「行間を埋める」ために

- この別冊 PDF ファイルは『**手を動かしてまなぶ　群論**』（裳華房，2024 年刊）の本文中の ✍ のマークについて，その行間を埋めるための**具体的なやり方**を一例としてまとめたものです．
- この別冊 PDF ファイルを印刷して利用するときは，**「小冊子」モード**で印刷して二つ折にすると，A5 判サイズで本の巻末に挟み込んで利用することができます．
- この別冊内の見出しの「p. ○ 下から○行目」という表記では，該当書籍の対応するページ内の**脚注は行数にカウントしていません**．
- 数学書は証明や計算の細部が省略されていることが多いため，精読する際はペンと紙を用意して，**自分で詳細を計算すること**が極めて重要です．論理の行間を埋めていくことで数学の基礎体力がついてきます．
- 証明や計算の論理を追うときは **1 行 1 行疑ってかかる**くらいの態度で望みましょう．
- 論理の行間を埋めた後は，**その数学的内容を改めて見直してみましょう**．定義や定理の主張はなにか，仮定はなぜ必要なのか，証明した定理の具体例を挙げることができるかなど，時間をかけてじっくりと味わうことが大切です．そうしないと**木を見て森を見ず**という状態に陥ったまま先へ進むことになりがちです．間違ってもよいので，慌てずに．
- 読者が手を動かしながら本書の隅々まで習熟され，さまざまな群の織りなす豊饒な世界を堪能できますように．健闘を祈ります．

(2024 年 10 月 31 日版)

§1 の ✍ のマーク

p.4 上から 1 行目

(1)　$a, b \in \mathbb{Z}$ に対して $n = ab$ と表されることと，a, b がともに n の倍数であることは同値である［⇨ **定義 1.4**］．さて，n が素数であるならば，n の約数は ± 1 または $\pm n$ しか存在せず，かつ a は n の約数なので，$a = \pm 1$ または $a = \pm n$ がなりたつ．$a = \pm p$ のときは，等式 $n = ab$ より $b = \pm 1$（複号同順）であるので，$a = \pm 1$ または $b = \pm 1$ がなりたつ．逆に $(\star)$「$n = ab$ と表したとき $a = \pm 1$ または $b = \pm 1$ がなりたつ」と仮定しよう．もし n が ± 1，$\pm n$ 以外の約数 d をもつならば，約数の定義より $n = dq$ をみたす整数 $q \in \mathbb{Z}$ が存在するが，これは $(\star)$ に反する．したがって，背理法により n が素数であることが示された．

(2)　「n は素数である」の否定が「n は合成数である」なので［⇨ **定義 1.6**］，(1) の同値条件 $(\star)$ の否定を考えればよいが，これは「$n = ab$ をみたす $a \neq \pm 1$ かつ $b \neq \pm 1$ が存在する」となるので，題意が従う．

※　主張 $(\star)$ を，より丁寧に書き直すと「$n = ab$ をみたす**すべての整数組** (a, b) は $a = \pm 1$ または $b = \pm 1$ をみたす」となる．このように書き直すと，$(\star)$ は「すべての…」に関する所謂(いわゆる)**全称命題**であることがはっきりとわかるだろう．記号論理学（数学の論証）の基礎知識として **全称命題（「すべての…」に関する命題）の否定は存在命題（「ある…」に対する命題，「…が存在する」という形の命題）となる**ので，命題 1.8 (2) の主張が「……をみたすものが**存在する**」となっているのである．なお，(2) では「または」が否定されて「かつ」となっていること（論理命題に関するド・モルガンの定理）にも注目しよう．

p.5 下から 7 行目　実際，$m_0 = |n_1 n_2 \cdots n_s|$ とおけば，$n_i \mid m_0$ $(i = 1, 2, \ldots, s)$ より $m_0 \in S$ なので，S は空ではない $\mathbb{N}$ の部分集合である（もちろん，m_0 として $n_1, n_2, \ldots, n_s$ の最小公倍数を考えてもよい）．

p.5 下から 8 行目　例えば $m_0 = |n_1 n_2 \cdots n_s|$ と定めれば，明らかに $n_i \mid m_0$（ただし $i = 1, 2, \ldots, s$）であるから $m_0 \in S$ である．したがって，S は空集合ではない．

※　今回のように，しばしば見られる「空集合でないこと」の確認は，その集合の条件をみたす元を**何でもよいから** 1 つ提示すればよいので，大抵の場合，極めて容易な作業である．ただし，この作業を怠ってしまうと，「空集合に対して証明を付ける」という壮大な労力の無駄遣いをすることにもなりかねないので，きちんとあたえられた集合が空集合でないか確認する癖をつけておこう．

p.8 上から 4 行目　整除記号 $x \mid y$ の定義から $b = d_2 q_1$, $r = d_2 q_2$ $(q_1,\ q_2 \in \mathbb{Z})$ と表せるので，(1.3) に代入して $a = bq + r = d_2(bq_1 + q_2)$ を得る．ゆえに $d_2 \mid a$ である．

p.8 上から 6 行目　d_1 は a と b の公約数なので，$d_1 \mid a$ かつ $d_1 \mid b$, すなわち $a = d_1 q_3$, $b = d_1 q_4$ $(q_3,\ q_4 \in \mathbb{Z})$ と表せるので，(1.3) 式に代入して $r = a - bq = d_1(q_3 + q_4 q)$, すなわち $d_1 \mid r$ を得る．したがって，d_1 は b と r の公約数にもなっているが，$d_2 = \mathrm{g.c.d.}(b, r)$ は b と r の**最大**公約数であるため $d_1 \leq d_2$ がなりたつ．

p.9 上から 3 行目　$n \in \mathbb{N}$ に対して $d = \mathrm{g.c.d.}(n, 0)$ とおくと，定義より $n = dq_1$, $0 = dq_2$ $(q_1, q_2 \in \mathbb{Z})$ と表せる．第 2 式より $d = 0$ または $q_2 = 0$ となるが，$d = 0$ であると第 1 式に代入して $n = 0$ となり，$n \geq 1$ と矛盾するので $q_2 = 0$ である．したがって，

第 2 式 $0 = d \cdot 0$ は任意の $d \in \mathbb{Z}$ に対してなりたつため，d が n と 0 の最大公約数であることは，d が $n = dq$ をみたす最大の整数であることと同値となる．$n, d \in \mathbb{N}$ より $q \in \mathbb{N}$，とくに $q \geq 1$ であるから，不等式 $n = dq \geq d$ がなりたつ．この不等式をみたす最大の自然数 d は $d = n$ であるので，$\mathrm{g.c.d.}(n, 0) = n$ が示された．

p.11 上から 6 行目　r は S の元なので $r = n - dq$ $(q \in \mathbb{Z})$ と表される．また，背理法の仮定より $r \geq |d|$ であるから，$\tilde{r} := r - |d| \geq 0$ がなりたつ．さらに

$$\tilde{r} = r - |d| = \begin{cases} n - d(q+1) & (d > 0 \text{ のとき}), \\ n - d(q-1) & (d < 0 \text{ のとき}) \end{cases}$$

と表されるため，$\tilde{r}$ は S の元の条件をみたしており，$\tilde{r} \in S$ が従う．

p.11 下から 4 行目　不等式 $0 \leq r_2 < |d|$ を辺々 (-1) 倍すると $-|d| < -r_2 \leq 0$ となるので，$0 \leq r_1 < |d|$ と足し合わせて $-|d| < r_1 - r_2 < |d|$ を得る．

§2 の ✍ のマーク

p.20 下から 6 行目　$d = \mathrm{g.c.d}(a, p)$ とおくと，$d \mid p$ であるから，素数の定義［⇨ **定義 1.6**］（と不等式 $d > 0$）より $d = 1$ または $d = p$ となる．ここで，もし $d = p$ であると仮定すると，d は定義から a と p の公約数なので $a = p \mid a$ がなりたつが，これは仮定 $p \nmid a$ と矛盾する．したがって $d \neq p$ であるため，$d = 1$，すなわち a と p が互いに素であることが示された．

p.21 上から 8 行目　補題 2.6 の等式 $ax = by \cdots (*)$ より $a \mid by$ がなりたつ．また，a と b は互いに素なので，補題 2.6 の a, b, y をそれぞれ命題 2.14 の n, a, b と対応させて命題 2.14 を適用することで $a \mid y$ を得る．まったく同様に，$(*)$ から $b \mid ax$ が従うので，補題 2.6 の b, a, x をそれぞれ命題 2.14 の n, a, b と対応させて命題 2.14 を適用することで $b \mid x$ も従う．

p.24 下から 4 行目　a, b を (2.6) の形で $a = \prod_{p:\ 素数} p^{e_p}$, $b = \prod_{p:\ 素数} p^{f_p}$ と素因数分解しておく．$m = \prod_{p:\ 素数} p^{h_p}$ を a と b の（正の）公倍数とすると，命題 2.19 (1) より各素数 p に対して $e_p \leq h_p$ かつ $f_p \leq h_p$，すなわち $\max\{e_p, f_p\} \leq h_p$ がなりたつ．一方で命題 2.19 (3) より $\mathrm{l.c.m.}(a, b) = \prod_{p:\ 素数} p^{\max\{e_p,\, f_p\}}$ であったから，命題 2.19 (1) より

l.c.m.$(a,b) \mid m$ が従う．

p.25 上から 11 行目　例えば $a>0$ ならば $a=a\cdot 1+b\cdot 0>0$ より $a\in S$ であるし，$a<0$ ならば $-a=a\cdot(-1)+b\cdot 0>0$ より $-a\in S$ である．$a=0$ であるならば，仮定より $b\neq 0$ なので，同様に $b>0$ ならば $b\in S$，$b<0$ ならば $-b\in S$ となり，いずれの場合でも S の元が存在するため $S\neq\emptyset$ である．

p.25 下から 3 行目　もし $r_2>0$ がなりたつとすると，r_2 は a と b の整数係数線形結合で表される正の整数であるため $r_2\in S$ となるが，一方で $r_2<m_0$ となり，m_0 が S の最小元であったことと矛盾する．したがって，背理法により $r_2=0$ である．

p.27 上から 14 行目　素数 n が $n=\pm k=\pm p_1p_2\cdots p_s$ と素因数分解されたと仮定する．まず，$k>0$ かつ $p_j>0$ $(j=1,2,\ldots,s)$ であるから，この等式の複号は同順である．したがって，$k=p_1p_2\cdots p_s$ がなりたつ．以下，素因数の個数 s が 1 であることを背理法により証明する．$s>1$ と仮定すると，$k=(p_1p_2\cdots p_{s-1})p_s$ $\cdots$ $(\diamond)$ と表されるので，k が素数であることの定義［⇨ **定義 1.6**］から $p_1=1$ または $p_2p_3\cdots p_s=1$ であるが，p_1 は素数であり，とくに **1 ではない**ため $p_2p_3\cdots p_s=1$ である．とくに $p_j\in\mathbb{N}$ であることに注意すると，この等式がなりたつのは $p_2=p_3=\cdots=p_s=1$ がなりたつときであるが，この式も $p_2,p_3,\ldots,p_s$ が素数である（とくに **1 ではない**）ことに矛盾する．以上より $s=1$ であることが示された．これを $(\diamond)$ に代入すると $k=p_1$ を得るので，$|n|$ が素数のときは素因数分解 $n=\pm k$ が一意的となることが示された．

p.27 下から 4 行目　$p_r\mid q_s$ であるが，q_s は素数なので（$p_r>0$ であることと合わせて）$p_r=1$ または $p_r=q_s$ がなりたつはずである．一方で p_r も素数なので，とくに **1 ではない**．したがって，$p_r\neq 1$ より $p_r=q_s$ が従う．

§3 の ✍ のマーク

p.32 下から 3 行目　a,b をそれぞれ n で割り算して $a=nq_1+r_1$，$b=nq_2+r_2$ $(q_1,q_2,r_1,r_2\in\mathbb{Z},\ 0\le r_1,r_2<|n|)$ と表しておこう．まず $a\equiv b\pmod{n}$ がなりたっているとすると，合同式の定義より $a-b=nq_3$ $(q_33\in\mathbb{Z})$ と表せるので，

$$r_1-r_2=(a-nq_1)-(b-nq_2)=\underbrace{(a-b)}_{=nq_3}-n(q_1-q_2)=n(q_3-q_1+q_2)$$

より $r_1-r_2\equiv 0\pmod{n}$ がなりたつ．つまり r_1-r_2 は n の倍数である．一方で

【p.11 下から 4 行目】の ✍ の解説とまったく同様に $-|n| < r_1 - r_2 < |n|$ がなりたつので，$r_1 - r_2 = n \cdot 0 = 0$，すなわち $r_1 = r_2$ が従う．逆に $r_1 = r_2$ がなりたっているとすると

$$a - b = nq_1 + r_1 - (nq_2 + r_2) = n(q_1 - q_2) + \underbrace{r_1 - r_2}_{=0} = n(q_1 - q_2)$$

より $a \equiv b \pmod{n}$ がなりたつ．以上より $a \equiv b \pmod{n}$ がなりたつことと $r_1 = r_2$ がなりたつことは同値である．

p.33 上から 3 行目　まず，合同式の定義より $x - y = nq_1$ $(q_1 \in \mathbb{Z})$ と表せる．一方で n_0 は n の約数なので $n = n_0 q_2$ $(q_2 \in \mathbb{Z})$ と表せる．したがって $x - y = nq_1 = n_0(q_1 q_2)$ より $x \equiv y \pmod{n_0}$ がなりたつ．

p.34 上から 9 行目　【p.33 上から 3 行目】と同様に，$x_1 - y_1 = na$，$x_2 - y_2 = nb$ $(a, b \in \mathbb{Z})$ と表すと，

$$(x_1 - x_2) - (y_1 - y_2) = (x_1 - y_2) - (x_2 - y_2) = na - nb = n(a - b)$$

であるから $x_1 - x_2 \equiv y_1 - y_2 \pmod{n}$ がなりたつ．

p.34 下から 8 行目　m に関する数学的帰納法により証明する．まず $m = 0$ のときは $x^0 - y^0 = 1 - 1 = 0$ より $x^0 \equiv y^0 \pmod{n}$ がなりたつ．続いて $m = k \in \mathbb{Z}_{\geq 0}$ に対して $x^k \equiv y^k \pmod{n}$ $\cdots (*)_1$ がなりたつと仮定しよう．一方で $x \equiv y \pmod{n}$ $\cdots (*)_2$ がなりたつことは仮定されているので，$(*)_1$, $(*)_2$ に命題 3.7 (2) を用いて

$$x^k x \equiv y^k y \pmod{n} \qquad \therefore\ x^{k+1} \equiv y^{k+1} \pmod{n}$$

がなりたつ．したがって，m に関する数学的帰納法により $x^m \equiv y^m \pmod{n}$ がなりたつことが示された．

p.36 上から 9 行目　$d = 24 \cdot 365 + 6 + 30 + 31 + 20$ であったことを思い出そう．同様に，$d \pmod{10}$ の値および $d \pmod{12}$ の値によって**十干**（じっかん）と**干支**（えと）の表を作成すると，以下のようになる．

$d \pmod{10}$	0	1	2	3	4	5	6	7	8	9
十干	己	庚	辛	壬	癸	甲	乙	丙	丁	戊

$d \pmod{12}$	0	1	2	3	4	5	6	7	8	9	10	11
十二支	丑	寅	卯	辰	巳	午	未	申	酉	戌	亥	子

このとき，

$$24 \equiv 4 \pmod{10}, \qquad 365 \equiv 5 \pmod{10}, \qquad 6 \equiv -4 \pmod{10},$$

$$30 \equiv 0 \pmod{10}, \qquad 31 \equiv 1 \pmod{10}, \qquad 20 \equiv 0 \pmod{10}$$

に注意すると，命題 3.7 より $d \equiv 4 \cdot 5 - 4 + 0 + 1 + 0 \equiv -3 \equiv 7 \pmod{10}$ と計算できる．さらに

$$24 \equiv 0 \pmod{12}, \qquad 365 \equiv 5 \pmod{12}, \qquad 6 \equiv 6 \pmod{12},$$

$$30 \equiv 6 \pmod{12}, \qquad 31 \equiv -5 \pmod{12}, \qquad 20 \equiv -4 \pmod{12}$$

に注意すると $d \equiv 0 \cdot 5 + 6 + 6 - 5 - 4 \equiv 3 \pmod{12}$ と計算できる．したがって，先程の表と照らし合わせて，2047 年 6 月 21 日の日干支が **丙辰**（ひのえたつ）であることがわかる．

§4 の ✍ のマーク

p.41 上から 11 行目　(4.1) が整数解 x_0 をもつとすると，$ax_0 - d = nq$ $(q \in \mathbb{Z})$ と表すことができる．さて，$d_0 := \mathrm{g.c.d.}(a, n)$ は a と n の公約数であるから，$a = d_0 a_0$, $n = d_0 n_0$ $(a_0,\, n_0 \in \mathbb{Z})$ と表せる．このとき

$$d = ax_0 + nq = d_0(a_0 x_0 + n_0 q)$$

と表せるので，$d_0 \mid d$ が従う．

p.42 上から 9 行目　$m = 0$ と仮定すると，$n = mk = 0 \cdot k = 0$ となるので，命題 4.2 の仮定「n を 0 でない整数とする」に反する．

p.42 下から 11 行目　$d_0 := \mathrm{g.c.d.}(m, n)$ は m と n の公約数だから，$m = d_0 m_0$, $n = d_0 n_0$ $(m_0, n_0 \in \mathbb{Z})$ と表せる．このとき，問 2.9 より m_0 と n_0 は互いに素である．したがって，あたえられた合同式を $d_0 m_0 a \equiv d_0 m_0 b \pmod{d_0 n_0}$ と書き直しておくと，まず，命題 4.2 (1) より $m_0 a \equiv m_0 b \pmod{n_0}$ がなりたち，m_0 と n_0 が互いに素であることに注意して命題 4.2 (2) を用いると，所望（しょもう）の合同式 $a \equiv b \pmod{n_0}$ を得る．

p.42 下から 10 行目　命題3.7 (2) より, 自明な合同式 $m \equiv m \pmod{n}$ と $a \equiv b \pmod{n}$ をかけ合わせてもよいので $\Longrightarrow$ の主張がなりたつ（この主張には m と n が互いに素という仮定は**必要ない！**）．一方で $\Longleftarrow$ の主張は命題 4.2 (2) より従う（こちらは m と n が互いに素という仮定が核心的である）．

p.43 上から 2 行目　例えば $a=27,\ b=19$ とすると，$a-b=8=4\cdot 2$ であるから $(\star\star)$: $a\equiv b \pmod 4$ はなりたつが，$(\star)$: $a\equiv b \pmod{12}$ はなりたたない．

p.43 下から 3 行目　$a,\ d,\ n$ を $D:=\mathrm{g.c.d.}(a,n)$ で割った商をそれぞれ $a_0,\ d_0,\ n_0$ とすると，問 2.9 より a_0 と n_0 は互いに素である．さらに，(4.1) を $a_0Dx\equiv d_0D \pmod{n_0D}$ とおくと，命題 4.2 (1) より $a_0x\equiv d_0 \pmod{n_0}$ もなりたつ．

p.44 下から 1 行目　$d_0:=\mathrm{g.c.d.}(a,n)$ は a と n の公約数なので，$a=a_0d_0,\ n=n_0d_0$ $(a_0,\ n_0\in\mathbb{Z})$ と表せる．ここで，$aw_0\equiv 1 \pmod n$ をみたす $w_0\in\mathbb{Z}$ が存在すると仮定すると，$aw_0-1=nk$ $(k\in\mathbb{Z})$ と表せるが，このとき $1=aw_0-nk=d_0(a_0w_0-n_0k)$ より $d_0\mid 1$ がなりたつ．1 の約数は ± 1 のみであるが，$d_0\neq 1$ と仮定していたので矛盾が生じた．したがって $\mathrm{g.c.d.}(a,n)\neq 1$ のときには，法 n での a の逆元 $a^{-1} \pmod n$ は存在しない．

p.50 下から 5 行目　**対偶**を示す．$i,j\in\{0,1,2,\ldots,n-1\}$ において $ai\equiv aj \pmod n$ がなりたつならば，$i=j$ であることを示せばよい．実際，仮定より a は n と互いに素なので，命題 4.2 (2) を $ai\equiv aj \pmod n$ に適用して $i\equiv j \pmod n$ を得る．つまり $i-j$ は n の倍数であるが，i,j の条件より $-(n-1)\leq i-j\leq n-1$ がなりたっているので，$i-j=0$，すなわち $i=j$ がなりたつ．

p.51 上から 2 行目　$aw_1\equiv 1 \pmod n$ および $aw_2\equiv 1 \pmod n$ がなりたっているとき，$w_1\equiv w_w \pmod n$ がなりたつことを示せばよい．ところが $aw_1\equiv 1\equiv aw_2 \pmod n$ であるから，$\mathrm{g.c.d.}(a,n)$ に注意して命題 4.2 (2) を用いると $w_1\equiv w_2 \pmod n$ が従う．

p.53 上から 6 行目　まず，$\begin{cases} x\equiv 0 \pmod 3 \\ x\equiv 3 \pmod 5 \\ x\equiv 0 \pmod 7 \end{cases}$ の解 x_2 を求めよう．第 1 式，第 3 式より，x_2 は 3 の倍数かつ 7 の倍数なので，x_2 は 21 の倍数であり，$x_2=21\tilde{x}_2$ $(\tilde{x}_2\in\mathbb{Z})$ と表せる．これを第 2 式に代入して，1 次合同式

$$21\tilde{x}_2\equiv 3 \pmod 5 \qquad \therefore\ \tilde{x}_2\equiv 3 \pmod 5$$

を得る．とくに $\tilde{x}_2=3$ として $x_2=21\tilde{x}_2$ に代入すると $x_2=21\cdot 3=63$ となる．定理 4.17 より，この連立 1 次合同式の解は法 $3\cdot 5\cdot 7=105$ で一意に定まるので，解は $x_2\equiv 63 \pmod{105}$ である（実際 $63=3\cdot 21+0=5\cdot 12+3=7\cdot 3+0$ がなりたっている）．

続いて，$\begin{cases} x \equiv 0 \pmod 3 \\ x \equiv 0 \pmod 5 \\ x \equiv 2 \pmod 7 \end{cases}$ の解 x_3 を求めよう．第 1 式，第 2 式より，x_3 は 3 の倍数かつ 5 の倍数なので，x_3 は 15 の倍数であり，$x_3 = 15\tilde{x}_3$ $(\tilde{x}_3 \in \mathbb{Z})$ と表せる．これを第 3 式に代入して，1 次合同式

$$15\tilde{x}_3 \equiv 2 \pmod 7 \qquad \therefore\ \tilde{x}_3 \equiv 2 \pmod 7$$

を得る．とくに $\tilde{x}_3 = 2$ として $x_3 = 15\tilde{x}_3$ に代入すると $x_3 = 15 \cdot 2 = 30$ となる．定理 4.17 より，この連立 1 次合同式の解は法 $3 \cdot 5 \cdot 7 = 105$ で一意に定まるので，解は $x_3 \equiv 30 \pmod{105}$ である（実際 $30 = 3 \cdot 10 + 0 = 5 \cdot 6 + 0 = 7 \cdot 4 + 2$ がなりたっている）．

$\boxed{\text{p.55 下から 8 行目}}$　〔**コメント**：ここでは，数学的帰納法ではなく，命題 2.19，命題 2.21 の証明を直接拡張します．そちらの方がわかりやすいので〕　一般に，自然数 a_i $(i = 1, 2, \ldots, s)$ が (2.6) の形で $a_i = \prod_{p:\ 素数} p^{e_p^i}$ $(e_p^i \in \mathbb{Z}_{\geq 0}$, 有限個の p を除いて 0) と表されているとする．このとき，$m = \prod_{p:\ 素数} p^{h_p}$ が $a_1, a_2, \ldots, a_s$ の公倍数であることと，$m/a_i = \prod_{p:\ 素数} p^{h_p - e_p^i}$ がすべての $i = 1, 2, \ldots, s$ に対して整数になること，つまり，すべての素数 p と i に対して $h_p \geq e_p^i$ がなりたつことが同値である．したがって，$a_1, a_2, \ldots, a_s$ の正の公倍数の最小値は，各素数 p の指数を $e_p^1, e_p^2, \ldots, e_p^s$ の最大値としたものとなるので

$$\mathrm{l.c.m}(a_1, a_2, \ldots, a_s) = \prod_{p:\ 素数} p^{\max\{e_p^1, e_p^2, \ldots, e_p^s\}}$$

がなりたつ．また，各 p, i に対して $e_p^i \leq h_p$ がなりたつことと，$\max\{e_p^1, e_p^2, \ldots, e_p^s\} \leq h_p$ がなりたつことは同値ゆえ，$a_1, a_2, \ldots, a_s$ の任意の（正の）公倍数は $\mathrm{l.c.m.}(a_1, a_2, \ldots, a_s)$ の倍数となることが示された．

$\boxed{\text{p.55 下から 6 行目}}$　〔**コメント**：こちらも数学的帰納法ではなく，直接示します〕　まず，$a_i = \prod_{p:\ 素数} p^{e_p^i}$ で表される自然数 $a_1, a_2, \ldots, a_s$ の**どの 2 つを選んでも互いに素である**という条件は，各素数 p において $e_p^i > 0$ をみたす i が高々 1 個であることと同値である（実際，$e_p^{i_0}, e_p^{j_0} > 0$ であったとすると，a_{i_0} と a_{j_0} は非自明な公約数 p を持つことになってしまい，互いに素ではなくなってしまう）．このとき，$p^{\max\{e_p^1, e_p^2, \ldots, e_p^s\}}$ は，$a_1, a_2, \ldots, a_s$ の中で **p を素因子にもつものの素因子**を表しているので，これを各素数 p についてかけ合わせれば，$a_1 a_2 \cdots a_s$ の素因数分解が得られる．以上より，$a_1, a_2, \ldots, a_s$ のどの 2 つを選ん

でも互いに素であれば，$\mathrm{l.c.m.}(a_1, a_2, \ldots, a_s) = a_1 a_2 \cdots a_s$ がなりたつことが示された．

※ 状況がわかりにくければ，$a_1 = 3^3 \cdot 7^2 \cdot 13$, $a_2 = 2^4 \cdot 5^2 \cdot 19$, $a_3 = 11^3 \cdot 17$ など，具体的な数で計算してみるとよい．

p.55 下から 3 行目　$\mathrm{g.c.d.}(n_k, N_k) \neq 1$ と仮定し，その素因子 p を 1 つ選ぶ．このとき，p は n_k と $N_k = n_1 n_2 \cdots n_{k-1} n_{k+1} \cdots n_s$ の公約数となる．さらにユークリッドの補題［⇨**命題 2.11**］より，p は $n_1, n_2, \ldots, n_{k-1}, n_{k+1}, \ldots, n_s$ のいずれか（n_l とする）を割り切ることになるが，これは n_k と n_l が互いに素であるという仮定と反する．したがって，背理法により，$\mathrm{g.c.d}(n_k, N_k) = 1$ であることが示された．

p.58 下から 5 行目　$\mathrm{g.c.d.}(36, 40) = 4$ であり，$-17 - (-1) = -16$ より，確かに合同式 $-17 \equiv -1 \pmod{\mathrm{g.c.d.}(36, 40)}$ がなりたつ．続いて，$\mathrm{g.c.d.}(36, 60) = 12$ であり，$-17 - 19 = -36$ より，確かに $-17 \equiv 19 \pmod{\mathrm{g.c.d.}(36, 60)}$ もなりたつ．最後に $\mathrm{g.c.d.}(40, 60) = 20$ であり，$-1 - 19 = -20$ より，確かに $-1 \equiv 19 \pmod{\mathrm{g.c.d.}(40, 60)}$ もなりたつ．

p.59 上から 3 行目　まず $\begin{cases} x \equiv -1 & \pmod 8 \\ x \equiv 0 & \pmod 9 \\ x \equiv 0 & \pmod 5 \end{cases}$ の解 x_1 を求めよう．第 2 式，第 3 式より，x_1 は 9 の倍数かつ 5 の倍数なので，x_1 は 45 の倍数であり，$x_1 = 45\tilde{x}_1$ $(\tilde{x}_1 \in \mathbb{Z})$ と表せる．これを第 1 式に代入して，1 次合同式

$$45\tilde{x}_1 \equiv -1 \pmod 8 \qquad \therefore\ 5\tilde{x}_1 \equiv -1 \pmod 8$$

を得る．両辺に $5^{-1} \equiv -3 \pmod 8$ をかけて $\tilde{x}_1 \equiv 3 \pmod 8$ となるので，とくに $\tilde{x}_1 = 3$ として $x_1 = 45\tilde{x}_1$ に代入すると $x_1 = 45 \cdot 3 = 135$ となる．定理 4.17 より，この連立 1 次合同式の解は法 $8 \cdot 9 \cdot 5 = 360$ で一意に定まるので，解は $x_1 \equiv 135 \pmod{360}$ である（実際，$135 = 8 \cdot 17 - 1 = 9 \cdot 15 + 0 = 5 \cdot 27 + 0$ が成り立っている）．

続いて $\begin{cases} x \equiv 0 & \pmod 8 \\ x \equiv 1 & \pmod 9 \\ x \equiv 0 & \pmod 5 \end{cases}$ の解 x_2 を求めよう．第 1 式，第 3 式より，x_2 は 8 の倍数かつ 5 の倍数なので，x_2 は 40 の倍数であり，$x_2 = 40\tilde{x}_2$ $(\tilde{x}_2 \in \mathbb{Z})$ と表せる．これを第 2 式に代入して，1 次合同式

$$40\tilde{x}_2 \equiv 1 \pmod 9 \qquad \therefore\ 4\tilde{x}_2 \equiv 1 \pmod 9$$

を得る．両辺に $4^{-1} \equiv -2 \pmod 9$ をかけて $\tilde{x}_2 \equiv -2 \pmod 9$ となるので，とくに $\tilde{x}_2 = -2$

として $x_2 = 40\tilde{x}_2$ に代入すると $x_2 = 40 \cdot (-2) = -80$ となる．定理 4.17 より，この連立 1 次合同式の解は法 $8 \cdot 9 \cdot 5 = 360$ で一意に定まるので，解は $x_2 \equiv -80 \pmod{360}$ である（実際，$-80 = 8 \cdot (-10) + 0 = 9 \cdot (-9) + 1 = 5 \cdot (-16) + 0$ が成り立っている）．

