v := f(A)v \quad (v \in M = K^n,\ f(x) \in K[x]).$$

$M = K^n$ は $K[x]$ 加群でかつ K 上のベクトル空間として有限次元である. K 上有限次元の $K[x]$ 加群を考えることと K の元を成分に持つ $n \times n$ 行列を考えることは同じことである.

もしも K 上有限次元な $K[x]$ 加群 M が

$$C_{\alpha,e} := K[x]/(x-\alpha)^e K[x]$$

に同型な $K[x]$ 加群の直和[4]になっていることがわかれば, 行列 A の Jordan 標準形が存在することが示されたことになる.

なぜならば, $C_{\alpha,e} = K[x]/(x-\alpha)^e K[x]$ の基底として $(x-\alpha)^{e-1}, (x-\alpha)^{e-2}, \ldots, (x-\alpha)^0$ の像を取るとき, x の作用が定める線形写像の行列表示がちょうど Jordan ブロックの形になるからである. そのことは以下のようにして確かめられる. 以下の $\equiv$ はすべて mod $(x-\alpha)^e$ の合同関係である:

$$\begin{aligned}
x(x-\alpha)^{e-1} &= (x-\alpha)^e + \alpha(x-\alpha)^{e-1} \equiv \alpha(x-\alpha)^{e-1},\\
x(x-\alpha)^{e-2} &= (x-\alpha)^{e-1} + \alpha(x-\alpha)^{e-2},\\
&\cdots\cdots\cdots\\
x(x-\alpha)^0 &= (x-\alpha)^1 + \alpha(x-\alpha)^0.
\end{aligned}$$

すなわち,

$$\begin{aligned}
&[x(x-\alpha)^{e-1}, x(x-\alpha)^{e-1}, \ldots, x(x-\alpha)^0]\\
&\qquad \equiv [(x-\alpha)^{e-1}, (x-\alpha)^{e-1}, \ldots, (x-\alpha)^0] \begin{bmatrix} \alpha & 1 & & \\ & \alpha & \ddots & \\ & & \ddots & 1 \\ & & & \alpha \end{bmatrix}.
\end{aligned}$$

ゆえに x の $C_{\alpha,e}$ への作用が定める線形写像の上の基底に関する行列表示は

$$J_{\alpha,e} = \begin{bmatrix} \alpha & 1 & & \\ & \alpha & \ddots & \\ & & \ddots & 1 \\ & & & \alpha \end{bmatrix} \quad (e \times e \text{ 行列})$$

という Jordan ブロックの形になる.

これで, 有限 Abel 群が素数べき位数の巡回群の直積に分解するという結果 (系 1.10) の類似を K 上有限次元の $K[x]$ 加群について証明できれば Jordan 標準形の存在を証明でき

[4] $K[x]$ 加群の有限直和と有限直積は同じもの

ることわかった. ($C_{\alpha,e} = K[x]/(x-\alpha)^e K[x]$ は素数べき位数の巡回群の類似物になっている.)

モニックな[5]多項式 $f(x) \in K[x]$ に対して, $f(x) = (x-\alpha_1)^{e_1} \cdots (x-\alpha_N)^{e_N}$ かつ, α_i たちが K の互いに異なる元であり, e_i たちが 0 以上の整数であるとき,

$$f(x) = (x-\alpha_1)^{e_1} \cdots (x-\alpha_N)^{e_N}$$

を $f(x)$ の素因数分解と呼ぶことにする.

多項式環でも中国式剰余定理がそのまま成立しており, たとえば素因数分解 $f(x) = (x-\alpha_1)^{e_1} \cdots (x-\alpha_N)^{e_N}$ について次が成立している:

$$K[x]/f(x)K[x] \cong C_{\alpha_1,e_1} \times \cdots \times C_{\alpha_N,e_N}.$$

このことから, 行列 A の Jordan 標準形の存在と一意性を証明するためには定理 1.9, 1.12 と類似の結果を K 上有限次元の $K[x]$ 加群について証明できればよいことがわかる. 次の節で有限 Abel 群の場合との類似をたどった証明の概略について説明しよう.

