memo

オ

2025 年 12 月 9 日

目次

1 雑多

1.1 poset の隣接代数

$(P, \leq)$ を poset とする．P は**局所有限**（locally small），つまり，任意の $x, y \in P$ に対して $|[x, y]| < \infty$ が成り立っているとする．

R を単位的可換環とする．$\mathrm{A}_R(P) = \{\, f \colon P \times P \to R \,|\, x \not\leq y \implies f(x, y) = 0 \,\}$ は自然に R 加群となり，さらに，$\mathrm{A}_R(P)$ 上の積 $*$ を

$$(f * g)(x, y) = \sum_{x \leq z \leq y} f(x, z) g(z, y) \quad (f, g \in \mathrm{A}_R(P),\, x, y \in P)$$

で定めれば，$\mathrm{A}_R(P)$ はこの積により R 代数となり，P の R 上の**隣接代数**（incidence algebra）と呼ばれる [小 22]．単位元 $\delta \in \mathrm{A}_R(P)$ は

$$\delta(x, y) = \begin{cases} 1_R & (x = y) \\ 0_R & (x \neq y) \end{cases}$$

で与えられる．

命題 1.1 P が有限集合[1] のとき，R 代数として $\mathrm{A}_R(P) \cong \mathrm{U}_{|P|}(R)$ である．ここで，$\mathrm{U}_{|P|}(R)$ は，各成分が R の元であるような $|P|$ 次の上三角行列全体の成す R 代数である．

証明 P を $I = [|P|]$ で，$i \leq j$ なら $x_i \leq x_j$ となるように添え字付けておく[2] ．$\phi \colon \mathrm{A}_R(P) \to \mathrm{U}_{|P|}(R)$ を

$$\phi(f) = (f(x_i, x_j))_{i,j \in I}$$

で定めると，ϕ が同型を与えている． ■

命題 1.2 ([小 22, 補題 7.18]) $f \in \mathrm{A}_R(P)$ とする．f が $\mathrm{A}_R(P)$ の単元であることの必要十分条件は，任意の $x \in P$ に対して $f(x, x)$ が R の単元であることである．

証明 f が単元であるとすると，任意の $x \in P$ に対して，

$$(f * f^{-1})(x, x) = f(x, x) f^{-1}(x, x) = 1_R$$

1) P が無限集合でも，任意の $x \in P$ に対して $(\infty, x]$ が有限集合でさえあれば，無限次元上三角行列を考えることで同型を与えられると思う．

2) 添え字付けられることは order-extension principle により保証される．つまり，P 上の全順序 $\leq^*$ で，任意の $x, y \in P$ に対して，$x \leq y$ なら $x \leq^* y$ を満たすようなものが存在する．このような $\leq^*$ を $\leq$ の linear extension と呼ぶらしい．

より $f(x,x) \neq 0$ が従う．逆を示すために，任意の $x \in P$ に対して $f(x,x)$ が単元であるとする．$g, h \in \mathrm{A}_R(P)$ を，任意の $x, y \in P$ に対して

$$g(x,y) = \begin{cases} f(x,x)^{-1} & (x=y) \\ -f(y,y)^{-1} \sum_{x \leq z < y} g(x,z) f(z,y) & (x<y) \\ 0_R & (x \not\leq y) \end{cases},$$

$$h(x,y) = \begin{cases} f(x,x)^{-1} & (x=y) \\ -f(x,x)^{-1} \sum_{x < z \leq y} f(x,z) h(z,y) & (x<y) \\ 0_0 & (x \not\leq y) \end{cases}$$

で定めれば，$g*f = f*h = \delta$ が成り立つ．したがって，f は単元であり，$f^{-1} = g = h$ である． ■

1.2 poset の Möbius 関数

P 上の R に値を持つ**ゼータ関数**（zeta function）$\zeta_P \in \mathrm{A}_R(P)$ を

$$\zeta_P(x,y) = \begin{cases} 1_R & (x \leq y) \\ 0_R & (x \not\leq y) \end{cases}$$

で定める．文脈によって P が明らかなとき，添え字は省略する．命題 1.2 より，ζ の逆元 $\mu_P \in \mathrm{A}_R(P)$ が存在して，さらに

$$\begin{aligned} \mu_P(x,y) &= \begin{cases} 1_R & (x=y) \\ -\sum_{x \leq z < y} \mu(x,z) & (x<y) \\ 0_R & (x \not\leq y) \end{cases} \\ &= \begin{cases} 1_R & (x=y) \\ -\sum_{x < z \leq y} \mu(z,y) & (x<y) \\ 1_R & (x \not\leq y) \end{cases} \end{aligned}$$

となる．この μ を P 上の R を値に持つ Möbius **関数**（Möbius function）と呼ぶ．μ は ζ の逆元なので，

$$\sum_{x \leq z \leq y} \mu(z,y) = \sum_{x \leq z \leq y} \mu(x,z) = \begin{cases} 1_R & (x=y) \\ 1_R & (x \neq y) \end{cases} \tag{1.1}$$

が成り立つ．

1.3 Möbius の反転公式

P の部分集合 $P_{\leq}$ と $P_{\geq}$ を，それぞれ

$$P_{\leq} = \{\, x \in P \,|\, |(\infty, x]| < \infty \,\}, \quad P_{\geq} = \{\, x \in P \,|\, |[x, \infty)| < \infty \,\}$$

で定める[3)]．また，$f\colon P \to R$ に対して，f の lower sum $S_{\leq}(f)\colon P_{\leq} \to R$ と upper sum $S_{\geq}(f)\colon P_{\geq} \to R$ をそれぞれ

$$S_{\leq}(f)(x) = \sum_{y \leq x} f(y), \quad S_{\geq}(f)(x) = \sum_{x \leq y} f(y)$$

で定める．

定理 1.3 (Möbius の反転公式 [Het07, Theorem 2.1]) 任意の $f, g\colon P \to R$ に対して，以下が成り立つ．

1. 任意の $x \in P_{\leq}$ に対して，$g(x) = S_{\leq}(f)(x) \iff f(x) = S_{\leq}(g(-)\,\mu(-, x))(x)$ が成り立つ．
2. 任意の $x \in P_{\geq}$ に対して，$g(x) = S_{\geq}(f)(x) \iff f(x) = S_{\geq}(g(-)\,\mu(x, -))(x)$ が成り立つ．

証明 定理 1.3.1 のみ示す．各 $x \in P_{\leq}$ に対して，$(\infty, x]$ は有限 poset となる．$S_{\leq}(f)(x) = \sum_{y \in x} \zeta(y, x) f(y)$ なので，命題 1.1 の記号を用いれば，主張は

$$(g(x_i))_{i \in I} = (f(x_i))_{i \in I} \phi(\zeta) \iff (f(x_i))_{i \in I} = (g(x_i))_{i \in I} \phi(\mu)$$

と同値である．したがって，$\phi(\zeta)^{-1} = \phi(\mu)$ を示せばよいが，これは μ の定義から明らかである．

■

1.4 全射準同型が素イデアルを保たない例

$\phi_1\colon \mathbb{Z}[x] \to \mathbb{Z}$ を代入写像とすると，(x) は $\mathbb{Z}[x]$ における素イデアルだが，$\phi_1((x)) = \mathbb{Z}$ は $\mathbb{Z}$ における素イデアルとならない．

1.5 共通部分の生成するイデアルについて

命題 1.4 R を環，$\{S_i\}_{i \in I}$ を R の部分集合の族とする．このとき，

$$\left(\bigcap_{i \in I} S_i \right) \subseteq \bigcap_{i \in I} (S_i)$$

が成り立つ．

3) 名称ないのかな．

証明　任意の $j \in I$ に対して $\bigcap_{i\in I} E_i \subseteq (E_j)$ なので，$\bigcap_{i\in I} E_i \subseteq \bigcap_{i\in I} (E_i)$ である．したがって，最小性より，$\left(\bigcap_{i\in I} E_i\right) \subseteq \bigcap_{i\in I} (E_i)$ が分かる．　■