最後に $\begin{cases} x \equiv 0 & \pmod 8 \\ x \equiv 0 & \pmod 9 \\ x \equiv -1 & \pmod 5 \end{cases}$ の解 x_3 を求めよう．第 1 式，第 2 式より，x_3 は 8 の倍数かつ 9 の倍数なので，x_3 は 72 の倍数であり，$x_3 = 72\tilde{x}_3$ $(\tilde{x}_3 \in \mathbb{Z})$ と表せる．これを第 3 式に代入して，1 次合同式

$$72\tilde{x}_3 \equiv -1 \pmod 5 \qquad \therefore\ 2\tilde{x}_3 \equiv -1 \pmod 7$$

を得る．両辺に $2^{-1} \equiv -2 \pmod 5$ をかけて $\tilde{x}_3 \equiv 2 \pmod 5$ となるので，とくに $\tilde{x}_3 = 2$ として $x_3 = 72\tilde{x}_3$ に代入すると $x_3 = 72 \cdot 2 = 144$ となる．定理 4.17 より，この連立 1 次合同式の解は法 $8 \cdot 9 \cdot 5 = 360$ で一意に定まるので，解は $x_3 \equiv 144 \pmod{360}$ である（実際，$144 = 8 \cdot 18 + 0 = 9 \cdot 16 + 0 = 5 \cdot 29 + -1$ が成り立っている）．

以上より，解 $x \equiv x_1 + x_2 + x_3 \equiv 135 - 80 + 144 \equiv 199 \pmod{360}$ を得る．

§5 の ✍ のマーク

p.64 上から 8 行目　表 5.2 の「2 の段」，すなわち $a \equiv 2 \pmod 7$ の行の数をすべてかけ合わせると，

$$(2 \cdot 1) \cdot (2 \cdot 2) \cdot (2 \cdot 3) \cdot (2 \cdot 4) \cdot (2 \cdot 5) \cdot (2 \cdot 6) \equiv 2 \cdot 4 \cdot 6 \cdot 1 \cdot 3 \cdot 5 \pmod 7$$
$$\therefore\ (6!)2^6 \equiv 6! \pmod 7$$

を得る．ここで，$6! = 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1$ は 7 と互いに素なので，上式の両辺を $6!$ で割ると［⇨ **命題 4.2** (2)］ $2^6 \equiv 1 \pmod 7$ を得る．

p.65 下から 6 行目　表 5.3 (右) で「1 の段」の数をすべてかけ合わせると，

$$(1 \cdot 1) \cdot (1 \cdot 3) \cdot (1 \cdot 7) \cdot (1 \cdot 9) \equiv 1 \cdot 3 \cdot 7 \cdot 9 \pmod{10}$$
$$\therefore\ (1 \cdot 3 \cdot 7 \cdot 9)1^4 \equiv 1 \cdot 3 \cdot 7 \cdot 9 \pmod{10}$$

となり，$1 \cdot 3 \cdot 7 \cdot 9$ は 10 と互いに素であるから命題 3.7 (2) より $1^4 \equiv 1 \pmod{10}$ が従う．同様に，表 5.3 (右) で「3 の段」の数をすべてかけ合わせると，

$$(3 \cdot 1) \cdot (3 \cdot 3) \cdot (3 \cdot 7) \cdot (3 \cdot 9) \equiv 3 \cdot 9 \cdot 1 \cdot 7 \pmod{10}$$

$$\therefore\quad (1\cdot 3\cdot 7\cdot 9)3^4 \equiv 1\cdot 3\cdot 7\cdot 9 \pmod{10}$$

となり，$1\cdot 3\cdot 7\cdot 9$ は 10 と互いに素であるから命題 3.7 (2) より $3^4 \equiv 1 \pmod{10}$ が従う．同様に，表 5.3 (右) で「9 の段」の数をすべてかけ合わせると

$$(9\cdot 1)\cdot(9\cdot 3)\cdot(9\cdot 7)\cdot(9\cdot 9) \equiv 9\cdot 7\cdot 3\cdot 1 \pmod{10}$$
$$\therefore\quad (1\cdot 3\cdot 7\cdot 9)9^4 \equiv 1\cdot 3\cdot 7\cdot 9 \pmod{10}$$

となり，$1\cdot 3\cdot 7\cdot 9$ は 10 と互いに素であるから命題 3.7 (2) より $9^4 \equiv 1 \pmod{10}$ が従う．

p.67 下から 9 行目　$k < p$ なる自然数 k に対しては，k は p を約数にもちえないので $\mathrm{g.c.d.}(k,p) = 1$ である．したがって，$1, 2, \ldots, p$ の p 個の整数の中で，p と互いに素でないものは $\mathrm{g.c.d.}(p,p) = p$ となる p のみなので，$\varphi(p) = p - 1$ が従う．

p.70 下から 5 行目　〔**コメント**：【p.20 下から 6 行目】の ✍ と同じ〕　$d = \mathrm{g.c.d}(a,p)$ とおくと，$d \mid p$ であるから，素数の定義［⇨ **定義 1.6**］（と不等式 $d > 0$）より $d = 1$ または $d = p$ となる．ここで，もし $d = p$ であると仮定すると，d は定義から a と p の公約数なので $a = p \mid a$ がなりたつが，これは仮定 $p \nmid a$ と矛盾する．したがって，$d \neq p$ であるため，$d = 1$，すなわち a と p が互いに素であることが示された．

p.71 上から 4 行目　$d = \mathrm{g.c.d.}((p-1)!, p) \neq 1$ とすると，$d \mid p$ かつ $d \neq 1$ だから $d = p$ となる．したがって $p \mid (p-1)!$ であるから，ユークリッドの補題［⇨ **命題 2.11**］より p は $1, 2, \ldots, p-1$ のいずれかを割り切ることになる．ところが，$1, 2, \ldots, p-1$ はいずれも p より真に小さい自然数であり，p を約数にもちえないので矛盾する．したがって，$\mathrm{g.c.d.}((p-1)!, p) = 1$ が従う．

p.72 下から 10 行目　$r_n(k)$ の定義から $k = nq_1 + r_n(k)$ $(q_1 \in \mathbb{Z})$ と表されるので，もし $r_n(k)$ と n が互いに素でないならば，k は $d_1 := \mathrm{g.c.d.}(r_n(k), n) > 1$ の倍数となる．とくに k と mn は公約数 $d_1 > 1$ をもつため，互いに素とならず矛盾する．したがって，$r_m(k)$ と m は互いに素である．

p.72 下から 1 行目　$k \in \Phi_{mn}$ に対して，$G \circ F(k) \equiv G(r_m(k), r_n(k))$ は，定義から連立 1 次合同式

$$\begin{cases} x \equiv r_m(k) \pmod{m} \\ x \equiv r_n(k) \pmod{n} \end{cases} \qquad \cdots (*)$$

の解 x_0 で $0 \leq x_0 \leq mn - 1$ をみたす唯一のものである．一方で，$r_m(k)$ と $r_n(k)$ の定

義から $k = mq_1 + r_m(k) = nq_2 + r_n(k)$ $(q_1, q_2, \in \mathbb{Z})$ と表され，$k \equiv r_m(k) \pmod{m}$ および $k \equiv r_n(k) \pmod{n}$ がなりたつので k は $(*)$ の解であり，さらに k の選び方から $0 \leq k \leq mn - 1$ をみたす．中国式剰余定理［⇨ **定理 4.17**］より，$(*)$ の解は法 mn で一意に定まるので，k は $0 \leq k \leq mn - 1$ をみたす唯一の $(*)$ の解となる．したがって $G(r_m(k), r_n(k)) = k$ となるため $G \circ F = \mathrm{id}_{\Phi_{mn}}$ が示された．

逆に，$(a, b) \in \Phi_m \times \Phi_n$ に対して，連立 1 次合同式

$$\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases} \quad \cdots (**)$$

の解で $0 \leq x \leq mn - 1$ をみたす唯一のものを $x_{a,b}$ とおくと，$G(a, b) = x_{a,b}$ となる．このとき，$(**)$ より $x_{a,b} \equiv a \pmod{m}$ であるから，注意 3.4（の ✍ マーク）より $x_{a,b}$ を m で割った余り $r_m(x_{a,b})$ と a を m で割った余りが一致する．一方で $a \in \Phi_m$ より $0 \leq a < m$ であるから，余りの定義より a を m で割った余りは a 自身であるから，$r_m(x_{a,b}) = a$ がなりたつ．まったく同様に，$x_{a,b} \equiv b \pmod{n}$ であるから $r_n(x_{a,b}) = r_n(b) = b$ もなりたつ．以上より，

$$F \circ G(a, b) = F(x_{a,b}) = (r_m(x_{a,b}), r_n(x_{a,b})) = (a, b)$$

と計算できるので，$F \circ G = \mathrm{id}_{\Phi_m \times \Phi_n}$ がなりたつことが示された．

p.76 下から 2 行目　すでに計算したように，$k_0 l_0$ は $(ab)^{l_0 l_0} \equiv 1 \pmod{p}$ $\cdots$ $(\star)$ をみたすので，もし $(ab)^e \equiv 1 \pmod{p}$ をみたす任意の自然数 e が $e \geq k_0 l_0$ をみたすことが示されたら，$k_0 l_0$ は $(\star)$ をみたす**最小の**自然数となるため，位数の定義より $k_0 l_0$ が ab の法 p での位数となることが従う．

p.77 上から 3 行目

$$1 \equiv (ab)^e \equiv (ab)^{ek_0} \equiv (a^{k_0})^e b^{ek_0} \equiv 1 \cdot b^{ek_0} \equiv b^{ek_0} \pmod{p}$$

であるから，命題 5.24 (1) より $l_0 \mid ek_0$ が従う．一方で，仮定より k_0 と l_0 は互いに素であるから，命題 2.14 より $l_0 \mid e$ が従う．

p.77 上から 13 行目　**対偶**を示す．$i, j \in \{0, 1, 2, \ldots, k_0 - 1\}$（ただし，$i \geq j$ としておく）に対して $a^i \equiv a^j \pmod{p}$ $\cdots$ $(\diamond)$ がなりたつ（つまり a^i と a^j が法 p で一致する）ならば，$i = j$ がなりたつことを示す．$a \not\equiv 0 \pmod{p}$ より p と a は互いに素であるため，命題 4.6 より a の法 a での逆元が存在する．そこで $(\diamond)$ の両辺に $a^{-j} := (a^{-1})^j \pmod{p}$ をかけると $a^{i-j} \equiv 1 \pmod{p}$ であり，かつ i, j の選び方から $0 \leq i - j < k_0$ をみたす．

$i-j$ が 0 より大きいと仮定すると，k_0 の定義（$a^{k_0} \equiv 1 \pmod p$ をみたす**最小の**自然数であること）と矛盾するので，$i-j=0$，すなわち $a^i \equiv a^j \pmod p$ が従う．

p.77 下から 1 行目　まず，$(a^{k_0/\tilde{k}_0})^{\tilde{k}_0} = a^{k_0} \equiv 1 \pmod p$ である（k_0 は a の法 p での位数なので）．一方で，$1 \leq m < \tilde{k}_0$ をみたす $m \in \mathbb{N}$ に対して $m\dfrac{k_0}{\tilde{k}_0} < \tilde{k}_0\dfrac{k_0}{\tilde{k}_0} = k_0$ であるから，$(a^{k_0/\tilde{k}_0})^m = a^{(mk_0)/\tilde{k}_0}$ は法 p で 1 と合同にはならない（a の位数 k_0 は $a^{k_0} \equiv 1 \pmod p$ をみたす**最小の**自然数だから）．したがって，$\tilde{k}_0$ は，$(a^{k_0/\tilde{k}_0})^{\tilde{k}_0} \equiv 1 \pmod p$ をみたす最小の自然数であるから，法 p での $a^{k_0/\tilde{k}_0}$ の位数となる．$\tilde{l}_0$ についても，まったく同様である（各自で証明を付けてみること）．

p.78 上から 1 行目　$l_0 \mid k_0$ であったと仮定すると，$k_0 = l_0 q$ $(q \in \mathbb{Z})$ と表せるので，合同式 $b^{k_0} \equiv (b^{l_0})^q \equiv 1 \pmod p$ がなりたつ．ところが，b は $x^{k_0} \equiv 1 \pmod p$ の解 $a_0, a_1, \ldots, a^{k_0-1}$ のいずれとも異なるように選んでいたはずなので矛盾する．ゆえに $l_0 \nmid k_0$ が従う．

p.80 上から 4 行目　〔**コメント**：命題 7.20 (1) の証明とほぼ同じ〕　$g^i \equiv g^j \pmod p$ $(0 \leq i < j \leq p-1)$ がなりたつと仮定して矛盾を導く（**背理法**）．両辺に $(g^{-1})^i \pmod p$ をかけて $g^{j-i} \equiv 1 \pmod p$ を得るが，$0 \leq j-i < p-1$ であるから，g が原始根であること（すなわち，g を $(p-1)$ 乗して初めて 1 と合同となること）より $j-i=0$，すなわち $i=j$ を得るが，これは i と j を $i<j$ となるようにしていたことと矛盾する．

§6 の ✍ のマーク

p.88 下から 8 行目　まず，$e \in G_0$ と G_0 の任意の元 $e \in G_0$ に対して[1] $e * e = e$ であるから，e は G_0 の単位元となっており，(G1) がなりたつ．次に，G_0 の任意の元 $e \in G$ に対して $e * e = e$ であるから，e が e の逆元となっており，(G2) がなりたつ．最後に G_0 の任意の 3 元 $e, e, e \in G_0$ に対して $(e * e) * e = e * e = e = e * e = e * (e * e)$ がなりたつので，結合法則 (G3) もなりたっている．以上より G_0 が群であることが確認された．

p.89 上から 12 行目　a を n で割った商を q，余りを r とすると，定理 1.1（余りの特徴付け）から $r \in \{0, 1, 2, \ldots, n-1\}$ であり，定義より $a = nq + r \equiv r \pmod n$ であ

---

[1] 「任意の元」といっても e しか元がないのだから，e を考えることになる．以下同様．

るから $\overline{a}=\overline{r}$ がなりたつ.

$\boxed{\text{p.91 脚注 4)}}$　例えば $n=18$ のとき, $\overline{4}$ は乗法に関する逆元をもたない．実際, $\overline{4}\cdot\overline{w}=\overline{1}$ をみたす $w\in\mathbb{Z}$ が存在したとすると, $4w\equiv 1 \pmod{18}$ がなりたつことになるが, $4w-1=18k$ $(k\in\mathbb{Z})$ と表すと $2(2w-9k)=1$ という両辺の偶奇が一致しない等式が導き出されて矛盾する.

※ 一般に, n が合成数であるならば, a (ただし $n\nmid a$) と n が互いに素でなければ $\overline{a}\in\mathbb{Z}/n\mathbb{Z}$ の乗法に関する逆元は存在しない．実際，$\overline{a}$ が逆元 $\overline{w}$ をもつことは，$aw\equiv 1 \pmod{n}$ が整数解をもつことと同値であるが，後者の 1 次合同式は a と n が互いに素なときのみ整数解をもつのであった［⇨ **定理 4.16**］.

$\boxed{\text{p.92 上から 4 行目}}$　$\mu_n(\mathbb{C})$ は $z^n=1$ の複素数解の集合とみなすことができるので，$z^n=1\ \cdots\ (\dagger)$ の複素数解をすべて求めればよい．そこで z を $z=r(\cos\theta+i\sin\theta)$（$r$ は 0 以上の実数，$\theta\in\mathbb{R}$）と極形式表示して $(\dagger)$ に代入すると $r^n(\cos\theta+i\sin\theta)^n=1$ となるので，ド・モアヴルの定理より等式

$$r^n(\cos n\theta+i\sin n\theta)=1=1(\cos 2\pi k+i\sin 2\pi k)\qquad (k\in\mathbb{Z})$$

を得る（右辺は $1\in\mathbb{C}$ の極形式表示．偏角を一般角で表しておくのがポイント）．両辺の絶対値と偏角を比較して,

$$r^n=1,\quad n\theta=2\pi k\qquad \therefore\ r=1,\quad \theta=\frac{2\pi k}{n}$$

を得る．これらを z の極形式に戻して

$$z=\cos\frac{2\pi k}{n}+i\sin\frac{2\pi k}{n}\overset{\text{ド・モアヴルの定理}}{=}\left(\cos\frac{2\pi}{n}+i\sin\frac{2\pi}{n}\right)^k=\zeta_n^k$$

を得る．$\zeta_n^n=1$ であることに注意して，$z^n=1$ の複素数解の集合は

$$\mu_n(\mathbb{C})=\{1,\zeta_n,\zeta_n^2,\ldots,\zeta_n^{n-1}\}$$

となることが示された[2]．なお，一般角の性質より $\zeta_n^k=\zeta_n^{k+nq}$ $(q\in\mathbb{Z})$ がなりたつことに注意しよう.

$\boxed{\text{p.92 上から 7 行目}}$　まず，極形式の積の公式

---

[2] **代数学の基本定理**より，n 次方程式 $z^n=1$ は（重複を込めて）n 個の複素数解を持つはずであるが，確かに $\#\mu_n(\mathbb{C})=n$ となっている.

$$\{r(\cos\theta + i\sin\theta)\}\{R(\cos\varphi + i\sin\varphi)\} = rR\bigl(\cos(\theta+\varphi) + i\sin(\theta+\varphi)\bigr) \cdots (\sharp)$$

より

$$\begin{aligned}\zeta_n^k + \zeta_n^l &= \left(\cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{2n}\right)\left(\cos\frac{2\pi l}{n} + i\sin\frac{2\pi l}{2n}\right)\\ &\overset{\because(\sharp)}{=} \cos\frac{2\pi(k+l)}{n} + i\sin\frac{2\pi(k+l)}{n} = \zeta_n^{k+l} \qquad (k, l \in \mathbb{Z})\end{aligned}$$

がなりたつことに注意しよう．まず，任意の $\zeta_n^k \in \mu_n(\mathbb{C})$ と $1 = \zeta_n^0 \in \mu_n(\mathbb{C})$ に対して $1 \cdot \zeta_n^k = \zeta_n^k \cdot 1 = \zeta_n^k$ であるから，1 は $\mu_n(\mathbb{C})$ の単位元であり，(G1) がなりたつ．続いて，任意の $\zeta_n^k \in \mu_n(\mathbb{C})$ に対して $\zeta_n^k \cdot \zeta_n^{-k} = \zeta_n^{-k} \cdot \zeta_n^k = \zeta_n^{k-k} = \zeta_n^0 = 1$ より，ζ_n^{-k} が ζ_n^k の逆元となっており，(G2) もなりたつ．さらに，任意の ζ_n^k, ζ_n^l, $\zeta_n^m \in \mu_n(\mathbb{C})$ に対して $(\zeta_n^k\zeta_n^l)\zeta_n^m = \zeta_n^{k+l}\zeta_n^m = \zeta_n^{k+l+m} = \zeta_n^k\zeta_n^{l+m} = \zeta_n^k(\zeta_n^l\zeta_n^m)$ となるので，結合法則 (G3) もなりたつ．最後に，任意の $k, l \in \mathbb{Z}$ に対して $\zeta_n^k\zeta_n^l = \zeta_n^{k+l} = \zeta_n^{l+k} = \zeta_n^l\zeta_n^k$ より，交換法則 (Ab) もなりたっているので，$\mu_n(\mathbb{C})$ はアーベル群である．

p.94 上から 3 行目　定義より $\mathrm{GL}_1(\mathbb{K}) = \{(a) \mid \det(a) = a \in \mathbb{K}^\times\} = \mathbb{K}^\times$ であるから，$\mathrm{GL}_1(\mathbb{K}) = (\mathbb{K}^\times, \cdot)$ となる．乗法群 $(\mathbb{K}^\times, \cdot)$ がアーベル群であることはすでに例 6.9 で確認しているので，$\mathrm{GL}_1(\mathbb{K})$ はアーベル群である．

p.95 上から 3 行目　実際に $\begin{pmatrix} \overline{2} & \overline{1} \\ -\overline{2} & \overline{0} \end{pmatrix}$ と $\begin{pmatrix} \overline{0} & \overline{2} \\ \overline{1} & \overline{1} \end{pmatrix}$ の積を計算してみると

$$\begin{aligned}\begin{pmatrix} \overline{2} & \overline{1} \\ -\overline{2} & \overline{0} \end{pmatrix}\begin{pmatrix} \overline{0} & \overline{2} \\ \overline{1} & \overline{1} \end{pmatrix} &= \begin{pmatrix} \overline{2}\cdot\overline{0} + \overline{1}\cdot\overline{1} & \overline{2}\cdot\overline{2} + \overline{1}\cdot\overline{1} \\ -\overline{2}\cdot\overline{0} + \overline{0}\cdot\overline{1} & -\overline{2}\cdot\overline{2} + \overline{0}\cdot\overline{1} \end{pmatrix}\\ &= \begin{pmatrix} \overline{1} & \overline{5} \\ \overline{0} & -\overline{4} \end{pmatrix} = \begin{pmatrix} \overline{1} & \overline{0} \\ \overline{0} & \overline{1} \end{pmatrix} = I_2,\end{aligned}$$

$$\begin{aligned}\begin{pmatrix} \overline{0} & \overline{2} \\ \overline{1} & \overline{1} \end{pmatrix}\begin{pmatrix} \overline{2} & \overline{1} \\ -\overline{2} & \overline{0} \end{pmatrix} &= \begin{pmatrix} \overline{0}\cdot\overline{2} + \overline{2}(-\overline{2}) & \overline{0}\cdot\overline{1} + \overline{2}\cdot\overline{0} \\ \overline{1}\cdot\overline{2} + \overline{1}(-\overline{2}) & \overline{1}\cdot\overline{1} + \overline{1}\cdot\overline{0} \end{pmatrix}\\ &= \begin{pmatrix} -\overline{4} & \overline{1} \\ \overline{0} & \overline{1} \end{pmatrix} = \begin{pmatrix} \overline{1} & \overline{0} \\ \overline{0} & \overline{1} \end{pmatrix} = I_2\end{aligned}$$

となることが確認できる．

p.96 上から 5 行目　ベクトル $\boldsymbol{a}_k$ は

$$W_{k-1} = \{c_1\boldsymbol{a}_1 + c_2\boldsymbol{a}_2 + \cdots + c_{k-1}\boldsymbol{a}_{k-1} \mid c_1, c_2, \ldots, c_{p-1} \in \mathbb{F}_p\}$$

に含まれないように選ぶ必要がある．$(c_1, c_2, \ldots, c_{k-1}) \in \mathbb{F}_p^{k-1}$ の選び方は p^{k-1} 通りなので $\#W_{k-1} = p^{k-1}$ であり，したがって，ベクトル $\boldsymbol{a}_k$ の選び方の総数は $(p^n - p^{k-1})$ 通りである．

p.96 下から 4 行目　実際，任意の $\sigma \in \mathfrak{S}_X$ および $x \in X$ に対して，合成写像の定義 $(f \circ g)(x) = f\bigl(g(x)\bigr)$ より，

$$(\sigma \circ \mathrm{id}_X)(x) = \sigma\bigl(\mathrm{id}_X(x)\bigr) = \sigma(x), \qquad (\mathrm{id}_X \circ \sigma)(x) = \mathrm{id}_x\bigl(\sigma(x)\bigr) = \sigma(x)$$

がなりたつので，$\sigma \circ \mathrm{id}_X = \mathrm{id}_X \circ \sigma = \sigma$ から，id_X が $\mathfrak{S}_X$ の単位元となる．

p.96 下から 3 行目　実際，任意の $\sigma \in \mathfrak{S}_X$ および $x \in X$ に対して，逆写像の定義 $f^{-1}\bigl(f(x)\bigr) = f\bigl(f^{-1}(x)\bigr) = x$ より，

$$(\sigma \circ \sigma^{-1})(x) = \sigma\bigl(\sigma^{-1}(x)\bigr) = x = \mathrm{id}_X(x), \quad (\sigma \circ \sigma)(x) = \sigma\bigl(\sigma(x)\bigr) = x = \mathrm{id}_X(x)$$

がなりたつので，$\sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma = \mathrm{id}_X$ から，σ^{-1} が σ の逆元となる．

p.97 下から 8 行目　〔**コメント**:σ の全単射性の言い換えに過ぎない〕　まず $\sigma\colon X_n \to X_n$ は全射である，つまり，任意の $a \in X_n$ に対して $\sigma(i) = a$ をみたす $i \in X_n$ が存在するので，X_n の元はすべて $\sigma(i)$ の形で表されることになる．言い換えると，$\sigma(1), \sigma(2), \ldots, \sigma(n)$ には X_n の元 $1, 2, \ldots, n$ がすべて現れる．

一方で，σ は単射である，すなわち，$\sigma(i) = \sigma(j)$ ならば $i = j$ がなりたつ．これは，対偶をとると「i と j が異なる X_n の元ならば，$\sigma(i)$ と $\sigma(j)$ は異なる」ことを表しているのに他ならない．言い換えると，$\sigma(1), \sigma(2), \ldots, \sigma(n)$ は X_n の相異(あい)なる[3] 元となる．

以上より，$\sigma\colon X_n \to X_n$ が全単射（全射かつ単射）であるならば，$\sigma(1), \sigma(2), \ldots, \sigma(n)$ には $1, 2, \ldots, n$ が 1 度ずつ現れることがわかる．

p.98 上から 2 行目　$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$, $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$ だから

$$1 \quad 2 \quad 3 \quad 4 \quad \xrightarrow{\sigma\text{ で置換}} \quad 3 \quad 1 \quad 4 \quad 2 \quad \xrightarrow{\tau\text{ で置換}} \quad 2 \quad 4 \quad 3 \quad 1$$

---

[3] 複数のもの，数値などがどれも異なる（より正確には，どの 2 つを選んできても異なる）こと．英語では distinct という表現をよく用いる．

より，$\underleftarrow{\tau\sigma} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$ である．

p.99 上から 5 行目　$\mathfrak{S}_2 = \mathfrak{S}_{X_2}$ であるから，$\mathfrak{S}_2$ が群であることは命題 6.22 より従う．したがって，$\mathfrak{S}_2 = \{e, (1\,2)\}$ の任意の 2 元 e, $(1\,2)$ の積 ee, $e(1\,2)$, $(1\,2)e$, $(1\,2)(1\,2)$ に対して交換法則がなりたっていることを確認すればよい．直接，計算をしてみると，

$$ee = e = e, \qquad e(1\,2) = (1\,2) = (1\,2)e, \qquad (1\,2)(1\,2) = e = (1\,2)(1\,2)$$

となっており，確かに交換法則 (Ab) なりたっていることが観察される．

p.99 下から 10 行目　恒等置換は単位元なので 1 つである［⇨ **問 6.4** (1)］．互換は $(i\,j)$ の形をした置換であり，i の選び方は 4 通り，j の選び方は（i 以外の）3 通りであるが，$(i\,j)$ と $(j\,i)$ は同じ互換を表すので，互換の総数は $\dfrac{4\cdot 3}{2} = 6$ である．3 次巡回置換は $(i\,j\,k)$ の形をした置換であり，i の選び方は 4 通り，j の選び方は（i 以外の）3 通り，k の選び方は（i, j 以外の）2 通りであるが，$(i\,j\,k)$, $(j\,k\,i)$, $(k\,i\,j)$ は同じ互換を表すので，3 次巡回置換の総数は $\dfrac{4\cdot 3\cdot 2}{3} = 8$ である．4 次巡回置換は $(i\,j\,k\,l)$ の形をした置換であり，i の選び方は 4 通り，j の選び方は（i 以外の） 3 通り，k の選び方は（i, j 以外の）2 通り，l の選び方は（i, j, k 以外の）1 通りであるが，$(i\,j\,k\,l)$, $(j\,k\,l\,i)$, $(k\,l\,i\,j)$, $(l\,i\,j\,k)$ は同じ互換を表すので，4 次巡回置換の総数は $\dfrac{4\cdot 3\cdot 2\cdot 1}{4} = 6$ である．

§7 の ✍ のマーク

p.108 上から 2 行目　$(H, *)$ は群なので，群の定義 (G2) より任意の $a \in H$ に関して a の逆元 $a' \in H$ が存在する．したがって，(H2) がなりたつ．また，$(H, *)$ は群なので，任意の 2 元 $a, b \in H$ に対して $a * b \in H$ が定義されるため (H3) もなりたつ．

p.108 下から 7 行目　任意の $a \in H$ に対して[4]，(H2) より a の逆元 $a' \in H$ が（H の元として）存在し，さらに，(H3) より $e_G = a * a'$ は (H3) の元となる．したがって，(H1) $e_G \in H$ が示された．

---

[4] この「H の元 a がとれる」という最初の一歩の部分で「$H \neq \emptyset$」という条件が暗に使われている．さらに細かいことをいえば，$a * a' = e_H$（H の単位元）が G の単位元 e_G と一致することには単位元の一意性［⇨ **問 6.4** (1)］を用いている．

p.110 上から 9 行目 σ と $\tau := \gamma_{2k}\gamma_{2k-1}\cdots\gamma_2\gamma_1$ が $\sigma\tau = \tau\sigma = e$ をみたすことを確認すれば，逆元の一意性［⇨ **問 6.4** (2)］より，$\tau = \sigma^{-1}$ であることが示される．なお，各 γ_j は互換なので，$\gamma_j\gamma_j = e$ をみたすことに注意しよう．このとき，

$$\begin{aligned}
\sigma\tau &= \gamma_1\gamma_2\cdots\gamma_{2k-1}\underbrace{\gamma_{2k}\gamma_{2k}}_{=e}\gamma_{2k-1}\cdots\gamma_2\gamma_1 \\
&= \gamma_1\gamma_2\cdots\gamma_{2k-2}\underbrace{\gamma_{2k-1}\gamma_{2k-1}}_{=e}\gamma_{2k-2}\cdots\gamma_2\gamma_1 \\
&= \cdots = \gamma_1\gamma_1 = e, \\
\tau\sigma &= \gamma_{2k}\gamma_{2k-1}\cdots\gamma_2\underbrace{\gamma_1\gamma_1}_{=e}\gamma_2\cdots\gamma_{2k-1}\gamma_{2k} \\
&= \gamma_{2k}\gamma_{2k-1}\cdots\gamma_3\underbrace{\gamma_2\gamma_2}_{=e}\gamma_3\cdots\gamma_{2k-1}\gamma_{2k} \\
&= \cdots = \gamma_{2k}\gamma_{2k} = e
\end{aligned}$$

