準同型の数え上げ

真中遥道
@GirlwithAHigoi

最終更新：2024 年 6 月 20 日

本稿の内容

院試対策をしていたところ，次のような問題があった．

問題 1.

p を素数とし，$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ を位数 p の有限体とする．行列の乗法による群 G を

$$G = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \middle| a, b, c \in \mathbb{F}_p \right\}$$

で定める．このとき，G から乗法群 $\mathbb{C}^\times = \mathbb{C} \setminus \{0\}$ への準同型写像の個数を求めよ．

（京大院　理・数学　2018 年度　院試 [1]）

本稿ではこのような準同型の数え上げの問題を解く方法を解説する．具体的には次のような問題を考える．

問題 2.

有限生成群 G から群 H への準同型の個数を求めよ．

1　関係群からの準同型の数え上げ

まず，生成元と関係式で定義された群（以後，関係群[*1]と呼ぶ）からある群への準同型の数え上げ問題について考える．まず関係群の基本的な性質を復習する．関係群の定義は本稿の **4 省略した証明**を参照せよ．

[*1] 一般的な用語ではない．任意の群はある関係群と必ず同型になるので，厳密な意味ではこの用語に意味はないかも知れない．しかし（定義にあるような）具体的な表示で与えられている群を考える，という場面はよくあり，そういう意味では実用的な用語である．

命題 3.

$X=\{x_1,\dots,x_n\}$ を生成元の集合，$R=\{R_i(x_1,\dots,x_n)=1 \mid i=1,\dots,m\}$ を関係式の集合とし，$G=\langle X \mid R\rangle$ とおく．H を群とする．写像 $f:X\to H$ であって $i=1,\dots,m$ に対して $R_i(f(x_1),\dots,f(x_n))=1$ なるものの集合を M とおく．任意の $f\in M$ に対して

$$\widetilde{f}(x_{i_1}\cdots x_{i_k})=f(x_{i_1})\cdots f(x_{i_k})$$

と $\widetilde{f}:G\to H$ を定めるとこれは準同型となり，逆に任意の準同型 $G\to H$ はこのようにして得られる．すなわちこの対応により M と $\mathrm{Hom}(G,H)$ は一対一に対応する．

（証明は最後に与える）つまり，関係群からの準同型を作るには，**関係式を満たすように生成元の行き先を決定すれば良い．**これを用いて準同型を数え上げてみよう．

例 4. 準同型 $f:\langle x,y \mid x^2=y^3=1\rangle\to\mathbb{C}^\times$ の個数を求める．$f(x),f(y)$ を決定すれば f は決定される．$x^2=y^3=1$ より $f(x)^2=f(y)^3=1$，つまり $f(x)=\pm1, f(y)=1,\omega,\omega^2$ であることが必要．（ただし ω は 1 の原始三乗根）逆にこのように決定すれば命題 3 より f は準同型となる．よって求める個数は $2\times3=6$ 個.

例 5. 準同型 $f:\langle x,y \mid xy^2=1\rangle\to\mathbb{Z}/n\mathbb{Z}$ の個数を求める．$f(x),f(y)$ を $f(x)+2f(y)=0$ となるように決定すればよい．$f(y)$ を自由に決めると条件を満たす $f(x)$ が一つに定まる．よって求める個数は n 個.

演習 6.

準同型 $f:\langle x,y \mid x^3=1, x^2y=y^3x\rangle\to D_6$ の個数を求めよ．（ただし D_6 は 6 次の二面体群である）

（解答） $f(x),f(y)$ を $f(x)^3=1, f(x)^2f(y)=f(y)^3f(x)$ を満たすように決定すれば準同型が一つ定まり，すべての準同型はこの方法によって実現される．よって $f(x),f(y)$ の決定の仕方を数え上げれば良い．$t^2=r^6=1, trt=r^{-1}$ なる $t,r\in D_6$ を用いて $D_6=\{t^ir^j \mid i=0,1,\ j=0,\dots,5\}$ と表せ，この表示は一意的であることに注意する．$f(x)=t^ir^j, f(y)=t^kr^l$ とおく．$f(x)^3=1$ より $(t^ir^j)^3=t^ir^{((-1)^i+2)j}=1$ ゆえ $i=0$ かつ $3j\equiv0 \mod 6$ である．$f(x)^2f(y)=f(y)^3f(x)$ より

$$\begin{aligned} r^{2j}t^kr^l &= (t^kr^l)^3r^j \\ t^kr^{(-1)^k2j+l} &= t^kr^{((-1)^k+2)l+j} \end{aligned}$$

ゆえ $k=0$ かつ $j\equiv2l \mod 6$, または $k=1$ かつ $l=j$ である．したがって $f(x),f(y)$ が条件を満たすには，$i=0$ と

$$k=0 \text{ かつ } j\equiv2l \mod 6, \text{ または } k=1 \text{ かつ } l=j=0,2,4$$

が必要で，逆にこのとき条件を満たす．よって求める個数は $6+3=9$ 個.

