

代数学（雪江明彦）

第 I 卷

群論入門（第 1 版第 9 刷）

第 4 章

群の作用と Sylow の定理

演習問題

■4.6.10 $G = \langle x, y, z | x^2 = y^3 = z^5 = xyz = 1 \rangle$ および $H = \langle z \rangle$ とする. $H \backslash G$ における 1_G の剰余類を 1 と表し, Todd-Coxeter の方法を実行する.

	y	y	y		z	z	z	z	z		y	z	y	z
1	2	3	1		1	1	1	1	1		2	4	5	1

$5z = 1z = 1$ なので $5 = 1$. $4y = 5 = 1 = 3y$ なので $4 = 3$. 1 行目を書き換えて 2 行目を計算する.

	y	y	y		z	z	z	z	z		y	z	y	z
1	2	3	1		1	1	1	1	1		2	3	1	1
2	3	1	2		3	4	5	6	2		3	4	7	2

$7z = 6z = 2$ なので $7 = 6$. 2 行目を書き換えて 3, 4 行目を計算する.

	y	y	y		z	z	z	z	z		y	z	y	z
1	2	3	1		1	1	1	1	1		2	3	1	1
2	3	1	2		3	4	5	6	2		3	4	6	2
3	1	2	3		4	5	6	2	3		1	1	2	3
4	7	8	4		5	6	2	3	4		7	9	10	4

$10z = 3z = 4$ なので $10 = 3$. $9y = 10 = 3 = 2y$ なので $9 = 2$. $7z = 9 = 2 = 6z$ なので $7 = 6$. $8 \rightarrow 7$ とする. 4 行目を書き換えて 5 行目を計算する.

	y	y	y		z	z	z	z	z		y	z	y	z
1	2	3	1		1	1	1	1	1		2	3	1	1
2	3	1	2		3	4	5	6	2		3	4	6	2
3	1	2	3		4	5	6	2	3		1	1	2	3
4	6	7	4		5	6	2	3	4		6	2	3	4
5	8	9	5		6	2	3	4	5		8	10	11	5

$11z = 4z = 5$ なので $11 = 4$. $10y = 11 = 4 = 7y$ なので $10 = 7$. 5 行目を書き換えて 6 行目を計算する.

	y	y	y	z	z	z	z	z	y	z	y	z
1	2	3	1	1	1	1	1	1	2	3	1	1
2	3	1	2	3	4	5	6	2	3	4	6	2
3	1	2	3	4	5	6	2	3	1	1	2	3
4	6	7	4	5	6	2	3	4	6	2	3	4
5	8	9	5	6	2	3	4	5	8	7	4	5
6	7	4	6	2	3	4	5	6	7	10	11	6

$11z = 5z = 6$ なので $11 = 5$, $10y = 11 = 5 = 9y$ なので $10 = 9$. 6 行目を書き換えて 7 行目を計算する.

	y	y	y	z	z	z	z	z	y	z	y	z
1	2	3	1	1	1	1	1	1	2	3	1	1
2	3	1	2	3	4	5	6	2	3	4	6	2
3	1	2	3	4	5	6	2	3	1	1	2	3
4	6	7	4	5	6	2	3	4	6	2	3	4
5	8	9	5	6	2	3	4	5	8	7	4	5
6	7	4	6	2	3	4	5	6	7	9	5	6
7	4	6	7	9	10	11	12	7	4	5	8	7

$12z = 8z = 7$ なので $12 = 8$. 7 行目を書き換えて 8 行目を計算する.

	y	y	y	z	z	z	z	z	y	z	y	z
1	2	3	1	1	1	1	1	1	2	3	1	1
2	3	1	2	3	4	5	6	2	3	4	6	2
3	1	2	3	4	5	6	2	3	1	1	2	3
4	6	7	4	5	6	2	3	4	6	2	3	4
5	8	9	5	6	2	3	4	5	8	7	4	5
6	7	4	6	2	3	4	5	6	7	9	5	6
7	4	6	7	9	10	11	8	7	4	5	8	7
8	9	5	8	7	9	10	11	8	9	10	12	8

$12z = 11z = 8$ なので $12 = 11$. 8 行目を書き換えて 9, 10, 11 行目を計算する.