より，所望（しょもう）の等式 $\sigma\tau = \tau\sigma = e$ がなりたつことが確認できた．

p.112 下から 10 行目 逆行列の公式より，

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}^{-1} = (ad - b\cdot 0)^{-1}\begin{pmatrix} d & -b \\ 0 & a \end{pmatrix} = ad^{-1}\begin{pmatrix} d & -b \\ 0 & a \end{pmatrix} = \begin{pmatrix} a^{-1} & -ba^{-1}d^{-1} \\ 0 & d^{-1} \end{pmatrix}$$

となる．

p.112 下から 8 行目 実際に $\begin{pmatrix} a_1 & b_1 \\ 0 & d_1 \end{pmatrix}, \begin{pmatrix} a_2 & b_2 \\ 0 & d_2 \end{pmatrix} \in \mathrm{B}_2(\mathbb{K})$ に対して，

$$\begin{pmatrix} a_1 & b_1 \\ 0 & d_1 \end{pmatrix}\begin{pmatrix} a_2 & b_2 \\ 0 & d_2 \end{pmatrix} = \begin{pmatrix} a_1a_2 & a_1b_2 + b_1d_2 \\ 0 & d_1d_2 \end{pmatrix}$$

は上三角行列であり，$\mathrm{B}_2(\mathbb{K})$ の元である．

p.112 下から 1 行目 線形代数の一般論より，n 次正方行列が正則行列である（すなわち逆行列をもつ）ことと，その行列式が 0 でないことは同値である［⇨［藤岡 1］9 · 3］．一方で，上三角行列 $A = (a_{i,j})_{1\le i,j\le n}$（ただし，$1 \le j < i \le n$ のとき $a_{ij} = 0$）の行列式は，その対角成分の積 $\det A = a_{11}a_{22}\cdots a_{nn}$ として計算されるのであった．したがって，上三角行列が正則行列であることは，その対角成分の積 $a_{11}a_{22}\cdots a_{nn}$ が 0 ではないこと，

すなわち，各対角成分 a_{ii} $(i=1,2,\ldots,n)$ が 0 ではない（$\mathbb{K}^\times=\mathbb{K}\setminus\{0\}$ の元である）ことと同値となる．

$\boxed{\text{p.116 上から 8 行目}}$ 〔**コメント**：通常の指数法則とまったく同じである〕 m,n がともに正の整数のときは

$$a^{*m}*a^{*n}=\underbrace{\underbrace{a*a*\cdots*a}_{m\text{ 個}}*\underbrace{a*a*\cdots*a}_{n\text{ 個}}}_{(m+n)\text{ 個}}=a^{*(m+n)}$$

がなりたち，m,n がともに負の整数のときは

$$a^{*m}*a^{*n}=\underbrace{\underbrace{a'*a'*\cdots*a'}_{(-m)\text{ 個}}*\underbrace{a'*a'*\cdots*a'}_{(-n)\text{ 個}}}_{\{-(m+n)\}\text{ 個}}=a^{*(m+n)}$$

がなりたつ．また，一方が 0 のときも，任意の整数 n に対して，

$$a^{*0}*a^{*n}\overset{\text{定義}}{=}e_G*a^{*n}\overset{\text{(G1)}}{=}a^{*n}=a^{*(0+n)}$$

がなりたつ．したがって，m と n が異符号のときのみが問題となる．以下，$m>0$, $n<0$ とし $n=-n_0$ $(n_0\in\mathbb{N})$ と表すことにしよう．このとき，$a*a'=e_G$ に注意すると

$$\begin{aligned}a^{*m}*a^{*n}&=\underbrace{a*a*\cdots*a}_{m\text{ 個}}*\underbrace{a'*a'*\cdots*a'}_{n_0\text{ 個}}\\&=\begin{cases}\underbrace{a*a*\cdots*a}_{(m-n_0)\text{ 個}}=a^{*(m-n_0)}=a^{*(m+n)} & (m>n_0\text{ のとき})\\ \underbrace{a'*a'*\cdots*a'}_{(n_0-m)\text{ 個}}=(a')^{*(n_0-m)}=a^{*(m+n)} & (m<n_0\text{ のとき})\end{cases}\end{aligned}$$

となるので，いずれの場合も $a^{*m}*a^{*n}=a^{*(m+n)}$ がなりたつことが確認できた．

$\boxed{\text{p.116 下から 9 行目}}$ 指数法則 $a^{*m}*a^{*n}=a^{*(m+n)}$ に注意すると，$\langle a\rangle$ の任意の元 $a_1*a_2*\cdots*a_r$ に対して，$a_1,a_2,\ldots,a_r$ の中に現れる a の個数を k 個，a' の個数を $l\,(=r-k)$ 個とすると，$a_1*a_2*\cdots*a_r=a^{*(k-l)}$ と計算できる．したがって，$\langle S\rangle\subset\{a^{*n}\mid n\in\mathbb{Z}\}$ がなりたつ．一方で，任意の a^{*n} $(n\in\mathbb{Z})$ は $\{a\}\cup\{a'\}$ の元の有限個の演算となっているので $\{a^{*n}\mid n\in\mathbb{Z}\}\subset\langle a\rangle$ も従う．以上より，$\langle S\rangle=\{a^{*n}\mid n\in\mathbb{Z}\}$ が示された．

$\boxed{\text{p.116 下から 5 行目}}$ 任意の $\overline{a}\in\mathbb{Z}/n\mathbb{Z}$ は

$$\overline{a} = \begin{cases} \underbrace{\overline{1} + \overline{1} + \cdots + \overline{1}}_{a\ \text{個}} & (a \geq 0\ \text{のとき}) \\ \underbrace{(-\overline{1}) + (-\overline{1}) + \cdots + (-\overline{1})}_{(-a)\ \text{個}} & (a < 0\ \text{のとき}) \end{cases}$$

と表されるので，加法群 $(\mathbb{Z}/n\mathbb{Z}, +)$ は $\overline{1}$ で生成される巡回群である．有限巡回群であることは，$\#\mathbb{Z}/n\mathbb{Z} = n$（有限値）より従う．

p.117 下から 4 行目 十分性とは，ここでは「$a^{*k} = e_G$ をみたす自然数 $k \in \mathbb{N}$ が存在するならば，$\langle a \rangle$ は有限巡回群である」という主張のことである．$G = \langle a \rangle$ が巡回群であることは仮定されているので，G の位数が有限であることを示せばよい．さて，G の任意の元は a^{*n} $(n \in \mathbb{Z})$ の形に表せる．ここで n を k で割り算して［⇨ **定理 1.1**］，$n = kq + r$ $(q, r \in \mathbb{Z},\ 0 \leq r < k)$ の形で表すと，

$$a^{*n} = a^{*(kq+r)} = \underbrace{(a^{*k})^{*q}}_{=e_G} * a^{*r} = a^{*r}$$

がなりたつ．つまり，G の任意の元は a^{*n} $(n = 0, 1, 2, \ldots, k-1)$ と表される．したがって，$\#G \leq k$ となるので，G は有限群である．

p.119 下から 1 行目 「位数 n の群が $(G, *)$ が巡回群 $\Rightarrow$ G が位数 n の元を含む」を示す．巡回群の定義より，$G = \langle g \rangle = \{e_G, g, g^{*2}, \ldots, g^{*(n-1)}\}$ をみたす元 $g \in G$ が存在する（G の生成元）．したがって，$\#\langle x \rangle = n$ であるから，G は位数 n の元を含む．

p.120 上から 4 行目 実際，

$$\overline{5}^2 = \overline{25} = \overline{1}, \quad \overline{7}^2 = \overline{49} = \overline{1}, \quad \overline{11}^2 = \overline{121} = \overline{1}$$

である．

p.120 下から 8 行目 法 p の原始根の定義［⇨ **定義 5.17**］より，$a^k \equiv 1 \pmod{p}$ をみたす最小の自然数 k は $\varphi(p) = p - 1$ である．このことを群 $((\mathbb{Z}/p\mathbb{Z})^\times, \cdot)$ の言葉で言い換えると，a が法 p の原始根であることは，$(\mathbb{Z}/p\mathbb{Z})^\times$ において $\overline{a}^k = \overline{1}$ をみたす最小の自然数 k が $p - 1$ であることを表しているのに他ならない．このとき，命題 7.25 (2) より $\overline{a}$ の $(\mathbb{Z}/p\mathbb{Z})^\times$ における位数は $p - 1$ である．

p.123 問 7.5 (1) 例題 6.16 とまったく同様に証明できる．

§8 の ✍ のマーク

p.129 下から 1 行目　$g\colon \mu_n(\mathbb{C}) \to \mathbb{Z}/n\mathbb{Z}$; $\zeta_n^k \mapsto \overline{k}$ が f の逆写像になっていることからわかる．実際，

$$g \circ f(\overline{k}) = g(\zeta_n^k) = \overline{k}, \qquad g \circ f(\zeta_n^k) = g(\overline{k}) = \zeta_n^k$$

より，$g \circ f = \mathrm{id}_{\mathbb{Z}/n\mathbb{Z}}$, $f \circ g = \mathrm{id}_{\mu_n(\mathbb{C})}$ がなりたつ．

p.129 脚注 1)　$\overline{k} = \overline{l}$ と仮定すると，これは $k \equiv l \pmod{n}$ と同値だから，$k - l = nq$ $(q \in \mathbb{Z})$ と表される．このとき，$\zeta_n^n = 1$ に注意すると，

$$\begin{aligned} f(\overline{l}) = \zeta_n^l = \zeta_n^{k-nq} &\overset{\text{指数法則}}{=} \zeta_n^k \cdot (\zeta_n^n)^q \\ &= \zeta_n^k \cdot 1^q = \zeta_n^k = f(\overline{k}) \end{aligned}$$

がなりたつので，f は $\mathbb{Z}/n\mathbb{Z}$ の元の表示（代表元の取り方）によらず矛盾なく定義されている．

p.130 上から 9 行目　任意の $a^{*k}, a^{*l} \in \langle a \rangle$ に対して，

$$f(a^{*k} * a^{*l}) = f(a^{*(k+l)}) = b^{\star(k+l)} = b^{\star k} \star b^{\star l} = f(a^{*k}) \star f(a^{*l})$$

がなりたつので，f は群準同型写像である．また，任意の $b^{*k} \in \langle b \rangle$ に対して $g(b^{\star k}) = a^{*k}$ と定義すると，$g \circ f(a^{*k}) = g(b^{\star k}) = a^{*k}$, $f \circ g(b^{\star k}) = f(a^{*k}) = g^{\star k}$ より，g は f の逆写像となるので，f は群同型写像となる［⇨ **問 8.4** (2)］．

p.130 上から 10 行目　**削除**〔**コメント**：有限巡回群のときとまったく同じなので，「(✍)」を削除します．第 2 版以降では削除済〕

p.130 下から 5 行目　$\log\colon \mathbb{R}_+ \to \mathbb{R}$ が全単射写像であることと，log が逆写像をもつことは同値であることから従う．

p.132 上から 5 行目　実際，任意の $a, b \in G_1$ に対して，

$$f(a * b) = e_{G_2} = e_{G_2} \star e_{G_2} = f(a) \star f(b)$$

がなりたつので，f は群準同型写像である．

p.135 下から 9 行目　f が全射であるならば，任意の $b \in G_2$ に対して $b = f(a)$ をみたす $a \in G_1$ が存在する．つまり，$b = f(a) \in \mathrm{Im}\, f$ となるので，$G_2 \subset \mathrm{Im}\, f$ が従う．もと

もと $\mathrm{Im}\, f$ は G_2 の部分集合（つまり $\mathrm{Im}\, f \subset G_2$）であるから，$\mathrm{Im}\, f = G_2$ が従う．

一方で $\mathrm{Im}\, f = G_2$ であるならば，任意の $b \in G_2 = \mathrm{Im}\, f = \{f(a) \mid a \in G_1\}$ は $b = f(a)$ $(a \in G_1)$ と表される．これは，f が全射であることを表しているのに他ならない．

p.135 下から 8 行目　準同型写像 f が同型写像であるとは，f が（準同型写像であり，かつ）全単射であることであった［⇨ **定義 8.2**］．したがって，f が全単射であることと $\mathrm{Ker}\, f = \{e_{G_1}\}$ かつ $\mathrm{Im}\, f = G_2$ がなりたつことが同値であることを示せばよいが，(2) より f の単射性と $\mathrm{Ker}\, f = \{e_{G_1}\}$ がなりたつことが同値であり，(3) より f の全射性と $\mathrm{Im}\, f = G_2$ がなりたつことが同値である．f が全単射であることは，f が単射かつ全射であることと同値であったので，結局，f の全単射性は $\mathrm{Ker}\, \{e_{G_1}\}$ かつ $\mathrm{Im}\, f = G_2$ がなりたつことと同値となる．

p.145 上から 5 行目　平面 Π 上の任意の 2 点 P, Q をとると，ρ は Π の合同変換なので (PQ 間の距離) = ($\rho(\mathrm{P})\rho(\mathrm{Q})$ 間の距離) がなりたち，τ も Π 上の合同変換なので，

$$\begin{aligned}(\rho(\mathrm{P})\rho(\mathrm{Q}) \text{ 間の距離}) &= (\tau(\rho(\mathrm{P}))\,\tau(\rho(\mathrm{Q})) \text{ 間の距離}) \\ &= (\tau \circ \rho(\mathrm{P}) \text{ と } \tau \circ \rho(\mathrm{Q}) \text{ の間の距離})\end{aligned}$$

がなりたつ．したがって，(PQ 間の距離) = ($\tau \circ \rho(\mathrm{P})$ と $\tau \circ \rho(\mathrm{Q})$ の間の距離) がなりたつので，$\tau \circ \rho$ は (9.1) をみたす．

p.145 上から 7 行目　平面 Π 上の任意の 2 点 P, Q をとると，ρ は Π の合同変換なので，

$$\begin{aligned}(\rho^{-1}(\mathrm{P})\rho^{-1}(\mathrm{Q}) \text{ 間の距離}) &= (\rho(\rho^{-1}(\mathrm{P}))\,\rho(\rho^{-1}(\mathrm{Q})) \text{ 間の距離}) \\ &= (\mathrm{PQ} \text{ 間の距離})\end{aligned}$$

がなりたつ．これは，ρ^{-1} が (9.1) をみたすことを表しているのに他ならない．

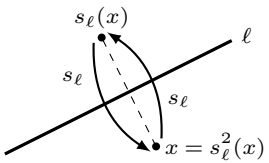
§9 の ✍ のマーク

p.145 下から 6 行目　部分群の条件 (H1), (H2), (H3) ［⇨ **命題 7.2**］を確認する．まず，恒等変換 e は任意の $x \in X$ を $e(x) = x$ にうつすので，$e(X) = X$ をみたす．したがって，$e \in \mathfrak{S}(X)$ となるので (H1) がなりたつ．続いて，一般に全単射写像 $f\colon X \to Y$

の部分集合 $A \subset X$ への制限 $f|_A\colon A \to f(A)$ は全単射になる[5]ことから，$\sigma \in \mathfrak{S}(X)$ に対して，σ^{-1} の X への制限 $\sigma^{-1}|_X\colon X \to X$ も全単射となる．つまり，$\sigma^{-1}(X) = X$ であるから $\sigma^{-1} \in \mathfrak{S}(X)$ となり，(H2) もなりたつ．最後に，$\sigma, \tau \in \mathfrak{S}(X)$ に対して $\tau \circ \sigma(X) = \tau(\sigma(X)) = \tau(X) = X$ であるから $\tau \circ \sigma \in \mathfrak{S}(X)$ となり，(H3) もなりたつ．以上より，$\mathfrak{S}(X)$ は $\mathfrak{S}(\Pi)$ の部分群である．

p.147 下から 1 行目　k を n で割り算して $k = nl + \rho_k$ $(l, \rho_k \in \mathbb{Z},\ 0 \leq \rho_k < n)$ と表しておこう．このとき，$r^k = r_1^k$ は，$k \geq 0$ のときは反時計回りに $\dfrac{2\pi}{n}$ 回転する回転移動を k 回続けて行う操作を表し，$k < 0$ のときは時計回りに $\dfrac{2\pi}{n}$ 回転する回転移動を $(-k)$ 回続けて行う操作を表す．一般角と同様に，「時計回りに θ 回転」は「反時計回りに $(-\theta)$ 回転」と解釈することにすると，r^k は，結局，（k の符号によらず）反時計回りに $\dfrac{2\pi k}{n} = 2\pi q + \dfrac{2\pi\rho_k}{n}$ 回転する操作を表す．ここで，「$2\pi q$ 回転移動する操作」は（反時計回り，または時計回りに）ちょうど $|q|$ 周する移動であり，結局，その図形に「何もしない」（恒等変換）ことと変わらない．したがって，r^k は「$\dfrac{2\pi\rho_k}{n}$ 回転移動」，すなわち r_{ρ_k} と一致する．$\rho_k = k \pmod n$ と表すことにすると，所望（しょもう）の等式 $r^k = r_{k \pmod n}$ が導かれる．

p.148 上から 2 行目　これは明らかであろうが，それでは解説にならないので図を付すことで解説の代わりとしよう（右図を参照）．

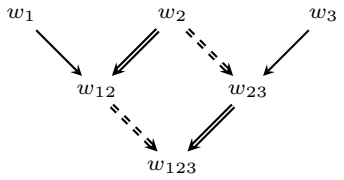


p.150 下から 4 行目　これは 1 が $\mathbb{H}$ の乗法における単位元であることから従う．演算表［⇨ **表 9.1**］からも確認できるだろう．

p.153 上から 6 行目　まず，語 w に対して「何もしない縮約」を施したものと，w に「何もしない縮約」を施したものは一致するので，反射律 $w \sim_{\mathrm{red}} w$ がなりたつ．次に，語 w_1, w_2 に対し $w_1 \sim_{\mathrm{red}} w_2$ がなりたつことは，w_1 の縮約かつ w_2 の縮約である語 w_{12} が存在することを表していた．このとき，w_{12} は「w_2 の縮約かつ w_1 の縮約」ともなっているので，反射律「$w_1 \sim_{\mathrm{red}} w_2$ ならば $w_2 \sim_{\mathrm{red}} w_1$」もなりたつ．

---

[5] ［藤岡 2］**定義 5.1** (1) の全射性の定義の言い換え「$f\colon X \to Y$ が全射であることとは，$Y = f(X)$ がなりたつこと」から明らか．



最後に，語 w_1, w_2, w_3 に対して $w_1 \sim_{\mathrm{red}} w_2$，$w_2 \sim_{\mathrm{red}} w_3$ がなりたっていたとする．このとき，$\sim_{\mathrm{red}}$ の定義から，w_1 の縮約かつ w_2 の縮約であるような語 w_{12} および，w_2 の縮約かつ w_3 の縮約であるような語 w_{23} が存在する．ここで，縮約 $w_2 \to w_{23}$（2 重点線）において $w_2 \to w_{12}$ の縮約過程（2 重線）で実行されていない基本縮約を w_{12} に施したものを w_{123} とすると，これは縮約 $w_2 \to w_{12}$（2 重線）において $w_2 \to w_{23}$ の縮約過程（2 重点線）で実行されていない基本縮約を w_{23} に施したものと一致する（右図参照：どちらも結局 w_2 にまったく同じ基本縮約を異なる順番で施したものとなるため）．このとき w_{123} は，w_1 の縮約（$w_1 \to w_{12} \to w_{123}$）かつ w_3 の縮約（$w_3 \to w_{23} \to w_{123}$）となっているため，推移律「$w_1 \sim_{\mathrm{red}} w_2$ かつ $w_2 \sim_{\mathrm{red}} w_3$ ならば $w_1 \sim_{\mathrm{red}} w_3$」もなりたつことが確認できた．

p.154 上から 11 行目　まず，空語 $(\,)$ と任意の語 $w \in F(X)$ に対して，連結積の意義から $(\,)w = w = w(\,)$ となるので $(\,)$ は単位元となり，(G1) がなりたつ．続いて，任意の語 $w = w_1 w_2 \cdots w_k \in F(X)$ に対して，

$$w_1 w_2 \cdots \underbrace{w_k w_k'}_{=(\,)} \cdots w_2' w_1' = w_1 w_2 \cdots \underbrace{w_{k-1} w_{k-1}'}_{=(\,)} \cdots w_2' w_1' = \cdots = \underbrace{w_1 w_1'}_{=(\,)} = (\,),$$

$$w_k' \cdots w_2' \underbrace{w_1' w_1}_{=(\,)} w_2 \cdots w_k = w_k' \cdots w_3' \underbrace{w_2' w_2}_{=(\,)} w_3 \cdots w_k = \cdots = \underbrace{w_k' w_k}_{=(\,)} = (\,)$$

であるから，w の逆元は $w^{-1} = w_k' w_{k-1}' \cdots w_2' w_1'$ であり，(G2) もなりたつ．最後に，任意の語 $u = u_1 u_2 \cdots u_k$, $v = v_1 v_2 \cdots v_l$, $w = w_1 w_2 \cdots w_m \in F(X)$ に対して，連結積の定義より $(uv)w = u_1 u_2 \cdots u_k v_1 v_2 \cdots v_l w_1 w_2 \cdots w_m = u(vw)$ となるので，結合法則 (G3) もなりたつ．以上より，$(F(X), \circ)$ が群であることが確認できた．

p.155 上から 3 行目　まず，推移律より，縮約同値な 2 つの語は，一方が他方の基本縮約である語の間の縮約同値で繋がれている．したがって，$wxx'v \sim_{\mathrm{red}} wv$ または $wx'xv \sim_{\mathrm{red}} wv$ $(w, v \in F(X),\ x \in X \sqcup X')$ に対して $f_\phi(wxx'v) = f_\phi(wv)$，$f_\phi(wx'xv) = f_\phi(wv)$ がなりたつことを確認しよう．実際，

[⇨ スペースの関係上，次のページに続きます]

$$f(wxx'v) \overset{\text{☺}\ f_\phi\text{の定義}}{=} f(w)\underbrace{\phi(x)\phi(x)'}_{(\,)}f_\phi(v) = f_\phi(w)f_\phi(v) \overset{\text{☺}\ f_\phi\text{の定義}}{=} f_\phi(wv),$$

$$f(wx'xv) \overset{\text{☺}\ f_\phi\text{の定義}}{=} f(w)\underbrace{\phi(x)'\phi(x)}_{(\,)}f_\phi(v) = f_\phi(w)f_\phi(v) \overset{\text{☺}\ f_\phi\text{の定義}}{=} f_\phi(wv)$$

であるから，f_ϕ が同値類の代表元の取り方によらず，矛盾なく定義されていることが確認できた．f_ϕ が準同型写像であることは，f_ϕ の定義から直ちに従う．最後に，f_ϕ が全単射であることは，

$$g_\phi(y) = \phi^{-1}(y), \qquad g_\phi(y') = \phi^{-1}(y)' \qquad (y \in Y),$$

$$g_\phi(w_1w_2\cdots w_s) = g_\phi(w_1)g_\phi(w_2)\cdots g(w_s) \qquad (x_i \in Y \sqcup Y')$$

で定められる $g_\phi\colon F(Y) \to F(X)$ が（矛盾なく定義された）f_ϕ の逆写像となっていることから従う．実際，各 $X \sqcup X'$ および $Y \sqcup Y'$ の元に対して，

$$g_\phi \circ f_\phi(x) = g_\phi(\phi(x)) = \phi^{-1} \circ \phi(x) = x,$$

$$g_\phi \circ f_\phi(x') = g_\phi(\phi(x)') = \phi^{-1} \circ \phi(x)' = x' \quad (x \in X),$$

$$f_\phi \circ g_\phi(y) = f_\phi(\phi^{-1}(y)) = \phi \circ \phi^{-1}(y) = y,$$

$$f_\phi \circ g_\phi(y') = f_\phi(\phi^{-1}(y)') = \phi \circ \phi^{-1}(y)' = y' \quad (y \in Y)$$

がなりたっている．$F(X)$ の元（または $F(Y)$）の任意の元は，$X \sqcup X'$（または $Y \sqcup Y'$）の元の連結積で表され，各文字（およびその逆元）に対しては $g_\phi \circ f_\phi = \mathrm{id}_{F(X)}$ かつ $f_\phi \circ g_\phi = \mathrm{id}_{F(Y)}$ がなりたつことを確認したので，準同型性を用いると $F(X)$ および $F(Y)$ の全体でも $g_\phi \circ f_\phi = \mathrm{id}_{F(X)}$ かつ $f_\phi \circ g_\phi = \mathrm{id}_{F(Y)}$ がなりたつことが従う．

p.155 下から 5 行目　命題 9.11 の証明と同様の構成を行う．$\phi\colon X \to G$ に対して，

$$f_\phi(x) = \phi(x), \qquad f_\phi(x)' = \phi(x)' \qquad (x \in X),$$

$$f_\phi(w_1w_2\cdots w_s) = f_\phi(w_1) * f_\phi(w_2) * \cdots * f_\phi(w_s)$$

と定めると，1 つ前の ✍ のマークの解説とまったく同様に，f_ϕ は矛盾なく定義された群準同型となる．また，任意の $x \in X$ に対しては，定義より $f_\phi(x) = \phi(x)$ であるから，$f_\phi|_X = \phi$ もなりたっている．

§10 の ✍ のマーク

p.162 下から 3 行目　$\sim_i$ に対しては，$x \in A$ に対し「x と x は（同一人物なので）イニシャルが同じ」であるから，反射律 $x \sim_i x$ がなりたつ．続いて，$x, y \in A$ に対して「x と y のイニシャルが一致する」ならば，当然「y と x のイニシャルは一致する」ため，反射律「$x \sim_i y$ ならば $y \sim_i x$ もなりたつ．最後に，$x, y, z \in A$ において「x と y のイニシャルが一致し，かつ y と z のイニシャルが一致するならば，x と z のイニシャルも一致する」ため，推移律「$x \sim_i y$ かつ $y \sim_i z$ ならば，$x \sim_i z$ である」もなりたつ．以上より，$\sim_i$ が同値関係であることが確認された．

$\sim_n$ に関しては，**対称律がなりたたない**．実際，$x, y \in A$ に対して，例えば y が学校中で知らぬ人のいない有名人だった場合など，「x は y の名前を知っているが，y は x の名前を知らない」ことは大いに起こり得る．したがって，$x \sim_n y$ だが $y \nsim_n x$ となることがあるため，$\sim_n$ は同値関係ではない．

p.162 下から 2 行目　実際，整数 n に対して $n = n$ であるから，反射律 (E1) がなりたつ．また，整数 m, n に対して $m = n$ ならば $n = m$ がなりたつので，対称律 (E2) もなりたつ．最後に，整数 m, n, l に対して $m = n$ かつ $n = l$ ならば $m = n = l$ より $m = l$ がなりたつので，推移律 (E3) もなりたつ．したがって，相等関係 $=$ は $\mathbb{Z}$ 上の同値関係である．

p.164 上から 7 行目　a と等しい整数は a 以外に存在しないため，同値類の定義 [⇨ **定義 10.5**] より，$C_{=(a)} = \{x \in \mathbb{Z} \mid x = a\} = \{a\}$ となる．また，$x \equiv a \pmod{n}$ をみたす $x \in \mathbb{Z}$ に対しては，合同式の定義 [⇨ **定義 3.1**] より，$n \mid (x - a)$，すなわち，$x - a = nq$ $(q \in \mathbb{Z})$ がなりたっているので，$C_{\equiv \pmod{n}}(a) = \{x \in \mathbb{Z} \mid x \equiv a \pmod{n}\} = \{a + nq \mid q \in \mathbb{Z}\} = a + n\mathbb{Z}$ となる．

p.164 下から 4 行目　$b \in C_\sim(a)$ より，$b \sim a$ がなりたっていたことを思い出そう．このとき，任意の $x \in C_\sim(b)$ に対して $x \sim b$ がなりたっているので，$x \sim b \sim a$ より推移律 (E3) から $x \sim a$，すなわち $x \in C_\sim(a)$ がなりたつ．

p.165 上から 6 行目　$x \in C_\sim(a) \cap C_\sim(b)$ より $x \sim a$ かつ $x \sim b$ がなりたつのだから，対称律 (E2) より $b \sim x$ がなりたち，$b \sim x \sim a$ より推移律 (E3) から $b \sim a$，すなわち $b \in C_\sim(a)$ がなりたつ．

p.165 上から 7 行目　$a, b \in A$ に対して，$C_\sim(a) = C_\sim(b)$ と $C_\sim(a) \neq C_\sim(b)$ の一方のみがなりたつ．したがって，$C_\sim(a) \neq C_\sim(b)$ と $C_\sim(a) \cap C_\sim(b) = \emptyset$ が同値である