2.2 K 上有限次元の $K[x]$ 加群の構造

M は K 上のベクトル空間として有限次元であるような $K[x]$ 加群であるとする. M の K 上の基底を取ることによって M は K^n と同一視できる. その同一視のもとで x の M への作用が定める M の一次変換は K の元を成分とするある $n \times n$ 行列 A と同一視される. 行列 A を直接扱う代わりに我々は $K[x]$ 加群 M を扱うことになる.

$\dim_K M = n$ なので任意の $v \in M$ に対して $n+1$ 個の元 $v, xv, x^2v, \ldots, x^nv$ は K 上一次従属になる. ゆえにあるモニックな多項式 $f(x) \in K[x]$ で $f(x)v = 0$ となるものが存在する. そのようなモニックな多項式の中で次数が最小の多項式が一意的に定まることを示せる[6]. そのモニックな多項式を $\phi_v(x) \in K[x]$ と書く.

$K[x]$ 加群の準同型定理によって同型 $K[x]v \cong K[x]/\phi_v(x)K[x]$ が成立していることを示せる. この結果は有限 Abel 群 G の元 a の位数を r と書くと $\langle a \rangle \cong \mathbb{Z}/r\mathbb{Z}$ が成立することの類似である.

$\dim_K K[x]v = \deg \phi_v(x) \leqq n$ が成立している. $v \in M$ に対する $\phi_v(x)$ は有限 Abel 群 G の元 a の位数 r の類似物であり, $\deg \phi_v(x) \leqq \dim_K M$ は $r \leqq |G|$ の類似である.

補題 2.1 (補題 1.5 の類似)**.** 任意の $u, v \in M$ に対して $\phi_u(x), \phi_v(x)$ の最小公倍多項式を $m(x)$ と書くと, ある $w \in M$ が存在して $\phi_w(x) = m(x)$ となる.

証明. あるモニック多項式 $f(x), g(x), h(x), k(x)$ で $\phi_u(x) = f(x)g(x)$, $\phi_v(x) = h(x)k(x)$, $m(x) = f(x)k(x)$ を満たし, $f(x)$ と $k(x)$ が互いに素であるものが存在する (多項式の素因数分解を使えば存在を示せる). $u' = g(x)u$, $v' = h(x)v$ とおくと, $\phi_{u'}(x) = f(x)$, $\phi_{v'}(x) = k(x)$ となり, それらは互いに素になる.

$z \in K[x]u' \cap K[x]v'$ に対する $\phi_z(x)$ は $f(x)$ と $k(x)$ の共約多項式になるので 1 になる. ゆえに $z = 1z = \phi_z(x)z = 0$ となる. これで $K[x]u' \cap K[x]v' = 0$ となることがわかった.

ゆえに $K[x]u' + K[x]v'$ は直和になる.

$K[x]$ に関する中国式剰余定理は, $(K[x]/f(x)K[x]) \times (K[x]/k(x)K[x])$ が

$$a = (1 \bmod f(x), 1 \bmod k(x))$$

[5]最高次の係数が 1 であるという意味. ある意味でモニックな多項式全体の集合は正の整数全体の集合の類似物だとみなされる.

[6]示してみよ

から生成される巡回 $K[x]$ 加群になり, $\phi_a(x) = f(x)k(x)$ となることを意味している ($K[x]a \cong K[x]/f(x)k(x)K[x]$). そのことから, $K[x]u' + K[x]v'$ は $w = u' + v'$ から生成される巡回 $K[x]$ 加群になり, $\phi_w(x) = f(x)k(x) = m(x)$ となることがただちに導かれる. □

上の証明は注意 1.4 の内容の焼き直しに過ぎない.

この補題 2.1 を使えば, 補題 1.6 の証明とまったく同様にして次の補題が示される.

補題 2.2 (補題 1.6 の類似)**.** w は M の元で $\deg \phi_w(x)$ が最大になるものであるとする. このとき任意の $v \in M$ に対して $\phi_v(x) | \phi_w(x)$ となる. ここで多項式 $f(x), g(x)$ に対して $f(x)|g(x)$ は $f(x)$ が $g(x)$ を割り切ることを意味する. □

補題 2.3 (補題 1.7 の類似)**.** w は M の元で $\deg \phi_w(x)$ が最大になるものであるとし, $M \neq K[x]w$ であると仮定する. このとき M の $K[x]$ 部分加群 $L \neq 0$ で $K[x]w \cap L = 0$ をみたすものが存在する.