逆は一般に成り立たない．実際，$R = \mathbb{Z}$ としたとき，

$$(2) \cap (3) = (6) \neq 0 = (\{2\} \cap \{3\})$$

である．

1.6　単位行列を E で表す由来

単位行列はドイツ語で Einheitsmatrix と呼ぶところから来ている．初出は Courant と Hilbert の *Methods of mathematical physics* [CH53] らしい．

1.7　G 集合の k-subsets

G を有限群とする．

命題 1.5　k を非負整数とする．任意の $H \leq G, N \trianglelefteq G$ に対して，

$$\left|\binom{G/N}{k}^H\right| = \begin{cases} \binom{(G:HN)}{k/(HN:N)} & ((HN:N) \mid k) \\ 0 & ((HN:N) \nmid k) \end{cases}$$

が成り立つ．

証明　ある $X \in \binom{G/N}{k}^H$ が存在したとする．このとき，H は X に作用しているので，X の H 集合としての軌道分解

$$X \cong \bigsqcup_{gN \in (H\backslash X)} H/H_{gN}$$

を得る．$H_{gN} = H \cap N$ だから，$|X| = k$ より

$$k = (H : H \cap N)\, |H\backslash X|$$

が分かるが，これは第 2 同型定理より $(HN:N) = (H : H \cap N) \mid k$ を意味する．さらに，このような X は $H\backslash(G/N)$ の元の $k/(HN:N)$ 個の直和となることも従うが，集合としての同型 $H\backslash(G/N) \cong G/HN$ より，直和因子の選び方は $\binom{(G:HN)}{k/(HN:N)}$ である．　■

系 1.6　$\Phi^G{}_H\binom{G/N}{k} = \Phi^G{}_{HN}\binom{G}{k|N|} = \Phi^{G/N}{}_{HN/N}\binom{G/N}{k}$ である．

命題 1.7　k を非負整数，$H, K \leq G$ とする．このとき，$\left|\binom{G/K}{k}^H\right| \neq 0$ ならば $|H| \mid k\,|K|$ である．

証明　$|\binom{G/K}{k}^H| \neq 0$ とする．このとき，$X \in \binom{G/K}{k}^H$ に対して，$\cup X \in \binom{G}{k|K|}^H$ であることを示す．$X = \{\, g_iK \mid i = 1, \ldots, k \,\}$ とすると，各 g_iK は互いに素であるから，$|\cup X| = k|K|$ である．さらに，H は X に作用しているので，任意の $h \in H, i$ に対して，$hg_iK = g_jK$ となる j が存在する．したがって，$h\cup X = \bigcup_{i=1}^{k} hg_iK \subseteq \cup X$ だから，H は $\cup X$ に作用する．よって，$\cup X \in \binom{G}{k|K|}^H$ である．このとき，命題 1.5 より $|H| \mid k|K|$ が成り立つ．■

証明　$X \in \binom{G/K}{k}^H$ の軌道分解を考えると，等式

$$k = \sum_{gK \in (H\backslash X)} \frac{|H|}{|H \cap {}^gK|}$$

を得る．この式の両辺に $|K| / |H|$ を乗じれば，

$$\frac{k|K|}{|H|} = \sum_{gK \in (H\backslash X)} \frac{|K|}{|H^g \cap K|} \in \mathbb{Z}$$

となるから，$|H| \mid k|K|$ が分かる．■

$\mathcal{X}_k = \{\, H \leq G \mid |H| \mid k \,\}$ とおく．

命題 1.8　任意の $H \leq G$ に対して，$\binom{G/H}{k/|H|} \in \Omega(G, \mathcal{X}_k)$ である．

予想 1.1　$\{\, \binom{G/H}{k/|H|} \mid H \in (\mathcal{X}_k/\mathrm{conj}) \,\}$ は $\mathbb{Q}\Omega(G, \mathcal{X}_k)$ の基底である．

予想 1.2　$k \mid |G|$ とする．環 R の中で $|G| / k$ のすべての約数が可逆なとき，$R \otimes_{\mathbb{Z}} \Omega(G, \mathcal{X}_k)$ は単位的環となる．特に，π を $|G| / k$ の素因数の集合とすれば，$\mathbb{Z}_{(\pi')} \otimes_{\mathbb{Z}} \Omega(G, \mathcal{X}_k)$ は単位的環となる．

1.8　Hall の部分群定理

定理 1.9 (Hall の部分群定理)　G を有限群とする．このとき，G が可解であることと，任意の素数の集合 π に対して，$|H| = |G|_\pi$ なる部分群 $H \leq G$ が存在することは同値である．

定理 1.9 における H を，G の Hall π 部分群と呼ぶ．この定理の別証明を考えたい．よく似た事実に，有限群に対する Sylow の定理が知られている，特に，G の Sylow p 部分群は，G の $|G|_p$-subsets $\binom{G}{|G|_p}$ を考えることで証明できる．

正整数 k を取ったとき，G の位数 k の部分群が存在する必要十分条件が，G の k-subsets を考えることで得られる．

命題 1.10　G を有限群，k を正整数とする．このとき，G の位数 k の部分群が存在することと，

等式

$$|\binom{G}{k}^H| = \frac{|G|}{k} \tag{1.2}$$

が成り立つような部分群 $H \leq G$ が存在することは同値である．特に，$k \neq |G|$ のとき，式 (1.2) における H が位数 k の部分群となる．

証明　$k = |G|$ のときは明らかなので，$k \neq |G|$ の場合を示す．

命題 1.5 より，任意の $H \leq G$ に対して，$|H| \mid k$ なら

$$|\binom{G}{k}^H| = \binom{(G:H)}{k/|H|}$$

が成り立つ．$H \leq G$ が $|H| = k$ を満たすとき，

$$\begin{aligned} |\binom{G}{k}^H| &= \binom{|G|/k}{1} \\ &= \frac{|G|}{k} \end{aligned}$$

である．逆に，H が式 (1.2) を満たすとすれば，命題 1.5 より $|H| \mid k$ であり，さらに

$$\begin{aligned} \frac{|G|}{k} &= |\binom{G}{k}^H| \\ &= \binom{(G:H)}{k/|H|} \\ &\geq \frac{|G|}{|H|} \\ &= \frac{|G|}{k}\frac{k}{|H|} \\ &\geq \frac{|G|}{k} \end{aligned}$$

だから，$|H| = k$ を得る．■

したがって，Hall の部分群定理は，有限可解群 G の $|G|_\pi$-subsets を G 集合として解析することで証明されることが期待できる．特に，$|\binom{G}{|G|_\pi}^H| \neq 0$ となるような最大の部分群 H を取り，$|G|_\pi \leq |H|$ を示すことができれば十分である．

予想 1.3　$\pi \neq \emptyset$ を素数の集合とする．このとき，以下は同値である．

1. G は可解群である．
2. $H \leq G$ を $\left|\binom{G}{k}^H\right| \neq 0$ となる G の部分群のうち，位数が最大のものとする．このとき，任意の $K \leq G$ に対して，$|K| \mid |G|_\pi$ ならば $\left|\binom{G/K}{|G|_\pi/|K|}^H\right| \neq 0$ が成り立つ．

この予想は正しくない！実際，$G = \mathrm{SL}(2,5)$ を $\mathbb{Z}/5\mathbb{Z}$ 上の 2 次特殊線形群とすると，G は非可解群で位数 15 の群を持たないにもかかわらず，$\binom{G/K}{15/|K|}$ $(|K| \mid 15)$ の各マークは

$$\Phi\left(\binom{G}{15}\right) = (4730523156632595024, 0, 658008, 0, 2024, 0, 0, 0, 0, 0, 0, 0),$$
$$\Phi\left(\binom{G/C_3}{5}\right) = (658008, 0, 72, 0, 8, 0, 0, 0, 0, 0, 0, 0),$$
$$\Phi\left(\binom{G/C_5}{3}\right) = (2024, 0, 8, 0, 4, 0, 0, 0, 0, 0, 0, 0)$$