ことを示せばよい．「$C_\sim(a) \neq C_\sim(b) \Rightarrow C_\sim(a) \cap C_\sim(b) = \emptyset$」の主張は命題 10.8 (2) の証明中で示されている．一方で $C_\sim(a) \cap C_\sim(b) = \emptyset$ であるならば，例えば $a \in C_\sim(a)$ かつ $a \notin C_\sim(b)$ であるから $C_\sim(a) \neq C_\sim(b)$ であることは明らかである．したがって，「$C_\sim(a) \cap C_\sim(b) = \emptyset \Rightarrow C_\sim(a) \neq C_\sim(b)$」の主張もなりたつので，$C_\sim(a) \neq C_\sim(b)$ と $C_\sim(a) \cap C_\sim(b) = \emptyset$ の同値性が示された．

p.166 下から 8 行目　同値類の定義 [⇨ **定義 10.5**] と反射律 (E1) $a \sim a$ より $a \in C_\sim(a)$ であるが，$C_\sim(a)$ は商集合 $A/\sim = \{C_\lambda \mid \lambda \in \Lambda\}$ の元であるため，ある添字 $\lambda_a \in \Lambda$ に対する $A/\sim$ の元 C_{λ_a} と一致する．したがって，$a \in C_\sim(a) = C_{\lambda_a} \subset \bigsqcup_{\lambda \in \Lambda} C_\lambda$ がなりたつ．

p.167 上から 2 行目　$\mathrm{P}(p_1, p_2, \ldots, p_{n+1})$ に対し $p_i = 1p_i$ $(i = 1, 2, \ldots, n+1)$ より反射律 (E1) $\mathrm{P} \sim \mathrm{P}$ が従う．次に，$\mathrm{P}(p_1, p_2, \ldots, p_{n+1})$ と $\mathrm{Q}(q_1, q_2, \ldots, q_{n+1})$ に対して $\mathrm{P} \sim \mathrm{Q}$ がなりたつ，すなわち $q_i = kp_i$ $(i = 1, 2, \ldots, n+1)$ をみたす $k \in \mathbb{K}^\times$ が存在するならば，$p_i = k^{-1}q_i$ $(i = 1, 2, \ldots, n+1)$ より $\mathrm{Q} \sim \mathrm{P}$ ゆえ対称律 (E2)「$\mathrm{P} \sim \mathrm{Q} \Rightarrow \mathrm{Q} \sim \mathrm{P}$」も従う．最後に，$\mathrm{P}(p_1, p_2, \ldots, p_{n+1})$, $\mathrm{Q}(q_1, q_2, \ldots, q_{n+1})$, $\mathrm{R}(r_1, r_2, \ldots, r_{n+1})$ に対して $\mathrm{P} \sim \mathrm{Q}$ かつ $\mathrm{Q} \sim \mathrm{R}$ がなりたつ，すなわち $q_i = kp_i$ と $r_i = lq_i$ $(i = 1, 2, \ldots, n+1)$ をみたす $k, l \in \mathbb{K}^\times$ が存在するならば，$r_i = klp_i$ $(i = 1, 2, \ldots, n+1)$ より $\mathrm{P} \sim \mathrm{R}$ ゆえ推移律 (E3)「$\mathrm{P} \sim \mathrm{Q}$ かつ $\mathrm{Q} \sim \mathrm{R} \Rightarrow \mathrm{P} \sim \mathrm{R}$」もなりたつ．以上より，$\sim$ が $\mathbb{K}^{n+1} \setminus \{\mathbf{0}\}$ 上の同値関係であることが示された．

p.167 下から 8 行目　$\mathbb{K}^n$ の 2 点 $(x_1, x_2, \ldots, x_n)$, $(y_1, y_2, \ldots, y_n)$ に対して等式 $[x_1 : x_2 : \cdots : x_n : 1] = [y_1 : y_2 : \cdots : y_n : 1]$ がなりたつとすると，記号 $[x_1 : x_2 : \cdots : x_n : 1]$ が $\sim$ に関する $(x_1, x_2, \ldots, x_n, 1)$ の属する同値類を表していたことと命題 10.8 (1) より $(x_1, x_2, \ldots, x_n, 1) \sim (y_1, y_2, \ldots, y_n, 1)$ がなりたつので，同値関係 $\sim$ の定義より $y_i = kx_i$ $(i = 1, 2, \ldots, n)$ かつ $1 = k \cdot 1$ をみたす [6] $k \in \mathbb{K}^\times$ が存在する．このとき後者の等式から $k = 1$ となるため，$y_i = x_i$ $(i = 1, 2, \ldots, n)$ より $(x_1, x_2, \ldots, x_n)$ と $(y_1, y_2, \ldots, y_n)$ は $\mathbb{K}^n$ 上の同じ点となる．したがって，当該の写像は単射である．

p.171 下から 2 行目　最初に，左合同関係 $\equiv_l \pmod{H}$ を考えよう．まず，任意の $a \in G$ に対して $a' * a = e_G \overset{\text{(H1)}}{\in} H$ であるから，反射律 (E1) $a \equiv_l a \pmod{H}$ が従う．続い

---

[6] 後者の式は $y_{n+1} = kx_{n+1}$ において $x_{n+1} = y_{n+1} = 1$ としたもの（第 $n+1$ 成分についての関係式）．

て，$a, b \in G$ に対して $a \equiv_l b \pmod H$ がなりたつ，すなわち $b' * a \in H$ がなりたつとすると，

$$a' * b = (b' * a)' \overset{\text{(H2)}}{\overset{\ddot{\smile}}{\in}} H$$

より $b \equiv_l a \pmod H$ がなりたつので，対称律 (E2)「$a \equiv_l b \pmod H \Rightarrow b \equiv_l a \pmod H$」も従う．最後に，$a, b, c \in G$ に対して $a \equiv_l b \pmod H$ かつ $b \equiv_l c \pmod H$ がなりたつ，すなわち $b' * a \in H$ かつ $c' * b \in H$ がなりたつとすると，

$$c' * a = c' * \underbrace{(b * b')}_{=e_G} * a = (c' * b) * (b' * a) \overset{\text{(H3)}}{\overset{\ddot{\smile}}{\in}} H$$

より $a \equiv_l c \pmod H$ であるので，推移律 (E3)「$a \equiv_l b \pmod H$ かつ $b \equiv_l c \pmod H$ $\Rightarrow a \equiv_l c \pmod H$」も従う．以上より左合同関係 $\equiv_l \pmod H$ が G 上の同値関係であることが示された．

右合同関係 $\equiv_r \pmod H$ についてもまったく同様だが，念のため証明をつけておこう．まず，任意の $a \in G$ に対して $a *' a = e_G \overset{\text{(H1)}}{\overset{\ddot{\smile}}{\in}} H$ であるから反射律 (E1) $a \equiv_r a \pmod H$ が従う．続いて，$a, b \in G$ に対して $a \equiv_r b \pmod H$ がなりたつ，すなわち $a * b' \in H$ がなりたつとすると，

$$b * a' = (a * b')' \overset{\text{(H2)}}{\overset{\ddot{\smile}}{\in}} H$$

より $b \equiv_r a \pmod H$ がなりたつので，対称律 (E2)「$a \equiv_r b \pmod H \Rightarrow b \equiv_r a \pmod H$」も従う．最後に，$a, b, c \in G$ に対して $a \equiv_r b \pmod H$ かつ $b \equiv_r c \pmod H$ がなりたつ，すなわち $a * b' \in H$ かつ $b * c' \in H$ がなりたつとすると，

$$a * c' = a * \underbrace{(b' * b)}_{=e_G} * c = (a * b') * (b * c') \overset{\text{(H3)}}{\overset{\ddot{\smile}}{\in}} H$$

より $a \equiv_r c \pmod H$ であるので，推移律 (E3)「$a \equiv_r b \pmod H$ かつ $b \equiv_r c \pmod H$ $\Rightarrow a \equiv_r c \pmod H$」も従う．以上より，右合同関係 $\equiv_r \pmod H$ が G 上の同値関係であることが示された．

$\boxed{\text{p.172 上から 6 行目}}$　$x \in G$ が $x \equiv_l a \pmod H$ をみたすことは，定義から $x = a * h$ をみたす $h \in H$ が存在することと同値である．したがって，

[⇨ スペースの関係上，次のページに続きます]

$$C_{\equiv_l \,(\mathrm{mod}\, H)}(a) \overset{\text{定義}}{=} \{x \in G \mid x \equiv_l a \,(\mathrm{mod}\, H)\}$$
$$= \{x = a * h \mid h \in H\} = a * H$$

がなりたつ．同様に x が $x \equiv_r a \,(\mathrm{mod}\, H)$ をみたすことは，定義から $x = h * a$ をみたす $h \in H$ が存在することと同値である．したがって，

$$C_{\equiv_r \,(\mathrm{mod}\, H)}(a) \overset{\text{定義}}{=} \{x \in G \mid x \equiv_r a \,(\mathrm{mod}\, H)\}$$
$$= \{x = h * a \mid h \in H\} = H * a$$

がなりたつ．

p.172 脚注 13)　左剰余類について　(1) $b \in a * H$ と仮定すると，左剰余類 $a * H$ の定義より，$b = a * h_0$ をみたす $h_0 \in H$ が存在する．したがって，

$$b * H = (a * h_0) * H := \{a * h_0 * h \mid h \in H\}$$

となるので，$(a * h_0) * H = a * H$ を示せばよい．まず，任意の $a * h_0 * h \in (a * h_0) * H$ に対して $a * \underbrace{h_0 * h}_{\in H} \in a * H$ であるから $(a * h_0) * H \subseteq a * H$ がなりたつ．また，任意の $a * h \in a * H$ に対して $a * h = (a * h_0) * \underbrace{h_0' * h}_{\in H} \in (a * h_0) * H$ であるから $(a * h_0) * H \supseteq a * H$ もなりたつ．以上より，$b * H = (a * h_0) * H = a * H$ が示された．逆に，$a * h = b * H$ であると仮定すると，$b = b * e_G \in b * H = a * H$ が従う．
(2) $a * H \neq b * H$ であることと $(a * H) \cap (b * H) = \emptyset$ であることが同値であることを示せばよい．まず，$(a * H) \cap (b * H) = \emptyset$ であるとすると，$a \in a * H$ だが $a \notin b * H$ であるから $a * H \neq b * H$ であることは明らかである．逆に，$a * H \neq b * H$ のときに $(a * H) \cap (b * H) \neq \emptyset$ であると仮定し，共通部分の元 $x \in (a * H) \cap (b * H)$ を考える．このとき左剰余類の定義より，$x = a * h_1 = b * h_2 \cdots (\sharp_l)$ をみたす $h_1, h_2 \in H$ が存在する．$(\sharp_l)$ の両辺の右から h_2' との演算を施すと $b \in a * \underbrace{h_1 * h_2'}_{\in H} \in a * H$ となるので，(1) より $a * H = b * H$ が導かれて矛盾が生じた．

右剰余類について　(1) $b \in H * a$ と仮定すると，右剰余類 $H * a$ の定義より $b = h_0 * a$ をみたす $h_0 \in H$ が存在する．したがって

$$H * b = H * (h_0 * a) := \{h * h_0 * a \mid h \in H\}$$

となるので，$H * (h_0 * a) = H * a$ を示そう．まず，任意の $h * h_0 * a \in H * (h_0 * a)$ に対し

て $\underbrace{h*h_0}_{\in H}*a \in H*a$ より $H*(h_0*a) \subseteq H*a$ がなりたつ．また，任意の $h*a \in H*a$ に対して $h*a = \underbrace{h*h_0'}_{\in H}*(h_0*a) \in H*(h_0*a)$ であるから $H*(h_0*a) \supseteq H*a$ もなりたつ．したがって，$H*b = H*(h_0*a) = H*a$ であることが示された．逆に，$H*a = H*b$ であると仮定すると，$b = e_G*b \in H*b = H*a$ が従う．

(2) $H*a \neq H*b$ であることと $(H*a)\cap(H*b) = \emptyset$ であることが同値であることを示せばよい．まず $(H*a)\cap(H*b) = \emptyset$ であるとすると，$a \in H*a$ だが $a \notin H*b$ であるから $H*a \neq H*b$ であることは明らかである．逆に $H*a \neq H*b$ のときに $(H*a)\cap(H*b) \neq \emptyset$ であると仮定し，共通部分の元 $x \in (H*a)\cap(H*b)$ を考える．このとき右剰余類の定義より，$x = h_1*a = h_2*b$ $\cdots$ $(\sharp_r)$ をみたす $h_1, h_2 \in H$ が存在する．$(\sharp_r)$ の両辺の左から h_2' との演算を施すと $b \in \underbrace{h_2'*h_1}_{\in H}*a \in H*a$ となるので，(1) より $H*a = H*b$ が導かれて矛盾が生じた．

$\boxed{\text{p.173 上から 5 行目}}$ $\eta = h*(h'*\eta)$ であり，命題 7.2 (H3) より $h' \in H$，(H3) より $h'*\eta \in H$ が従うので，$\eta = h*\underbrace{(h'*\eta)}_{\in H} \in h*H$ が従う．

$\boxed{\text{p.175 脚注 15)}}$ 例えば，$(2\,3) \in \mathfrak{S}_3 \setminus H$ に対する左剰余類は

$$(2\,3)H = \{(2\,3)e,\ (2\,3)(1\,2)\} = \{(2\,3),\ (1\,3\,2)\}$$

となり（これは $(1\,3\,2)H$ と一致している），$(1\,2\,3) \in \mathfrak{S}_3 \setminus (H \sqcup (2\,3)H)$ に関する左剰余類は

$$(1\,2\,3)H = \{(1\,2\,3)e,\ (1\,2\,3)(1\,2)\} = \{(1\,2\,3),\ (1\,3)\}$$

となる （これは $(1\,3)H$ と一致）．したがって，現れる剰余類の順番は異なっているものの，最終的な計算結果

$$\begin{aligned}\mathfrak{S}_3/H &= \{H,\ (2\,3)H,\ (1\,2\,3)H\}\\ &= \{\{e\,(1\,2)\},\ \{(2\,3),\ (1\,3\,2)\},\ \{(1\,2\,3),\ (1\,3)\}\}\end{aligned}$$

は，例題 10.19 (2) の解答と一致している．

$\boxed{\text{p.176 上から 7 行目}}$ $(1\,3) \in \mathfrak{S}_3 \setminus H$ に対する右剰余類は

$$H(1\,3)H = \{e(1\,3),\ (1\,2)(1\,3)\} = \{(1\,3),\ (1\,3\,2)\}$$

となり，$(2\,3) \in \mathfrak{S}_3 \setminus (H \sqcup H(1\,3))$ に関する右剰余類は

$$H(2\,3) = \{e(2\,3),\ (1\,2)(2\,3)\} = \{(2\,3),\ (1\,2\,3)\}$$

となる．したがって，

$$\begin{aligned} H\backslash\mathfrak{S}_3 &= \{H,\ H(1\,3),\ H(2\,3)\} \\ &= \{\{e\,(1\,2)\},\ \{(1\,3),\ (1\,3\,2)\},\ \{(2\,3),\ (1\,2\,3)\}\} \end{aligned}$$

を得る．

$\boxed{\text{p.177 上から 9 行目}}$　$g \circ f(x) = g(b * a' * x) = a * \underbrace{b' * b}_{=e_G} * a' * x = \underbrace{a * a'} * x = x$ および $f \circ g(y) = f(a * b' * y) = b * \underbrace{a' * a}_{=e_G} * b' * y = \underbrace{b * b'} * y = y$ と計算できる．

$\boxed{\text{p.177 上から 11 行目}}$　同様に，

$$f\colon H * a \to H * b\,;\, x \mapsto x * a' * b, \qquad g\colon H * b \to H * a\,;\, y \mapsto y * b' * a$$

と定義すると，$g \circ f(x) = g(x * a' * b) = x * a' * \underbrace{b * b'}_{=e_G} * a = x * \underbrace{a' * a}_{=e_G} = x$ および $f \circ g(y) = f(y * b' * a) = y * b' * \underbrace{a * a'}_{=e_G} * b = y * \underbrace{b' * b}_{=e_G} = y$ と計算されるので，f, g は全単射であり，$\#(H * a) = \#(H * b)$ がなりたつ．

$\boxed{\text{p.177 下から 6 行目}}$　$b_1, b_2 \in G$ に対して $H * b_1 = H * b_2$ と仮定すると，$b_2 \in H * b_1$ より $b_2 = h * b_1$ $(h \in H)$ と表されるので［⇨ **命題 10.12** (1)］，

$$\begin{aligned} \psi(H * b_2) &= b_2' * H = (h * b_1)' * H = b_1' * h' * H \quad (\because\ \text{問 } 6.4\,(3)) \\ &= H * b_1' \quad (\because\ \text{例題 } 10.13) \\ &= \psi(H * b_1) \end{aligned}$$

がなりたつので，ψ は右剰余類の代表元の選び方によらず矛盾なく定義されている．

$\boxed{\text{p.177 下から 5 行目}}$　実際，$\psi \circ \varphi(a * H) = \psi(H * a') = (a')' * H = a * H$ および $\varphi \circ \psi(H * b) = \varphi(b' * H) = H * (b')' = H * b$ と計算されるので，φ と ψ は互いに逆写像となっている．

$\boxed{\text{p.180 上から 7 行目}}$　G が有限群であれば，G を空でない部分集合で分割すると，高々 $\#G$

個の部分集合に分割される．指数 $(G:H)$ は，G の H による剰余類分割 $G=\bigsqcup_{\lambda\in\Lambda} a_\lambda * H$ における剰余類の個数 $\#\Lambda$ のことなので，任意の H に対して $(G:H)=\#\Lambda<\#G\,(<+\infty)$ が従う．

p.180 下から 3 行目　簡単なものだと $X=\{1,2,3,4,5\}$，$A=\{1,2,3\}$ など．

p.181 下から 8 行目　n を自然数とする．例題 10.24 (1) より，n と互いに素な整数 a に対して，$\overline{a}$ の $((\mathbb{Z}/n\mathbb{Z})^\times,\cdot)$ における位数 $k_0=\#\langle\overline{a}\rangle$ は $\#(\mathbb{Z}/n\mathbb{Z})=\varphi$ ［⇨ **例題 6.11**］の約数であるため，$\varphi=k_0q$ $(q\in\mathbb{Z})$ と表せる．このとき $\overline{a}^\varphi=(\overline{a}^{k_0})^q=\overline{1}^q=\overline{1}$ より，$a^{\varphi(n)}\equiv 1\pmod n$（オイラーの定理［⇨ 5・10］）が従う．

§11 の ✍ のマーク

p.189 上から 5 行目　実際，任意の[7] $e_G\in\{e_G\}$ と $g\in G$ に対し，

$$g*e_G*g'=g*g'=e_G\in\{e_G\}$$

であるから，自明な部分群 $\{e_G\}$ は $(G,*)$ の正規部分群である．

p.189 下から 8 行目　まず，$\mathfrak{S}_3=N\subseteq(1\,2)N$ であるから[8]，命題 11.4 より，任意の $\sigma\in N$ に対して $e\sigma e^{-1}\in N$ および $(1\,2)\sigma(1\,2)^{-1}\in N$ がなりたつことを示せばよい．前者は $e\sigma e^{-1}=e\sigma e=\sigma\in N$ より自明になりたつ．後者に関しては，$\sigma=e$, $(1\,2\,3)$, $(1\,3\,2)$ について，それぞれ計算してみると，

$$(1\,2)e(1\,2)^{-1}=(1\,2)(1\,2)=e\in N$$

$$(1\,2)(1\,2\,3)(1\,2)^{-1}=(2\,3)(1\,2)=(1\,3\,2)\in N$$

$$(1\,2)(1\,3\,2)(1\,2)^{-1}=(1\,3)(1\,2)=(1\,2\,3)\in N$$

となるので，$N=\langle(1\,2\,3)\rangle$ が $\mathfrak{S}_3$ の正規部分群であることが確認できた．

---

7) といっても $\{e_G\}$ の元は e_G だけなので，必然的に e_G が選ばれるが．

8) この剰余類分割は，ラグランジュの定理［⇨ **定理 10.23**］から直ちに求まる．実際，$(\mathfrak{S}_3:N)=\#\mathfrak{S}_3/\#=3!/3=2$ であるから，剰余類の個数は 2 個だけであり，そのうちの 1 つは N 自身である．したがって，$(1\,2)\in\mathfrak{S}_3\smallsetminus N$ を 1 つ選んでくれば，$(1\,2)N$ が自動的にもう 1 つの剰余類となるのである．

p.190 上から 1 行目　任意の $kI_n \in Z(\mathrm{GL}_n(\mathbb{K}))$ と $A \in \mathrm{GL}_n(\mathbb{K})$ に対して，

$$A(kI_n)A^{-1} = k(AI_nA^{-1}) = k(AA^{-1}) = kI_n \in Z(\mathrm{GL}_n(\mathbb{K}))$$

であるから，$Z(\mathrm{GL}_n(\mathbb{K})) = \{kI_n \mid k \in \mathbb{K}^\times\}$ は $\mathrm{GL}_n(\mathbb{K})$ の正規部分群である．

p.190 上から 3 行目　〔**コメント**：直前の ✍ とほぼ同じ〕　任意の $Z \in Z(H)$ は, $\mathrm{GL}_2(\mathbb{K})$ の中心 $Z(\mathrm{GL}_n(\mathbb{K}))$ の元でもあるので，ある $k \in \mathbb{K}^\times$ に対して $Z = kI_n$ と表される．したがって，任意の $A \in H$ に対して，

$$AZA^{-1} = k(AI_nA^{-1}) = k(AA^{-1}) = kI_n = Z \in Z(H)$$

であるから，$Z(H)$ は H の正規部分群である．

p.191 下から 5 行目　$x \in S$, $a \in G$ に対して，$a * x' * a' = (a * x * a')'$ である［⇨ **問 6.4** (3)］ことに注意すると，仮定より $a * x * a' \in \langle S \rangle$ であり，$\langle S \rangle$ は G の部分群であるから，(H2) より，その逆元 $(a * x * a')' = a * x' * a'$ も $\langle S \rangle$ の元となる．

p.191 下から 2 行目　実際,

$$\begin{aligned}
&(a * x_1 * a') * (a * x_2 * a') * (a * x_3 * a') * \cdots * (a * x_s * a') \\
&\quad = a * x_1 * \underbrace{a' * a}_{=e_G} * x_2 * \underbrace{a' * a}_{=e_G} * x_3 * \cdots * x_{s-1} * \underbrace{a' * a}_{=e_G} * x_s * a' \\
&\qquad = a * \underbrace{x_1 * x_2 * \cdots * x_s}_{=x} * a' = a * x * a'
\end{aligned}$$

と計算できる [9]．

p.192 上から 11 行目　任意の $a, b \in G$ に対して，

$$\pi(a * b) = (a * b) * N \overset{\because (11.4)}{=} (a * N) \overline{*} (b * N) = \pi(a) \overline{*} \pi(b)$$

がなりたつので, π は群準同型写像である．また, 任意の $a * N \in G/N$ に対して $\pi(a) = a * N$ であるから，π は全射である．

p.192 下から 5 行目　まず，任意の $a * N \in G/N$ に対して，

---

[9] この計算は, 行列の対角化の応用で扱われる**行列の n 乗計算** $(P^{-1}AP)^n = P^{-1}A^nP$ ［⇨［藤岡 1］**例題 21.1**］とまったく同じ原理に基づくものであることを観察されたい．

$$(a * N)\overline{*}N = (a * e_G) * N = a * N = (e_G * a) * N = N\overline{*}(a * N)$$

であるから，$N = e_G * N$ が G/N の単位元であり，(G1) がなりたつ．続いて，任意の $a * N \in G/N$ に対して，

$$(a * N)\overline{*}(a' * N) = (a * a') * N = N = (a' * a) * N = (a' * N)\overline{*}(a * N)$$

であるから，$a' * N$ が $a * N$ の逆元であり，(G2) がなりたつ．最後に，任意の $a * N$, $b * N$, $c * N \in G/N$ に対して，

$$\begin{aligned}\big((a * N)\overline{*}(b * N)\big)\overline{*}(c * N) &= (a * b)\overline{*}(c * N) = \big((a * b) * c\big) * N \\ &= \big(a * (b * c)\big) * N \quad (\because G \text{ に対する (G3)}) \\ &= (a * N)\overline{*}(b * c) * N = (a * N)\overline{*}\big((b * N)\overline{*}(c * N)\big)\end{aligned}$$

より，(G3) もなりたつ．

$\boxed{\text{p.193 上から 6 行目}}$　命題 10.20 (3) で構成した全単射写像 $\varphi\colon G/N \to N\backslash G$ が，剰余群の間の反準同型写像であることを確認すればよい［⇨ **問 8.4** (2)］が，任意の $a * N$, $b * N \in G/N$ に対して，

$$\begin{aligned}\varphi((a * N)\overline{N}(b * N)) &= \varphi((a * b) * N) = N * (a * b)' \quad (\because\ \varphi \text{ の定義}) \\ &\overset{\because\ \text{問 6.4 (3)}}{=} N * (b' * a') = (N * b')\overline{*}(N * a') \\ &= \varphi(b * N)\overline{*}\varphi(a * N)\end{aligned}$$

であるから，確かに φ は反準同型写像となっている．

※　一般に，群の間の写像 $f\colon (G_1, *) \to (G_2, \star)$ が $f(a * b) = f(b) \star f(a)$ $(a, b \in G_1)$ をみたすとき，f を**反準同型写像 anti-homomorphism** とよび，全単射な反準同型写像を**反同型写像 anti-isomorphism** とよぶ（f でうつすと**演算の順序が入れ換わる**ような写像のこと）．反準同型写像が登場する場面は多くはないが，本書第 4 章では，群の右作用の説明の際に活躍している［⇨ p.237 脚注 1)］．

$\boxed{\text{p.193 下から 8 行目}}$　仮定の下で $Z(\mathrm{SL}_n(\mathbb{K})) = \{I_n\}$ となることを示せばよい．任意の $Z \in Z(\mathrm{SL}_n(\mathbb{K}))$ は，定義から $Z = kI_n \in \mathrm{SL}_n(\mathbb{K})$ $(k \in \mathbb{K}^\times)$ と表される．このとき $\det(kI_n) = k^n$ が 1 と一致する必要があるが，$\mathbb{K}$ は ± 1 以外に 1 の冪根（べきこん）を含まないので，$k = 1$ または $k = -1$ である．また，n は奇数なので $(-1)^n = -1$ となり $-I_n \notin \mathrm{SL}_n(\mathbb{K})$ である．したがって，$Z(\mathrm{SL}_n(\mathbb{K})) = \{I_n\}$ が従う．

$\boxed{\text{p.194 下から 4 行目}}$　$I_n \in \mathrm{U}_2(\mathbb{F}_3)$ より (H1) がなりたち，任意の $\begin{pmatrix} \overline{1} & x \\ \overline{0} & \overline{1} \end{pmatrix} \in \mathrm{U}_2(\mathbb{F}_3)$ に対して $\begin{pmatrix} \overline{1} & x \\ \overline{0} & \overline{1} \end{pmatrix}^{-1} = \begin{pmatrix} \overline{1} & -x \\ \overline{0} & \overline{1} \end{pmatrix} \in \mathrm{U}_2(\mathbb{F}_3)$ であるから，(H2) もなりたつ．最後に任意の $\begin{pmatrix} \overline{1} & x \\ \overline{0} & \overline{1} \end{pmatrix}, \begin{pmatrix} \overline{1} & y \\ \overline{0} & \overline{1} \end{pmatrix} \in \mathrm{U}_2(\mathbb{F}_3)$ に対して $\begin{pmatrix} \overline{1} & x \\ \overline{0} & \overline{1} \end{pmatrix}\begin{pmatrix} \overline{1} & y \\ \overline{0} & \overline{1} \end{pmatrix} = \begin{pmatrix} \overline{1} & x+y \\ \overline{0} & \overline{1} \end{pmatrix} \in \mathrm{U}_2(\mathbb{F}_3)$ より，(G3) もなりたつ．以上より，$\mathrm{U}_2(\mathbb{F}_3)$ は $\mathrm{B}_2(\mathrm{F}_3)$ の部分群である．

$\boxed{\text{p.194 下から 2 行目}}$　任意の $\begin{pmatrix} \overline{1} & x \\ \overline{0} & \overline{1} \end{pmatrix} \in \mathrm{U}_2(\mathbb{F}_3)$ と $\begin{pmatrix} a & b \\ \overline{0} & d \end{pmatrix} \in \mathrm{B}_2(\mathbb{F}_3)$ に対して，

$$\begin{aligned} \begin{pmatrix} a & b \\ \overline{0} & d \end{pmatrix}\begin{pmatrix} \overline{1} & x \\ \overline{0} & \overline{1} \end{pmatrix}\begin{pmatrix} a & b \\ \overline{0} & d \end{pmatrix}^{-1} &= \begin{pmatrix} a & ax+b \\ \overline{0} & d \end{pmatrix}\begin{pmatrix} a^{-1} & -ba^{-1}d^{-1} \\ \overline{0} & d^{-1} \end{pmatrix} \\ &= \begin{pmatrix} \overline{1} & ad^{-1}x \\ \overline{0} & \overline{1} \end{pmatrix} \in \mathrm{U}_2(\mathbb{F}_3) \end{aligned}$$

がなりたつので，$\mathrm{U}_2(\mathbb{F}_3)$ は $\mathrm{B}_2(\mathbb{F}_3)$ の正規部分群である．

$\boxed{\text{p.194 脚注 2)}}$　始めに，$\mathrm{U}_n(\mathbb{K})$ が $\mathrm{B}_n(\mathbb{K})$ の部分群であることを示す．まず，単位行列 I_n は $\mathrm{U}_n(\mathbb{K})$ に含まれるので，(H1) がなりたつ．続いて，任意の $h = (h_{ij})_{1 \le i,j \le n}$（ただし，$k = 1, 2, \ldots, n$ に対して $h_{kk} = 1$ かつ $1 \le l < k \le n$ に対して $h_{kl} = 0$）に対して，$h^{-1} \in \mathrm{U}_n(\mathbb{K})$ であることを示す（つまり，(H2) を示す）．$h \in \mathrm{B}_n(\mathbb{K})$ より，問 7.7 (1) から $h^{-1} \in \mathrm{B}_n(\mathbb{K})$ であるから，あとは h^{-1} の対角成分が 1 であることを示せばよい．ここで，h の第 k 行と第 k 列を取り除いて得られる行列 H_{kk} は，対角成分に $h_{11}, \ldots, h_{k-1,k-1}, h_{k+1,k+1}, \ldots, h_{nn}$ が並ぶ $(n-1)$ 次正方行列であるから，各 $k = 1, 2, \ldots, n$ に対して $h^{-1} = (\det h)^{-1}\tilde{h}$（$\tilde{h} = (\tilde{h}_{ij})_{1 \le i,j \le n}$ は h の余因子行列）の (k,k) 成分は，

$$\begin{aligned} &(\det h)^{-1}\tilde{g}_{kk} = (\det h)^{-1}\det H_{kk} \\ (\dagger)_1 : \qquad &= (h_{11}h_{22}\cdots h_{kk})^{-1}(h_{11}\cdots h_{k-1,k-1}h_{k+1,k+1}\cdots h_{nn}) \\ &= h_{kk}^{-1} = 1 \end{aligned}$$

なので，$h^{-1} \in \mathrm{U}_n(\mathbb{K})$ となり，(H2) がなりたつ．最後に，任意の $g = (g_{ij})_{1 \le i,j \le n}$ および $h = (h_{ij})_{1 \le i,j \le n} \in \mathrm{U}_n(\mathbb{K})$（ただし，$k = 1, 2, \ldots, n$ に対して $g_{kk} = h_{kk} = 1$ か

つ $1 \leq l < k \leq n$ に対して $g_{kl} = h_{kl} = 0$）に対して，その積 gh は上三角行列であり，各 $k = 1, 2, \ldots, n$ に対して gh の (k, k) 成分は，

$$(\dagger)_2 : \sum_{l=1}^{n} g_{kl} h_{lk} = \sum_{l=1}^{k-1} \underbrace{g_{kl}}_{=0} h_{lk} + g_{kk} h_{kk} + \sum_{l=k+1}^{n} g_{kl} \underbrace{h_{lk}}_{=0} = g_{kk} h_{kk} = 1 \cdot 1 = 1$$

であるから $gh \in \mathrm{U}_n(\mathbb{K})$ であり，(H3) もなりたつ．以上より，$\mathrm{U}_n(\mathbb{K})$ は $\mathrm{B}_n(\mathbb{K})$ の部分群である．

