代数学 I 第 4 回講義資料

担当：大矢 浩徳 (OYA Hironori)*

いよいよ本講義の主題である『群』が登場する．今回の講義資料では，3.1 章で群と部分群の基本性質について抽象的に解説をし，3.2 章で例について解説する．抽象的な話よりも早く例を知りたいという方は，群と部分群の定義 3.1, 3.2, 3.3 だけ読んだらすぐに 3.2 章に飛び，必要になる度に 3.1 章に戻ってくるという読み方でも良いであろう．

3.1 群と部分群

それでは群とそれに関連する概念の定義を始めよう．

定義 3.1

空でない集合 G にある写像

$$\cdot : G \times G \to G, \quad (g_1, g_2) \mapsto g_1 \cdot g_2$$

(**二項演算**と呼ばれる) が与えられていて，以下の 3 条件を満たすとき，G を**群 (group)** であるという:

(I) 任意の $g_1, g_2, g_3 \in G$ に対して，$(g_1 \cdot g_2) \cdot g_3 = g_1 \cdot (g_2 \cdot g_3)$ が成り立つ．(**結合法則**)

(II) ある $e \in G$ が存在して，任意の $g \in G$ に対し，$e \cdot g = g = g \cdot e$ が成り立つ．(この e を G の**単位元**と呼ぶ．)

(III) 任意の $g \in G$ に対して，ある $g' \in G$ が存在し，$g' \cdot g = e = g \cdot g'$ が成り立つ．(この g' を G における g の**逆元**と呼ぶ．以下でも用いるが，g^{-1} と書かれることが多い．)

さらに，G の二項演算 $\cdot$ が

(IV) 任意の $g, h \in G$ に対し，$g \cdot h = h \cdot g$

を満たすとき，G を**可換群 (commutative group)** 又は**アーベル群 (abelian group)** という．

定義 3.2

群 G の**部分群**とは，群 G の空でない部分集合であって，G の二項演算によって群をなすものである．

定義 3.3

G を群とする．G に含まれる元の数を G の**位数 (order)** といい，$|G|$ や $\#G$ 等と書く．$|G|$ が有限のとき，G を**有限群 (finite group)** といい，$|G| = \infty$ のとき，G を**無限群 (infinite group)** という．

以下は抽象的な群と部分群の基本性質である．

* *e-mail*：hoya@shibaura-it.ac.jp

命題 3.4

群 G とその部分群 H において，以下が成立する．

(1) G の単位元 e はただ 1 つに定まる．
(2) 任意の $g \in G$ に対し，G における g の逆元 g' はただ 1 つに定まる．
(3) H の単位元は G の単位元に一致する．
(4) 任意の $h \in H$ に対し，H における h の逆元は G における h の逆元に一致する．

証明． <u>(1)</u> $e, e' \in G$ が G の単位元であったとすると，

$$\begin{aligned} e &= e \cdot e' && (e'\text{は単位元なので}) \\ &= e'. && (e\text{ は単位元なので}) \end{aligned}$$

よって，G の単位元 e はただ 1 つに定まる． □

<u>(2)</u> $g', g'' \in G$ が G における g の逆元であったとすると，

$$\begin{aligned} g' &= g' \cdot e && (e\text{ は単位元なので}) \\ &= g' \cdot (g \cdot g'') && (g''\text{は } g \text{ の逆元なので}) \\ &= (g' \cdot g) \cdot g'' && (\text{結合法則}) \\ &= e \cdot g'' && (g'\text{は } g \text{ の逆元なので}) \\ &= g''. && (e\text{ は単位元なので}) \end{aligned}$$

よって，G における g の逆元 g' はただ 1 つに定まる． □

<u>(3)</u> H の単位元を e_H，G の単位元を e_G，G における e_H の逆元を $e_H^{-1,G}$ と書くと，

$$\begin{aligned} e_H &= e_G \cdot e_H && (e_G\text{は } G \text{ の単位元なので}) \\ &= (e_H^{-1,G} \cdot e_H) \cdot e_H && (e_H^{-1,G}\text{は } G \text{ における } e_H\text{の逆元なので}) \\ &= e_H^{-1,G} \cdot (e_H \cdot e_H) && (\text{結合法則}) \\ &= e_H^{-1,G} \cdot e_H && (e_H\text{は } H \text{ の単位元なので}) \\ &= e_G. && (e_H^{-1,G}\text{は } G \text{ における } e_H\text{の逆元なので}) \end{aligned}$$