	y	y	y	z	z	z	z	z	y	z	y	z
1	2	3	1	1	1	1	1	1	2	3	1	1
2	3	1	2	3	4	5	6	2	3	4	6	2
3	1	2	3	4	5	6	2	3	1	1	2	3
4	6	7	4	5	6	2	3	4	6	2	3	4
5	8	9	5	6	2	3	4	5	8	7	4	5
6	7	4	6	2	3	4	5	6	7	9	5	6
7	4	6	7	9	10	11	8	7	4	5	8	7
8	9	5	8	7	9	10	11	8	9	10	11	8
9	5	8	9	10	11	8	7	9	5	6	7	9
10	11	12	10	11	8	7	9	10	11	8	9	10
11	12	10	11	8	7	9	10	11	12	13	14	11

$14z = 10z = 11$ なので $14 = 10$, $13y = 14 = 10 = 12y$ なので $13 = 12$. 11 行目を書き換えて 12 行目を計算する.

	y	y	y	z	z	z	z	z	y	z	y	z
1	2	3	1	1	1	1	1	1	2	3	1	1
2	3	1	2	3	4	5	6	2	3	4	6	2
3	1	2	3	4	5	6	2	3	1	1	2	3
4	6	7	4	5	6	2	3	4	6	2	3	4
5	8	9	5	6	2	3	4	5	8	7	4	5
6	7	4	6	2	3	4	5	6	7	9	5	6
7	4	6	7	9	10	11	8	7	4	5	8	7
8	9	5	8	7	9	10	11	8	9	10	11	8
9	5	8	9	10	11	8	7	9	5	6	7	9
10	11	12	10	11	8	7	9	10	11	8	9	10
11	12	10	11	8	7	9	10	11	12	12	10	11
12	10	11	12	12	12	12	12	12	10	11	12	12

以上から, $H \setminus G$ の代表は 12 個.

第 II 卷

環と体と Galois 理論 (第 1 版第 9 刷)

第 2 章

環上の加群

2.6 $GL_n(\mathbb{Z}/m\mathbb{Z})$

■定理 2.6.19

$$NF = G$$

証明 まず, $SL_n(K)$ の元による F の共役が U を含むことを示す. $\sigma(1) = i, \sigma(2) = j$ となる $\sigma \in \mathfrak{S}(n)$ を適当に定め $(M)_{\alpha\beta} = \delta_{\alpha\sigma(\beta)} \in SL_n(K)$ とする. $R_{n,12}(c) \in F$ であるので,

$$\begin{aligned} (MR_{n,12}(c))_{\alpha\gamma} &= (M)_{\alpha\beta}(R_{n,12}(c))_{\beta\gamma} = \delta_{\alpha\sigma(\beta)}(\delta_{\beta\gamma} + c\delta_{\beta 1}\delta_{\gamma 2}) = \delta_{\sigma^{-1}(\alpha)\beta}(\delta_{\beta\gamma} + c\delta_{\beta 1}\delta_{\gamma 2}) \\ &= \delta_{\sigma^{-1}(\alpha)\gamma} + c\delta_{\sigma^{-1}(\alpha)1}\delta_{\gamma 2} = \delta_{\alpha\sigma(\gamma)} + c\delta_{\alpha i}\delta_{\gamma 2}. \end{aligned}$$

さらに

$$\begin{aligned} (R_{n,ij}(c)M)_{\alpha\gamma} &= (R_{n,ij}(c))_{\alpha\beta}(M)_{\beta\gamma} = (\delta_{\alpha\beta} + c\delta_{\alpha i}\delta_{\beta j})\delta_{\beta\sigma(\gamma)} = \delta_{\alpha\sigma(\gamma)} + c\delta_{\alpha i}\delta_{j\sigma(\gamma)} \\ &= \delta_{\alpha\sigma(\gamma)} + c\delta_{\alpha i}\delta_{\gamma 2} \end{aligned}$$

なので $MR_{n,12}(c) = R_{n,ij}(c)M$ すなわち $MR_{n,12}(c)M^{-1} = R_{n,ij}(c)$ となる. $NF \triangleleft NP = G$ なので $U \leq NF$. 命題 2.6.12 から $G = NF$ となる. \square

2.12 単項イデアル整域上の有限生成加群

■定理 2.12.1 構成された同型について, $M = \langle x_1, \dots, x_m \rangle$ である. 全射準同型

$$\phi: R^m \ni e_i \mapsto x_i \in M$$

の核の生成元を $\{y_1, \dots, y_n\}$ とする: $\ker \phi = \langle y_1, \dots, y_n \rangle \subset R^m$. さらに

$$f: R^n \ni e'_j \mapsto y_j \in R^m$$

とする. 準同型定理から

$$\text{Coker}(f) = R^m / \text{Im } f = R^m / \ker \phi \simeq \text{Im } \phi = M.$$