次に，$\mathrm{U}_n(\mathbb{K}) \lhd \mathrm{B}_n(\mathbb{K})$ であることを示そう．任意の $h = (h_{ij})_{1 \leq i,j \leq n} \in \mathrm{U}_n(\mathbb{K})$ および $g = (g_{ij})_{1 \leq i,j \leq n} \in \mathrm{B}_n(\mathbb{K})$（ただし，$k = 1, 2, \ldots, n$ に対して $h_{kk} = 1$ かつ $1 \leq l < k \leq n$ に対して $h_{kl} = g_{kl} = 0$）に対して，$(\dagger)_1$ と同じ計算により g^{-1} の (k, k) 成分は g_{kk}^{-1} $(k = 1, 2, \ldots, n)$ となり，$(\dagger)_2$ と同じ計算により $A, B \in \mathrm{B}_n(\mathbb{K})$ 積の (k, k) 成分は $a_{kk} b_{kk}$ $(k = 1, 2, \ldots, n)$ となることがわかる．したがって，ghg^{-1} の (k, k) 成分は

$$g_{kk} h_{kk} g_{kk}^{-1} = g_{kk} 1 g_{kk}^{-1} = 1 \qquad (k = 1, 2, \ldots, n)$$

であるから，$ghg^{-1} \in \mathrm{U}_n(\mathbb{K})$ となり，$\mathrm{U}_n(\mathbb{K})$ が $\mathrm{B}_n(\mathbb{K})$ の正規部分群であることが示された．

$\boxed{\text{p.195 下から 6 行目}}$　まず $g_0 = I_2$ より，任意の $i = 1, 2, 3$ に対して $\overline{g}_0 \overline{g}_i = \overline{I_2 g_i} = \overline{g}_i$ および $\overline{g}_i \overline{g}_0 = \overline{g_i I_2} = \overline{g}_i$ がなりたつことは容易にわかる．したがって，以下では $\overline{g}_0$ と無関係な積 $\overline{g}_i \overline{g}_j$ $(1 \leq i, j \leq 3)$ のうち，すでに計算してある $\overline{g}_2 \overline{g}_3$ 以外の計算結果をまとめておこう．

$$g_1 g_1 = \begin{pmatrix} \overline{1} & \overline{0} \\ \overline{0} & -\overline{1} \end{pmatrix} \begin{pmatrix} \overline{1} & \overline{0} \\ \overline{0} & -\overline{1} \end{pmatrix} = \begin{pmatrix} \overline{1} & \overline{0} \\ \overline{0} & \overline{1} \end{pmatrix} \in g_0 \mathrm{U}_2(\mathbb{F}_3) \qquad \therefore\ \overline{g}_1 \overline{g}_1 = \overline{g}_0$$

$$g_1 g_2 = \begin{pmatrix} \overline{1} & \overline{0} \\ \overline{0} & -\overline{1} \end{pmatrix} \begin{pmatrix} -\overline{1} & \overline{1} \\ \overline{0} & \overline{1} \end{pmatrix} = \begin{pmatrix} -\overline{1} & \overline{1} \\ \overline{0} & -\overline{1} \end{pmatrix} \in g_3 \mathrm{U}_2(\mathbb{F}_3) \qquad \therefore\ \overline{g}_1 \overline{g}_2 = \overline{g}_3,$$

$$g_1 g_3 = \begin{pmatrix} \overline{1} & \overline{0} \\ \overline{0} & -\overline{1} \end{pmatrix} \begin{pmatrix} -\overline{1} & \overline{1} \\ \overline{0} & -\overline{1} \end{pmatrix} = \begin{pmatrix} -\overline{1} & \overline{1} \\ \overline{0} & \overline{1} \end{pmatrix} \in g_2 \mathrm{U}_2(\mathbb{F}_3) \qquad \therefore\ \overline{g}_1 \overline{g}_3 = \overline{g}_2,$$

$$g_2 g_1 = \begin{pmatrix} -\overline{1} & \overline{1} \\ \overline{0} & \overline{1} \end{pmatrix} \begin{pmatrix} \overline{1} & \overline{0} \\ \overline{0} & -\overline{1} \end{pmatrix} = \begin{pmatrix} -\overline{1} & -\overline{1} \\ \overline{0} & -\overline{1} \end{pmatrix} \in g_3 \mathrm{U}_2(\mathbb{F}_3) \qquad \therefore\ \overline{g}_2 \overline{g}_1 = \overline{g}_3,$$

[⇨ スペースの関係上，次のページに続きます]

$$g_2g_2 = \begin{pmatrix} -\overline{1} & \overline{1} \\ \overline{0} & \overline{1} \end{pmatrix}\begin{pmatrix} -\overline{1} & \overline{1} \\ \overline{0} & 1\overline{1} \end{pmatrix} = \begin{pmatrix} \overline{1} & \overline{0} \\ \overline{0} & \overline{1} \end{pmatrix} \in g_0\mathrm{U}_2(\mathbb{F}_3) \qquad \therefore\ \overline{g}_2\overline{g}_2 = \overline{g}_0,$$

$$g_3g_1 = \begin{pmatrix} -\overline{1} & \overline{1} \\ \overline{0} & -\overline{1} \end{pmatrix}\begin{pmatrix} \overline{1} & \overline{0} \\ \overline{0} & -\overline{1} \end{pmatrix} = \begin{pmatrix} -\overline{1} & -\overline{1} \\ \overline{0} & \overline{1} \end{pmatrix} \in g_2\mathrm{U}_2(\mathbb{F}_3) \qquad \therefore\ \overline{g}_3\overline{g}_1 = \overline{g}_2,$$

$$g_3g_2 = \begin{pmatrix} -\overline{1} & \overline{1} \\ \overline{0} & -\overline{1} \end{pmatrix}\begin{pmatrix} -\overline{1} & \overline{1} \\ \overline{0} & \overline{1} \end{pmatrix} = \begin{pmatrix} \overline{1} & \overline{0} \\ \overline{0} & -\overline{1} \end{pmatrix} \in g_1\mathrm{U}_2(\mathbb{F}_3) \qquad \therefore\ \overline{g}_3\overline{g}_2 = \overline{g}_1,$$

$$g_3g_3 = \begin{pmatrix} -\overline{1} & \overline{1} \\ \overline{0} & -\overline{1} \end{pmatrix}\begin{pmatrix} -\overline{1} & \overline{1} \\ \overline{0} & -\overline{1} \end{pmatrix} = \begin{pmatrix} \overline{1} & \overline{0} \\ \overline{0} & \overline{1} \end{pmatrix} \in g_0\mathrm{U}_2(\mathbb{F}_3) \qquad \therefore\ \overline{g}_3\overline{g}_3 = \overline{g}_0.$$

§12 の ✍ のマーク

p.202 上から 3 行目　任意の $a * N,\ b * N \in G/N$ に対して，

$$\overline{f}\big((a * N)\overline{*}(b * N)\big) = \overline{f}\big((a * b) * N\big) = f(a * b) = f(a) \star f(b) \qquad (\because\ f \text{ の準同型性})$$

であるから，$\overline{f}\colon G_1/N \to G_2$ は群準同型写像である．

p.202 上から 6 行目　$\mathrm{Im}\, f$ の任意の元 $b \in \mathrm{Im}\, f$ は $b = f(a)$ $(a \in G)$ と表されるので，$\overline{f}$ の定義より $\overline{f}(a * \mathrm{Ker}\, f) = f(a) = b$ がなりたつ．したがって，$\overline{f}\colon G_1/\mathrm{Ker}\, f \to \mathrm{Im}\, f$ は全射である．

p.202 上から 13 行目　$\mathrm{Ker}\, \varphi_{\mathrm{triv}} = G$ および $\mathrm{Im}\, \varphi_{\mathrm{triv}} = \{e\}$ であるから，群準同型定理［⇨ **定理 12.1**］より，群の同型 $\overline{\varphi}_{\mathrm{triv}}\colon G/G \xrightarrow{\sim} \{e\}$ を得る．また，$\mathrm{Ker}\, \mathrm{id}_G = \{e_G\}$ かつ $\mathrm{Im}\, \mathrm{id}_G = G$ であるから，同じく群準同型定理より，群の同型 $\overline{\mathrm{id}}_G\colon G/\{e_G\} \xrightarrow{\sim} G$ を得る．

p.203 上から 5 行目　合成 $H \to G \xrightarrow{\pi} G/N$ を φ_H とするとき，$\varphi_H(h) = h * N = N$ がなりたつのは $h \in N$ のときであるので，$\mathrm{Ker}\, \varphi_H = N$ である．したがって，群準同型定理［⇨ **定理 12.1**］より，群の同型 $\overline{\varphi}_H\colon H/N \xrightarrow{\sim} \mathrm{Im}\, \varphi_H$ が誘導されるので，自然な包含写像 $\mathrm{Im}\, \varphi_H \hookrightarrow G/N$ と合成して，単射準同型 $H/N \hookrightarrow G/N$ を得る．

p.203 上から 7 行目　群準同型写像 $f\colon (G_1, *) \to (G_2, \star)$ と $(G_2, \star)$ の部分群 $H \subseteq$

G_2 に対して，$f^{-1}(H)$ が G_1 の部分群であることを示す．まず $f(e_{G_1}) = e_{G_2} \in H$ であるから $e_{G_1} \in f^{-1}(H)$ であり，(H1) がなりたつ．続いて，任意の $a \in f^{-1}(H)$（つまり $f(a) \in H$）に対して，$f(a') = f(a)' \overset{\because H \text{ の}}{\underset{\text{(H2)}}{\in}} H$ より $a' \in f^{-1}(H)$ であり，(H2) もなりたつ．最後に，任意の $a, b \in f^{-1}(H)$（つまり $f(a), f(b) \in H$）に対して $f(a * b) = f(a) \star f(b) \overset{\because H \text{ の}}{\underset{\text{(H3)}}{\in}} H$ より $a * b \in f^{-1}(H)$ であり，(H3) もなりたつ．以上より，$f^{-1}(H)$ が $(G_1, *)$ の部分群であることが示された．

p.203 下から 8 行目　まず，合成写像 $H \to G \xrightarrow{\pi} G/N$ を φ_H としたとき，同型写像 $\overline{\varphi}_H \colon H/N \xrightarrow{\sim} \operatorname{Im}\varphi_H$ によって H/N と $\operatorname{Im}\varphi_H = \pi(H)$ を同一視していたことに注意しよう．このとき $H \in \mathcal{S}_N(G)$ に対して $\Psi \circ \Phi(H) = \Psi(\pi(H)) = \pi^{-1}(\pi(H)) = H$ がなりたち，$\overline{H} \in \mathcal{S}(G/N)$ に対して $\Phi \circ \Psi(\overline{H}) = \Phi(\pi^{-1}(\overline{H})) = \pi(\pi^{-1}(\overline{H})) = \overline{H}$ がなりたつ．つまり，$\Psi \circ \Phi$ も $\Phi \circ \Psi$ も恒等写像である．

p.206 上から 9 行目　まず，$\mathfrak{S}_n = \mathfrak{A}_n \sqcup (1\ 2)\mathfrak{A}_n$ であり，$\mathfrak{A}_n$ は偶置換のなす剰余類（部分群）であり，$(1\ 2)\mathfrak{A}_n$ は奇置換のなす剰余類である．また，群準同型定理によると，$\operatorname{sgn}(\mathfrak{A}_n) = +1$ であり，$\operatorname{sgn}((1\ 2)\mathfrak{A}_n) = -1$ である．したがって，$(+1)^2 = (-1)^2 = +1$ という等式が，同型 $\mathfrak{S}_n/\mathfrak{A}_n \cong \{\pm 1\}$ によって剰余類の積の関係式

$$(\mathfrak{A}_n)(\mathfrak{A}_n) = ((1\ 2)\mathfrak{A}_n)((1\ 2)\mathfrak{A}_n) = \mathfrak{A}_n$$

（偶置換どうしの積，あるいは奇置換どうしの積が偶置換となる）と対応し，$(+1)(-1) = -1$ という等式が，同型 $\mathfrak{S}_n/\mathfrak{A}_n \cong \{\pm 1\}$ によって剰余類の積の関係式

$$(\mathfrak{A}_n)((1\ 2)\mathfrak{A}_n) = (1\ 2)\mathfrak{A}_n$$

（偶置換と奇置換の積が奇置換となる）と対応していることが観察される．

p.206 上から 10 行目　同型 $\mathfrak{S}_n/\mathfrak{A}_n = \{\pm 2\}$ より，$(\mathfrak{S}_n : \mathfrak{A}_n) = \#\{\pm 1\} = 2$ であるから，ラグランジュの定理［⇨ **定理 10.23**］より $\#\mathfrak{A}_n = \#\mathfrak{S}_n/(\mathfrak{S}_n : \mathfrak{A}_n) = \dfrac{n!}{2}$ が従う．

p.206 下から 7 行目　任意の $a, b \in \mathbb{Z}$ に対して，

［⇨ スペースの関係上，次のページに続きます］

$$
\begin{aligned}
f(a+b) &= \big((a+b)+3\mathbb{Z},(a+b)+5\mathbb{Z}\big)\\
&= \big((a+3\mathbb{Z})+(b+3\mathbb{Z}),(a+5\mathbb{Z})+(b+5\mathbb{Z})\big)\\
&= (a+3\mathbb{Z},a+5\mathbb{Z})+(b+3\mathbb{Z},b+5\mathbb{Z})\\
&\qquad\qquad\qquad\qquad (\because\ \text{直積群の演算の定義［⇨ \textbf{定義 6.34}］})\\
&= f(a)+f(b)
\end{aligned}
$$

であるから，f は群準同型写像である．

$\boxed{\text{p.207 下から 4 行目}}$ $\Phi(\overline{x})=(x+n_1\mathbb{Z},x+n_2\mathbb{Z},\ldots,x+n_s\mathbb{Z})\in\prod_{k=1}^{s}\mathbb{Z}/n_k\mathbb{Z}$ が $(a_1+n_1\mathbb{Z},a_2+n_2\mathbb{Z},\ldots,a_s+n_s\mathbb{Z})$ と一致することは，$k=1,2,\ldots,s$ に対して剰余類の等式 $x+n_k\mathbb{Z}=a_k+n_k\mathbb{Z}$ がなりたつことを意味しているのに他ならず，命題 10.12 (1) より，これは $x\in a_k+n_k\mathbb{Z}$ $(k=1,2,\ldots,s)$ がなりたつことと同値である．したがって，$\Phi(\overline{x})=(a_1+n_1\mathbb{Z},a_2+n_2\mathbb{Z},\ldots,a_s+n_s\mathbb{Z})$ をみたす $\overline{x}\in\mathbb{Z}/n_1n_2\cdots n_s\mathbb{Z}$ を求めることは，注意 12.13 の連立 1 次合同式 $(*)$ をみたす整数 x を法 $n_1n_2\cdots n_s$ で求めることと等価である．

§13 の ✍ のマーク

$\boxed{\text{p.213 上から 5 行目}}$ 任意の $(x_1,x_2)\,(y_1,y_2)\in N_1\times N_2$ に対して，

$$
\begin{aligned}
\Phi\big((x_1,x_2)*(y_1,y_2)\big) &= \Phi\big((x_1*y_1,x_2*y_2)\big)=x_1*y_1*x_2*y_2\\
&= x_1*x_2*y_1*y_2\\
&\qquad\qquad (\because\ y_1\in N_1,x_2\in N_2\text{より}\ y_1*x_2=x_2*y_1)\\
&= \Phi\big((x_1,x_2)\big)*\Phi\big((y_1,y_2)\big)
\end{aligned}
$$

であるから, Φ は群準同型写像である．また, $G=N_1*N_2$ より, 任意の $g\in G$ は $g=n_1*n_2$ $(n_1\in N_1,\ n_2\in N_2)$ と表されるので, $\Phi\big((n_1,n_2)\big)=n_1*n_2=g$ より，Φ は全射である．

$\boxed{\text{p.213 下から 11 行目}}$ まず，任意の $\sigma\in\mathfrak{V}_4$ に対して $e\sigma=\sigma=\sigma e$ がなりたち，

$$
\begin{aligned}
\big((1\,2)(3\,4)\big)\big((1\,3)(2\,4)\big) &= (1\,4)(2\,3)=\big((1\,3)(2\,4)\big)\big((1\,2)(3\,4)\big),\\
\big((1\,2)(3\,4)\big)\big((1\,4)(2\,3)\big) &= (1\,3)(2\,4)=\big((1\,4)(2\,3)\big)\big((1\,2)(3\,4)\big),\\
\big((1\,3)(2\,4)\big)\big((1\,4)(2\,3)\big) &= (1\,2)(3\,4)=\big((1\,4)(2\,3)\big)\big((1\,3)(2\,4)\big)
\end{aligned}
$$

であるから，$\mathfrak{V}_4$ はアーベル群であり，　$N_1 \lhd \mathfrak{V}_4$ および $N_2 \lhd \mathfrak{V}_4$ [10]がなりたつ［⇨ 例 11.6］．また，$(1\,4)(2\,3) = \big((1\,2)(3\,4)\big)\big((1\,3)(2\,4)\big) \in N_1N_2$ より $\mathfrak{V}_4 \subseteq N_1N_2$ となるので（$N_1N_2 \subseteq \mathfrak{V}_4$ とあわせて）$\mathfrak{V}_4 = N_1N_2$ もなりたつ．最後に，$N_1 = \{e,\ (1\,2)(3\,4)\}$，$N_2 = \{e,\ (1\,3)(2\,4)\}$ より，　$N_1 \cap N_2 = \{e\}$ である．

p.216 上から 2 行目　実際，$[x, y] = x * y * x' * y' \overset{\text{(Ab)}}{=} x * x' * y * y' = e_G$ が任意の $x, y \in G$ に対してなりたつので，$[G, G] = \{e_G\}$ となる．

p.216 下から 7 行目　2 行目の式から 3 行目の式の行間を埋めると，以下のようになる．

$$
\begin{aligned}
&\begin{pmatrix} a_1 & b_1 \\ 0 & d_1 \end{pmatrix}\begin{pmatrix} a_2 & b_2 \\ 0 & d_2 \end{pmatrix}\begin{pmatrix} a_1 & b_1 \\ 0 & d_1 \end{pmatrix}^{-1}\begin{pmatrix} a_2 & b_2 \\ 0 & d_2 \end{pmatrix}^{-1} \\
&= \begin{pmatrix} a_1 & b_1 \\ 0 & d_1 \end{pmatrix}\begin{pmatrix} a_2 & b_2 \\ 0 & d_2 \end{pmatrix}(a_1d_1)^{-1}\begin{pmatrix} d_1 & -b_1 \\ 0 & a_1 \end{pmatrix}(a_2d_2)^{-1}\begin{pmatrix} d_2 & -b_2 \\ 0 & a_2 \end{pmatrix} \\
&= \begin{pmatrix} a_1a_2 & a_1b_2 + b_1d_2 \\ 0 & d_1d_2 \end{pmatrix}(a_1a_2d_1d_2)^{-1}\begin{pmatrix} d_1d_2 & -d_1b_2 - b_1a_2 \\ 0 & a_1a_2 \end{pmatrix} \\
&= (a_1a_2d_1d_2)^{-1}\begin{pmatrix} a_1a_2d_1d_2 & -a_1a_2(d_1b_2 + b_1a_2 - a_1b_2 - b_1d_2) \\ 0 & a_1a_2d_1d_2 \end{pmatrix} \\
&= \begin{pmatrix} 1 & (d_1d_2)^{-1}(a_1b_2 + b_1d_2 - d_1b_2 - b_1a_2) \\ 0 & 1 \end{pmatrix}.
\end{aligned}
$$

p.216 下から 2 行目　任意の $\begin{pmatrix} a_1 & b_1 \\ 0 & d_1 \end{pmatrix}, \begin{pmatrix} a_2 & b_2 \\ 0 & d_2 \end{pmatrix} \in \mathrm{B}_2(\mathbb{K})$ に対して，

$$
\begin{aligned}
f\left(\begin{pmatrix} a_1 & b_1 \\ 0 & d_1 \end{pmatrix}\begin{pmatrix} a_2 & b_2 \\ 0 & d_2 \end{pmatrix}\right) &= f\left(\begin{pmatrix} a_1a_2 & a_1b_2 + b_1d_2 \\ 0 & d_1d_2 \end{pmatrix}\right) \\
&= (a_1a_2, d_1d_2) = (a_1, d_1)(a_2, d_2) \\
&= f\left(\begin{pmatrix} a_1 & b_1 \\ 0 & d_1 \end{pmatrix}\right) f\left(\begin{pmatrix} a_2 & b_2 \\ 0 & d_2 \end{pmatrix}\right)
\end{aligned}
$$

であるから，$f\colon \mathrm{B}_2(\mathbb{K}) \to \mathbb{K} \times \mathbb{K}^\times$ は群準同型写像である．また，任意の $a, d \in \mathbb{K}^\times$ に対し

---

[10]　直接，$\big((1\,3)(2\,4)\big)N_1\big((1\,3)(2\,4)\big)^{-1} \subset N_1$ などを調べてもよい．

て，$f\left(\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}\right) = (a, d)$ より，f は全射である．最後に，$f\left(\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}\right) = (a, d) = (1, 1)$ となるのは $a = 1, d = 1$ のときのみであるから，$\operatorname{Ker} f = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \middle| \, b \in \mathbb{K} \right\} = \mathrm{U}_2(\mathbb{K})$ がなりたつ．

p.216 脚注 1)　一般に，群 $(G, *)$ の部分群 H に対して $\langle H \rangle = H$ であることを確認しよう．$H \subset \langle H \rangle$ は定義から明らかなので，$\langle H \rangle \subseteq H$ を示せばよい．ここで，$\langle H \rangle$ の任意の元は $x_1 * x_2 * \cdots * x_s$（ただし，$x_i \in H \cup H'$）と表される［⇨ **命題 7.14**］が，(H2) より $H' = H$ なので各 x_i は H の元であり，(H3) より $x_1 * x_2 * \cdots * x_s \in H$ となるので $\langle H \rangle \subseteq G$ が示された．

p.217 下から 3 行目　$\overline{x * y} = \overline{y * x}$ の右から $\overline{x' * y'}$ をかけて $\overline{x * y * x' * y'} = e_{G/N}$，すなわち，$[x, y] * N = N$ を得る．ゆえに，$[x, y] \in N$ が従う．

p.219 上から 7 行目　任意の $x \in \gamma_k(G)$ と $g \in G$ に対して，$g' * x' * g * x \in \gamma_{k+1}(G)$ が $\gamma_{k+1}(G)$ の定義 $\gamma_{k+1}(G) = [G, \gamma_k(G)]$ から従う．したがって，剰余群 $G/\gamma_{k+1}(G)$ において $(g' * x' * g * x) * \gamma_{k+1}(G) = \gamma_{k+1}(G)$ がなりたつので，左から $(x * g) * \gamma_{k+1}(G)$ との演算を施（ほどこ）して $(g * x) * \gamma_{k+1}(G) = (x * g) * \gamma_{k+1}(G)$ を得る．すなわち，$x * \gamma_{k+1}(G)$ は $G/\gamma_{k+1}(G)$ の任意の元と可換なので，$G/\gamma_{k+1}(G)$ の中心の元となる．

p.220 上から 7 行目　実際，群 G が群表示 $\langle X \mid R \rangle$ $(\#X < \infty)$ をもつならば，群 G は同型 $G \cong F(X)/N_R$ を介して X の有限個の元 $x_1, x_2, \ldots, x_s$ と対応する G の元 $g_1, g_2, \ldots, g_s$ によって生成されるので，G は有限生成である．逆に，$G = \langle g_1, g_2, \ldots, g_s \rangle$ が有限生成であるならば，（文字の）集合 $X = \{x_1, x_2, \ldots, x_s\}$ に対して x_i を g_i にうつす写像 $\phi\colon X \to G\,; x_i \mapsto g_i$ は全射準同型写像 $f_\phi\colon F(X) \to G$ を誘導する［⇨ **命題 9.13**］．そこで $N := \operatorname{Ker} f_\phi$ とおくと，群表示の定義から G は生成元の集合 X が有限集合であるような群表示 $\langle X \mid N \rangle$ をもつことが示された．

p.221 上から 5 行目　$G = \langle S \rangle$ の定義から，G の任意の元は S の元，または，S の元の逆元を有限個集めて演算を施したもの $a_1 * a_2 * \cdots * a_r$（ただし，$a_i \in S \cup S'$）として表される．ところが，ϕ の全射性より，各 a_i に対して $\bar{f}_\phi(x_i) = a_i$ をみたす $x_i \in X \cup X'$ が存在するので，$\bar{f}_\phi(x_1 * x_2 * \cdots * x_s) = a_1 * a_2 * \cdots * a_s$ より，$\bar{f}_\phi$ は全射である．

p.221 上から 11 行目　いろいろな方法があるが，ここではラグランジュの定理［⇨ **定理**

10.23］を用いた方法を紹介しよう．まず，$\langle(1\,2),\,(1\,2\,3)\rangle$ には $\langle(1\,2\,3)\rangle$ が含まれ，さらに $(1\,2)$ も含まれているので，$\#\langle(1\,2),\,(1\,2\,3)\rangle \geq 4$ がなりたつ．一方で，ラグランジュの定理より，$\#\langle(1\,2),(1\,2\,3)\rangle \mid \mathfrak{S}_3 = 3! = 6$ であるから，$\#\langle(1\,2),(1\,2\,3)\rangle = 6$ であり，したがって，$\mathfrak{S}_3 = \langle(1\,2),(1\,2\,3)\rangle$ がなりたつ．

$\boxed{\text{p.221 下から 4 行目}}$ G_1 の任意の元は，定義から r, s，および，それらの逆元の有限個の積で表されるが，まず，関係式 $r' = r^2$，および，$s' = s$ を積表示に現れる r', s' に代入することで積表示に r', s' が現れない形に変形でき，さらに $r^3 = s^2 = e$ を用いることで，r^α $(\alpha \in \{0,1,2\})$ または

$$r^{i_0} s r^{i_1} s \cdots s r^{i_t} s r^{i_{t+1}} \quad (t \in \mathbb{Z}_{\geq 0},\ i_0,\ i_{t+1} \in \{0,\ 1,\ 2\}, \text{それ以外の } i_k \in \{1,\ 2\})$$

という形に変形できる．ここで $sr = r^2 s$ を用いると，$t = 0$ のときは $r^{i_0} s r^{i_1} = r^\alpha s$（$\alpha$ は $i_0 + 2i_1$ を 3 で割った余り）となり，$t \geq 1$ のときは

$$r^{i_0} s r^{i_1} s \cdots s i^{i_{t-1}} \underbrace{s r^{i_t}}_{= r^{2i_t} s} s r^{i_{t+1}} = r^{i_0} s r^{i_1} s \cdots r^{i_{t-2}} s r^{j_{t-1}}$$

（ただし，j_{t-1} は $i_{t-1} + 2i_t + i_{t+1}$ を 3 で割った余り）となる．これらを繰り返し用いることで，最終的に $r^\alpha s^\beta$ $(\alpha \in \{0,1,2\},\ \beta \in \{0,1\})$ の形にすることができる．

$\boxed{\text{p.221 下から 1 行目}}$ 一般に，有限集合の間の写像 $f\colon X \to Y$ が全射であるならば，$\#X \geq \#Y$ であることに注意すると，直前の ✍ の計算で $\#G_1 \leq 6$ がわかり，全射 $G_1 \twoheadrightarrow \mathfrak{S}_3$ の存在により $\#D_1 \leq \#\mathfrak{S}_3 = 6$ がわかるので，$\#G_1 = 6$ が従う．

$\boxed{\text{p.222 上から 10 行目}}$ $ij = k$ および $i \cdot i^3 = 1$ より，$1, i, j, k \in \langle i, j\rangle$ である．さらに，$i^2 = -1 \in \langle i, j\rangle$ であるから，$1, i, j, k$ に -1 をかけた $-1, -i, -j, -k$ も $\langle i, j\rangle$ の元である．したがって，Q_8 のすべての元が $\langle i, j\rangle$ に含まれるため，$Q_9 = \langle i, j\rangle$ である．

$\boxed{\text{p.222 下から 10 行目}}$ G_2 の任意の元は，定義から r, s，および，それらの逆元の有限個の積で表されるが，まず，関係式 $r' = r^3$，および，$s' = s^3$ を積表示に現れる r', s' に代入することで，積表示に r', s' が現れない形に変形でき，さらに $s^2 = r^2$ を代入した上で $r^4 = e$ を用いることで，r^α $(\alpha \in \{0,1,2,3\})$ または

$$r^{i_0} s r^{i_1} s \cdots s r^{i_t} s r^{i_{t+1}} \quad (t \in \mathbb{Z}_{\geq 0},\ i_0,\ i_{t+1} \in \{0,1,2,3\}, \text{それ以外の } i_k \in \{1,2,3\})$$

という形に変形できる．ここで $sr^3 = sr' = rs$ より $sr = sr^9 = r^3 s$ であることを用いると，$t = 0$ のときは $r^{i_0} s r^{i_1} = r^\alpha s$（$\alpha$ は $i_0 + 3i_1$ を 4 で割った余り）となり，$t \geq 1$ の

ときは

$$r^{i_0}sr^{i_1}s\cdots si^{i_{t-1}}\underbrace{sr^{i_t}}_{=r^{3i_t}s}sr^{i_{t+1}}=r^{i_0}sr^{i_1}s\cdots r^{i_{t-2}}sr^{j_{t-1}}$$

（ただし，j_{t-1} は $i_{t-1}+3i_t+i_{t+1}$ を 3 で割った余り）となる．これらを繰り返し用いることで，最終的に $r^\alpha s^\beta$ $(\alpha\in\{0,1,2,3\},\ \beta\in\{0,1\})$ の形にすることができる．

p.222 下から 9 行目　直前の計算による $\#G_2\le 8$ と，全射 $G_2\twoheadrightarrow Q_8$ の存在による $\#G_2\le\#Q_8=8$ から $\#G_2=8$ とわかるため，全射準同型写像 $G_2\twoheadrightarrow Q_8$ は同型であり，$G_2\cong Q_8$ が従う．

p.222 下から 2 行目　直後の ✍ で見るように，Q_{4m} は

$$\{r^\alpha s^\beta\mid\alpha\in\{0,1,\dots,2m-1\},\ \beta\in\{0,1\}\}$$

という $4m$ 個の元からなる集合である．まず，$\beta=0$ のときは，$(r^\alpha)^2=r^{2\alpha}$ であり，これが e と一致するのは $2\alpha=0,\ 2m$ のとき，すなわち $\alpha=0,\ m$ のときのみである．続いて，$\beta=1$ のときは

$$\begin{aligned}(r^\alpha\beta)^2&=r^\alpha sr^\alpha s=r^{2m\alpha}s^2\quad(\because sr=r^{2m-1}s,\ \text{直後の ✍ も参照})\\&=r^m\qquad(\because r^{2m}=e,\ s^2=r^m)\end{aligned}$$