である．特に，これは e_G が必ず部分群 H に含まれることも意味していることに注意する． □

<u>(4)</u> H における h の逆元を $h^{-1,H}$，G における h の逆元を $h^{-1,G}$ と書くと，

$$\begin{aligned} h^{-1,H} &= h^{-1,H} \cdot e && (e\text{ は } G \text{ の単位元なので}) \\ &= h^{-1,H} \cdot (h \cdot h^{-1,G}) && (h^{-1,G}\text{は } G \text{ における } h \text{ の逆元なので}) \\ &= (h^{-1,H} \cdot h) \cdot h^{-1,G} && (\text{結合法則}) \\ &= e \cdot h^{-1,G} && (h^{-1,H}\text{は } H \text{ における } h \text{ の逆元であり，(3) より } H \text{ の単位元も } e \text{ なので}) \\ &= h^{-1,G}. && (e\text{ は } G \text{ の単位元なので}) \end{aligned}$$

□

また，与えられた群の部分集合が部分群であるかどうかは以下の命題を用いて判定できる．

命題 3.5

群 G の部分集合 H に対し，以下は同値である．

(1) H は G の部分群．

(2) H は空ではなく，H は二項演算と逆元をとる操作で閉じている．つまり，任意の $h, k \in H$ に対し，

$$h \cdot k \in H \quad \text{かつ} \quad h^{-1} \in H$$

となる．

証明. 群 G の部分集合 H が部分群であるとは，H が G の二項演算によって群をなすということであるが，これは以下のように書き下せる：

H は空ではなく，G の二項演算

$$\cdot\colon G \times G \to G, \quad (g_1, g_2) \mapsto g_1 \cdot g_2$$

の定義域を $H \times H$ に制限したとき，これが

$$\cdot\colon H \times H \to H$$

を与え，以下の 3 条件を満たす：

(i) 任意の $h_1, h_2, h_3 \in H$ に対して，$(h_1 \cdot h_2) \cdot h_3 = h_1 \cdot (h_2 \cdot h_3)$ が成り立つ．

(ii) ある $e_H \in H$ が存在して，任意の $h \in H$ に対し，$e_H \cdot h = h = h \cdot e_H$ が成り立つ．

(iii) 任意の $h \in H$ に対して，ある $h' \in H$ が存在し，$h' \cdot h = e_H = h \cdot h'$ が成り立つ．

この枠で囲んだ主張が (2) の主張と同値であることを示せばよい．

枠で囲んだ主張 $\Rightarrow$(2)：まず $\cdot$ が $\cdot\colon H \times H \to H$ を定めるということより，任意の $h, k \in H$ に対し，$h \cdot k \in H$ は成立する．さらに，性質 (iii) より各 $h \in H$ に対して，H における h の逆元は H 内に存在するが，命題 3.4(4) より，これは G における h の逆元 h^{-1} と一致するので，結局 $h^{-1} \in H$ である．よって，(2) の主張が成立する．

(2)$\Rightarrow$ 枠で囲んだ主張：任意の $h, k \in H$ に対し，$h \cdot k \in H$ が成立することより，G の二項演算 $\cdot$ は確かに $\cdot\colon H \times H \to H$ を与える．さらに，この二項演算は G の二項演算を制限したものなので，(i) の性質は自明に成り立つ．

次に，$H \neq \emptyset$ より，任意に 1 つ元 $h \in H$ をとると，(2) の性質より $h^{-1} \in H$ であり，さらに，$H \ni h \cdot h^{-1} = e$．よって，H は G の単位元 e を含み，この元を e_H とすると確かに (ii) の条件を満たす．

(2) の性質より，$h \in H$ に対して，G における h の逆元 h^{-1} は H の元であるが，これは $hh^{-1} = e (= e_H) = h^{-1}h$ を満たすので，H における逆元でもある．よって，(iii) の条件も満たされる． □

3.2 群と部分群の例 (その 1)

以下ではこれまでにすでに学習したものの中から，群と部分群の例となるものについて列挙する．なお，『$(G, \cdot)$』という書き方をした場合には，『集合 G に二項演算 $\cdot$ を考えたもの』という意味であると解釈する．

例 1 (加法群)**.** $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +)$ は群である．これらは**加法群**とよばれる．群の二項演算の 3 性質は以下のように確かめられる ($\mathbb{X} = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ とする)：