よって, $x_i \in M$ は $[e_i] \in R^m / \text{Im } f$ に対応する. さらに $\text{Im}(f) = \{(e_1 r_1, \dots, e_t r_t, 0, \dots, 0)\}$ となるので,

$$M \ni x_i \mapsto (\dots, 0, 1, 0, \dots) \in R/(e_1) \oplus \dots \oplus R/(e_t) \oplus R^{m-t}$$

に対応する.

2.13 完全系列と局所化

■例 2.13.12

(1) $u = x + iy, v = x - iy$ とすれば $\mathbb{C}[x, y]/(x^2 + y^2) \simeq \mathbb{C}[u, v]/(uv)$ が分かる.

第 3 章

体論の基本

3.3 分離拡大

■命題 3.3.5

(3) の n は一意に定まる

証明 主張を満たす n が一意に定まらないと仮定する. $f(x) = g(x^{p^m}) = h(x^{p^n})$ を満たす $n > m > 0$ 及び既約分離多項式 $g(x), h(x)$ が存在する. $g(x) = h(x^{p^{n-m}})$ となるので $g'(x) = 0$. 命題 3.3.5 の主張より $g(x)$ は重根を持ち, 分離性に矛盾する. \square

第 4 章

Galois 理論

4.6 Galois 拡大の推進定理

■定理 4.6.1

$$\sigma(M) \subset \bar{K} \cap L$$

証明 $\sigma \in \text{Gal}(L/N)$ なので $\sigma(M) \subset L$. $x \in M$ とする. $\sigma(x)$ は $x \in M \subset L$ の N 上の共役である. すなわち $\sigma(x)$ は $x \in L$ の N 上最小多項式の根. 命題 3.1.24 から $\sigma(x)$ は $x \in L$ の K 上最小多項式の根なので $\sigma(x) \in \bar{K}$. \square

4.11 正規底

■定理 4.11.2 定理 3.6.3 より $f(x_1, \dots, x_n) \neq 0$ となる $x \in L$ が存在すれば, $f(x_1, \dots, x_n) \neq 0$ となる $x \in K$ が存在する.

系 4.10.3 から $\sum_k \sigma_i(a_k)x_k = \delta_{1i}$ となる $x_k \in L$ が存在する. $\sigma_1 = 1$ としているので

$$\sum_{k=1}^n \sigma_i^{-1} \circ \sigma_i(a_k)x_k = \sum_{k=1}^n a_k x_k = \sum_{k=1}^n \sigma_1(a_k)x_k = \delta_{1i} = 1.$$

$\text{Gal}(L/K)$ において $\sigma_i^{-1} \circ \sigma_j = \sigma_{p(i,j)}$ と定める. $i \neq j$ なら $\sigma_{p(i,j)} = \sigma_i^{-1} \circ \sigma_j \neq 1 = \sigma_1$ なので $p(i,j) \neq 1$. よって

$$\sum_{k=1}^n \sigma_i^{-1} \circ \sigma_j(a_k)x_k = \sum_{k=1}^n \sigma_{p(i,j)}(a_k)x_k = \delta_{i1(i,j)} = 0 \quad (i \neq j).$$

以上から

$$\sum_{k=1}^n \sigma_i^{-1} \circ \sigma_j(a_k)x_k = \delta_{ij}.$$

■定理 4.11.4

$$x^n - 1 = \text{LCM}(p_1(x)^{a_1}, \dots, p_m(x)^{a_m}) =: L(x)$$

証明 L は $K[x]$ 加群として有限生成であるが、その生成元を $\{\alpha_1, \dots, \alpha_m\}$ とする。単項イデアル整域上の有限生成加群の構造定理 2.12.1 (と証明における同型の構成) から同型

$$\Phi: L \ni \sum_{i=1}^m f_i(\sigma)\alpha_i \mapsto (f_i(x) + (p_i(x)^{a_i}))_i \in \bigoplus_{i=1}^m K[x]/(p_i(x)^{a_i})$$