となり，第 5 成分が消失していない．

1.9 GAP で Hasse 図を出力する

有限群 g の Hasse 図は，GAP と GraphViz を組み合わせて出力できる．以下にその手順を示す．

1. GAP 上で g の部分群束 l を計算する．
2. l から g の Hasse 図の dot ファイル D8.dot を出力する．
3. GraphViz で D8.dot を pdf ファイルなどに変換する．

例 1.11 位数 8 の二面体群 D_4 の Hasse 図を出力しよう．コード 1 と 2 は，D_4 の Hasse 図の pdf ファイル D4.pdf を出力する例である．

コード 1 GAP での操作

```
gap> g := DihedralGroup(8);;
gap> l := LatticeSubgroups(g);
<subgroup lattice of <pc group of size 8 with 3 generators>, 8 classes, 10 subgroups>
gap> DotFileLatticeSubgroups(l, "D4.dot");
gap>
```

コード 2 コマンドプロンプト上での操作

```
C:\Users\user\Documents>dot -T pdf "D4.dot" -o "D4.pdf"
```

コード 1 と 2 によって，D4.dot の置かれているフォルダ（今の場合は C:\User\user\Documents）に，D_4 の Hasse 図 D4.pdf が生成される（図 1.1）．

図 1.1 において，一番左の列の数字は，対応する行に位置する群の位数を表している．また，四角で囲まれたノードは正規部分群に対応し，丸で囲まれたノードでは，1 つ目の数字が同じであれば，対応する部分群は同じ共役類に属する．各ノード a-b に対応する部分群が知りたければ，今回の場合は `ConjugacyClassesSubgroup(l)[a][b]` とすればよい．

もし，pdf ファイルを出力した際に，各ノードをつなぐ線が消えてしまうようであれば，dot ファイルの size を編集すればよい．

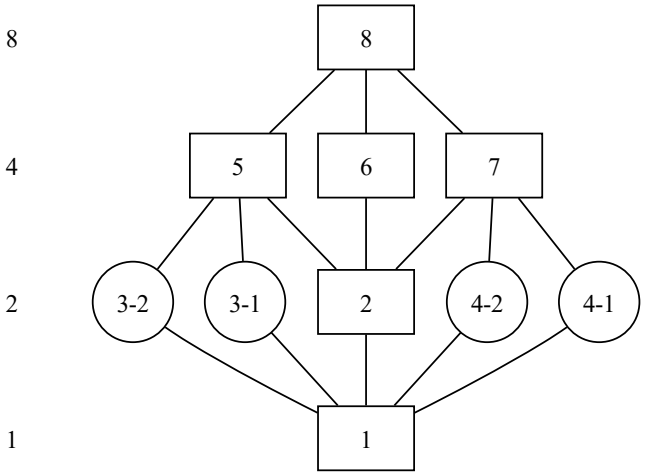

図 1.1　D4.pdf（D_4 の Hasse 図）

1.10　Burnside 環の基本定理

G を有限群とする．$\mathcal{X}$ を G の部分群の集合で，G 共役で閉じていると仮定する．G の Burnside 環 $\Omega(G)$ の部分群 $\Omega(G,\mathcal{X})$ を

$$\Omega(G,\mathcal{X}) = \langle\, [G/H] \mid H \in (\mathcal{X}/\mathrm{conj}) \,\rangle$$

で定める．また, $\tilde{\Omega}(G,\mathcal{X}) = \mathbb{Z}^{|\mathcal{X}/\mathrm{conj}|}$ と置く．さらに, マーク準同型写像 $\Phi\colon \Omega(G,\mathcal{X}) \to \tilde{\Omega}(G,\mathcal{X})$ を

$$\Phi([X]) = (|X^S|)_{S\in(\mathcal{X}/\mathrm{conj})}$$

と定める．また，任意の $H \le G$ に対して $\overline{H} = \cap\{\, S \in \mathcal{X} \mid H \le S \,\}$ と置く．

定理 1.12 (Yoshida [Yos90, Theorem 3.11])　任意の $S \in \mathcal{X}$ に対して，$gS \in \mathrm{W}_G S$ なら $\overline{\langle g\rangle S} \in \mathcal{X}$ が成り立つとき，$\Omega(G,\mathcal{X})$ は Φ が環準同型となるような唯一の環構造を持つ．

定理 1.13 (Fundamental theorem; Yoshida [Yos90, Theorem 3.10])　写像 $\psi\colon \tilde{\Omega}(G,\mathcal{X}) \to \mathrm{Obs}(G,\mathcal{X})$ を

$$\psi(v) := \left(\sum_{gS\in \mathrm{W}_G S} v_{\overline{\langle g\rangle S}} \mod |\mathrm{W}_G S| \right)_{S\in(\mathcal{X}/\mathrm{conj})} \qquad (v = (v_S)_{S\in(\mathcal{X}/\mathrm{conj})} \in \tilde{\Omega}(G,\mathcal{X}))$$

で定める．このとき，Abel 群の系列

$$0 \longrightarrow \Omega(G,\mathcal{X}) \xrightarrow{\Phi} \tilde{\Omega}(G,\mathcal{X}) \xrightarrow{\psi} \mathrm{Obs}(G,\mathcal{X}) \longrightarrow 0$$

は完全である．

1.11 $\mathbb{Z}$ 加群の余像

命題 1.14 M, N を有限生成自由 $\mathbb{Z}$ 加群とし，$\operatorname{rank} M = \operatorname{rank} N = n$ だとする．このとき，任意の準同型 $f\colon M \to N$ に対して，$\det f \neq 0$ なら $|\operatorname{Coker} f| = \det f$ が成り立つ．

証明 f の Smith 標準形を

$$\begin{pmatrix} e_1 & & & \\ & e_2 & & \\ & & \ddots & \\ & & & e_n \end{pmatrix} \quad (e_i \in \mathbb{Z},\ e_i \mid e_{i+1})$$

と置けば，$\det f \neq 0$ より $e_i \neq 0$ である．よって，$\operatorname{Im} f \cong \prod_{i=1}^{n} e_i\mathbb{Z}$ であり，したがって

$$|\operatorname{Coker} f| = \prod_{i=1}^{n} e_i = \det f$$

が成り立つ． ■

1.12 制限，誘導，deflation，inflation 覚書

G を群とする．右 G 集合 X と左 G 集合 Y に対して，直積 $X \times Y$ への G の右からの作用を

$$(x, y)g = (xg, g^{-1}y) \quad ((x, y) \in X \times Y,\ g \in G)$$

で定め，この作用による G 軌道全体の集合を $X \times_G Y$ と置く．$X \times_G Y$ を X と Y の**合成**（composition）と呼ぶ．

命題 1.15 G' を群，X を (G', G)-biset，Y を左 G 集合とする．このとき，$X \times_G Y$ は左 G' 集合となる．

証明 $(x, y)G = (x', y')G \in X \times_G Y$ とすると，ある $g \in G$ が存在して $(x, y) = (x'g, g^{-1}y)$ が成り立つ．このとき

$$\begin{aligned}(g'x, y)G &= (g'x'g, g^{-1}y')G \\ &= (g'x', y')G\end{aligned}$$