(I) (結合法則) 任意の $a, b, c \in \mathbb{X}$ に対し，$(a + b) + c = a + (b + c)$．

(II) (単位元の存在) 単位元は $0 \in \mathbb{X}$ である．実際，任意の $a \in \mathbb{X}$ に対し，$0 + a = a = a + 0$ が成立する．

(III) (逆元の存在) 任意の $a \in \mathbb{X}$ に対し，$-a \in \mathbb{X}$ であって，$(-a) + a = 0 = a + (-a)$ が成立する．

さらに，加法 $+$ は

(IV) 任意の $a,b \in \mathbb{X}$ に対し，$a+b=b+a$

をみたすので，これらは可換群である．いずれも集合に含まれる元の個数は無限なので，無限群である．また，$(\mathbb{C},+) \supset (\mathbb{R},+) \supset (\mathbb{Q},+) \supset (\mathbb{Z},+)$ であり，小さいものは大きいものの部分群である．

なお，二項演算として引き算 $-$ を考えると，$(\mathbb{X},-)$ は群にはならない！なぜなら，一般に $a,b,c \in \mathbb{X}$ に対して，

$$(a-b)-c = a-b-c \neq a-b+c = a-(b-c)$$

となり，結合法則が成り立たないためである．

また，$(\mathbb{N},+)$ も群にはならない！これは，$a \in \mathbb{N}$ が 0 でないとき，$a+a'=0$ を満たす a' は $-a$ であるが，$-a \notin \mathbb{N}$ であるため，性質 (III)(逆元の存在) を満たさないのである．

例 2 (乗法群)**.** $(\mathbb{Q}^\times,\times),(\mathbb{R}^\times,\times),(\mathbb{C}^\times,\times)$ は群である．これらは**乗法群**とよばれる．群の二項演算の 3 性質は以下のように確かめられる ($\mathbb{K}^\times = \mathbb{Q}^\times,\mathbb{R}^\times,\mathbb{C}^\times$ とする)：

(I) (結合法則) 任意の $a,b,c \in \mathbb{K}^\times$ に対し，$(a\times b)\times c = a\times(b\times c)$.

(II) (単位元の存在) 単位元は $1 \in \mathbb{K}^\times$ である．実際，任意の $a \in \mathbb{X}^\times$ に対し，$1\times a = a = a\times 1$ が成立する．

(III) (逆元の存在) 任意の $a \in \mathbb{K}^\times$ に対し，$a^{-1} \in \mathbb{X}^\times$ であって，$a^{-1}\times a = 1 = a\times a^{-1}$ が成立する．

さらに，乗法 $\times$ は

(IV) 任意の $a,b \in \mathbb{K}^\times$ に対し，$a\times b = b\times a$

をみたすので，これらは可換群である．いずれも集合に含まれる元の個数は無限なので，無限群である．また，$(\mathbb{C}^\times,\times) \supset (\mathbb{R}^\times,\times) \supset (\mathbb{Q}^\times,\times)$ であり，小さいものは大きいものの部分群である．

さらに，

$$\mathbb{K}^\times_{>0} \coloneqq \{a \in \mathbb{K}^\times \mid a>0\}$$

とすると，$\mathbb{K}^\times_{>0}$ は $\mathbb{K}^\times$ の部分群である。これは，正の数の積は再び正の数であり，正の数の逆数は再び正の数であることから，命題 3.5 よりわかる．

なお，二項演算として割り算 $\div$ を考えると，$(\mathbb{K}^\times,\div)$ は群にはならない！なぜなら，一般に $a,b,c \in \mathbb{K}^\times$ に対して，

$$(a\div b)\div c = \frac{\frac{a}{b}}{c} = \frac{a}{bc} \neq \frac{ac}{b} = \frac{a}{\frac{b}{c}} = a\div(b\div c)$$

となり，結合法則が成り立たないためである．

また，$(\mathbb{Z}\setminus\{0\},\times)$ も群にはならない！これは，$a \in \mathbb{Z}\setminus\{0\}$ が 1 でないとき，$a\times a' = 1$ を満たす a' は a^{-1} であるが，$a^{-1} \notin \mathbb{Z}\setminus\{0\}$ であるため，性質 (III)(逆元の存在) を満たさないのである．一方，$\{1,-1\}$ という 2 つだけの元からなる集合を考えると，$(\{1,-1\},\times)$ は群をなす．実際積を全通り考えると，

$$1\times 1 = 1 \qquad (-1)\times 1 = -1 \qquad 1\times(-1) = -1 \qquad (-1)\times(-1) = 1$$