であるから，$(r^\alpha s)^2=e$ となることはあり得ない．以上より，Q_{4m} の元で 2 乗すると e と一致するものは $e=r^0$ と r^m のみであり，したがって，Q_{4m} は位数 2 の元 r^m を唯一つもつ（単位元 e は位数 1 の元なので除外する）．

p.222 下から 1 行目　Q_{4m} の任意の元は，定義から r,s，および，それらの逆元の有限個の積で表されるが，まず，関係式 $r'=r^{m-1}$，および，$s'=s^3$ を積表示に現れる r',s' に代入することで積表示に r',s' が現れない形に変形でき，さらに $s^2=r^m$ を代入した上で $r^{2m}=e$ を用いることで，r^α $(\alpha\in\{0,1,\dots,2m-1\})$ または

$$r^{i_0}sr^{i_1}s\cdots sr^{i_t}sr^{i_{t+1}}$$

$$(t\in\mathbb{Z}_{\ge 0},\ i_0,\ i_{t+1}\in\{0,1,\dots,2m-1\},\text{それ以外の } i_k\in\{1,2,\dots,2m-1\})$$

という形に変形できる．ここで $sr^{2m-1}=sr'=rs$ より $sr=s(r^{2m-1})^{2m-1}=r^{2m-1}s$ であることを用いると，$t=0$ のときは $r^{i_0}sr^{i_1}=r^\alpha s$（$\alpha$ は $i_0+(2m-1)i_1$ を $2m$ で割った余り）となり，$t\ge 1$ のときは，

$$r^{i_0}sr^{i_1}s\cdots si^{i_{t-1}}\underbrace{sr^{i_t}}_{=r^{(2m-1)i_t}s}sr^{i_{t+1}}=r^{i_0}sr^{i_1}s\cdots r^{i_{t-2}}sr^{j_{t-1}}$$

（ただし，j_{t-1} は $i_{t-1}+(2m-1)i_t+i_{t+1}$ を $2m$ で割った余り）となる．これらを繰り返し用いることで，最終的に $r^\alpha s^\beta$ $(\alpha\in\{0,1,\ldots,2m-1\},\ \beta\in\{0,1\})$ の形にすることができるため，$\#Q_{4m}\leq 4m$ であることがわかる．

実際に $\#Q_{4m}=4m$ であることを示すには多少工夫が必要である．まず，$\langle r\rangle\subset Q_{4m}$ は，生成元 r と関係式 r^{2m} のみをもつ群であるから，位数 $2m$ の巡回群 C_{2m} であり，とくに $r^m\neq e$ である．また，r^m に対して $s'r^ms=(s'rs)^m=(r')^m=(r^m)'=r^m$ であるから，r_m は r, s と可換である．したがって，$\langle r^m\rangle$ は Q_{4m} の中心 $Z(Q_{4m})$ に含まれる位数 2 の部分群（∵ $(r^m)^2=r^{2m}=e$ より）であり，とくに Q_{4m} の正規部分群である．したがって，剰余群 $Q_{4m}/\langle r^m\rangle$ が考えられる．$\langle r^m\rangle$ で剰余をとることは，Q_{4m} に関係式 r^m を追加することに相当するため，

$$Q_{4m}/\langle r^m\rangle=\langle r,s\mid r^m,s^2,s'rs=r'\rangle$$

となるが，これは位数 $2m$ の 2 面体群 D_{2m} の群表示であった［⇨ 問 13.6］．したがって，$\#\bigl(Q_{4m}/\langle r^m\rangle\bigr)=2m$ であり，ラグランジュの定理［⇨ **定理 10.23**］より，

$$\#Q_{4m}=(Q_{4m}:\langle r^m\rangle)\#\langle r^m\rangle=2m\cdot 2=4m$$

が従う．

§14 の ✍ のマーク

p.236 上から 11 行目　実際，$x\in X$ に対して，

$$x\bullet_r e_G\overset{\because\text{定義}}{=}e_G\bullet_l x\overset{\because\text{(LA1)}}{=}x$$

より，(RA1) がなりたち，$x\in X$，$g_1,g_2\in G$ に対して，

$$\begin{aligned}x\bullet_r(g_1*g_2)&\overset{\because\text{定義}}{=}(g_1*g_2)\bullet_l x\overset{\because\text{(Ab)}}{=}(g_2*g_1)\bullet_l x\\&\overset{\because\text{(LA2)}}{=}g_2\bullet_l(g_1\bullet_l x)\overset{\because\text{定義}}{=}g_2\bullet_l(x\bullet_r g_1)\overset{\because\text{定義}}{=}(x\bullet_r g_1)\bullet_r g_2\end{aligned}$$

より，(RA2) もなりたつので，$\bullet_r$ は $(G,*)$ の X への右作用となっている．

p.236 下から 7 行目　実際，$x\in X$ に対して，

$$e_G \bullet_l x \overset{\text{定義}}{\overset{\cdot\cdot}{=}} x \bullet_r e'_G = x \bullet_r e_G \overset{\text{(RA1)}}{\overset{\cdot\cdot}{=}} x$$

より，(LA1) がなりたち，$x \in X$，$g_1, g_2 \in G$ に対して，

$$(g_1 * g_2) \bullet_l x \overset{\text{定義}}{\overset{\cdot\cdot}{=}} x \bullet_r (g_1 * g_2)' \overset{\text{問 6.4 (3)}}{\overset{\cdot\cdot}{=}} x \bullet_r (g'_2 * g'_1)$$

$$\overset{\text{(RA2)}}{\overset{\cdot\cdot}{=}} (x \bullet_r g'_2) \bullet_r g'_1 \overset{\text{定義}}{\overset{\cdot\cdot}{=}} (g_2 \bullet_l x) \bullet_r g'_1 \overset{\text{定義}}{\overset{\cdot\cdot}{=}} g_1 \bullet_l (g_2 \bullet_l x)$$

より，(LA2) もなりたつので，$\bullet_l$ は $(G, *)$ の X への左作用となっている．

$\boxed{\text{p.236 下から 3 行目}}$　実際，$x \in X$ および $a, b \in G$ に対して，

$$\rho_{\bullet_l}(a * b)(x) \overset{\text{定義}}{\overset{\cdot\cdot}{=}} (a * b) \bullet_l x \overset{\text{(LA2)}}{\overset{\cdot\cdot}{=}} a \bullet_l (b \bullet_l x)$$

$$\overset{\text{定義}}{\overset{\cdot\cdot}{=}} a \bullet_l \rho_{\bullet_l}(b)(x) \overset{\text{定義}}{\overset{\cdot\cdot}{=}} \rho_{\bullet_l}(a)\big(\rho_{\bullet_l}(b)(x)\big) = \big(\rho_{\bullet_l}(a) \circ \rho_{\bullet_l}(b)\big)(x)$$

であるから，$\rho_{\bullet_l}(a * b) = \rho_{\bullet_l}(a) \circ \rho_{\bullet_l}(b)$ がなりたっているため，$\rho_{\bullet_l}$ は $(G, *)$ から $\mathfrak{S}_X$ への群準同型写像となっている．

$\boxed{\text{p.236 下から 1 行目}}$　実際，$x \in X$ に対して，

$$e_G \bullet_{l,\rho} x \overset{\text{定義}}{\overset{\cdot\cdot}{=}} \rho(e_G)(x) \overset{\text{補題 8.7 (1)}}{\overset{\cdot\cdot}{=}} e(x) = x$$

（ただし，e は $\mathfrak{S}_X$ の単位元である恒等置換）より，(LA1) がなりたち，$x \in X$ および $a, b \in G$ に対して，

$$(a * b) \bullet_{l,\rho} x \overset{\text{定義}}{\overset{\cdot\cdot}{=}} \rho(a * b)(x) \overset{\rho\ \text{の準同型性}}{\overset{\cdot\cdot}{=}} \rho(a) \circ \rho(b)(x)$$

$$\overset{\text{定義}}{\overset{\cdot\cdot}{=}} \rho(a)\big(b \bullet_{l,\rho} x\big) \overset{\text{定義}}{\overset{\cdot\cdot}{=}} a \bullet_{l,\rho} (b \bullet_{l,\rho})$$

より，(LA2) もなりたつため，$\bullet_{l,\rho}$ は $(G, *)$ の X への左作用となっている．

$\boxed{\text{p.237 脚注 1)}}$　実際，群 $(G, *)$ の集合 X への右作用 $\bullet_r$ に対し，$\rho^{\mathrm{op}}_{\bullet_r}(a)(x) = x \bullet_r a$ $(a \in G,\ x \in X)$ と定めると，$x \in X$ および $a, b \in G$ に対して，

$$\rho^{\mathrm{op}}_{\bullet_r}(a * b)(x) \overset{\text{定義}}{\overset{\cdot\cdot}{=}} x \bullet_r (a * b) \overset{\text{(RA2)}}{\overset{\cdot\cdot}{=}} (x \bullet_r a) \bullet_r b$$

$$\overset{\text{定義}}{\overset{\cdot\cdot}{=}} \rho^{\mathrm{op}}_{\bullet_r}(a)(x) \bullet_r b \overset{\text{定義}}{\overset{\cdot\cdot}{=}} \rho^{\mathrm{op}}_{\bullet_r}(b)\big(\rho_{\bullet_r}(a)(x)\big) = \big(\rho^{\mathrm{op}}_{\bullet_r}(b) \circ \rho^{\mathrm{op}}_{\bullet_r}(a)\big)(x)$$

であるから，$\rho^{\mathrm{op}}_{\bullet_r}(a * b) = \rho^{\mathrm{op}}_{\bullet_r}(b) \circ \rho^{\mathrm{op}}_{\bullet_r}(a)$ がなりたっているため，$\rho^{\mathrm{op}}_{\bullet_r}$ は $(G, *)$ から $\mathfrak{S}_X$ への反群準同型写像となっている．

逆に，反群準同型写像 $\rho^{\mathrm{op}}\colon (G,*) \to \mathfrak{S}_X$ に対し，$x \bullet_{r,\rho^{\mathrm{op}}} a = \rho^{\mathrm{op}}(a)(x)$ $(a \in G,\ x \in X)$ と定めると，$x \in X$ に対して，

$$x \bullet_{r,\rho^{\mathrm{op}}} e_G \overset{\text{定義}}{=} \rho^{\mathrm{op}}(e_G)(x) \overset{\text{補題 8.7 (1)}}{=} e(x) = x$$

（ただし e は $\mathfrak{S}_X$ の単位元である恒等置換）より，(RA1) がなりたち [11]，$x \in X$ および $a, b \in G$ に対して，

$$\begin{aligned} x \bullet_{r,\rho^{\mathrm{op}}} (a * b) &\overset{\text{定義}}{=} \rho^{\mathrm{op}}(a * b)(x) \overset{\rho\text{ の反準同型性}}{=} \rho^{\mathrm{op}}(b) \circ \rho^{\mathrm{op}}(a)(x) \\ &\overset{\text{定義}}{=} \rho^{\mathrm{op}}(b)\bigl(x \bullet_{r,\rho^{\mathrm{op}}} a\bigr) \overset{\text{定義}}{=} (x \bullet_{r,\rho^{\mathrm{op}}} a) \bullet_{r,\rho^{\mathrm{op}}} b \end{aligned}$$

より，(RA2) もなりたつため，$\bullet_{r,\rho^{\mathrm{op}}}$ は $(G,*)$ の X への右作用となっている．

p.238 脚注 5)　実際，$\rho(\sigma)(a_i) := a_{\sigma^{-1}(i)}$ $(\sigma \in \mathfrak{S}_n,\ i = 1, 2, \ldots, n)$ と定義したときに $\rho(\sigma) \circ \rho(\tau)(a_i) = a_{\sigma^{-1}\tau^{-1}(i)}$ がなりたっているとすると，

$$\rho(\sigma) \circ \rho(\tau)(a_i) = a_{\sigma^{-1}\tau^{-1}(i)} \overset{\text{問 6.4 (3)}}{=} a_{(\tau\sigma)^{-1}(i)} = \rho(\tau\sigma)(a_i)$$

であるから，$\rho\colon \mathfrak{S}_n \to \mathfrak{S}_n$ は**反準同型**となり，したがって，p.237 の脚注 1) より対応する作用は**右作用**となる．なお，この作用は置換作用［⇨ **例 14.6**］を，注意 14.3 を用いて右作用にしたものに相当する．

p.241 下から 1 行目　任意の $\boldsymbol{x} \in \mathbb{K}^{n+1} \smallsetminus \{\boldsymbol{0}\}$ に対して $\boldsymbol{x} = 1\boldsymbol{x}$ であるから，反射律 (E1) $\boldsymbol{x} \sim \boldsymbol{x}$ がなりたつ．また，$\boldsymbol{x}, \boldsymbol{y} \in \mathbb{K}^{n+1} \smallsetminus \{\boldsymbol{0}\}$ に対し，$\boldsymbol{x} \sim \boldsymbol{y}$ である，すなわち，$\boldsymbol{x} = k\boldsymbol{y}$ をみたす $k \in \mathbb{K}^{\times}$ が存在するとき，$\boldsymbol{y} = k^{-1}\boldsymbol{x}$ より $\boldsymbol{y} \sim \boldsymbol{x}$ がなりたつため，対称律 (E2) もみたされる．最後に，$\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z} \in \mathbb{K}^{n+1} \smallsetminus \{\boldsymbol{0}\}$ に対し，$\boldsymbol{x} \sim \boldsymbol{y}$ かつ $\boldsymbol{y} \sim \boldsymbol{z}$ である，すなわち $\boldsymbol{x} = k\boldsymbol{y}$, $\boldsymbol{y} = l\boldsymbol{z}$ をみたす $k, l \in \mathbb{K}^{\times}$ が存在するとき，$\boldsymbol{x} = kl\boldsymbol{z}$ より $\boldsymbol{x} \sim \boldsymbol{z}$ がなりたつため，推移律 (E3) もみたされる．以上より，$\sim$ は $\mathbb{K}^{n+1} \smallsetminus \{\boldsymbol{0}\}$ 上の同値関係を定める．

p.243 上から 5 行目　第 1 列が (14.1) の第 1 式，第 2 列が (14.1) の第 2 式と対応するように，1 つの行列の等式に結合した等式が，直前に出てきた式 $\begin{pmatrix} 3a & b \\ a & 0 \end{pmatrix} = A \begin{pmatrix} 2 & 3 \\ 1 & 1 \end{pmatrix}$ である．この式の両辺に右から

---

[11] 実際，群反準同型が単位元を単位元に，逆元を逆元に移すことは，補題 8.7 とまったく同様に証明できる．

$$\begin{pmatrix} 2 & 3 \\ 1 & 1 \end{pmatrix}^{-1} = (2 \cdot 1 - 3 \cdot)^{-1} \begin{pmatrix} 1 & -3 \\ -1 & 2 \end{pmatrix} = \begin{pmatrix} -1 & 3 \\ 1 & -2 \end{pmatrix}$$

をかけて，

$$A = \begin{pmatrix} 3a & b \\ a & 0 \end{pmatrix} \begin{pmatrix} -1 & 3 \\ 1 & -2 \end{pmatrix} = \begin{pmatrix} -3a+b & 9a-2b \\ -a & 3a \end{pmatrix}$$

を得る．

$\boxed{\text{p.244 上から 2 行目}}$　まず，射影直線上の 3 点 $0 = [0:1]$, $\infty[1:0]$, $1 = [1:1]$ を，相異なる点 P_1, P_2, P_3 にうつす射影変換が一意に定まることを示す．ここで，$i = 1, 2, 3$ に対し，点 P_i の斉次座標を $[x_i : y_i]$ とすると，点 P_1, P_2, P_3 が相異（あいこと）なることは，どの $\begin{pmatrix} x_i \\ y_i \end{pmatrix}$ も他の $\begin{pmatrix} x_j \\ y_j \end{pmatrix}$ のスカラー倍ではないこと（したがって，$\begin{pmatrix} x_i & x_j \\ y_i & y_j \end{pmatrix}$ が正則行列となること）と同値であることに注意しよう．

さて，求める射影変換の行列表示を $[A] \in \mathrm{PGL}_2(\mathbb{K})$ とすると，点 0 を P_1 に，点 ∞ を P_2 に移すという条件から，例題 14.15 と同様に

$$a \begin{pmatrix} x_1 \\ y_1 \end{pmatrix} = A \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \qquad b \begin{pmatrix} x_1 \\ y_1 \end{pmatrix} = A \begin{pmatrix} 0 \\ 1 \end{pmatrix} \qquad (a, b \in \mathbb{K}^\times)$$

と表せるので，

$$\begin{pmatrix} ax_1 & bx_2 \\ ay_1 & by_2 \end{pmatrix} = A \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \therefore\ A = \begin{pmatrix} ax_1 & bx_2 \\ ay_1 & by_2 \end{pmatrix} \quad \cdots (\star)$$

と表せる．さらに，$[A]$ が $[1:1]$ を $[x_3 : y_3]$ に移すという条件から

$$c \begin{pmatrix} x_3 \\ y_3 \end{pmatrix} = A \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} ax_1 & bx_2 \\ ay_1 & by_2 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} ax_1 + bx_2 \\ ay_1 + by_2 \end{pmatrix} \quad (c \in \mathbb{K}^\times)$$

となるので，両辺を比較して未知数 a, b に関する連立 1 次方程式

$$\begin{cases} ax_1 + bx_2 = cx_3 \\ ay_1 + by_2 = cy_3 \end{cases} \qquad \therefore \begin{pmatrix} x_1 & x_2 \\ y_1 & y_2 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} cx_3 \\ cy_3 \end{pmatrix}$$

を得る．最初に注意したように，係数行列 $\begin{pmatrix} x_1 & x_2 \\ y_1 & y_2 \end{pmatrix}$ は仮定から正則であるから，両辺に

左から係数行列の逆行列 $(x_1y_2 - x_2y_1)^{-1}\begin{pmatrix} y_2 & -x_2 \\ -y_1 & x_1 \end{pmatrix}$ をかけて

$$\begin{aligned}\begin{pmatrix} a \\ b \end{pmatrix} &= (x_1y_2 - x_2y_1)^{-1}\begin{pmatrix} y_2 & -x_2 \\ -y_1 & x_1 \end{pmatrix}\begin{pmatrix} cx_3 \\ cy_3 \end{pmatrix} \\ &= c(x_1y_2 - x_2y_1)^{-1}\begin{pmatrix} y_2x_3 - x_2y_3 \\ -y_1x_3 + x_1y_3 \end{pmatrix}\end{aligned}$$

を得る．これを $(\star)$ に代入して，$\mathrm{PGL}_2(\mathbb{K})$ での像を考えると

$$\begin{aligned}[A] &= \left[c(x_1y_2 - x_2y_1)^{-1}\begin{pmatrix} (y_2x_3 - x_2y_3)x_1 & (-y_1x_3 + x_1y_3)x_2 \\ (y_2x_3 - x_2y_3)y_1 & (-y_1x_3 + x_1y_3)y_2 \end{pmatrix}\right] \\ &= \begin{bmatrix} x_1y_2x_3 - x_1x_2y_3 & -y_1x_2x_3 + x_1x_2y_3 \\ y_1y_2x_3 - y_1x_2y_3 & -y_1y_2x_3 + x_1y_2y_3 \end{bmatrix}\end{aligned}$$

を得る [12]．とくに $[A]$ は，P_1, P_2, P_3 の斉次座標から一意に定まる．

同様に，点 $0, 1, \infty$ を相異なる 3 点 Q_1, Q_2, Q_3 に移す射影変換の行列表示を $[B]$ とすると，構成から $[R] := [QP^{-1}]$ は点 P_1, P_2, P_3 を Q_1, Q_2, Q_3 に移す射影変換の行列表示をあたえる．$[R']$ も P_1, P_2, P_3 を Q_1, Q_2, Q_3 に移す射影変換の行列表示と仮定すると，$[R'][P]$ は点 0, 1, ∞ を Q_1, Q_2, Q_3 に移す射影変換であり，この射影変換が Q_1, Q_2, Q_3 の斉次座標から一意に定まることはすでに確認しているので，$[R'][P] = [Q]$ がなりたつ．両辺に右から $[P]^{-1}$ をかけると $[R'] = [Q][P]^{-1} = [R]$ となるため，P_1, P_2, P_3 を Q_1, Q_2, Q_3 に移す射影変換が一意に存在することが示された．

p.244 下から 4 行目　まず，

$$A\begin{pmatrix} x \\ 1 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x \\ 1 \end{pmatrix} = \begin{pmatrix} ax + b \\ cx + d \end{pmatrix}$$

であるから，$f_{[A]}([x:1]) = [ax + b : cx + d]$ となる．斉次座標のすべての成分に同じ (0 でない) スカラーをかけても同じ点 (の代表元) をあたえるので，斉次座標の各成分を $(cx + d)^{-1}$

---

[12] 剰余群 $\mathrm{PGL}_2(\mathbb{K})$ では，スカラー倍しても同じ元 (剰余類) をあたえるので，$c(x_1y_2 - y_1x_2)^{-1}$ は無視しても差し支えない．実際に，この $[A]$ によって $[1:0]$, $[0:1]$, $[1:1]$ がそれぞれ $[x_1 : y_1]$, $[x_2 : y_2]$, $[x_3 : y_3]$ にうつることを確認してみよう．

倍して $f_{[A]}([x:1]) = \left[\dfrac{ax+b}{cx+d} : 1\right]$ を得る．

p.245 下から 6 行目　2 直線の方程式 $a_1x+b_1y+c_1z=0$, $a_2x+b_2y+c_2z=0$ の共通解の $\mathbb{KP}^2$ での像が唯一つであることを示せばよい．ここで，$a_1+b_1y+c_1z=0$ と $a_2x+b_2y+c_2z=0$ が $\mathbb{KP}^2$ において一致するということは，$a_1x+b_1y+c_1z=0$ の解と $c_2x+b_2y+c_2z=0$ の解が一致することを意味するが，これがなりたつのは (a_2,b_2,c_2) が (a_1,b_1,c_1) の（0 でない）スカラー倍となっているときのみである [13]．このとき，連立 1 次方程式

$$\begin{cases} a_1x+b_1y+c_1z=0 \\ a_2x+b_2y+c_2z=0 \end{cases} \qquad \therefore \begin{pmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

の係数行列は（第 2 行目が第 1 行目のスカラー倍ではないため）階数が 1 であるので，線形代数学の一般論により，解空間の次元は 1 となり，連立 1 次方程式の解は（$(0,0,0)$ 以外の）特殊解 (x_0,y_0,z_0) のスカラー倍 $(x,y,z)=(tx_0,ty_0,tz_0)$ $(t\in\mathbb{Z})$ で表される．このとき $[x:y:z]=[x_0:y_0:z_0]$ であるから，$\mathbb{KP}^2$ の 2 直線は必ず唯一つ交点をもつことが示された．

p.247 上から 9 行目　$\bullet$ の定義から，

$$(f\bullet e_G)(x) = f(e_G * x * e_G') = f(e_G * x * e_G) = f(x) \quad (x\in X)$$

となるので，$f\bullet_{e_G} = f$ より (RA1) がなりたつ．

p.248 上から 3 行目　実際，任意の $x\in G$ に対して $e_G \bullet_{L_{\mathrm{reg}}} x \overset{\text{定義}}{=} e_G * x = x$ であるから，(LA1) がなりたち，任意の $g_1,g_2,x\in G$ に対して，

---

13) 実際，$a_1x+b_1y+c_1z=0$ の解 $(x,y,z)=(b_1,-a_1,0)$ が $a_2x+b_2y+c_2z=0$ の解にもなっているので，$a_2b_1-a_1b_2=0$，すなわち，$\det\begin{pmatrix} a_1 & a_2 \\ b_1 & b_2 \end{pmatrix}=0$ がなりたつので，$(a_1,b_1)\neq(0,0)$ であれば $(a_2,b_2)=k_1(a_1,a_2)$ $(k\in\mathbb{K}^\times)$ がなりたつ．まったく同様に，$(a_1,c_1)\neq(0,0)$ であれば $(a_2,c_2)=k_2(a_1,c_1)$ $(k_2\in\mathbb{K}^\times)$ が，$(b_1,c_1)\neq(0,0)$ であれば $(b_2,c_2)=k_3(b_1,c_1)$ $(k_3\in\mathbb{K}^\times)$ がなりたつ．仮定より $(a_1,b_1,c_1)\neq(0,0,0)$ であるから，上記の 3 つの等式のうち少なくとも 2 つはなりたち，そこから $(a_2,b_2,c_2)=k(a_1,b_1,c_1)$ $(k\in\mathbb{K}^\times)$ と表せることが従う．

$$(g_1 * g_2) \bullet_{L_{\mathrm{reg}}} x \overset{\because\text{定義}}{=} (g_1 * g_2) * x \overset{\because\text{(G3)}}{=} g_1 * (g_2 * x)$$
$$\overset{\because\text{定義}}{=} g_1 * (g_2 \bullet_{L_{\mathrm{reg}}} x) = g_1 \bullet_{L_{\mathrm{reg}}} (g_2 \bullet_{L_{\mathrm{reg}}} x)$$

より，(LA2) もなりたつので，左正則作用 $\bullet_{L_{\mathrm{reg}}}$ は $(G, *)$ の G 自身への左作用となる．

$\boxed{\text{p.248 下から 5 行目}}$ $g = x_3 = \overline{3}$ より，

$$gx_1 = \overline{3} \cdot \overline{1} = \overline{3} = x_3, \qquad gx_2 = \overline{3} \cdot \overline{2} = \overline{6} = \overline{1} = x_1,$$
$$gx_3 = \overline{3} \cdot \overline{3} = \overline{9} = \overline{4} = x_4, \qquad gx_4 = \overline{3} \cdot \overline{4} = \overline{12} = \overline{2} = x_2$$

と計算できる．

$\boxed{\text{p.248 下から 2 行目}}$ $g = x_1 = \overline{1}$ のとき $gx_i = x_i$ $(i = 1, 2, 3, 4)$ がなりたつので，$L(x_1) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = e$ がなりたつ．また，$g = x_2 = \overline{2}$ のとき，

$$gx_1 = \overline{2} \cdot \overline{1} = \overline{2} = x_2, \qquad gx_2 = \overline{2} \cdot \overline{2} = \overline{4} = x_4,$$
$$gx_3 = \overline{2} \cdot \overline{3} = \overline{6} = \overline{1} = x_1, \qquad gx_4 = \overline{2} \cdot \overline{4} = \overline{8} = \overline{3} = x_3$$

より，$L(x_2) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix} = (1\ 2\ 4\ 3)$ である．最後に，$g = x_4 = \overline{4}$ のとき，

$$gx_1 = \overline{4} \cdot \overline{1} = \overline{4} = x_4, \qquad gx_2 = \overline{4} \cdot \overline{2} = \overline{8} = \overline{3} = x_3,$$
$$gx_3 = \overline{4} \cdot \overline{3} = \overline{12} = \overline{2} = x_2, \qquad gx_4 = \overline{4} \cdot \overline{4} = \overline{16} = \overline{1} = x_1$$

より，$L(x_4) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = (1\ 4)(2\ 3)$ である．

$\boxed{\text{p.248 脚注 15)}}$ 実際，任意の $x \in G$ に対して，$x \bullet_{R_{\mathrm{reg}}} e_G \overset{\because\text{定義}}{=} x * e_G = x$ であるから，(RA1) がなりたち，任意の $g_1, g_2, x \in G$ に対して，

$$x \bullet_{R_{\mathrm{reg}}} (g_1 * g_2) \overset{\because\text{定義}}{=} x * (g_1 * g_2) \overset{\because\text{(G3)}}{=} (x * g_1) * g_2$$
$$\overset{\because\text{定義}}{=} (x \bullet_{R_{\mathrm{reg}}} g_1) * g_2 = (x \bullet_{R_{\mathrm{reg}}} g_1) \bullet_{L_{\mathrm{reg}}} g_2$$

より，(RA2) もなりたつので，右正則作用 $\bullet_{R_{\mathrm{reg}}}$ は $(G, *)$ の G 自身への右作用となる．

$\boxed{\text{p.250 上から 2 行目}}$ 実際，任意の $x \in G$ に対して，$e_G \odot_{\mathrm{c}} x \overset{\text{定義}}{=} e_G * x * e_G' = x$ であるから，(LA1) がなりたち，任意の $g_1, g_2, x \in G$ に対して，

$$(g_1 * g_2) \odot_{\mathrm{c}} x \overset{\text{定義}}{=} (g_1 * g_2) * x * (g_1 * g_2)' \overset{\text{問 6.4 (3)}}{=} g_1 * (g_2 * x * g_2') * g_1'$$
$$\overset{\text{定義}}{=} g_1 * (g_2 \odot_{\mathrm{c}} x) * g_1' = g_1 \odot_{\mathrm{c}} (g_2 \odot_{\mathrm{c}} x)$$

より，(LA2) もなりたつので，共役作用 $\odot_{\mathrm{c}}$ は $(G, *)$ の G 自身への左作用となる．最後に，任意の $g, x, y \in G$ に対して，

$$g \odot_{\mathrm{c}} (x * y) \overset{\text{定義}}{=} g * (x * y) * g' \overset{g' * g = e_G}{=} (g * x * g') * (g * y * g')$$
$$\overset{\text{定義}}{=} (g \odot_{\mathrm{c}} x) * (g \odot_{\mathrm{c}} y)$$

より，$\odot_{\mathrm{c}}$ が (LA3) をみたすことも確認できた．

$\boxed{\text{p.250 上から 4 行目}}$ 実際，任意の $x \in G$ に対して，$x \odot_{\mathrm{c},r} e_G \overset{\text{定義}}{=} e_G' x * e_G = x$ であるから，(RA1) がなりたち，任意の $g_1, g_2, x \in G$ に対して，

$$x \odot_{\mathrm{c},r} (g_1 * g_2) \overset{\text{定義}}{=} (g_1 * g_2)' x * (g_1 * g_2) \overset{\text{問 6.4 (3)}}{=} g_2' * (g_1' x * g_1) * g_2$$
$$\overset{\text{定義}}{=} g_2' * (x \odot_{\mathrm{c},r} g_1) * g_2 = (x \odot_{\mathrm{c},r} g_1) \bullet_{L_{\mathrm{reg}}} g_2$$