だから，G' の $X \times_G Y$ への作用を

$$g'(x, y)G = (g'x, y)G \quad ((x, y)G \in X \times_G Y,\ g' \in G')$$

で定められる． ■

定義 1.16 (Bouc [Bou10, 2.3.9])　$H \leq G$, $N \trianglelefteq G$ とする．

1. G 集合 X に対して，H 集合 $\mathrm{Res}^G_H X = G \times_G X$ を X の G から H への**制限** （restriction）と呼ぶ．ここで，G への左 H 作用，右 G 作用はどちらも G の積である．
2. H 集合 Y に対して，G 集合 $\mathrm{Ind}^G_H Y = G \times_H Y$ を Y の H から G への**誘導** （induction）と呼ぶ．ここで，G への左 G 作用，右 H 作用はどちらも G の積である．
3. G 集合 U に対して，G/N 集合 $\mathrm{Def}^G_{G/N} U = G/N \times_G U$ を U の G から G/N への deflation と呼ぶ．ここで，G/N への左 G/N 作用は G/N の積，右 G 作用は G/N への射影と積である．
4. G/N 集合 V に対して，G 集合 $\mathrm{Inf}^G_{G/N} V = G/N \times_{G/N} V$ を V の G/N から G への inflation と呼ぶ．ここで，G/N への左 G 作用は標準的な作用，右 G/N 作用は G/N の積である．

命題 1.17　$H \leq G$, $N \trianglelefteq G$ とする．

1. 任意の G 集合 (X, ρ) に対して，$\mathrm{Res}^G_H X \cong (X, \rho|_H)$ が成り立つ．
2. 任意の G 集合 U に対して，$\mathrm{Def}^G_{G/N} U \cong N\backslash U$ が成り立つ．
3. 任意の G/N 集合 (V, σ) に対して，$\mathrm{Inf}^G_{G/N} V \cong (V, \sigma \circ \pi)$ が成り立つ．ここで，$\pi\colon G \to G/N$ は自然な射影である．

命題 1.18　$H \leq G$ とする．

1. 任意の $K \leq G$ に対して，$\mathrm{Res}^G_H G/K \cong \bigsqcup_{HgK \in H\backslash G/K} H/(H \cap {}^gK)$ が成り立つ．
2. 任意の $L \leq H$ に対して，$\mathrm{Ind}^G_H H/L \cong G/L$ が成り立つ．
3. 任意の $K \leq G$ に対して，$\mathrm{Def}^G_{G/N} G/K = G/NK$ が成り立つ．
4. 任意の $M/N \leq G/N$ に対して，$\mathrm{Inf}^G_{G/N}(G/N)/(M/N) = G/M$ が成り立つ．

証明

1. 任意の $gK \in G/K$ と $h \in H$ に対して，

$$hgK = gK \iff h \in {}^gK$$

が成り立つから，gK の H 固定化群は $H \cap {}^gK$ である．また，任意の $gK, g'K \in G/K$ に対して，

$$\text{ある } h \in H \text{ が存在して } hgK = g'K \iff HgK = Hg'K$$

だから，

$$\mathrm{Res}^G_H G/K \cong \bigsqcup_{HgK \in H\backslash G/K} H/(H \cap {}^gK)$$

である．

■

命題 1.19　G-**set** における図式 $G/H \xrightarrow{\phi} G/L \xleftarrow{\psi} G/K$ に対して，$\phi(H) = aL$, $\psi(K) = bL$ としたとき，

$$\begin{array}{ccc} \bigsqcup_{HgK \in H\backslash aLb^{-1}/K} G/(H \cap {}^gK) & \xrightarrow{\pi_\phi} & G/K \\ {\scriptstyle \pi_\psi}\downarrow & & \downarrow{\scriptstyle \psi} \\ G/H & \xrightarrow[\phi]{} & G/L \end{array} \qquad \begin{aligned} &\pi_\phi(x(H \cap {}^gK)) = xg^{-1}K, \\ &\pi_\psi(x(H \cap {}^gK)) = xH \end{aligned}$$

は G-**set** における引き戻しである．

証明　直積のイコライザーを取ればよい．　■

命題 1.20　$H, K \leq G$ とする．任意の $H(gK) \in H\backslash(G/K)$ に対して，$|H(gK)| = (H : H \cap {}^gK)$ である．

証明　$H(gK) \cong H/H_{gK}$ であり，$H_{gK} = H \cap {}^gK$ である．したがって，$|H(gK)| = (H : H \cap {}^gK)$ が成り立つ．　■

命題 1.21　$\iota H \to G$ を包含写像とする．このとき，$\iota^{-1}\colon \mathbf{Set}^G \to \mathbf{Set}^H$ は Res^G_H である．さらに，$(\iota^{-1})^\dagger \cong \mathrm{Ind}^G_H$, $(\iota^{-1})^\ddagger \cong \mathrm{Hom}_{\mathbf{Set}^H}(G, -)$ が成り立つ．したがって，随伴

$$\mathrm{Ind}^G_H \dashv \mathrm{Res}^G_H \dashv \mathrm{Hom}_{\mathbf{Set}^H}(G, -)$$

が成り立つ．

証明　$\mathrm{Obj}(G) = \{\bullet\}$, $\mathrm{Obj}(H) = \{*\}$ とする．

$\rho\colon G \to \mathbf{Set}$ を G 集合とし，$\rho(\bullet) = X$ とする．このとき，$\iota^{-1}(\rho) = \rho \circ \iota$ であり，とすれば，

$$\iota^{-1}(\rho)(*) = X = \mathrm{Res}^G_H(X),$$
$$\iota^{-1}(\rho)(h) = \rho(h) = \rho|_H(h) = \mathrm{Res}^G_H(h)$$

が成り立つ．よって，$\iota^{-1} = \mathrm{Res}^G_H$ である．

$\sigma \in \mathbf{Set}^H$ を H 集合とし，$\sigma(*) = Y$ とする．**Set** は余完備なので，σ の ι^{-1} に沿った各点左 Kan 拡張 $(\iota^{-1})^\dagger\sigma$ が存在する．$P_0\colon \iota \downarrow \bullet \to H$ を $P_0(\langle *, g\rangle) = *$ とし，$T = \sigma \circ P_0$ とすれば，任意の $\langle *, g\rangle \in \iota \downarrow \bullet$ と $h \in \mathrm{Hom}_{\iota\downarrow\bullet}(\langle *, g_0\rangle, \langle *, g_1\rangle)$ に対して $T(\langle *, g\rangle) = \sigma(*) = Y$, $T(h) = \sigma(h)$ であり，

$$(\iota^{-1})^\dagger\sigma(\bullet) \cong \mathrm{colim}\, T$$

が成り立つ．このとき，$\mu\colon T \Rightarrow \Delta\,\mathrm{colim}\, T$ を普遍射とすれば，図式

$$\begin{array}{ccc} Y & \xrightarrow{\sigma(h)} & Y \\ & {\scriptstyle \mu_{g_0}}\searrow & \downarrow{\scriptstyle \mu_{g_1}} \\ & & \mathrm{colim}\, T \end{array}$$

が可換になる．$\langle \mathfrak{Y} = \bigsqcup_{g\in G} Y, \kappa_g\rangle$ を Y の $|G|$ 個の直和，$\mathfrak{Y}$ 上の 2 項関係 R を

$$y_{g_0} R y_{g_1} \iff \text{ある } h \in \mathrm{Hom}_{\iota\downarrow\bullet}(\langle *, g_0\rangle, \langle *, g_1\rangle) \text{ が存在して } \sigma(h)(y_{g_0}) = y_{g_1} \text{ が成り立つ}$$

とし，R を含む最小の同値関係を $\sim$ と置けば，一般論より $\operatorname{colim} T \cong \mathfrak{Y}/\sim$ である．さらに，$\mathfrak{Y} \cong G \times Y$ が $y_g \mapsto (g, y)$ で定まり，この同型により R から誘導される 2 項関係 R_H は，$h \in \mathrm{Hom}_{\iota\downarrow\bullet}(\langle *, g_0\rangle, \langle *, g_1\rangle)$ と $h = {g_1}^{-1} g_0$ が同値であることを用いて

$$(g_0, y) R_H (g_1, y') \iff {g_1}^{-1} g_0 \in H \text{ かつ } \sigma({g_1}^{-1} g_0)(y) = y' \text{ が成り立つ}$$