を得る。 $g(x) \in I$ なら $0 = g(\sigma)\alpha_i \mapsto 0$ なので $g(x) \in (p_i(x)^{a_i})$ である。これが任意の i に対して成立するので $L(x) \mid g(x)$ 。特に $L(x) \mid x^n - 1$ である。

任意の $\alpha \in L$ に対して $L(\sigma)\alpha = 0$ となることを示す。 $\alpha = \sum f_i(\sigma)\alpha_i$ となる $f_i(x) \in K[x]$ が存在する。最小公倍元の定義から

$$\Phi(L(\sigma)\alpha) = (L(x)f_i(x) + (p_i(x)^{a_i}))_i = 0.$$

Φ は単射なので $L\alpha = 0$ 。すなわち $L(x) \in I$ 。従って $x^n - 1 \mid L(x)$ 。

以上から $x^n - 1 = L(x)$ 。 □

4.12 トレース・ノルム

■命題 4.12.6

α が非分離的で $L = K(\alpha)$ の場合、 $p^m = [L : K]_i$

証明 命題 3.3.5 から分離既約多項式 $g(x) \in K[x]$ によって $\alpha \in L$ の K 上最小多項式は $g(x^{p^m})$ となる。 $g(x)$ は $\alpha^{p^m} \in L$ を根に持つ。もし $h(\alpha^{p^m}) = 0$ かつ $\deg h < \deg g$ となる $h(x) \in K[x]$ が存在すれば、 $h(x^{p^m})$ も α を根に持ち、 g の最小性に矛盾する。よって $g(x)$ は $\alpha^{p^m} \in L$ の K 上最小多項式である。従って、 $K(\alpha^{p^m})$ は K の分離拡大であり、 $[K(\alpha^{p^m}) : K] = \deg g(x) = n$ 。さらに $[L : K] = \deg g(x^{p^m}) = np^m$ 。 $L/K(\alpha^{p^m})$ が純非分離拡大であることは容易に分かる。

L における K の分離閉包を L_s とする。体の拡大列 $K \subset K(\alpha^{p^m}) \subset L_s \subset L = K(\alpha)$ を得る。命題 3.3.27 から L_s/K は分離拡大、 L/L_s は純非分離拡大である。

$L_s \subset L$ なので $L_s/K(\alpha^{p^m})$ も純非分離拡大。命題 3.3.2 から $L_s/K(\alpha^{p^m})$ は分離拡大でもある。命題 3.3.14 と併せれば $L_s = K(\alpha^{p^m})$ と分かる。

以上から $[L : K]_i = [L : K(\alpha^{p^m})] = p^m$ 。 □

■命題 4.12.13

有限体の乗法群は巡回群

証明 $\#K^\times = n$ とする。位数 $d \mid n$ の元 $\alpha \in K^\times$ が存在すれば、 $\{1, \alpha, \dots, \alpha^{d-1}\}$ は全て相異なり、 $x^d = 1$ を満たす。 $x^d = 1$ は高々 d 個の解しか持たないので、 $x^d = 1$ を満たす $x \in K$ は α^i という形をしている。 α^i の位数が d となるのは i が d と互いに素な場合なので、 $\phi(d)$ 個存在する。位数が d の元の集合を G_d とすれば、 $\#G_d$ は 0 か $\phi(d)$ である。

$$n = \#K^\times = \sum d \mid n \#G_d \leq \sum d \mid n \phi(d) = n$$

となるので、全ての $d \mid n$ に対して $\#G_d = \phi(d)$ である。特に位数 n の元が存在するので K^\times は巡回群。 □

■例 4.12.14 定理 4.9.7 において $R = \{2^l 3^m (K^\times)^p\}$ とすれば $\text{Gal}(K(\sqrt[p]{2}, \sqrt[p]{3})/K) \simeq R/(K^\times)^p$ である. 全射準同型

$$\phi: \mathbb{Z} \times \mathbb{Z} \ni (l, m) \mapsto 2^l 3^m (K^\times)^p \in R/(K^\times)^p$$

を考える. $(l, m) \in \ker \phi$ とする. $2^l 3^m = x^p$ となる $x \in K^\times$ が存在する. ノルムを考えれば

$$2^{l(p-1)} 3^{m(p-1)} = N_{K/\mathbb{Q}}(x)^p \in \mathbb{Q}^p$$

であるので $p \mid l, m$ である. よって $\ker \phi = p\mathbb{Z} \times p\mathbb{Z}$ である. よって準同型定理から

$$\text{Gal}(K(\sqrt[p]{2}, \sqrt[p]{3})/K) \simeq R/(K^\times)^p \simeq (\mathbb{Z} \times \mathbb{Z})/(p\mathbb{Z} \times p\mathbb{Z}) \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}.$$

4.16 4 次多項式の Galois 群

■命題 4.16.3 (1) 証明に出てくる ϕ は命題 4.4.8 で考えた制限写像 $\phi: \text{Gal}(L/K) \rightarrow \text{Gal}(M/K)$.