より，(RA2) もなりたつので，右共役作用 $\odot_{\mathrm{c},r}$ は $(G, *)$ の G 自身への右作用となる．最後に，任意の $g, x, y \in G$ に対して，

$$(x * y) \odot_{\mathrm{c}} g \overset{\text{定義}}{=} g' * (x * y) * g \overset{g * g' = e_G}{=} (g' * x * g) * (g' * y * g)$$
$$\overset{\text{定義}}{=} (x \odot_{\mathrm{c},r} g) * (y \odot_{\mathrm{c},r} g)$$

より，$\odot_{\mathrm{c},r}$ が (LA3) に対応する性質

(RA3)　$(x * y) \odot_r g = (x \odot_r g) * (y \odot_r g) \quad (g \in G_2,\ x, y \in G_1)$

をみたすことも確認できた．

$\boxed{\text{p.250 上から 6 行目}}$ 任意の $h \in H$ および $n \in N$ に対して，

$$h \odot_l n \overset{\text{定義}}{=} h * n * h' \overset{N \text{ の正規性}}{\in} N$$

であることに注意しよう．$\odot_l$ が (LA1), (LA2) をみたすことはすでに確認したので，$\odot_l$

が H の N への左共役作用を誘導することが従う．

$\boxed{\text{p.250 下から 9 行目}}$ 実際，

$$\begin{aligned}
(g_1, g_2) \diamond_{\odot} (g_2' \odot g_1', g_2') &\overset{\text{定義}}{=} (g_1 * (g_2 \odot (g_2' \odot g_1')), g_2 \star g_2') \\
&\overset{\text{(LA2)}}{=} (g_1 * (\underbrace{(g_2 \star g_2')}_{=e_{G_2}} \odot g_1'), e_{G_2}) \\
&\overset{\text{(LA1)}}{=} (g_1 * g_1', e_{G_2}) = (e_{G_1}, e_{G_2}), \\
(g_2' \odot g_1', g_2') \diamond_{\odot} (g_1, g_2) &\overset{\text{定義}}{=} ((g_2' \odot g_1') * (g_2' \odot g_1), g_2' \star g_2) \\
&\overset{\text{(LA3)}}{=} (g_2' \odot (\underbrace{g_1' * g_1}_{=e_{G_1}}), e_{G_2}) \overset{(\sharp)}{=} (e_{G_1}, e_{G_2})
\end{aligned}$$

より，逆元の一意性 [⇨ $\boxed{\text{問 6.4}}$ (2)] から $(g_1, g_2)^{-1} = (g_2' \odot g_1', g_2')$ であることが従う．なお，等号 $(\sharp)$ は (LA3) をみたす左作用について，任意の $g_2 \in G_2$ に対して $g_2 \odot e_{G_1} = e_{G_1}$ がなりたつという事実から従う．実際，(LA3) より，

$$g_2 \odot e_{G_1} = g_2 \odot (e_{G_1} * e_{G_1}) \overset{\text{(LA3)}}{=} (g_2 \odot e_{G_1}) * (g_2 \odot e_{G_1})$$

となるので，両辺に $(g_2 \odot e_{G_1})'$ との演算を施して $g_2 \odot e_{G_1} = e_{G_1}$ を得る．

$\boxed{\text{p.251 上から 4 行目}}$ まず，$\pi\colon G_1 \rtimes_{\odot} G_2 \to G_2$ を $\pi(g_1, g_2) = g_2$ により定めると，π は明らかに全射であり，任意の $(g_1, g_2), (h_1, h_2) \in G_1 \rtimes_{\odot} G_2$ に対して，

$$\begin{aligned}
\pi\big((g_1, g_2) \diamond_{\odot} (h_1, h_2)\big) &= \pi((g_1 * (g_2 \odot h_1), g_2 \star h_2)) \\
&\overset{\text{定義}}{=} g_2 \star h_2 \overset{\text{定義}}{=} \pi((g_1, g_2)) \star \pi((h_1, h_2))
\end{aligned}$$

であるから，π は全射準同型写像となる．このとき $\operatorname{Ker} \pi = \{(g_1, e_{G_2}) \mid g_1 \in G_1\} = \widetilde{G}_1$ であるから，例題 12.11 より $\widetilde{G}_1$ が $G_1 \rtimes_{\odot} G_2$ の正規部分群であることが示された [14]．なお，$i_1\colon G_1 \to \widetilde{G}_1\,; g_1 \mapsto (g_1, e_{G_2})$ と定める と，任意の $g_1, h_1 \in G_1$ に対して，

[⇨ スペースの関係上，次のページに続きます]

[14] もちろん，直接，(H1) – (H3) を確認して，$\widetilde{G}_1$ が $G_1 \rtimes_{\odot} G_2$ の部分群であることを確認した後に，$\widetilde{G}_1$ の正規性を確認しても構わない．

$$
\begin{aligned}
i_1(g_1) \diamond_{\odot} i_1(h_1) &\overset{\text{定義}}{=} (g_1, e_{G_2}) \diamond_{\odot} (h_1, e_{G_2}) \overset{\text{定義}}{=} (g_1 * (e_{G_2} \odot h_1), e_{G_2}) \\
&\overset{(\mathrm{LA1})}{=} (g_1 * g_2, e_{G_2}) \overset{\text{定義}}{=} i_1(g_1 * h_1)
\end{aligned}
$$

より i_1 は群準同型写像であり，明らかに $\widetilde{G}_1 \to G_1\,;(g_1, e_{G_2}) \mapsto g_1$ が逆写像となるので，$\widetilde{G}_1$ は G_1 と同型である．続いて，$i_2\colon G_1 \to \widetilde{G}_2\,; g_2 \mapsto (e_{G_1}, g_2)$ と定めると，任意の $g_2, h_2 \in G_2$ に対して，

$$
\begin{aligned}
i_2(g_2) \diamond_{\odot} i_2(h_2) &\overset{\text{定義}}{=} (e_{G_1}, g_2) \diamond_{\odot} (e_{G_1}, h_2) \overset{\text{定義}}{=} (e_{G_1} * (g_2 \odot e_{G_1}), g_2 \star h_2) \\
&\overset{(\sharp)}{=} (e_{G_1} * e_{G_1}, g_2 \star h_2) = i_2(g_2 \star h_2)
\end{aligned}
$$

であるから（($\sharp$) については直前の ✍ の解説を参照せよ），i_2 は群準同型写像であり，さらに $\operatorname{Im} i_2 = \{(e_{G_1}, g_2) \mid g_2 \in G_2\} = \widetilde{G}_2$ であるから，問 8.3 より $\widetilde{G}_2$ は $G_1 \rtimes_{\odot} G_2$ の部分群である．また，π を $\widetilde{G}_2$ に制限したものが明らかに i_2 の逆写像となっているので，$\widetilde{G}_2$ は G_2 と同型である．

p.251 上から 12 行目（1 つ目）　$(h \odot_{\mathrm{c}} n) * h \overset{\text{定義}}{=} (h * n * h') * h = h * n$ である．

p.251 上から 12 行目（2 つ目）　実際，$(h_1, n_1), (h_2, n_2) \in H \rtimes_{\odot_{\mathrm{c}}} N$ に対して，

$$
\begin{aligned}
\Psi((h_1, n_1) \diamond_{\odot_{\mathrm{c}}} (h_2, n_2)) &\overset{\diamond_{\odot_{\mathrm{c}}}\text{の定義}}{=} \Psi(h_1 * (n_1 \odot_{\mathrm{c}} h_2), n_1 * n_2) \\
&\overset{\Psi\text{の定義}}{=} (h_1 * (n_1 \odot_{\mathrm{c}} h_2)) * n_1 * n_2 \\
&\overset{(\mathrm{G3})}{=} h_1 * \underbrace{\big((n_1 \odot_{\mathrm{c}} h_2) * n_1\big)}_{=n_1 * h_2} * n_2 \\
&= (h_1 * n_1) * (h_2 * n_2) \\
&= \Psi((h_1, n_1)) * \Psi((n_2 * h_2))
\end{aligned}
$$

であるから，Ψ は群準同型写像である．

p.251 上から 13 行目　$G = N * H$ であるから，任意の G の元は $g = n * h$ ($n \in N$, $h \in H$) と表せる．したがって，$\Psi\big((n, h)\big) = n * h = g$ より Ψ は全射である．一方で，$\Psi\big((n, h)\big) = n * h = e_G$ ($n \in N$, $h \in H$) がなりたつのは $n = h' \in N \cap H$ がなりたつときであるが，仮定より $N \cap H = \{e_G\}$ であるから $n = h = e_G$ が従う．つまり，$\operatorname{Ker} \Psi = (e_G, e_G)$ であるから，Ψ は単射でもある．以上より，Ψ が群同型写像であることが確認できた．

p.251 下から 7 行目 $N \lhd \mathfrak{S}_3$ および $\mathfrak{S}_3 = N \sqcup N(1\,2)$ となることは【p.189 下から 8 行目】の ✍ で確認した[15]．後者より，$NH \supseteq N \sqcup N(1\,2) = \mathfrak{S}_3$ となり，$NH = \mathfrak{S}_3$ も従う．さらに，$N = \{e,\,(1\,2\,3),\,(1\,3\,2)\}$, $H = \{e,\,(1\,2)\}$ より，$N \cap H = \{e_G\}$ もなりたつ．

p.251 下から 5 行目 同型 $N \xrightarrow{\sim} \mathbb{Z}/3\mathbb{Z};\ (1\,2\,3)^a \mapsto \overline{a}$ および $H \xrightarrow{\sim} \mathbb{Z}/2;\ (1\,2)^l \mapsto \overline{b}$ によって，N および H を加法的巡回群 $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}$ と同一視していることに注意しよう．この同一視のもとで，

$$e \odot_{\mathrm{c}} (1\,2\,3)^a = (1\,2\,3) \odot_{\mathrm{c}}, \qquad (1\,2) \odot_{\mathrm{c}} (1\,2\,3)^a = (1\,3\,2)^a = (1\,2\,3)^{-a}$$

で定まる H の N への作用 $\odot_{\mathrm{c}}$ は，

$$\overline{0} \odot_{\mathrm{inv}} \overline{a} = \overline{a}, \qquad \overline{1} \odot_{\mathrm{inv}} \overline{a} = -\overline{a}$$

により定義される，$\mathbb{Z}/2\mathbb{Z}$ の $\mathbb{Z}/3\mathbb{Z}$ への作用 $\odot_{\mathrm{inv}}$ に翻訳される．

p.252 上から 3 行目 どちらも単位元 (e, e) とは異なる元であるため，自分自身との演算を計算すると (e, e) となることを確かめればよい．ここで (LA3) より，任意の $x \in C_2$ に対して，

$$x \odot e = x \odot (e * e) \overset{\text{☺}}{=}{}^{\text{(LA3)}} (x \odot e) * (x \odot e)$$

となるので，$(x \odot e)'$ との演算を考えると $x \odot e = e$ となることに注意しよう．このとき

$$(s^{*2}, e) \diamond_{\odot} (s^{*2}, e) \overset{\text{☺}}{=}{}^{\text{定義}} (s^{*2} * (e \odot s^{*2}), e * e) \overset{\text{☺}}{=}{}^{\text{(LA1)}} (s^{*2} * s^{*2}, e) = (e, e),$$

$$(e, t) \diamond_{\odot} (e, t) \overset{\text{☺}}{=}{}^{\text{定義}} (e * (t \odot e), t * t) \overset{\text{☺}}{=}{}^{\text{上式}} (e * e, t^{*2}) = (e, e)$$

となるので，(s^{*2}, e), (e, t) は確かに $C_4 \rtimes_{\odot} C_2$ の（異なる）2 元であることが確かめられた．

p.252 下から 5 行目（1 つ目） 実際，任意の $x \in G_1$ に対して，

$$e_{G_2\,\phi} \tilde{\odot} x \overset{\text{☺}}{=}{}^{\text{定義}} \phi(e_{G_2}) \odot x \overset{\text{☺}}{=}{}^{\text{補題 8.7 (1)}} e_{G_2} \odot x \overset{\text{☺}}{=}{}^{\odot\ \text{の (LA1)}} x$$

より (LA1) がなりたち，任意の $x \in G_1$, $a, b \in G_2$ に対して，

---

15) p.189 では左剰余類分割 $\mathfrak{S}_3 = N \sqcup (1\,2)N$ を求めているが，まったく同じ議論で右剰余類分割も求められる．

$$
\begin{aligned}
(a \star b)_\phi \tilde{\odot} x &\overset{\text{定義}}{=} \phi(a \star b) \odot x \overset{\text{準同型性}}{=} \big(\phi(a) \star \phi(b)\big) \odot x \\
&\overset{\odot\text{ の}}{=}^{(\mathrm{LA2})} \phi(a) \odot \big(\phi(b) \odot x\big) \overset{\text{定義}}{=} a_\phi \tilde{\odot} (b_\phi \tilde{\odot} x)
\end{aligned}
$$

であるから (LA2) もなりたつ．最後に，任意の $x, y \in G_1$, $g \in G_2$ に対して，

$$
\begin{aligned}
g_\phi \tilde{\odot} (x * y) &\overset{\text{定義}}{=} \phi(g) \odot (x * y) \overset{\odot\text{ の}}{=}^{(\mathrm{LA3})} \big(\phi(g) \odot x\big) * \big(\phi(g) \odot y\big) \\
&\overset{\text{定義}}{=} (g_\phi \tilde{\odot} x) * (g_\phi \tilde{\odot} y)
\end{aligned}
$$

であるから (LA3) もなりたつ．

$\boxed{\text{p.252 下から 5 行目（2 つ目）}}$　まず，任意の $x \in G_1$ および $g \in G_2$ に対して，${}_\phi\tilde{\odot}$ の定義から $\phi^{-1}(g)_\phi \tilde{\odot} x \overset{\text{定義}}{=} \phi\big(\phi^{-1}(g)\big) \odot x = g \odot x$ がなりたつことに注意しよう．すると，任意の $(g_1, g_2), (h_1, h_2) \in G_1 \rtimes_\odot G_2$ に対して，

$$
\begin{aligned}
\Phi((g_1, g_2) \diamond_\odot (h_1, h_2)) &\overset{\diamond_\odot\text{ の定義}}{=} \Phi\big((g_1 * (g_2 \odot h_1), g_2 \star h_2)\big) \\
&\overset{\Phi\text{ の定義}}{=} (g_1 * (g_2 \odot h_1), \phi^{-1}(g_2 \star h_2)) \\
&= (g_1 * \big(\phi^{-1}(g_2)_\phi \tilde{\odot} h_1\big), \phi^{-1}(g_2) \star \phi^{-1}(h_2)) \\
&\overset{\diamond_{\phi\tilde{\odot}}\text{ の定義}}{=} (g_1, \phi^{-1} l(g_2)) \diamond_{\phi\tilde{\odot}} (h_1, \phi^{-1}(h_2)) \\
&\overset{\Phi\text{ の定義}}{=} \Phi((g_1, h_1)) \diamond_{\phi\tilde{\odot}} \Phi((g_2, h_2))
\end{aligned}
$$

より，Φ が群準同型写像であることが確認できた．

$\boxed{\text{p.252 下から 1 行目}}$　実際，$x \in G_1$, $a, b \in G_2$ に対して，

$$
\begin{aligned}
(a \star b) \tilde{\odot}_\psi x &\overset{\text{定義}}{=} (a \star b) \odot \psi(x) \overset{\odot\text{ の}}{=}^{(\mathrm{LA2})} a \odot (b \odot \psi(x)), \\
a \odot_\psi (b \odot_\psi x) &\overset{\text{定義}}{=} a \odot_\psi (b \odot \psi(x)) \overset{\text{定義}}{=} a \odot \psi(b \odot \psi(x))
\end{aligned}
$$

と計算されるため，一般に $(a \star b) \tilde{\odot}_\psi x \neq a \tilde{\odot}_\psi (b \tilde{\odot}_\psi x)$ であるから (LA2) がなりたたず，$\tilde{\odot}_\psi$ は左作用とならない．

$\boxed{\text{p.252 脚注 20)}}$　$\mathrm{Aut}(C_2) \cong (\mathbb{Z}/2\mathbb{Z})^\times \cong \{e\}$（自明な群）であるから，群準同型写像 $C_4 \to \mathrm{Aut}(C_2)$ は自明な準同型写像のみであり，したがって，C_4 の C_2 への作用は自明な作用のみである．よって，$C_2 \rtimes_\odot C_4$ として考えられるものは $C_2 \rtimes_{\odot_{\mathrm{triv}}} C_4 = C_2 \times C_4$

のみである．

§15 の ✍ のマーク

$\boxed{\text{p.256 下から 5 行目}}$ まず，$e_G \bullet_l x \overset{\because\,(\mathrm{LA1})}{=} x$ であるから $e_G \in \mathrm{Stab}_G(x)$ であり，(H1) がなりたつ．続いて，$g \in \mathrm{Stab}_G(x)$ に対して定義より $x = g \bullet_l x$ であるから，両辺に g' を作用させると，

$$g' \bullet_l x = g' \bullet_l (g \bullet_l x) \overset{\because\,(\mathrm{LA2})}{=} \underbrace{(g' * g)}_{=e_G} \bullet_l x \overset{\because\,(\mathrm{LA1})}{=} x$$

より $g' \in \mathrm{Stab}_G(x)$ となり，(H2) もなりたつ．最後に，$g, h \in \mathrm{Stab}_G(x)$ に対して，

$$(g * h) \bullet_l \overset{\because\,(\mathrm{LA2})}{=} g \bullet_l \underbrace{(h \bullet_l x)}_{=x} = g \bullet_l x = x \qquad (\because g, h \in \mathrm{Stab}_G(x))$$

より，(H3) もなりたつ．以上より，$\mathrm{Stab}_G(x)$ が $(G, *)$ の部分群であることが示された．

$\boxed{\text{p.257 上から 1 行目}}$ $x_0 \in \mathrm{Fix}_G(X)$ より，任意の $g \in G$ に対して $g \bullet_l x_0 = x_0$ であるから，$\mathrm{Orb}_G(x_0) = \{g \bullet_l x_0 \mid g \in G\} = \{x_0\}$ である．

$\boxed{\text{p.258 上から 10 行目}}$ $x \in X$ に対し，$x \overset{\because\,(\mathrm{LA1})}{=} e \bullet_l x$ より，反射律 (E1) $x \sim_{\bullet_l} x$ が従う．次に，$x, y \in X$ に対して，$x \sim_{\bullet_l} y$ がなりたつ，すなわち，$x = g \bullet_l y$ をみたす $g \in G$ が存在するならば，両辺に（左から）g' を作用させて $y = g' \bullet_l x$ となるので，$y \sim_{\bullet_l} x$ ゆえ，対称律 (E2)「$x \sim_{\bullet_l} y \Rightarrow y \sim_{\bullet_l} x$」も従う．最後に，$x, y, z \in X$ に対して，$x \sim_{\bullet_l} y$ かつ $y \sim_{\bullet_l} z$ がなりたつ， すなわち，$x = g \bullet_l y$ と $y = h \bullet_l z$ をみたす $g, h \in G$ が存在するならば，$x = g \bullet_l (h \bullet_l z) \overset{\because\,(\mathrm{LA2})}{=} (g * h) \bullet_l z$ より， $x \sim_{\bullet_l}$ ゆえ，推移律 (E3)「$x \sim_{\bullet_l} y$ かつ $y \sim_{\bullet_l} z \Rightarrow x \sim_{\bullet_l} z$」もなりたつ．以上より，$\sim_{\bullet}$ は X 上の同値関係である．

$\boxed{\text{p.258 下から 8 行目}}$ まず，$y = g \bullet_l x$ の両辺に（左から）g' を作用させて $x = g' \bullet_l y$ を得る．このとき，任意の $g * t * g' \in g * \mathrm{Stab}_G(x) * g'$（つまり $t \in \mathrm{Stab}_G(x)$）に対し，

$$\begin{aligned}
(g * t * g') \bullet_l y &\overset{\because\,(\mathrm{LA2})}{=} g \bullet_l \big(t \bullet_l (g' \bullet_l y)\big) = g \bullet_l (t \bullet_l x) \qquad (\because x = g' \bullet_l y) \\
&= g \bullet_l x \qquad (\because t \in \mathrm{Stab}_G(x)) \\
&= y \qquad (\because y = g \bullet_l x)
\end{aligned}$$

であるから，$g * t * g' \in \mathrm{Stab}_G(y)$ であり，$g * \mathrm{Stab}_G(x) * g' \subset \mathrm{Stab}_G(y)$ が従う．

p.258 下から 3 行目　定義より，

$$\mathrm{Orb}_H(g) \overset{\text{定義}}{=} \{g \bullet_{R_{\mathrm{reg}}} h \mid h \in H\} \overset{R_{\mathrm{reg}}\text{ の定義}}{=} \{g * h \mid h \in H\} = g * H$$

である．

p.259 上から 6 行目　$z \in \mathbb{C}^\times$ のとき，$wz = z$ をみたす複素数 w は $w = 1$ のみであるから（両辺に $z^{-1} = \dfrac{1}{z}$ をかければよい），

$$\mathrm{Stab}_{\mathbb{S}^1}(z) \overset{\text{定義}}{=} \{w \in \mathbb{S}^1 \mid w \bullet z = z\} = \{w \in \mathbb{S}^1 \mid wz = z\} = \{1\}$$

である．また，$|w \bullet z| = \underbrace{|w|}_{=1}|z| = |z|$ $(w \in \mathbb{S}^1)$ より，$\mathrm{Orb}_{\mathbb{S}^1}(z) \subseteq \{\tilde{z} \in \mathbb{C} \mid |\tilde{z}| = |z|\}$ である．逆に，$|\tilde{z}| = |z|$ をみたす任意の複素数 $\tilde{z}$ に対して $w := \tilde{z}z^{-1}$ と定めると，$|w| = |\tilde{z}||z|^{-1} = 1$（$\because$ $|\tilde{z}| = |z|$）であり，さらに，$w \bullet z = wz = \tilde{z}z^{-1}z = \tilde{z}$ となるので，$\tilde{z} \in \mathrm{Orb}_{\mathbb{S}^1}(z)$ である．したがって，$\{\tilde{z} \in \mathbb{C} \mid |\tilde{z}| = |z|\} \subseteq \mathrm{Orb}_{\mathbb{S}^1}(z)$ も従うので，$\mathrm{Orb}_{\mathbb{S}^1}(z)$ が原点 0 中心，半径 $|z|$ の円周 $\{\tilde{z} \in \mathbb{C} \mid |\tilde{z}| = |z|\}$ と一致することが示された．

p.260 上から 2 行目　$a \in \mathbb{R}$ に対して，$a \bullet (0, C) = (a + 0, e^a C) = (a, e^a C)$ であり，$\{(a, Ce^a) \mid a \in \mathbb{R}\}$ は指数関数 $y = Ce^x$ の媒介変数表示をあたえている．したがって，$\mathrm{Orb}_{\mathbb{R}}\big((0, C)\big) = \{(x, y) \in \mathbb{R}^2 \mid y = Ce^x\}$ である．

p.260 上から 3 行目　x_0, y_0 はともに実数で，$e^{x_0} \neq 0$ であるから $C = y_0 e^{-x_0}$ とおけばよい．

p.261 下から 7 行目　任意の $g \in G \smallsetminus \{e_G\}$ に対して，$g \bullet_l x_0 \neq x_0$ をみたす $x_0 \in X$ が存在するので，$\rho_{\bullet_l}(g)(x_0) \neq x_0$ より，$\rho_{\bullet_l}(g) \neq e$ がなりたつ．対偶をとると「$\rho_{\bullet_l}(g) = e$ ならば $g = e_G$」となるが，これは $\rho_{\bullet_l}$ が単射であることを表しているのに他ならない．

p.261 脚注 4)　$\mathbb{K} \neq \mathbb{F}_2$（より一般に標数 2 でない体）として $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \in \mathrm{Stab}_G(\boldsymbol{e}_2)$，$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \mathrm{B}_2(\mathbb{K})$ を考えると，

[⇨ スペースの関係上，次のページに続きます]

$$\begin{pmatrix}1&1\\0&1\end{pmatrix}\begin{pmatrix}-1&0\\0&1\end{pmatrix}\begin{pmatrix}1&1\\0&1\end{pmatrix}^{-1}=\begin{pmatrix}-1&1\\0&1\end{pmatrix}\begin{pmatrix}1&-1\\0&1\end{pmatrix}=\begin{pmatrix}-1&2\\0&1\end{pmatrix}\notin \mathrm{Stab}_G(\boldsymbol{e}_2)$$

だから，$\mathrm{Stab}_G(\boldsymbol{e}_2)$ は $\mathrm{B}_2(\mathbb{K})$ の正規部分群とはならない．

p.262 上から 3 行目 実際，任意の $(x,y)\in\mathbb{R}^2$ において，$a\bullet(x,y)=(a+x,e^a y)$ が (x,y) と一致するのは $a=0$ のときのみであり（第 1 成分を比較せよ），$\mathrm{Stab}_{\mathbb{R}}\big((x,y)\big)=\{0\}$ となるため，$\bullet$ は自由な作用である．

p.262 上から 5 行目 置換 $\sigma\in\mathfrak{S}_n$ が恒等置換 e でなければ，定義より $\sigma(i)\neq i$ をみたす $i\in\{1,2,\dots,n\}$ が存在するので，$\sigma\bullet_{\mathrm{pm}} i\neq i$ であり，$\bullet_{\mathrm{pm}}$ は忠実な作用である．また，任意の $i,j\in\{1,2,\dots,n\}$ に対して，$\sigma\bullet_{\mathrm{pm}} i=\sigma(i)=j$ をみたす $\sigma\in\mathfrak{S}_n$ は存在するので（例えば $\sigma=(i\,j)$）$\bullet_{\mathrm{pm}}$ は推移的な作用である．しかし，$n\geq 3$ とするとき，例えば $\mathrm{Stab}_{\mathfrak{S}_n}(1)$ は恒等置換 e 以外に $(2\,3)$ も含む，つまり，$\mathrm{Stab}_{\mathfrak{S}_n}(1)\neq\{e\}$ であるため，$\bullet_{\mathrm{pm}}$ は $n\geq 3$ のとき自由な作用ではない．

p.263 上から 12 行目 $g_2'*g_1\in\mathrm{Stab}_G(x)$ より，$g_2'*g_1=h$ $(h\in\mathrm{Stab}_G(x))$ と表せるので，両辺に左から g_2 との演算を施して $g_1=g_2*h\in g_2*\mathrm{Stab}_G(x)$ を得る．したがって，命題 10.12 (1) が適用でき，$g_1*\mathrm{Stab}_G(x)=g_2*\mathrm{Stab}_G(x)$ を得る．

p.263 下から 1 行目 固定点 x_0 の軌道が $\{x_0\}$ となることは，【p.257 上から 1 行目】の ✍ で確認した．逆に，$\mathrm{Orb}_G(x_0)=\{x_0\}$ であるならば，定義からすべての $g\in G$ に対して $g\bullet_l x_0=x_0$ がなりたつ必要があり，したがって，x_0 は固定点である．

p.264 上から 6 行目 $\mathfrak{S}_6$ の部分群 $H_1=\{e,(1\,2),(1\,3),(2\,3),(1\,2\,3),(1\,3\,2)\}$（これは $\mathfrak{S}_3$ と同型な部分群である）と $H_2=\langle(4\,5)\rangle=\{e,(4\,5)\}$ を考えると，H_1 の元は $1,2,3$ の間の置換のみを引き起こし，H_2 は $4,5$ の間の置換のみを引き起こすことから，H_1 の任意の元と H_2 の任意の元が可換であることが直ちに従う．このとき，$H_1H_2=\{\sigma\tau\mid\sigma\in H_1,\sigma\in H_2\}$ は $\mathfrak{S}_6$ の部分群をなすことは容易に確認できる．$G=H_1\sqcup H_1(4\,5)\subset H_1H_2$ であり，$H_1\cap H_2=\{e\}$ より $\#H_1H_2=6\cdot 2=12=\#G$ であることから $G=H_1H_2$ が従うので，G は $\mathfrak{S}_6$ の部分群である．

p.264 上から 11 行目 各 k に対して，k を動かさない G の元 σ は，k を含まない巡回置換の積になっているもののみである．また，軌道に関しては，$k=1,2,3$ は H_2 の元では動かないので，H_1 の元の作用での軌道を考えれば十分である．H_1 は $1,2,3$ に関するすべての置換を含んでいるため，$k=1,2,3$ を含む軌道は $\{1,2,3\}$ となる．同様に，$k=4,5$

は H_1 の元では動かないので，H_2 の元の作用での軌道を考えれば十分である．H_2 は $4,5$ に関するすべての置換を含んでいるため，$k=4,5$ を含む軌道は $\{4,5\}$ となる．G の中には 6 を動かす置換は含まれていないので，$\mathrm{Stab}_{\mathfrak{S}_6}(6)=\mathfrak{S}_6$ であり，$\mathrm{Orb}_{\mathfrak{S}_6}(6)=\{6\}$（固定点）となる．以上をまとめると，表 15.1 のようになる．

p.266 上から 8 行目　仮定より $\begin{pmatrix} x \\ y \end{pmatrix} \notin \mathbb{K}^2 \smallsetminus \{\mathbf{0}\}$ であるから，$xw-yz\neq 0$ をみたす $(z,w)\in\mathbb{K}^2$ が存在する [16]．この $(z,w)\in\mathbb{K}^2$ を用いて $A=\begin{pmatrix} x & z \\ y & w \end{pmatrix}$ とおけばよい．

p.268 上から 11 行目　$[A]\bullet_{\mathrm{ptf}}[\boldsymbol{e}_1]=\begin{bmatrix} a \\ c \end{bmatrix}$ より，これが $[\boldsymbol{e}_1]=\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ と一致するのは $c=0$ かつ $a\in\mathbb{K}^\times$ のときとなる．

§16 の ✍ のマーク

p.272 下から 7 行目　まず，$x\in G$ に対して $x=e_G*x*e_G'$ より，反射律 (E1) $x\sim_{\mathrm{c}} x$ がなりたつ．また，$x,y\in G$ に対して $x\sim_{\mathrm{c}} y$ がなりたつ，つまり，$x=g*y*g'$ をみたす $g\in G$ が存在するとき，両辺に左から g' と，右から $g=(g')'$ との演算を施すと $y=g'*x*(g')'$ より $y\sim_{\mathrm{c}} x$ となり，対称律 (E2) が従う．最後に，$x,y,z\in G$ に対して $x\sim_{\mathrm{c}} y$ かつ $y\sim_{\mathrm{c}} z$ がなりたつ，つまり，$x=g*y*g'$ および $y=h*z*h'$ をみたす $g,h\in G$ が存在するとき，$x=(g*h)*z*(h'*g')\overset{\text{問 6.4 (3)}}{=}(g*h)*z*(g*h)'$ より $x\sim_{\mathrm{c}} z$ となり，推移律 (E3) も従う．以上より，$\sim_{\mathrm{c}}$ が G 上の同値関係を定めることが確認できた．

p.274 上から 2 行目　転置行列の性質 ${}^t(AB)={}^tB\,{}^tA$ および ${}^t({}^tA)=A$ ［⇨［藤岡 1］**定理 2.5** (2) および (1.19)］より，

$$ {}^t({}^tUAU)={}^tU\,{}^tA\,{}^t(\,{}^tU)={}^tUAU \qquad (\because A\in\mathrm{Sym}_n(\mathbb{R}) \text{ より } {}^tA=A) $$