となる[4]．したがって，任意の $(g, y) \in G \times Y$ と $h \in H$ に対して

$$(g, \sigma(h)(y)) = (g, \sigma(g^{-1}gh)(y)) R_H (gh, y) \tag{1.3}$$

が成り立つ．よって，R_H を含む最小の同値関係 $\sim_H$ は式 (1.3) を満たしている．したがって，$\operatorname{colim} T \cong (G \times Y)/\sim_H = \mathrm{Ind}_H^G Y$ が成り立つ． ■

1.13 群の性質を測る指標

G を有限群とする．F を，G の部分群全体の集合 $\mathrm{S}(G)$ からそれ自身への写像とし，μ を $\mathrm{S}(G)$ から $\mathbb{R}$ への単調写像とする．任意の部分群 $H \leq G$ に対して $H \leq F(H)$ が成り立つとき，写像 $c^F(\mu)\colon \mathrm{S}(G) \setminus \{G\} \to [0, 1]$ を

$$c^F(H) = \frac{\mu F(H) - \mu H}{\mu G - \mu H}$$

で定める．このとき，有理数 $a \in \mathbb{Q}$ に対して，G の部分集合の族 $\mathcal{X}^F(a)$ を

$$\mathcal{X}^F(a) = \{\, H \leq G \,|\, c^F(H) = a \,\}$$

と置く．また，任意の部分群 $H \leq G$ に対して $(H) \leq H$ が成り立つとき，写像 $c_F(\mu)\colon \mathrm{S}(G)\setminus\{\mathbf{1}\} \to [0, 1]$ を，先ほどと同様に

$$c_F(H) = \frac{\mu F(H) - \mu H}{\mu \mathbf{1} - \mu H}$$

で定める．このとき，有理数 $a \in \mathbb{Q}$ に対して，G の部分集合の族 $\mathcal{X}_F(a)$ を

$$\mathcal{X}_F(a) = \{\, H \leq G \,|\, c_F(H) = a \,\}$$

と置く．

例 1.22 $\mu(H) = |H|$ とする．$F(H) = \mathrm{N}_G(H)$ と置くと，

$$\mathcal{X}^F(0) = \{\, H < G \,|\, H\colon \text{self-normalizing in } G \,\},$$
$$\mathcal{X}^F(1) = \{\, H < G \,|\, H\colon \text{normal in } G \,\}$$

4) 分かりやすく書けば，$(g_0, y) R_H (g_1, \sigma({g_1}^{-1} g_0)(y))$ である．

である．$F(H) = [H, H]$ と置くと，

$$\mathcal{X}^F(0) = \{\, H \leq G \,|\, H\text{: perfect group}, H \neq \mathbf{1} \,\},$$
$$\mathcal{X}^F(1) = \{\, H \leq G \,|\, H\text{: Abelian group}, H \neq \mathbf{1} \,\}$$

である．

1.14 variety of groups [Mat]

定義 1.23 $\mathfrak{V}$ を群からなる空でないクラスとする[5]．$\mathfrak{V}$ が部分群，準同型像，直積について閉じているとき，$\mathfrak{V}$ を variety of groups という．

$\mathfrak{V}$ は自明群 $\mathbf{1}$ を含む．実際，$G \in \mathfrak{V}$ を取れば，$\mathbf{1} \cong G/G \in \mathfrak{V}$ である．

命題 1.24 G を群，$\mathfrak{V}$ を variety of group とする．このとき，$\mathfrak{V}(G) \trianglelefteq G$ であって，$G/\mathfrak{V}(G) \in \mathfrak{V}$ かつ，$G/N \in \mathfrak{V}$ となる G の正規部分群 N の中で最小となるようなものがただ一つ存在する．

証明

$$\mathfrak{V}(G) = \bigcap_{G/N \in \mathfrak{V}} N$$

とおくと，$\mathfrak{V}(G) \trianglelefteq G$ である．各 $N \trianglelefteq G$ に対して，自然な射影を $\pi_N \colon G \to G/N$ とおき，$\pi = (\pi_N)_{G/N \in \mathfrak{V}} \colon G \to \prod_{G/N \in \mathfrak{V}} G/N$ とする．$\operatorname{Ker}\pi = \mathfrak{V}(G)$ なので，準同型定理より単射 $G/\mathfrak{V}(G) \to \prod_{G/N \in \mathfrak{V}} G/N$ が存在する．$\prod_{G/N \in \mathfrak{V}} G/N \in \mathfrak{V}$ だから，$G/\mathfrak{V}(G) \in \mathfrak{V}$ である．

また，$G/N \in \mathfrak{V}$ となる任意の $N \trianglelefteq G$ に対して，$\mathfrak{V}(G)$ はそのような N の共通部分だから，$\mathfrak{V}(G) \leq N$ である．唯一性もここから分かる． ■

定義 1.25 $\mathfrak{P}$ を群からなる空でないクラスとする[6]．$\mathfrak{P}$ が部分群，準同型像，有限直積について閉じているとき，$\mathfrak{P}$ を pseudovariety of groups という．

pseudovariety of groups に対しても，命題 1.24 と同様の結果が成り立つ．

命題 1.26 G を有限群, $\mathfrak{P}$ を variety of group とする．このとき, $\mathfrak{P}(G) \trianglelefteq G$ であって, $G/\mathfrak{P}(G) \in \mathfrak{P}$ かつ，$G/N \in \mathfrak{P}$ となる G の正規部分群 N の中で最小となるようなものがただ一つ存在する．

証明 命題 1.24 の証明と同様である． ■

5) $\mathfrak{V}$ はフラクトゥールにおける V である．
6) $\mathfrak{P}$ はフラクトゥールにおける P である．

例 1.27　π を素数の集合とする．O^π を π 可解群[7]全体から成るクラスとすると，これは pseudovariety of groups である．したがって，命題 1.26 より，任意の有限群 G に対して，$G/O^\pi(G)$ が π 可解群となるような最小の $O^\pi(G) \trianglelefteq G$ がただ一つ存在する．

1.15　skew brace の作用（試み）

定義 1.28 (Guarnieri and Vendramin [GV17, Definition 1.1])　A を集合，$\cdot, \circ$ を A 上の 2 項演算とする．組 $\langle A, \cdot, \circ\rangle$ が skew (left) brace であるとは，以下の条件を満たすことを言う：

1. $\langle A, \cdot\rangle, \langle A, \circ\rangle$ は群である．
2. 任意の $a, b, c \in A$ に対して
$$a \circ (b \cdot c) = (a \circ b) \cdot a^{-1} \cdot (a \circ c)$$
が成り立つ．ここで，a^{-1} は a の $\langle A, \cdot\rangle$ における逆元を表す．

以下，$A = \langle A, \cdot, \circ\rangle$ は skew brace を表すことにする．$a \in A$ の $\langle A, \circ\rangle$ における逆元は $\bar{a}$ で表す．$\langle A, \cdot\rangle$ を A の**加法群**（additive group），$\langle A, \circ\rangle$ を A の**乗法群**（multiplicative group）と呼ぶ．加法群が可換群であるような skew brace を brace と呼び，Yang-Baxter 方程式の集合論的対合解 (set-theoretical involutive solution) の研究の中で Rump [Rum07] が定義した．

$a, b \in A$ に対して，a から $a \cdot b$ を得ることを，a に右から b を足す，加えると言い表す．また，a から $a \circ b$ を得ることを，a に右から b を掛ける，乗じると言い表す．