証明. $\overline{M} = M/K[x]w$ とおき, 自然な射影を $\pi : M \to \overline{M}$, $v \mapsto v + K[x]w$ と書く. 仮定 $M \neq K[x]w$ より, ある $z \in M$ で $z \notin K[x]w$ となるものが存在する. 補題 2.2 より, $\phi_z(x)$ は $\phi_w(x)$ を割り切る.

$z \notin K[x]w$ なので $\pi(w) \neq 0$ である. $\phi_{\pi(z)}(x)$ は $\phi_z(x)$ を割り切り, $\pi(z) \neq 0$ より $\deg \phi_{\pi(z)}(x) > 1$ となる. $\pi(\phi_{\pi(z)}(x)z) = 0$ なので $\phi_{\pi(z)}(x)z \in K[x]w$ となる. ゆえにある多項式 $g(x) \in K[x]$ で $\phi_{\pi(z)}(x)z = g(x)w$ を満たすものが存在する. このとき

$$0 = \phi_z(x)z = \frac{\phi_z(x)}{\phi_{\pi(z)}(x)}\phi_{\pi(z)}(x)z = \frac{\phi_z(x)}{\phi_{\pi(z)}(x)}g(x)w$$

なので, ある多項式 $h(x) \in K[x]$ が存在して $\phi_z(x)g(x)/\phi_{\pi(z)}(x) = h(x)\phi_w(x)$ となる. このとき $g(x)/\phi_{\pi(z)}(x) = h(x) \cdot \phi_w(x)/\phi_z(x) \in K[x]$ となる. ゆえに M の元 u を次のように定めることができる:

$$u = z - \frac{g(x)}{\phi_{\pi(z)}(x)}w.$$

$L = K[x]u$ が構成したい M の $K[x]$ 部分加群であることを示そう. まず, $\pi(u) = \pi(z)$ なので $\phi_{\pi(u)}(x) = \phi_{\pi(z)}(x)$ の次数は 1 より大きく, ゆえに $\phi_u(x)$ の次数も 1 より大きいので, $L = K[x]u \neq 0$ である. 次に, $v \in K[x]w \cap L = K[x]w \cap K[x]u$ とすると, $v = p(x)w = q(x)u$, $p(x), q(x) \in K[x]$ と書ける. $0 = \pi(p(x)w) = \pi(v) = \pi(q(x)u) = q(x)\pi(u)$ より, $q(x)$ は $\phi_{\pi(u)}(x) = \phi_{\pi(z)}(x)$ で割り切れる. しかし, $\phi_{\pi(z)}(x)u = \phi_{\pi(z)}(x)z - g(x)w = 0$ なので $v = q(x)u = (q(x)/\phi_{\pi(z)}(x))\phi_{\pi(z)}(x)u = 0$ となる. これで $K[x]w \cap L = K[x]w \cap K[x]u = 0$ となることもわかった. □

上の証明は補題 1.7 の証明の焼き直しに過ぎない.

以上の準備のもとで, 以下の結果は有限 Abel 群の場合とまったく同様に証明できる.

補題 2.4 (補題 1.8 の類似)**.** w を M の元で $\deg \phi_w(x)$ が最大になるものとすると, M は巡回 $K[x]$ 部分加群 $K[x]w$ とある $K[x]$ 部分加群 W の直和に分解する. □

定理 2.5 (定理 1.9 の類似)**.** K 上有限次元の $K[x]$ 加群 M に対して, 0 以外の $w_1, w_2, \ldots, w_N \in M$ で以下の条件を満たすものが存在する ($M = 0$ の場合には $N = 0$ とみなす):

- M は巡回 $K[x]$ 部分加群 $K[x]w_1, \ldots, K[x]w_N$ の直和に分解する.
- $d_i(x) = \phi_{w_i}(x)$ とおくと, $d_N(x)| \cdots |d_2(x)|d_1(x)$. □

定理 2.6 (定理 1.12 の類似)**.** 定理 2.5 の多項式 $d_1(x), d_2(x), \ldots, d_N(x)$ は M から一意的に決まる. (この $(d_1(x), d_2(x), \ldots, d_N(x))$ を M の**単因子 (elementary divisors)** と呼ぶ.) □

注意 2.7. 定理 2.5, 2.6 は K が代数閉体とは限らない任意の体の場合にも成立している. □

証明を省略した部分を自力で埋めよ.
このノートの全体を自分好みに書き直してみよ.
このノートの内容に誤りがあれば訂正せよ.