となり，確かに $\{1,-1\}$ は積で閉じていて，しかも 1 の逆元は 1，-1 の逆元は -1 となるため，逆元をとる操作でも閉じている．よって，命題 3.5 より，$\{1,-1\}$ は $(\mathbb{K}^\times,\times)$ の部分群である．さらに，$\#\{1,-1\} = 2$ なので，これは位数 2 の有限群の例となる．

注意. 集合としては $\mathbb{K}^\times \subset \mathbb{K}$ であるが，$(\mathbb{K}^\times,\times)$ は $(\mathbb{K},+)$ の部分群ではない！ ($\mathbb{K}=\mathbb{Q},\mathbb{R},\mathbb{C}$) これは，$(\mathbb{K}^\times,\times)$ と $(\mathbb{K},+)$ で考えている二項演算が異なるため，部分群の定義 3.2 の，『G の二項演算によって』という部分を満たしていないのである．

例 3 (ベクトル空間)**.** ベクトル空間も加法 $+$ に関して群をなす．念のためベクトル空間の定義を復習しておこう．

復習

$\mathbb{K}$ を $\mathbb{Q}, \mathbb{R}$ または $\mathbb{C}$ とする．$(V, +, \cdot)$ が $\mathbb{K}$ **上のベクトル空間**であるとは，これが以下のような 3 つ組であることである：

- V は空でない集合，
- $+$ は写像 $+ \colon V \times V \to V,\ (\boldsymbol{u}, \boldsymbol{v}) \mapsto \boldsymbol{u} + \boldsymbol{v}$,
- $\cdot$ は写像 $\cdot \colon \mathbb{K} \times V \to V,\ (c, \boldsymbol{v}) \mapsto c\boldsymbol{v}$

であって，以下が成立する：

(v1) 任意の $\boldsymbol{u}, \boldsymbol{v} \in V$ に対し，$\boldsymbol{u} + \boldsymbol{v} = \boldsymbol{v} + \boldsymbol{u}$,

(v2) 任意の $\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{w} \in V$ に対し，$(\boldsymbol{u} + \boldsymbol{v}) + \boldsymbol{w} = \boldsymbol{u} + (\boldsymbol{v} + \boldsymbol{w})$,

(v3) ある元 $\boldsymbol{0} \in V$ が存在して，任意の $\boldsymbol{u} \in V$ に対し，$\boldsymbol{u} + \boldsymbol{0} = \boldsymbol{u}$,（この $\boldsymbol{0}$ を**零ベクトル**という）

(v4) 任意の $\boldsymbol{v} \in V$ に対して，ある元 $-\boldsymbol{v} \in V$ が存在して，$\boldsymbol{v} + (-\boldsymbol{v}) = \boldsymbol{0}$,（この $-\boldsymbol{v}$ を $\boldsymbol{v}$ **の逆元**という）

(v5) 任意の $c, d \in \mathbb{K}, \boldsymbol{v} \in V$ に対し，$(c + d)\boldsymbol{v} = c\boldsymbol{v} + d\boldsymbol{v}$,

(v6) 任意の $c \in \mathbb{K}, \boldsymbol{u}, \boldsymbol{v} \in V$ に対し，$c(\boldsymbol{u} + \boldsymbol{v}) = c\boldsymbol{u} + c\boldsymbol{v}$,

(v7) 任意の $c, d \in \mathbb{K}, \boldsymbol{v} \in V$ に対し，$(cd)\boldsymbol{v} = c(d\boldsymbol{v})$,

(v8) 任意の $\boldsymbol{v} \in V$ に対し，$1\boldsymbol{v} = \boldsymbol{v}$.

このとき，確かに $+$ は V における二項演算となっており，(v2) が結合法則，(v3) が単位元 $\boldsymbol{0}$ の存在 ((v1) より，$\boldsymbol{0} + \boldsymbol{u} = \boldsymbol{u}$ も成立する)，(v4) が各元 $\boldsymbol{v} \in V$ の逆元 $-\boldsymbol{v}$ の存在 ((v1) より，$(-\boldsymbol{v}) + \boldsymbol{v} = \boldsymbol{0}$ も成立する) に対応する．(v1) より，これは可換群である．ベクトル空間は可換群 $(V, +)$ にスカラー倍 $\cdot$ の構造を加えたものであると言うことができる．

例 4 (整数の剰余類群)**.** 正の整数 n に対して，$(\mathbb{Z}/n\mathbb{Z}, +)$ は群である．これは n を法とする**整数の剰余類群**とよばれる．群の二項演算の 3 性質は以下のように確かめられる：

(I) (結合法則) 任意の $[a]_n, [b]_n, [c]_n \in \mathbb{Z}/n\mathbb{Z}$ に対し，$([a]_n + [b]_n) + [c]_n = [a+b+c]_n = [a]_n + ([b]_n + [c]_n)$.