$a \cdot b$ を ab で表すことがある．

命題 1.29　A の加法群と乗法群の単位元は一致する．

証明　$1 \in \langle A, \cdot\rangle$ を加法群の単位元とすると，任意の $a \in A$ に対して

$$\begin{aligned} a \circ 1 &= a \circ (1 \cdot 1) \\ &= (a \circ 1)a^{-1}(a \circ 1) \end{aligned}$$

が成り立つ．この式の両辺に右から $(\overline{a \circ 1})a$ を加えると，$a = a \circ 1$ を得る．よって，1 は $\langle A, \circ\rangle$ の単位元である．■

定義 1.30　$a \in A$ とする．A から A 自身への写像 $\lambda_a, {\lambda^{\mathrm{op}}}_a$ を，それぞれ

$$\begin{aligned} \lambda_a(b) &= a^{-1}(a \circ b), \\ {\lambda^{\mathrm{op}}}_a(b) &= (a \circ b)a^{-1} \end{aligned}$$

と置く．

7)　可解な π 群のことである．

命題 1.31　任意の $a \in A$ に対して，$\lambda_a, {\lambda^{\mathrm{op}}}_a \in \mathrm{Aut}(\langle A, \cdot \rangle)$ である．

証明　任意の $x, y \in A$ に対して，

$$\begin{aligned} \lambda_a(xy) &= a^{-1}(a \circ xy) \\ &= a^{-1}(a \circ x)a^{-1}(a \circ y) \\ &= \lambda_a(x)\,\lambda_a(y), \\ {\lambda^{\mathrm{op}}}_a(xy) &= (a \circ xy)a^{-1} \\ &= (a \circ x)a^{-1}(a \circ y)a^{-1} \\ &= {\lambda^{\mathrm{op}}}_a(x)\,{\lambda^{\mathrm{op}}}_a(y) \end{aligned}$$

が成り立つから，$\lambda_a, {\lambda^{\mathrm{op}}}_a \in \mathrm{End}(\langle A, \cdot \rangle)$ である．また，$x \mapsto \overline{a} \circ (ax), x \mapsto \overline{a} \circ (xa)$ がそれぞれ $\lambda_a, {\lambda^{\mathrm{op}}}_a$ の逆写像となるから，$\lambda_a, {\lambda^{\mathrm{op}}}_a \in \mathrm{Aut}(\langle A, \cdot \rangle)$ である． ■

命題 1.32　$\langle A, \circ \rangle$ から $\mathrm{Aut}(\langle A, \cdot \rangle)$ への群準同型写像 $\lambda, \lambda^{\mathrm{op}}$ が

$$\lambda(a) = \lambda_a, \quad \lambda^{\mathrm{op}}(a) = {\lambda^{\mathrm{op}}}_a$$

で定まる．

証明　簡単． ■

λ を lambda map と呼ぶことがある [KT24]．

定義 1.33　$I \subset A$ は部分集合とする．任意の $a \in A$ に対して $\lambda_a(I) \subseteq I$ を満たすとき，I は A の左イデアルであるという．

定義 1.34　$I \subseteq A$ が A の**イデアル**（ideal）であるとは，次の条件を満たすことを言う：

1. I は $\langle A, \cdot \rangle, \langle A, \circ \rangle$ の正規部分群である．
2. 任意の $a \in A$ に対して，$\lambda_a(I) \subseteq I$ が成り立つ．

$B \subseteq A$ が定義 1.34.2 を満たすとき，B は A 内で安定していると言うことにする．

定義 1.35　$H \subseteq A$ が $\langle A, \cdot \rangle, \langle A, \circ \rangle$ の部分群であり，かつ A 内で安定しているとき，H を A の半イデアルと呼ぶ．また，$Q \subseteq A$ が $\langle A, \cdot \rangle$ の部分群であり，かつ A 内で安定しているとき，Q を A の準イデアルと呼ぶ．

明らかに，イデアルは半イデアルであり，半イデアルは準イデアルである．

命題 1.36　A を skew brace とし，$Q \subseteq A$ を A の準イデアルとする．

1. 任意の $a \in A$ に対して，$aQ = a \circ Q$ が成り立つ．
2. Q が半イデアルのとき，$\langle Q, \cdot, \circ \rangle$ は skew brace である．また，加法群としての自然な射影 $\pi\colon A \to A/Q$ は，乗法群の準同型となる．
3. Q がイデアルのとき，$\langle A/Q, \cdot, \circ \rangle$ は skew brace である．

証明　$\lambda_a(Q) \subseteq Q$ の両辺に左から a を加えて $a \circ Q \subseteq aQ$ を得る．さらに，左から $\overline{a}$ を乗じて $Q \subseteq \overline{a} \circ aQ = (\overline{a})^{-1}(\overline{a} \circ Q)$ を得る．左から $\overline{a}$ を加えて $\overline{a}Q \subseteq \overline{a} \circ Q$ を得る．この式の a を $\overline{a}$ に取り換えれば，$aQ \subseteq a \circ Q$ を得る．■

定義 1.37　X を集合とする．群準同型写像 $\beta\colon \langle A, \cdot \rangle \to \mathrm{Iso}(X)$，$\rho\colon \langle A, \circ \rangle \to \mathrm{Iso}(X)$ が，任意の $a, b \in A$ に対して，関係式

$$\beta(\lambda^{\mathrm{op}}{}_a(b)) = {}^{\rho(a)}\beta(b) \tag{1.4}$$

を満たすとき，組 $\langle X, \beta, \rho \rangle$ を（左）A 集合という．

$X = \langle X, \beta, \rho \rangle$ を A 集合とする．任意の $a \in A$, $x \in X$ に対して，$ax = \beta(a)(x)$, $a \circ x = \rho(a)(x)$ と書くことがある．brace relation をこの記法で表すと

$$(a \circ b)a^{-1}x = a \circ (b(\overline{a} \circ x)) \quad (x \in X)$$

となる．

命題 1.38　X は $\langle A, \cdot \rangle$ 集合であり，かつ $\langle A, \circ \rangle$ 集合でもあるとする．このとき，以下は同値である．

1. 任意の $a, b \in A$ に対して式 (1.4) が成り立つ．したがって，X は A 集合である．
2. 任意の $a, b \in A$ と $x \in A$ に対して

$$a \circ bx = (a \circ b)a^{-1}(a \circ x)$$

が成り立つ．

証明　式 (1.4) を変形すれば $\rho(a)\beta(b) = \beta(\lambda^{\mathrm{op}}{}_a(b))\rho(a)$ を得る．■

A は自然に A 集合となる．実際，2 つの写像 $\beta_{\mathrm{reg}}\colon \langle A, \cdot \rangle \to \mathrm{Iso}\, X$, $\rho_{\mathrm{reg}}\colon \langle A, \circ \rangle \to \mathrm{Iso}\, X$ を

$$\begin{cases} \beta_{\mathrm{reg}}(a)(x) = ax, \\ \rho_{\mathrm{reg}}(a)(x) = a \circ x \end{cases}$$

で定めれば，これらは明らかに群準同型写像であり，さらに，任意の $a, b, x \in A$ に対して

$$\begin{aligned} a \circ (b(\overline{a} \circ x)) &= (a \circ b)a^{-1}(a \circ \overline{a} \circ x) \\ &= (a \circ b)a^{-1}x \end{aligned}$$

が成り立つ．したがって，$\langle A, \beta_{\mathrm{reg}}, \rho_{\mathrm{reg}} \rangle$ は A 集合である．一般に，$Q \subseteq A$ を準イデアルとしたとき，A/Q は同様の方法で A 集合となる．