(3) $\text{Gal}(L/K) = \langle (1234) \rangle$ の場合. (1234) により $\tau_1 \leftrightarrow \tau_3$ および $\tau_2 \mapsto \tau_2$ であるので, Galois 理論の基本定理から $\tau_2 \in K$ および $\tau_1, \tau_3 \in L \setminus K$ である. よって $g(y) = (y - \tau_1)(y - \tau_2)(y - \tau_3)$ は K 上の一次式 $y - \tau_2$ と K 上既約な二次式 $(y - \tau_1)(y - \tau_3)$ の積である.

$h(z)$ の根 β_1, β_2 は (4.5.2) と同様に構成される:

$$\beta_1 = \tau_1^2 \tau_2 + \tau_2^2 \tau_3 + \tau_3^2 \tau_1, \quad \beta_2 = \tau_1 \tau_2^2 + \tau_2 \tau_3^2 + \tau_3 \tau_1^2.$$

$(1234) \in \text{Gal}(L/K)$ により $\tau_1 \leftrightarrow \tau_3$ および $\tau_2 \mapsto \tau_2$ であるので, $\beta_1 \leftrightarrow \beta_2$. よって $\beta_1, \beta_2 \in L \setminus K$ である. 従って $h(z) = (z - \beta_1)(z - \beta_2)$ は K 上既約な二次式である.

■定理 4.16.18

$\text{ch } K = 2$ なら

$$\{x^2 + x \mid x \in K(\tau_1), x^2 + x \in K\} = \{\alpha d_2 d_1^{-2} + \beta^2 + \beta \mid \alpha \in \mathbb{F}_2, \beta \in K\}.$$

証明 τ_1 は $g(y) = y^2 + d_1 y + d_2 = y^2 - d_1 y - d_2 \in K[y]$ の根である. $d_1 \neq 0$ なので $\tau_1 d_1^{-1}$ は $y^2 - y - d_2 d_1^{-2}$ の根となる.

$x^2 + x \in K$ となる $x \in K(\tau_1 d_1^{-1}) = K(\tau_1)$ が存在すれば, 補題 4.15.2 から

$$x = \beta + \alpha \tau_1, \quad x^2 + x = \beta^2 + \beta + \alpha d_2 d_1^{-2}$$

となる $\alpha \in \mathbb{F}_2$ と $\beta \in K$ が存在する. よって

$$\{x^2 + x \mid x \in K(\tau_1), x^2 + x \in K\} \subset \{\alpha d_2 d_1^{-2} + \beta^2 + \beta \mid \alpha \in \mathbb{F}_2, \beta \in K\}.$$

$\alpha \in \mathbb{F}_2, \beta \in K$ とする. $\tau_1 d_1^{-1}$ は $y^2 - y - d_2 d_1^{-2}$ の根なので,

$$\begin{aligned} K \ni \alpha d_2 d_1^{-2} + \beta^2 + \beta &= \alpha [(\tau_1 d_1^{-1})^2 + \tau_1 d_1^{-1}] + \beta^2 + \beta \\ &= \alpha (\tau_1 d_1^{-1})^2 + \alpha \tau_1 d_1^{-1} + \beta^2 + \beta \\ &= \alpha^2 (\tau_1 d_1^{-1})^2 + \alpha \tau_1 d_1^{-1} + \beta^2 + \beta \end{aligned}$$

$$= (\alpha\tau_1 d_1^{-1} + \beta)^2 + (\alpha\tau_1 d_1^{-1} + \beta).$$

$\alpha\tau_1 d_1^{-1} + \beta \in K(\tau_1)$ なので

$$\{x^2 + x \mid x \in K(\tau_1), x^2 + x \in K\} \supset \{\alpha d_2 d_1^{-2} + \beta^2 + \beta \mid \alpha \in \mathbb{F}_2, \beta \in K\}.$$

□