3 有限 Abel 群の巡回群の直積への分解の別証明

第 1 節 の証明と内容的には本質的に同じなのだが, 正方行列の一般固有空間分解と類似の分解を使ったより短い証明も可能なので紹介しておく.

有限 Abel 群 G が巡回群の直積に分解することを証明しよう.

証明. G は位数 n の有限 Abel 群であるとし, n の素因数分解を $n = p_1^{e_1} \cdots p_N^{e_N}$ (p_i たちは互いに異なる素数で e_i たちは正の整数) と書いておく. 任意の $a \in G$ について $a^n = 1$ となる.

$q_i = n/p_i^{e_i}$ とおく. $q_1, \ldots, q_N$ の最大公約数は 1 なので, ある整数 $k_1, \ldots, k_N$ で

$$k_1 q_1 + \cdots + k_N q_N = 1$$

を満たすものが存在する. $r_i = k_i q_i$ とおくと $r_1 + \cdots + r_N \equiv 1 \pmod{n}$ となり, $i \neq j$ のとき $q_i q_j$ は n で割り切れるので $r_i r_j \equiv 0 \pmod{n}$ となる. $r_1 + \cdots + r_N \equiv 1 \pmod{n}$ の両辺に r_i をかけることによって $r_i^2 \equiv r_i \pmod{n}$ も得られる.

G の部分集合 G_i を

$$G_i = G^{r_i} = \{\, a^{r_i} \mid a \in G \,\}$$

と定めると, G_i は G の部分群になる.

G が $G_1, \ldots, G_N$ の直積に分解することを示そう.

任意の $a \in G$ に対して,

$$a = a^{r_1 + \cdots + r_N} = a^{r_1} \cdots a^{r_N}$$

が成立するので, $G = G_1 \cdots G_N$.

$a_i \in G_i$ かつ $a_1 \cdots a_N = 1$ のとき, 各 a_i はある $b_i \in G$ によって $a_i = b_i^{r_i}$ と表される. ゆえに

$$1 = (a_1 \cdots a_N)^{r_i} = b_1^{r_1 r_i} \cdots b_i^{r_i^2} \cdots b_N^{r_N r_i} = b_i^{r_i} = a_i$$

となり, $a_1 = \cdots = a_N = 1$ となることがわかる.

以上の結果を合わせると, G が $G_1, \ldots, G_N$ の直積に分解することがわかる.

各 G_i はそのすべての元の位数が p_i のべきであるような有限 Abel 群になる. ゆえにすべての元の位数が素数 p のべきであるような有限 Abel 群 G が巡回群の直積に分解することを示せば十分である. そのことを G の位数に関する数学的帰納法で証明しよう.

G はすべての元の位数が素数 p のべきであるような有限 Abel 群であると仮定する. G の位数最大の元 a を取り, その位数を p^r と表わす. G が $\langle a \rangle$ とある部分群の直積に分解することを G の位数に関する数学的帰納法で証明しよう.

もしも $G = \langle a \rangle$ なら証明するべきことはないので, $G \neq \langle a \rangle$ と仮定してよい. そのとき, ある $b \in G$ で $b \notin \langle a \rangle$ をみたすものが存在する. b の位数は p^s, $s \leqq r$ の形をしている.

$G/\langle a\rangle$ での b の像の位数を p^t, $0 < t \leqq s$ と書くと, $b^{p^t} \in \langle a\rangle$ となるので, ある整数 k が存在して $b^{p^t} = a^k$ となる. このとき $1 = b^{p^s} = b^{p^t p^{s-t}} = a^{kp^{s-t}}$ より, kp^{s-t} は p^m で割り切れるので, p^s でも割り切れる. ゆえに $c \in G$ を $c = a^{-kp^{-t}}b$ と定めることができる. c と b の $G/\langle a\rangle$ での像は等しく, その像の位数 p^t は 1 より大きいので, c の位数も 1 より大きい. ゆえに $\langle c\rangle \neq \{1\}$.