X が $\langle A, \circ \rangle$ 集合として推移的であるとする．このとき，$\langle A, \circ \rangle$ 集合として $X \cong \langle A, \circ \rangle / H$ ($H \leq \langle A, \circ \rangle$) であり，$\langle A, \cdot \rangle$ 集合としての軌道分解

$$\langle A, \circ \rangle / H \cong \bigsqcup_{x \in (\langle A, \cdot \rangle \backslash X)} Ax \cong \bigsqcup_{x \in (\langle A, \cdot \rangle \backslash X)} A/A_x$$

が得られる．

1.16 braiding 作用素を持つ群と skew brace

定義 1.39 Z を集合とする．全単射 $r\colon Z \times Z \to Z \times Z$ が**ブレイド関係式を満たす**（satisfies braiding relation）とは，等式

$$(r \times \mathrm{id}_Z)(\mathrm{id}_Z \times r)(r \times \mathrm{id}_Z) = (\mathrm{id}_Z \times r)(r \times \mathrm{id}_Z)(\mathrm{id}_Z \times r) \tag{BRel}$$

が成り立つことをいう．

定義 1.40 $\langle A, \circ \rangle$ を群とする．$r\colon A \times A \to A \times A$ が A 上の**ブレイド作用素**（braiding operator）であるとは，以下の等式たちを満たすことを言う：

$$\begin{gathered} r(\circ \times \mathrm{id}_A) = (\mathrm{id}_A \times \circ)(r \times \mathrm{id}_A)(\mathrm{id}_A \times r), \\ r(\mathrm{id}_A \times \circ) = (\circ \times \mathrm{id}_A)(\mathrm{id}_A \times r)(r \times \mathrm{id}_A), \\ r(\mathrm{id}_A \times \eta) = \eta \times \mathrm{id}_A, \qquad r(\eta \times \mathrm{id}_A), = \mathrm{id}_A \times \eta \\ \circ r = \circ. \end{gathered}$$

ここで，$\eta\colon \mathbf{1} \to A$ はただ一つ存在する群準同型写像である．また，このとき，組 $\langle A, \circ, r \rangle$ を**ブレイド作用素を持つ群**（group with a braiding operator）と呼ぶ．

補題 1.41 $\langle A, \circ, r \rangle$ をブレイド作用素を持つ群とする．このとき，r は全単射かつ，ブレイド関係式を満たす．

2 リレーショナルデータベースまとめ

リレーショナルデータベースの設計について，自分なりに理解しやすいようにまとめようと思う．

定義 2.1　$\mathcal{A} = \{A_1, \ldots, A_n\}$ $(n \in \mathbb{Z}_{\geq 0})$ を集合とし，$F \subseteq \{\, f \mid \operatorname{dom} f \subseteq \prod_{i=1}^{n} A_i \,\}$ とする．組 $\langle \mathcal{A}, F \rangle$ を**リレーションスキーマ**（relation schema）と呼び，$\mathcal{R}(\mathcal{A})$ または単に $\mathcal{R}$ で表す．また，このとき，各 $A_i \in \mathcal{A}$ を $\mathcal{R}$ の**属性名**（attribute name）と呼ぶ．

以下，属性名の集合 $\mathcal{A}$ と，$\mathcal{A}$ 上のリレーションスキーマ $\mathcal{R}(\mathcal{A})$ を固定する．

定義 2.2　$\mathcal{R}(\mathcal{A})$ を $\mathcal{A}$ 上のリレーションスキーマとする．点付き集合 $\langle D_i, A_i \rangle$ $(1 \leq i \leq n)$ と，部分集合 $\langle R, (A_1, \ldots, A_n) \rangle \subseteq \prod_{i=1}^{n} \langle D_i, A_i \rangle$ の組 $\langle R, D_1, \ldots, D_n \rangle$ を，$\mathcal{R}(\mathcal{A})$ の**インスタンス**（instance）と呼び，$R(\mathcal{A})$ または単に R で表す．また，このときの R を**テーブル名**（table name），各 D_i を**ドメイン**（domain）と呼ぶ．

リレーションスキーマ $\mathcal{R}(\mathcal{A})$ のインスタンス R の各ドメイン D_i を，D_i の基点である属性名 A_i を用いて $\operatorname{dom} A_i$ と表すことがある．

定義 2.3

3 Biset Functors for Finite Groups [Bou10]

命題 3.1 (Proposition 5.6.1)　任意の有限群 G に対して，

$$m_{G,G} = \begin{cases} \dfrac{\varphi(|G|)}{|G|} & (G\text{: cyclic}) \\ 0 & (\text{otherwise}) \end{cases}$$

が成り立つ．

証明　定義より，

$$\begin{aligned} m_{G,G} &= \frac{1}{|G|} \sum_{X \leq G} |X|\, \mu(X, G) \\ &= \frac{1}{|G|} \sum_{X \leq G} \sum_{x \in X} \mu(X, G) \end{aligned}$$

が成り立つ．集合として

$$\begin{aligned} \bigsqcup_{X \leq G} \{\, x \mid x \in X \,\} &\cong \{\, (x, X) \mid x \in X \leq G \,\} \\ &\cong \bigsqcup_{x \in G} \{\, X \mid \langle x \rangle \leq X \leq G \,\} \end{aligned}$$

が成り立つから，

$$\frac{1}{|G|}\sum_{X\leq G}\sum_{x\in X}\mu(X,G)=\frac{1}{|G|}\sum_{x\in G}\sum_{\langle x\rangle\leq X\leq G}\mu(X,G).$$

式 (1.1) より，

$$\begin{aligned}\frac{1}{|G|}\sum_{x\in G}\sum_{\langle x\rangle\leq X\leq G}\mu(X,G)&=\frac{1}{|G|}\sum_{x\in G}\delta_{\langle x\rangle,G}\\&=\begin{cases}\dfrac{\varphi(|G|)}{|G|} & (G\text{: cyclic})\\ 0 & (\text{otherwise})\end{cases}.\end{aligned}$$

■

4 Atiyah–MacDonald 可換代数入門 [AM06]

本章では，環と言えば単位的可換環を指す．

命題 4.1 (p. 16; 演習問題 1)　A を環とする．任意の冪零元 $x\in A$ と単元 $u\in A$ に対して，$u+x$ は A における単元である．

証明　$x^m=0$ であるとすれば，

$$(u+x)\sum_{i=0}^{m-1}(-u^{-1}x)^i=u$$

である．したがって，$u^{-1}\sum_{i=0}^{m-1}(-u^{-1}x)^i=(u+x)^{-1}$ である． ■

証明　$\mathfrak{N}$ を A の冪零元根基，$\mathfrak{R}$ を A の Jacobson 根基とすると，$-x\in\mathfrak{N}\subseteq\mathfrak{R}$ が成り立つ．任意の $y\in\mathfrak{R}$ と $a\in A$ に対して，$1-ay$ は単元である [AM06, 命題 1.9] から，$1+x=1-(-x)$ は単元である． ■

命題 4.2 (p. 16; 演習問題 2)　A を環とし，$f=\sum_{i=0}^{n}a_ix^i\in A[x]$ $(a_n\neq 0)$ とする．

1. f が $A[x]$ において可逆であることは，a_0 が A における単元かつ $a_1,\ldots,a_n$ が冪零元であることと同値である．
2. f が冪零元であることと，$a_0,\ldots,a_n$ が冪零元であることは同値である．

証明

1. a_0 が $A[x]$ において可逆かつ $a_1,\ldots,a_n$ が冪零元ならば，命題 4.1 より，f は単元である．そこで，逆を $\deg f=n$ に関する帰納法で示す．$n=0$ のときは明らか．$n\neq 0$ とし，次数が n 未満の任意の多項式に対して示すべき命題が成り立つと仮定する．f が $A[x]$ において可逆で

あるとすると，f の逆元 $g = \sum_{j=0}^{m} b_j x^j \in A[x]$ が存在する．fg の定数項は $a_0 b_0 = 1$ だから，a_0 は単元である．