(II) (単位元の存在) 単位元は $[0]_n \in \mathbb{Z}/n\mathbb{Z}$ である．実際，任意の $[a]_n \in \mathbb{Z}/n\mathbb{Z}$ に対し，$[0]_n + [a]_n = [a]_n = [a]_n + [0]_n$ が成立する．

(III) (逆元の存在) 任意の $[a]_n \in \mathbb{Z}/n\mathbb{Z}$ に対し，$[-a]_n \in \mathbb{Z}/n\mathbb{Z}$ であって，$[-a]_n + [a]_n = [0]_n = [a]_n + [-a]_n$ が成立する．

さらに，$+$ は

(IV) 任意の $[a]_n, [b]_n \in \mathbb{Z}/n\mathbb{Z}$ に対し，$[a]_n + [b]_n = [b]_n + [a]_n$

をみたすので，これは可換群である．また，$|\mathbb{Z}/n\mathbb{Z}| = n$ であったので，これは位数 n の有限群である．

例 5 ($\mathbb{Z}/n\mathbb{Z}$ の乗法群)**.** 正の整数 n に対して，$((\mathbb{Z}/n\mathbb{Z})^\times, \times)$ は群である ($\times$ が $(\mathbb{Z}/n\mathbb{Z})^\times$ の二項演算として定義できることについては，第 3 回講義資料命題 2.4(1) を参照)．これは $\mathbb{Z}/n\mathbb{Z}$ **の乗法群**とよばれる．群の二項演算の 3 性質は以下のように確かめられる：

(I) (結合法則) 任意の $[a]_n, [b]_n, [c]_n \in (\mathbb{Z}/n\mathbb{Z})^\times$ に対し，$([a]_n[b]_n)[c]_n = [abc]_n = [a]_n([b]_n[c]_n)$.

(II) (単位元の存在) 単位元は $[1]_n \in (\mathbb{Z}/n\mathbb{Z})^\times$ である．実際，任意の $[a]_n \in (\mathbb{Z}/n\mathbb{Z})^\times$ に対し，$[1]_n[a]_n = [a]_n = [a]_n[1]_n$ が成立する．

(III) (逆元の存在) 任意の $[a]_n \in (\mathbb{Z}/n\mathbb{Z})^\times$ に対し，第 3 回講義資料命題 2.4(2) より $[a]_n^{-1} \in (\mathbb{Z}/n\mathbb{Z})^\times$ であって，$[a]_n^{-1}[a]_n = [1]_n = [a]_n[a]_n^{-1}$ が成立する．

第 3 回講義資料の定義 2.1 で $[1]_n$ を “1” としたのは，$[1]_n$ が単位元の満たすべき性質を満たすためだったのである．また，(III) の逆元の存在のために，$(\mathbb{Z}/n\mathbb{Z}, \times)$ ではなく，$((\mathbb{Z}/n\mathbb{Z})^\times, \times)$ を考える必要がある．

演算 $\times$ は,

(IV) 任意の $[a]_n, [b]_n \in (\mathbb{Z}/n\mathbb{Z})^\times$ に対し，$[a]_n[b]_n = [b]_n[a]_n$

をみたすので，これは可換群である．また，第 3 回講義資料命題 2.7 より，$|(\mathbb{Z}/n\mathbb{Z})^\times| = \varphi(n)$ (φ はオイラーの φ 関数) であったので，これは位数 $\varphi(n)$ の有限群である．

例 6 (一般線型群，特殊線型群)**.** n を正の整数とし，$\mathbb{K}$ を $\mathbb{Q}, \mathbb{R}$ または $\mathbb{C}$ とする．

$$GL_n(\mathbb{K}) \coloneqq \{A \mid A \text{ は } \mathbb{K} \text{ を成分とする } n \times n \text{ 行列で}, \det A \neq 0\}.$$