2　同型な関係群の見つけ方

一般の場合を考える．関係群の場合に帰着できれば良いので，同型な関係群の見つけ方について解説する．次の方法は万能ではないだろうが実践的には有用である．

同型な関係群の見つけ方

1. 生成元を見つける．
2. 生成元の関係式を調べる．
3. 関係群を定義し，同型な群であることを示す．

具体例を用いて解説していく．

例 7. $G = \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.

1. 生成元を見つける．
   $(a,b) = a(1,0) + b(0,1)$ ゆえ $(1,0),(0,1)$ が生成元として取れる．
2. 生成元の関係式を調べる．
   $n(1,0) = (0,0), m(0,1) = (0,0), (1,0)+(0,1) = (0,1)+(1,0)$ である．
3. 関係群を定義し，同型な群であることを示す．
   上で調べたことをもとに，$H = \langle x, y \mid x^n = y^m = 1, xy = yx \rangle$ と定める．まず $(1,0),(0,1)$ は関係式を満たす G の生成元ゆえ，全射準同型 $f : H \to G$ が存在する．よって $|H| \geq |G| = nm$．また H の元は関係式より $x^i y^j (i = 0,\ldots,n-1,\ j = 0,\ldots,m-1)$ と表せる．よって $|H| \leq nm$．したがって f は同型で $G \cong H$ である．

例 8. $G = \left\{ \begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix} \middle| a, b \in \mathbb{F}_p, b \neq 0 \right\}$．（ただし p は素数）

1. 生成元を見つける．
   $M(a,b) = \begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix}$ とおく．

$$\begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix} \begin{pmatrix} 1 & c \\ 0 & d \end{pmatrix} = \begin{pmatrix} 1 & ad+c \\ 0 & bd \end{pmatrix}$$

   より $M(a,b)M(c,d) = M(ad+c, bd)$ であるので，

$$M(1,1)^a = M(a,1), \quad M(0,b)^n = M(0,b^n)$$

   である．$\mathbb{F}_p^\times$ は位数 $p-1$ の巡回群ゆえ，生成元 u が取れる．$b \in \mathbb{F}^\times$ に対して $k(b)$ を $u^{k(b)} = b$ なる整数とすると，

$$M(1,1)^{ab^{-1}} M(0,u)^{k(b)} = M(ab^{-1},1)M(0,b) = M(a,b)$$

   ゆえ，$M(1,1), M(0,u)$ が生成元として取れる．

2. 生成元の関係式を調べる．

$$M(1,1)^p = I_2, \quad M(0,u)^{p-1} = I_2, \quad M(0,u)M(1,1) = M(1,u) = M(1,1)^{u^{-1}}M(0,u)$$

である．

3. 関係群を定義し，同型な群であることを示す．
上で調べたことをもとに，n を $n \equiv u^{-1} \mod p, 0 \leq n \leq p-1$ なる整数とし，$H = \langle x, y \mid x^p = 1, y^{p-1} = 1, yx = x^n y \rangle$ と定める．まず $M(1,1), M(0,u)$ は関係式を満たす G の生成元ゆえ，全射準同型 $f : H \to G$ が存在する．よって $|H| \geq |G| = p(p-1)$．また H の元は関係式より $x^i y^j (i = 0, \ldots, p-1,\ j = 0, \ldots, p-2)$ と表せる．よって $|H| \leq p(p-1)$．したがって f は同型で $G \cong H$ である．

生成元は多くとることができるが，多すぎると関係式の記述が大変になるので，ある程度の個数で取ると良いだろう．また生成元についての関係式は 3 で同型を示す際に位数を評価するために使うので，積における元の交換がどのように振る舞うかを記述すると良い．

問題 9.