さらに $x \in \langle a\rangle \cap \langle c\rangle$ のとき, $x = a^i = c^j$, $i, j \in \mathbb{Z}$ と書け, その $G/\langle a\rangle$ での像は 1 になり, b^j の像に一致するので, j は p^t で割り切れることになり, $x = c^j = c^{p^t \cdot j/p^t} = (a^{-k}b^t)^{j/p^t} = 1^{j/p^t} = 1$. これで $\langle a\rangle \cap \langle c\rangle = \{1\}$ が示された.

$G/\langle c\rangle$ の位数は G より小さく, その元の位数は p のべきになる. ゆえに $G/\langle c\rangle$ は $\langle a\rangle$ の像とある部分群 $\overline{H}$ の直積に分解する. G が $\langle a\rangle$ と $\overline{H}$ の逆像 H の直積に分解することを示せる.

G が $\langle a\rangle$ とある部分群 H の直積に分解することを示せた. H の位数は G の位数より小さいと仮定してよい. ゆえに帰納法の過程によって H は巡回群の直積に分解する. したがって G も巡回群の直積に分解する. □

K が代数閉体であるとき, K の元を要素とする任意の n 次正方行列 A について K^n が A の一般固有空間の直和に分解されることは以下のようにして示される. 上の証明の最初の部分と比較してみよ.

証明. A の特性多項式を $\varphi(x) = |xE - A|$ と書くと, Cayley-Hamilton の定理より, $\varphi(A) = 0$ が成立する. $\varphi(x)$ の素因数分解を $\varphi(x) = (x-\alpha_1)^{e_1} \cdots (x-\alpha_N)^{e_N}$ (α_i たちは K の互いに異なる元であり, e_i たちは正の整数) と書いておく. $\varphi_i(x) = \varphi_i(x)/(x-\alpha_i)^{e_i}$ とおくと, $\varphi_i(x)$ たちの最大公約公式は 1 なのである $a_1(x), \ldots, a_N(x) \in K[x]$ が存在して

$$a_1(x)\varphi_1(x) + \cdots + a_N(x)\varphi_N(x) = 1$$

となる. このとき, $P_i = a_i(A)\varphi_i(A)$ とおくと, $P_1 + \cdots + P_N = E$ であり, $i \neq j$ のとき $\varphi_i(x)\varphi_j(x)$ は $\varphi(x)$ で割り切れるので $P_iP_j = 0$ となる. $P_1 + \cdots + P_N = E$ の両辺に P_i をかけることによって $P_i^2 = P_i$ も得られる.

K^n の部分空間 W_i を $W_i = P_iK^n$ と定める. $(x-\alpha_i)^{e_i}\varphi_i(x) = \varphi(x)$ より $(A-\alpha_i)^{e_i}W_i = \{0\}$ となることもわかる. ゆえに K^n が W_i たちの直和に分解されていることを示せれば, K^n が一般固有空間の直和に分解することを示せたことになる.

$P_1 + \cdots + P_N = E$ より $W_1 + \cdots + W_N = K^n$ となることがわかる. $w_i \in W_i$, $w_1 + \cdots + w_N = 0$ のとき, 両辺に P_i を作用させると $P_i^2 = P_i$, $P_iP_j = 0$ $(i \neq j)$ より, $w_i = 0$ を得る. これで直和分解 $K^n = W_1 \oplus \cdots \oplus W_N$ が成立していることが示された. □

4 良書紹介

有限 Abel 群の構造論と Jordan 標準形の理論の類似性は単項イデアル整域上 (PID 上) の有限生成加群の構造定理に統一される. その辺りの話は次の本の第 3 話に書いてある (最初に pp. 50–51 を参照せよ):

- 堀田良之, 加群十話—代数学入門—, すうがくぶっくす 3, 朝倉書店, 1988 年, ii 頁 +186 頁