ただし，$\det A$ は A の行列式．このとき，$GL_n(\mathbb{K})$ は行列の積に関して群をなす．これを**一般線型群 (general linear group)** という．ここで，$n \times n$ 行列 A, B に対し，$\det(AB) = \det A \cdot \det B$ であったので，$GL_n(\mathbb{K})$ は行列の積に関して閉じているということに注意しよう． 群の二項演算の 3 性質は以下のように確かめられる：

(I) (結合法則) 任意の $A, B, C \in GL_n(\mathbb{K})$ に対し，$(AB)C = A(BC)$．(行列の積の性質)

(II) (単位元の存在) 単位元は単位行列 $I_n = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$ である．実際，任意の $A \in GL_n(\mathbb{K})$ に対し，$I_n A = A = A I_n$ が成立する．

(III) (逆元の存在) 任意の $A \in GL_n(\mathbb{K})$ に対し，$\det A \neq 0$ より，逆行列 $A^{-1} \in GL_n(\mathbb{K})$ が存在する．逆行列は $A^{-1}A = I_n = AA^{-1}$ を満たすので，群論の意味での逆元となっている．

逆元の存在を保証するために，$\det A \neq 0$ を満たす行列のなす集合を考えている．また，$n \geq 2$ のとき，行列の積は一般に $AB = BA$<u>とはならない</u>ので，$GL_n(\mathbb{K})$ は非可換群である．さらに，

$$SL_n(\mathbb{K}) = \{A \in GL_n(\mathbb{K}) | \det A = 1\}$$

とすると，$SL_n(\mathbb{K})$ は $GL_n(\mathbb{K})$ の部分群であり，**特殊線型群 (special linear group)** と呼ばれる．これは以下のように確かめられる：

$I_n \in SL_n(\mathbb{K})$ より，$SL_n(\mathbb{K})$ は空ではない．任意の $A, B \in SL_n(\mathbb{K})$ に対し，

$$\det(AB) = \det(A) \cdot \det(B) = 1 \cdot 1 = 1 \qquad \det(A^{-1}) = \det(A)^{-1} = 1^{-1} = 1$$

より，$AB \in SL_n(\mathbb{K})$ かつ $A^{-1} \in SL_n(\mathbb{K})$ である．よって，命題 3.5 より，$SL_n(\mathbb{K})$ は $GL_n(\mathbb{K})$ の部分群である．

注意 (**群の定義補足 (興味のある方向け)**)**.** 群の定義で (II) や (III) にある等式を『$g = g \cdot e$』のみ，『$g' \cdot g = e$』のみというようにさぼってはいけない．例えば，2×2 行列のなす集合

$$G' \coloneqq \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \middle| a \in \mathbb{C}^\times, b \in \mathbb{C} \right\}$$

を考える．すると，

$$\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \begin{pmatrix} a' & 0 \\ b' & 0 \end{pmatrix} = \begin{pmatrix} aa' & 0 \\ ba' & 0 \end{pmatrix}$$

より，G' には行列の積から定まる二項演算が定まっている (結合法則 (I) を満たす)．

さらに，$e \coloneqq \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in G'$ と定めると，任意の $g = \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \in G'$ に対し，

$$ge = \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} = g$$

が成立する．さらに，任意の $g = \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \in G'$ に対し，$g' = \begin{pmatrix} a^{-1} & 0 \\ 0 & 0 \end{pmatrix} \in G'$ とすると，

$$g'g = \begin{pmatrix} a^{-1} & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = e$$

となる．これより，G' は群の性質のうち二項演算の存在，(I)，(II) の一部 (『$g = g \cdot e$』のみにしたもの)，(III) の一部 (『$g' \cdot g = e$』のみにしたもの) を満たすが，$\underline{G'\text{ は群ではない}}$．実際，$G'$ が群であるなら単位元の存在から，任意の $g = \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \in G'$ に対し，$e'g = g$ を満たす $e' = \begin{pmatrix} e_1 & 0 \\ e_2 & 0 \end{pmatrix} \in G'$ が存在するはずである．しかし，このとき

$$e'g = \begin{pmatrix} e_1 & 0 \\ e_2 & 0 \end{pmatrix} \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} = \begin{pmatrix} e_1 a & 0 \\ e_2 a & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} = g$$

なので，特に $e_2 a = b$ が任意の $a \in \mathbb{C}^{\times}$、$b \in \mathbb{C}$ に対して成り立つことになるが，そのような定数 e_2 は存在せず，矛盾する．