ここで，任意の m 以下の正整数 r に対して ${a_n}^{r+1} b_{m-r} = 0$ が成り立つことを，r に関する帰納法で示す．$r = 0$ のとき，fg の $m+n$ 次の係数に注目すれば，$a_n b_m = 0$ を得る．さらに，$m-1$ 以下の任意の正整数 r に対して ${a_n}^{r+1} b_{m-r} = 0$ であると仮定すれば，$m+n-(r+1)$ 次の係数

$$\sum_{i+j=m+n-(r+1)} a_i b_j = a_n b_{m-(r+1)} + (b_{m-r}, b_{m-(r-1)}, \ldots, b_0 \text{ の 1 次結合})$$

に ${a_n}^{r+1}$ を乗じることで ${a_n}^{r+2} b_{m-(r+1)} = 0$ を得る．

特に，${a_n}^{m+1} b_0 = 0$ であるから，この式の両辺に a_0 を乗じて ${a_n}^{m+1} = 0$ を得る．したがって，a_n は冪零元である．$n = 1$ ならこの時点で証明は完了する．$n > 1$ のとき，命題 4.1 から $f - a_n x^n$ は単元であり，$\deg(f - a_n x^n) = n - 1$ であるから，帰納法の仮定により，$a_{n-1}, \ldots, a_1$ は冪零元である．

2. a_i $(0 \leq i \leq n)$ が冪零ならば，f は冪零元の和なので冪零である．逆を $\deg f$ に関する帰納法で示すために，$f^s = 0$ とする．$\deg f = 0$ のときは明らか．そこで，$\deg f > 0$ とし，次数が $\deg f$ 未満であるすべての多項式に対して示すべきことが成り立つと仮定する．f^s の sn 次の係数は ${a_n}^{sn} = 0$ なので，a_n は冪零である．よって，$f - a_n x^n$ も冪零なので，帰納法の仮定から $a_0, \ldots, a_{n-1}$ も冪零となる． ■

命題 4.3 (p. 19; 演習問題 15)　A を環，X を A の素イデアル全体の集合とする．任意の $E \subseteq A$ に対して，$V(E) = \{\, \mathfrak{p} \in X \mid E \subseteq \mathfrak{p} \,\}$ と置く．このとき，以下を満たす．

1. 任意の $E \subseteq A$ に対して，$\mathfrak{a} = (E)$ と置けば，$V(E) = V(\mathfrak{a}) = V(\mathrm{r}(\mathfrak{a}))$ が成り立つ．つまり，

$$\{\, V(E) \mid E \subseteq A \,\} = \{\, V(\mathfrak{a}) \mid \mathfrak{a} \text{ は } A \text{ のイデアル} \,\}$$

が成り立つ．

2. $V(0) = X,\ V((1)) = \emptyset$ である．
3. 任意の A のイデアルの族 $\{\mathfrak{a}_i\}_{i \in I}$ に対して，

$$\bigcap_{i \in I} V(\mathfrak{a}_i) = V\left(\bigcup_{i \in I} \mathfrak{a}_i \right)$$

が成り立つ．

4. 任意のイデアル $\mathfrak{a}, \mathfrak{b} \subseteq A$ に対して，$V(\mathfrak{a}) \cup V(\mathfrak{b}) = V(\mathfrak{a} \cap \mathfrak{b}) = V(\mathfrak{a}\mathfrak{b})$ が成り立つ．

証明

1. $E \subseteq \mathfrak{a} \subseteq \mathrm{r}(\mathfrak{a})$ より，$V(E) \supseteq V(\mathfrak{a}) \supseteq V(\mathrm{r}(\mathfrak{a}))$ だから，$V(E) \subseteq V(\mathrm{r}(\mathfrak{a}))$ を示せば十分である．任意に $\mathfrak{p} \in V(E)$ を取る．任意の $x \in \mathrm{r}(\mathfrak{a})$ に対して，$x^n \in \mathfrak{a}$ となる正整数 n が存在する．$\mathfrak{a}$ の最

小性より $\mathfrak{a} \subseteq \mathfrak{p}$ であり，かつ $\mathfrak{p}$ は素イデアルなので，$x \in \mathfrak{p}$ が分かる．したがって，$\mathrm{r}(\mathfrak{a}) \subseteq \mathfrak{p}$ であり，つまり $\mathfrak{p} \in V(\mathrm{r}(\mathfrak{a}))$ である．

2. 明らか．
3. $\mathfrak{p}$ をイデアルとしたとき，任意の $i \in I$ に対して $\mathfrak{a}_i \subseteq \mathfrak{p}$ であることと，$\bigcup_{i \in I} \mathfrak{a}_i \subseteq \mathfrak{p}$ であることは同値である．
4. $\mathfrak{p}$ を素イデアルとしたとき，$\mathfrak{a} \cap \mathfrak{b} \subseteq \mathfrak{p}$ ならば，$\mathfrak{a} \subseteq \mathfrak{p}$ または $\mathfrak{b} \subseteq \mathfrak{p}$ が成り立つ [AM06, pp. 11-12; 命題 1.11.ii] ので，$V(\mathfrak{a}) \cup V(\mathfrak{b}) = V(\mathfrak{a} \cap \mathfrak{b})$ が分かる．あとは，$V(\mathfrak{ab}) \subseteq V(\mathfrak{a}) \cup V(\mathfrak{b})$ を示せばよい．そのために，任意に $\mathfrak{p} \in V(\mathfrak{ab})$ を取り，$\mathfrak{b} \not\subseteq \mathfrak{p}$ であるとする．このとき，$x \in \mathfrak{b} \setminus \mathfrak{p}$ が存在する．この x と任意の $a \in \mathfrak{a}$ に対して $ax \in \mathfrak{ab} \subseteq \mathfrak{p}$ が成り立つが，$\mathfrak{p}$ は素イデアルだから，$a \in \mathfrak{p}$ でなければならない．したがって，$\mathfrak{a} \subseteq \mathfrak{p}$ を得る． ■

参考文献

[AM06] M. F. Atiyah and I. G. MacDonald, *Atiyah–MacDonald* **可換代数入門**, 共立出版, February 2006.

[Bou10] Serge Bouc, *Biset functors for finite groups*, Lecture Notes in Mathematics, vol. 1990, Springer-Verlag, Berlin, 2010. MR 2598185

[CH53] R. Courant and D. Hilbert, *Methods of mathematical physics. Vol. I*, Interscience Publishers, Inc., New York, 1953. MR 65391

[GAP] *GAP - Reference Manual*, `https://docs.gap-system.org/doc/ref/chap0.html`.

[GV17] L. Guarnieri and L. Vendramin, *Skew braces and the Yang-Baxter equation*, Mathematics of Computation **86** (2017), no. 307, 2519–2534. MR 3647970

[Het07] Gábor Hetyei, *The Möbius function of a partially ordered set*, Lecture material distributed in the University of North Carolina at Charlotte, `https://webpages.charlotte.edu/ghetyei/courses/old/S07.3166/mobius.pdf`, 2007.

[KT24] Yuta Kozakai and Cindy Tsang, *Representation theory of skew braces*, 2024.

[Mat] *Abstract algebra - Smallest normal subgroup such that the factor group is a p-group*, `https://math.stackexchange.com/questions/4504722/smallest-normal-subgroup-such-that-the-factor-group-is-a-p-group`.

[Rum07] Wolfgang Rump, *Braces, radical rings, and the quantum Yang-Baxter equation*, Journal of Algebra **307** (2007), no. 1, 153–170. MR 2278047

[Yos90] Tomoyuki Yoshida, *The generalized Burnside ring of a finite group*, Hokkaido Mathematical Journal **19** (1990), no. 3, 509–574. MR 1078504

[小 22] 文仁 小田, **有限群のバーンサイド環**, 近畿大学大学院 群論特論 配布資料, 2022.