生成元が二つ以下の四元数群と同型な関係群を一つ見つけよ．ただし四元数群とは $\mathrm{GL}_2(\mathbb{C})$ において

$$\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}$$

が生成する部分群である．

（解答）略．気が向いたら書く．

3　演習

以上を踏まえて問題に取り組もう．

問題 1（再掲）

p を素数とし，$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ を位数 p の有限体とする．行列の乗法による群 G を

$$G = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \middle| a, b, c \in \mathbb{F}_p \right\}$$

で定める．このとき，G から乗法群 $\mathbb{C}^\times = \mathbb{C} \setminus \{0\}$ への準同型写像の個数を求めよ．

（京大院　理・数学　2018 年度　院試 [1]）

（解答）p^2 個．詳細は気が向いたら書く．

4　省略した証明

省いた証明を記載する．まず関係群の定義を確認する．

定義 10.（有限生成，有限表示な関係群）

F_n を $\{x_1,\dots,x_n\}$ が生成する自由群，$i = 1,\dots,m$ について $R_1(x_1,\dots,x_n),\dots,R_m(x_1,\dots,x_n) \in F_n$ とする．$\{gR_i(x_1,\dots,x_n)g^{-1} \mid g \in F_n, i = 1,\dots,m\}$ が生成する F_n の部分群を N とおく[*2]．N は F_n の正規部分群である．この状況で，

$$\langle x_1,\dots x_n \mid R_1(x_1,\dots,x_n) = 1,\dots,R_m(x_1,\dots,x_n) = 1\rangle = F_n/N$$

と定め，$x_1,\dots,x_n$ が生成する関係式 $R_1(x_1,\dots,x_n) = 1,\dots,R_m(x_1,\dots,x_n) = 1$ で定義された群と呼ぶ．

これは $x_1,\dots,x_n$ で生成され $R_1(x_1,\dots,x_n) = 1,\dots,R_m(x_1,\dots,x_n) = 1$ を満たすような最大の群である．

例 11. いくつか関係群の例を見る．

- $\langle x \mid x^n = 1\rangle (= \{1, x, \dots, x^{n-1}\}) \cong \mathbb{Z}/n\mathbb{Z}$.
- $\langle x, y \mid x^n = 1, y^m = 1, yx = xy\rangle \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.
- $\langle x, y \mid x^n = 1, y^2 = 1, yxy = x^{-1}\rangle \cong D_n$.

F_n の定義や N が正規部分群であることなどは [2] に詳細がある．命題を再掲し証明を与える．

命題 3（再掲）

$X = \{x_1,\dots,x_n\}$ を生成元の集合，$R = \{R_i(x_1,\dots,x_n) = 1 \mid i = 1,\dots,m\}$ を関係式の集合とし，$G = \langle X \mid R\rangle$ とおく．H を群とする．写像 $f : X \to H$ であって $i = 1,\dots,m$ に対して $R_i(f(x_1),\dots,f(x_n)) = 1$ なるものの集合を M とおく．任意の $f \in M$ に対して

$$\widetilde{f}(x_{i_1}\cdots x_{i_k}) = f(x_{i_1})\cdots f(x_{i_k})$$

と $\widetilde{f} : G \to H$ を定めるとこれは準同型となり，逆に任意の準同型 $G \to H$ はこのようにして得られる．すなわちこの対応により M と $\mathrm{Hom}(G,H)$ は一対一に対応する．

証明. $f \in M$ が誘導する準同型 $\widehat{f} : F_n \to H$ が存在する．$i = 1,\dots,m$ に対して $\widehat{f}(R_i(x_1,\dots,x_n)) = R_i(f(x_1),\dots,f(x_n)) = 1$ より，任意の $g \in F_n$ について $gR_i(x_1,\dots,x_n)g^{-1} \in \mathrm{Ker}\,\widehat{f}$. よって $N \subseteq \mathrm{Ker}\,\widehat{f}$. ゆえに準同型定理より $\widetilde{f} : G \to H$ で $\widetilde{f}(x_{i_1}\cdots x_{i_k}) = f(x_{i_1})\cdots f(x_{i_k})$ なるものが存在．逆に準同型 $\widetilde{f} : G \to H$ に対して $\widetilde{f}|_X$ は M の

[*2] これは $\{R_i(x_1,\dots x_n) \mid i \in I\}$ を含む最小の正規部分群である

元である．この対応は互いに逆になっているので，一対一の対応であることが示された． □

参考文献

[1] “過去の入試問題”．京都大学大学院理学研究科／理学部数学教室．https://www.math.kyoto-u.ac.jp/files/master_exams/2017math_kiso.pdf

[2] 雪江明彦．代数学 1　群論入門．2010．日本評論社．