がなりたつので，${}^tUAU$ は対称行列である．

---

16) 例えば，$x\neq 0$ ならば $(z,w)=(0,1)$ ととればよいし，$y\neq 0$ ならば $(z,w)=(1,0)$ ととればよい．

p.274 下から 7 行目　対角化の一意性より，任意の実対称行列の対角化は，対角成分に並ぶ固有値の順番の違いを除いて一意的に定まる．したがって，とくに $\mathrm{T}_n(\mathbb{R})$ の 2 元で，対角成分を入れ換えたものになっていないものは異なる共役類に属する．一方で，基本行列 E_{ij}（単位行列 I_n の (i,i) 成分および (i,j) 成分を 0 に，(i,j) 成分および (j,i) 成分の 0 を 1 に置き換えてできる行列）による共役作用 ${}^tE_{ij}TE_{ij}$ により，対角行列 T の第 (i,i) 成分 x_i と第 (j,j) 成分 x_j が入れ換わるので，$\mathrm{T}_n(\mathbb{R})$ の元で対角成分を並べ換えたものはすべて同じ共役類に属する．以上より，$\mathrm{T}_n(\mathbb{R})$ の元で同じ共役類に属するものが，対角成分を入れ換えたものに限ることが示された．

p.275 上から 6 行目　まず，$J \in \mathcal{J}_n$ に対して J のジョルダン細胞を「入れ換えない」（**恒等置換**）と J と一致するので，反射律 (E1) $J \sim J$ がなりたつ．また，$J_1, J_2 \in \mathcal{J}_n$ に対して $J_1 \sim J_2$ がなりたつ，つまり，J_1 のジョルダン細胞を入れ換えると J_2 と一致するとき，J_1 に施（ほどこ）したジョルダン細胞の入れ換えの逆操作（**逆置換**）を J_2 のジョルダン細胞に施すと J_1 に戻るため，$J_2 \sim J_1$ となり，対称律 (E2) が従う．最後に，$J_1, J_2, J_3 \in \mathcal{J}_n$ に対して $J_1 \sim J_2$ かつ $J_2 \sim J_3$ がなりたつ，つまり，J_1 のジョルダン細胞を入れ換えると J_2 と一致し，J_2 のジョルダン細胞を入れ換えると J_3 と一致するとき，J_1 のジョルダン細胞を入れ換えて J_2 にしてから，さらにジョルダン細胞を置換することで J_3 に変形できるため，$J_1 \sim J_3$ となり，推移律 (E3) も従う．以上より，$\sim$ が $\mathcal{J}_n$ 上の同値関係を定めることが確認できた．

p.275 下から 3 行目　これはすでに【p.250 上から 6 行目】の ✍ で確認した．

p.275 下から 2 行目　定義から，

$$\mathrm{Orb}_G(x_\lambda) = \{g \bullet_{\mathrm{c}} x_\lambda \mid g \in G\} = \{g * x_\lambda * g' \mid g \in G\} = C(x_\lambda)$$

である．

p.276 上から 10 行目　まず，$x \in G$ の中心化群 $Z_G(x)$ について，$e_G * x = x * e_G = x$ より $e_G \in Z_G(x)$ であるから，(H1) がなりたつ．次に，任意の $g \in Z_G(x)$ に対して，定義より $g * x = x * g$ がなりたつから，両辺に左右から g' との演算を施して $x * g' = g' * x$ を得る．したがって，$g' \in Z_G(x)$ であるから，(H2) もなりたつ．最後に，任意の $g_1, g_2 \in Z_G(x)$ に対して，

[⇨ スペースの関係上，次のページに続きます]

$$(g_1 * g_2) * x = g_1 * x * g_2 \qquad (\because g_2 \in Z_G(x) \text{ より } g_2 * x = x * g_2)$$
$$= x * (g_1 * g2) \qquad (\because g_1 \in Z_G(x) \text{ より } g_1 * x = x * g_1)$$

より，$g_1 * g_2 \in Z_G(x)$ だから，(H3) もなりたつ．以上より，$Z_G(x)$ が $(G, *)$ の部分群であることが示された．

続いて，中心 $Z(G)$ について，任意の $g \in G$ に対して $g * e_G = e_G * g = g$ であるから，$e_G \in Z(G)$ であり，(H1) がなりたつ．次に，定義より任意の $x \in Z(x)$ は任意の $g \in G$ に対して $g * x = x * g$ をみたすので，両辺に左右から x' との演算を施して $x' * g = g * x'$ を得る．したがって，$x' \in Z(G)$ であるから，(H2) もなりたつ．最後に，任意の $x_1, x_2 \in Z(G)$ および任意の $g \in G$ に対して，

$$g * (x_1 * x_2) = x_1 * g * x_2 \qquad (\because x_1 \in Z(G) \text{ より } g * x_1 = x_1 * g)$$
$$= (x_1 * x_2) * g \qquad (\because x_2 \in Z(G) \text{ より } g * x_2 = x_2 * g)$$

より，$x_1 * x_2 \in Z(G)$ だから，(H3) もなりたつ．以上より，$Z(G)$ は $(G, *)$ の部分群である．最後に，任意の $x \in Z(G)$ と $g \in G$ に対して，

$$g * x * g' = \underbrace{g * g'}_{=e_G} * x = x \in Z(G) \qquad (\because x \in Z(G) \text{ より } g * x = x * g)$$

であるから，$Z(G)$ は G の正規部分群である．

p.276 上から 12 行目　$\odot_{\mathrm{c}}$ に対して $\mathrm{Orb}_G(x) = C(x)$, $\mathrm{Stab}_G(x) = Z_G(x)$ であることに注意すると，軌道・固定部分群定理［⇨ **定理 15.11**］より全単射 $G/Z_G(x) \xrightarrow{\sim} C(x)$ が存在するので，位数を比較して $\#C(x) = \#G/Z_G(x) = (G : Z_G(x))$ を得る．指数 $(G : Z_G(x))$ は $\#G$ の約数であるから，$\#C(x)$ も $\#G$ の約数である．以上で，命題 16.8 (1) が示された．

命題 16.8 (2) は，$\odot_c$ に対して $\mathrm{Orb}_G(x) = C(x)$, $\mathrm{Fix}_G(G)0 = Z(G)$, $G \backslash G = \mathrm{Conj}(G)$ であることに注意して，系 15.11 (2) の式に代入すればよい．

p.281 上から 3 行目　$\sigma_2 = \tau_1^{(2)} \tau_2^{(2)} \cdots \tau_s^{(2)}$ であり，

$$\rho \sigma_1 \rho^{-1} = \rho \tau_1^{(1)} \tau_2^{(1)} \cdots \tau_s^{(1)} \rho^{-1} = (\rho \tau_1^{(1)} \rho^{-1})(\rho \tau_2^{(1)} \rho^{-1}) \cdots (\rho \tau_s^{(1)} \rho^{-1})$$

であるから，各 $k = 1, 2, \ldots, s$ に対して $\tau_k^{(2)} = \rho \tau_k^{(1)} \rho^{-1}$ がなりたつことを示せばよい．これは，$\tau_k^{(1)} = (i_{k,1}\ i_{k,2}\ \cdots\ i_{k,t_k})$ であることに注意して補題 16.17 を用いることで，以下のように示される．

$$\begin{aligned}\rho\tau_k^{(1)}\rho &= (\rho(i_{k,1})\,\rho(i_{k,2})\,\cdots\,\rho(i_{k,t_k}))\\ &= (j_{k,1}\,j_{k,2}\,\cdots\,j_{k,t_k}) = \tau_k^{(2)} \qquad (\because \rho \text{ の定義})\end{aligned}$$

p.281 下から 2 行目 まず，$e_G = g * g' = g * e_G * g' \in g \bullet_{\mathrm{c}} H$ より，(H1) がなりたつ．続いて，任意の $g * h * g' \in g \bullet_{\mathrm{c}} H$（つまり，$h \in H$）に対して，

$$(g * h * g')' \overset{\because \text{問 } 6.4\ (3)}{=} g * h' * g' \in g \bullet_{\mathrm{c}} H \qquad (\because h' \in H)$$

より，(H2) もなりたつ．最後に，任意の $g * h_1 * g', g * h_2 * g' \in g \bullet_{\mathrm{c}} H$（つまり，$h_1, h_2 \in H$）に対して，

$$(g * h_1 * g') * (g * h_2 * g') = g * (h_1 * h_2) * g' \in g \bullet_{\mathrm{c}} H \qquad (\because h_1 * h_2 \in H)$$

より，(H3) もなりたつ．以上より，$g \bullet_{\mathrm{c}} H$ は $(G, *)$ の部分群である．

p.281 下から 1 行目 【p.250 上から 2 行目】の ✍ の解説と（(LA3) の証明を除いて）まったく同様の計算で確認できる．

p.282 上から 8 行目 まず，$e_G \bullet_c H = e_G * H * e_G = H$ であるから，$e_G \in N_G(H)$ であり，(H1) がなりたつ．続いて，任意の $g \in N_G(H)$ に対して $g \bullet_c H = H$ であるから，両辺に（左から）g' を作用させて $H = g' \bullet_{\mathrm{c}} H$ を得る．したがって，$g' \in N_G(H)$ であり，(H2) もなりたつ．最後に，任意の $g_1, g_2 \in N_G(H)$ に対して

$$(g_1 * g_2) \bullet_{\mathrm{c}} H \overset{\because (\mathrm{LA2})}{=} g_1 \bullet_{\mathrm{c}} \underbrace{(g_2 \bullet_{\mathrm{c}} H)}_{=H} = g_1 \bullet_{\mathrm{c}} H = H \qquad (\because g_1, g_2 \in N_G(H))$$

であるから，$g_1 * g_2 \in N_G(H)$ であり，(H3) もなりたつ．以上より，$N_G(H)$ は $(G, *)$ の部分群である．

p.282 上から 11 行目 任意の $g \in N_G(H)$ に対して $g \bullet_{\mathrm{c}} H = g * H * g' = H$ がなりたつが，これは H が $N_G(H)$ の正規部分群であることを表している．実際，任意の $h \in H$ と任意の $g \in N_G(H)$ に対して $g * h * g' \in g * H * g' = H$ がなりたつので，$H \lhd N_G(H)$ である．

p.286 問 16.10 (2) $\odot_{\mathrm{c}}$ は $\mathfrak{S}_4$ および $\mathfrak{A}_4$ の $\mathfrak{A}_4$ への左作用をあたえる（【p.250 上から 6 行目】の ✍）．したがって，$C(\sigma)$ が $\mathfrak{A}_4$ での共役の作用で閉じていることを示せばよいが，これは任意の $\tau\sigma\tau^{-1} \in C(\sigma)$ と $\rho \in \mathfrak{A}_4$ に対して $\rho \odot_{\mathrm{c}} (\tau\sigma\tau^{-1}) = (\rho\tau)\sigma(\rho\tau)^{-1} \in C(\sigma)$ であることから従う．

§17 の ✍ のマーク

p.288 下から 2 行目　実際に作用させてみると，確かに

$$\big((2\,3)\bullet_{\mathrm{pm}} g\big)(x_1,x_2,x_3)=(x_1-x_3)(x_1-x_2)(x_3-x_2)=-g(x_1,x_2,x_3),$$
$$\big((1\,3)\bullet_{\mathrm{pm}} g\big)(x_1,x_2,x_3)=(x_3-x_2)(x_3-x_1)(x_2-x_1)=-g(x_1,x_2,x_3)$$

となる．

p.291 下から 5 行目　あたえられた写像の逆写像が

$$\mathfrak{S}_n/\mathrm{Stab}_{\mathfrak{S}_n}(\boldsymbol{x}^{\boldsymbol{\lambda}})\xrightarrow{\sim}\mathfrak{S}_n/\mathrm{Stab}_{\mathfrak{S}_n}(\boldsymbol{x}^{\boldsymbol{\lambda}});\ \rho\mathrm{Stab}_{\mathfrak{S}_n}(\boldsymbol{x}^{\boldsymbol{\lambda}})\mapsto\sigma^{-1}\rho\mathrm{Stab}_{\mathfrak{S}_n}(\boldsymbol{x}^{\boldsymbol{\lambda}})$$

であたえられることは，ほぼ明らかである．

p.291 下から 3 行目　$\{\tau_i\}_{i=1}^{s}$ は商集合 $G/\mathrm{Stab}_{\mathfrak{S}_n}(\boldsymbol{x}^{\boldsymbol{\lambda}})$ の完全代表系なので，とくに，各 $i=1,2,\ldots,s$ に対して，剰余類 $\sigma\tau_i\mathrm{Stab}_{\mathfrak{S}_n}(\boldsymbol{x}^{\boldsymbol{\lambda}})$ はある $\tau_{j_{\sigma,i}}\mathrm{Stab}_{\mathfrak{S}_n}(\boldsymbol{x}^{\boldsymbol{\lambda}})$ と一致する．写像

$$\mathfrak{S}_n/\mathrm{Stab}_{\mathfrak{S}_n}(\boldsymbol{x}^{\boldsymbol{\lambda}})\xrightarrow{\sim}\mathfrak{S}_n/\mathrm{Stab}_{\mathfrak{S}_n}(\boldsymbol{x}^{\boldsymbol{\lambda}});\ \tau\mathrm{Stab}_{\mathfrak{S}_n}(\boldsymbol{x}^{\boldsymbol{\lambda}})\mapsto\sigma\tau\mathrm{Stab}_{\mathfrak{S}_n}(\boldsymbol{x}^{\boldsymbol{\lambda}})$$

の全単射性より，各 $j_{\sigma,i}\in\{1,2,\ldots,s\}$ が相異(あいこと)なることが従う．また，剰余類の等式 $\sigma\tau_i\mathrm{Stab}_{\mathfrak{S}_n}(\boldsymbol{x}^{\boldsymbol{\lambda}})=\tau_{j_{\sigma,i}}\mathrm{Stab}_{\mathfrak{S}_n}(\boldsymbol{x}^{\boldsymbol{\lambda}})$ より，命題 10.12 (1) から $\sigma\tau_i\in\tau_{j_{\sigma,i}}\mathrm{Stab}_{\mathfrak{S}_n}(\boldsymbol{x}^{\boldsymbol{\lambda}})$ であるから，$\sigma\tau_i=\tau_{j_{\sigma,i}}\rho_{\sigma,i}$ $(\rho_{\sigma,i}\in\mathrm{Stab}_{\mathfrak{S}_n}(\boldsymbol{x}^{\boldsymbol{\lambda}}))$ と表せる．

p.292 上から 6 行目　定義より，

$$\begin{aligned}
\big(\sigma\bullet_{\mathrm{pm}}(f+g)\big)(x_1,x_2,\ldots x_n)&=(f+g)(x_{\sigma(1)},x_{\sigma(2)},\ldots,x_{\sigma(n)})\\
&=f(x_{\sigma(1)},x_{\sigma(2)},\ldots,x_{\sigma(n)})+g(x_{\sigma(1)},x_{\sigma(2)},\ldots,x_{\sigma(n)})\\
&=(\sigma\bullet_{\mathrm{pm}} f)(x_1,x_2,\ldots,x_n)+(\sigma\bullet_{\mathrm{pm}} g)(x_1,x_2,\ldots,x_n)\\
&=f(x_1,x_2,\ldots,x_n)+g(x_1,x_2,\ldots,x_n)\qquad(\because f,g\in\mathrm{Fix}_{\mathfrak{S}_n}(\mathbb{K}[\boldsymbol{x}])),\\
\big(\sigma\bullet_{\mathrm{pm}}(kf)\big)(x_1,x_2,\ldots x_n)&=(kf)(x_{\sigma(1)},x_{\sigma(2)},\ldots,x_{\sigma(n)})\\
&=kf(x_{\sigma(1)},x_{\sigma(2)},\ldots,x_{\sigma(n)})=k(\sigma\bullet_{\mathrm{pm}} f)(x_1,x_2,\ldots,x_n)\\
&=kf(x_1,x_2,\ldots,x_n)\qquad(\because f\in\mathrm{Fix}_{\mathfrak{S}_n}(\mathbb{K}[\boldsymbol{x}]))
\end{aligned}$$

がなりたつ．したがって，$f+g$, kf $(k\in\mathbb{K})$ も対称式（つまり，$\mathrm{Fix}_{\mathrm{S}_n}(\mathbb{K}[\boldsymbol{x}])$）である．

p.292 下から 6 行目　軌道 $\mathrm{Orb}_{\mathfrak{S}_n}(\boldsymbol{\lambda})$ は，d の分割 $\boldsymbol{\lambda}=(\lambda_1,\lambda_2,\ldots,\lambda_n)$ の成分を

入れ換えたものすべてで構成されているため，とくに成分を大きい順に並べた分割が含まれる．したがって，任意の軌道の代表元として $\mathrm{Part}_n^{0,\geq}(d)$ の元がとれるので，あとは $\mathrm{Part}_n^{0,\geq}(d)$ の異なる 2 元が異なる軌道を代表することを示せばよい．このことは，$\mathrm{Part}_n^{0,\geq}(d)$ の異なる 2 元は，成分を並べ換えてももう一方にうつることはないという簡単な事実から従う．

p.293 下から 10 行目　$\boldsymbol{\lambda}_1 = (3,1,1,1)$ の並べ換えは，3 がどの位置にあるかで 4 通り（具体的には $(3,1,1,1)$, $(1,3,1,1)$, $(1,1,3,1)$, $(1,1,1,3)$）あり，$\boldsymbol{\lambda}_2 = (2,2,0,0)$ の並べ換えは $(2,2,0,0)$, $(2,0,2,0)$, $(2,0,0,2)$, $(0,2,2,0)$, $(9,2,0,2)$, $(0,0,2,2)$ の 6 通りである．これらを文字式 $x_1^{f_1}x_2^{f_2}x_3^{f_3}x_4^{f_4}$ の指数 (f_1,f_2,f_3,f_4) に配置して，$\mathrm{Orb}_{\mathfrak{S}_4}(\boldsymbol{x}^{\boldsymbol{\lambda}_1})$ および $\mathrm{Orb}_{\mathfrak{S}_4}(\boldsymbol{x}^{\boldsymbol{\lambda}_2})$ は p.293 で示した通りとなる．

p.294 下から 2 行目　線形関係式 $\displaystyle\sum_{\boldsymbol{\lambda}\in\mathrm{Part}_n^{0,\geq}(d)} a_{\boldsymbol{\lambda}} m_{\boldsymbol{\lambda}}(\boldsymbol{x}) = 0$ $(a_{\boldsymbol{\lambda}} \in \mathbb{K})$ において，左辺の各 $m_{\boldsymbol{\lambda}}(\boldsymbol{x})$ に現れる単項式はすべて相異なる．したがって，$\mathbb{K}[\boldsymbol{x}]$ における単項式の線形独立性より $a_{\boldsymbol{\lambda}} = 0$ も従う．

p.297 上から 5 行目　各 $e_k(\boldsymbol{x})^{\lambda_k-\lambda_{k+1}}$（ただし，$\lambda_{n+1}=0$ とおいた）を展開したときに現れる単項式の中で，指数に関する辞書式順序で最も大きいものは $(x_1x_2\cdots x_k)^{\lambda_k-\lambda_{k-1}}$ である（係数は 1）．したがって，$F_{\boldsymbol{\lambda}}(\boldsymbol{x})$ には

$$x_1^{\lambda_1-\lambda_2}(x_1x_2)^{\lambda_2-\lambda_3}\cdots(x_1x_2\cdots x_{n-1})^{\lambda_{n-1}-\lambda_n}(x_1x_2\cdots x_n)^{\lambda_n} = x^{\lambda_1}x^{\lambda_2}\cdots x_{n-1}^{\lambda_{n-1}}x_n^{\lambda_n} = \boldsymbol{x}^{\boldsymbol{\lambda}}$$

を含む単項対称式 $m_{\boldsymbol{\lambda}}(\boldsymbol{x})$ が（係数 1 で）現れる．

p.297 下から 4 行目　$(1+\alpha_1T)(1+\alpha_2T)\cdots(1+\alpha_nT) = 1 + a_2T^2 + \cdots + a_nT^n$ であるから，基本対称式の定義 (17.5) より $a_k = e_k(\alpha_1,\alpha_2,\ldots,\alpha_n)$ $(k=1,2,\ldots,n)$ がなりたつ．

p.298 上から 7 行目，10 行目　実際に展開して確認すればよいが，単項対称式の和になることはすでにわかっているので，項の数に気をつければ最後まで展開しきる必要はない．例えば，

$$\begin{aligned} F_{(3,1,0)}(\boldsymbol{x}) &= (x_1+x_2+x_3)^2(x_1x_2+x_1x_3+x_2x_3) \\ &= (x_1^2+x_2^2+x_3^2+2x_1x_2+2x_2x_3+2x_1x_3)(x_1x_2+x_1x_3+x_2x_3) \\ &= x_1^3x_2+\cdots+2x_1^2x_2^2+\cdots+5x_1^2x_2x_3+\cdots \end{aligned}$$

は，総計 $3^2 * 3 = 27$ 個の単項式の総和となるが，$x_1^3 x_2$ を含む単項対称式 $m_{(3,1,0)}(\boldsymbol{x})$ は $3! = 6$ 個の単項式の和となっており，$2x_1^2 x_2^2$ を含む単項対称式 $2m_{(2,2,0)}(\boldsymbol{x})$ は $2 \cdot 3 = 6$ 個の単項式の和となっており，$5x_1^2 x_2 x_3$ を含む単項対称式 $5m_{(2,1,1)}(\boldsymbol{x})$ は $5 \cdot 3 = 15$ 個の単項式の和であるため，$m_{(3,1,0)}(\boldsymbol{x}) + 2m_{(2,2,0)}(\boldsymbol{x}) + 5m_{(2,1,1)}(\boldsymbol{x})$ で $F_{(3,1,0)}(\boldsymbol{x})$ を展開した際に現れる 27 個の単項式の和が尽くされる．したがって，等式

$$F_{(3,1,0)}(\boldsymbol{x}) = m_{(3,1,0)}(\boldsymbol{x}) + 2m_{(2,2,0)}(\boldsymbol{x}) + 5m_{(2,1,1)}(\boldsymbol{x})$$

がなりたつことがわかる．

$$\begin{aligned} F_{(2,1,1)}(\boldsymbol{x}) &= (x_1 + x_2 + x_3)x_1 x_2 x_3 \\ &= x_1^2 x_2 x_3 + x_1 x_2^2 x_3 + x_1 x_2 x_3^2 = m_{(2,1,1)}(\boldsymbol{x}) \end{aligned}$$

は簡単に確認できる．また，

$$\begin{aligned} F_{(2,2,0)}(\boldsymbol{x}) &= (x_1 x_2 + x_2 x_3 + x_3 x_1)^2 \\ &= (x_1 x_2)^2 + (x_2 x_3)^2 + (x_3 x_1)^2 + 2(x_1 x_2^2 x_3 + x_1 x_2 x_3^2 + x_1^2 x_2 x_3) \\ &= x_1^2 x_2^2 + \cdots + 2x_1^2 x_2 x_3 + \cdots \end{aligned}$$

は，総計 $3^2 = 9$ 個の単項式の総和となるが，$x_1^2 x_2^2$ を含む単項対称式 $m_{(2,2,0)}(\boldsymbol{x})$ は 3 個の単項式の和となっており，$2x_1^2 x_2 x_3$ を含む単項対称式 $2m_{(2,1,1)}(\boldsymbol{x})$ は $2 \cdot 3 = 6$ 個の単項式の和であるため，$m_{(2,2,0)}(\boldsymbol{x}) + 2m_{(2,1,1)}(\boldsymbol{x})$ で $F_{(2,2,0)}(\boldsymbol{x})$ を展開した際に現れる 9 個の単項式の和が尽くされる．したがって，$F_{(2,2,0)}(\boldsymbol{x}) = m_{(2,2,0)}(\boldsymbol{x}) + 2m_{(2,1,1)}(\boldsymbol{x})$ がなりたつことがわかる．

p.299 上から 8 行目　実際，σ が互換 k 個の積で表されるならば，$\operatorname{sgn}\sigma = (-1)^k$ であり，定理 17.6 の証明と同様の計算により $\sigma \bullet_{\mathrm{pm}} f = (-1)^k f = (\operatorname{sgn}\sigma) f$ がなりたつ．

p.299 下から 6 行目　任意の $\sigma \in \mathfrak{S}_n$ と交代式 f に対して $\sigma \bullet_{\mathrm{pm}} f = (\operatorname{sgn}\sigma) f = \pm f$ であるが，$\mathbb{K} = \mathbb{F}_2$ のときは $-\overline{1} = \overline{1}$ となるため，$\sigma \bullet_{\mathrm{pm}} f = (\pm\overline{1}) f = f$ となる．つまり f は任意の置換の作用で不変となるので対称式となってしまう．

p.300 上から 11 行目　**削除**　〔**コメント**：「(✍)」を削除．第 2 版以降では削除済〕

§18 の ✍ のマーク

p.306 上から 4 行目　$G = C_p$ の真部分群は $\{e\}$ のみである．任意の $g \in G$ に対して

$g \bullet_{\mathrm{c}} \{e\} = \{g * e * g'\} = \{e\}$ であるから $g \in N_G(\{e\})$，すなわち $N_G(\{e\}) = G \supsetneq \{e\}$ となる．

p.306 上から 6 行目　任意の $g \in Z(G)$ に対して $g \bullet_{\mathrm{c}} H = g * H * g' = g * g' * H = H$ であるから，$g \in N_G(H)$ である．つまり，$Z(G) \subset N_G(H)$ である．

p.306 上から 8 行目　**背理法**で示す．$H/Z(G) = G/Z(G)$ であったと仮定すると，命題 12.4 より $H = \pi^{-1}(H/Z(G)) = \pi^{-1}(G/Z(G)) = G$（ただし，$\pi\colon G \to G/Z(G)$ は自然な全射準同型）となり，H が G の真部分群であったことと矛盾する．

p.306 上から 9 行目　**削除**　〔**コメント**：「(✍)」を削除．第 2 版以降では削除済〕

p.306 下から 3 行目　$H/Z(G) \subset N_{G/Z(G)}(H/Z(G))$ に命題 12.4 を用いることで，$H = \pi^{-1}(H/Z(G)) \subsetneq \pi^{-1}(N_{G/Z(G)}(H/Z(G))) = N$ を得る．さて，$\pi\colon G \to G/Z(G)$ を自然な全射準同型とすると，任意の $g \in N_G(H)$ および $h \in H$ に対して，

$$\begin{aligned} \pi(g) \bullet_{\mathrm{c}} \pi(h) &= \pi(g) * \pi(h) * \pi(g)' \overset{\because\ \text{準同型性}}{=} \pi(g * h * g') \\ &= \pi(g \bullet_{\mathrm{c}} h) \overset{\because\ g \in N_G(H)}{\in} \pi(H) = H/Z(G) \end{aligned}$$

であるから，$\pi(g) \bullet_{\mathrm{c}} H/Z(G) = H/Z(G)$ より $\pi(g) \in N_{G/Z(G)}(H/Z(G)) = N/Z(G)$，すなわち、$g \in N$ がなりたつ．したがって，$N_G(H) \subseteq N$ である．逆に，任意の $g \in N$ に対し，$\pi(g) \in N/Z(G) = N_{G/Z(G)}(H/Z(G))$ であるから，$\pi(g) \bullet_{\mathrm{c}} H/Z(G) = H/Z(G)$ がなりたつ．すなわち，任意の $\pi(h) \in H/Z(G)$ に対して $\pi(g) \bullet_{\mathrm{c}} \pi(h) = \pi(g \bullet_{\mathrm{c}} h) \in H/Z(G)$ がなりたつ．つまり，$g \bullet_{\mathrm{c}} h = h_1 * z$ $(h_1 \in H,\ z \in Z(G))$ と表せるので，$g \bullet_{\mathrm{c}} H \subset H$ であり，$g \in N_G(H)$，すなわち，$N \subseteq N_G(H)$ もなりたつ．以上より，$N = N_G(H)$ であることが示された．

p.307 下から 3 行目　位数 $p^e m$ $(p \nmid m)$ の有限群 $(G, *)$ が位数 p^e の部分群 P をもつとする．このとき，P を含む G の p 部分群 $Q \supseteq P$ をとると，ラグランジュの定理［⇨ **定理 10.23**］より $p^e \mid \#Q$ および $\#Q \mid p^e m$ がなりたつ．さらに，仮定から $\#Q$ は p の冪乗（べきじょう）であるため，$\#Q = p^e$ でなければならない．したがって，$Q \supseteq P$ とあわせて $Q = P$ を得る．これは，P が G の極大な p 部分群であることを表しているのに他ならない．

p.308 下から 8 行目　命題 6.21 より，

$$\begin{aligned}\#\mathrm{GL}_n(\mathbb{F}_p) &= \prod_{k=1}^{n}(p^n - p^{k-1}) = \prod_{k=1}^{n} p^{k-1}(p^{n-k+1}-1) \\ &= p^{\sum_{k=1}^{n}(k-1)} \prod_{k=1}^{n}(p^{n-k+1}-1) = p^{\frac{n(n-1)}{2}} \prod_{k=1}^{n}(p^{n-k+1}-1)\end{aligned}$$

がなりたつ．

p.309 上から 2 行目　$\mathfrak{A}_4$ が位数 6 の部分群 H を持つならば，H は位数 2 の元および位数 3 の元を含む．$\mathfrak{A}_4$ の 12 個の元は，クラインの 4 元群 $\mathfrak{V}_4$ の元 4 個と，位数 3 の巡回置換 8 個で構成される．したがって，H はクラインの 4 元群 $\mathfrak{V}_4$ の非自明な元 $(i\,j)(k\,l)$（ただし，$\{i,j\}\cap\{k,l\}=\emptyset$）と，位数 3 の巡回置換 τ を含む．τ は i,j,k,l のうち 3 つの数に関する巡回置換であるため，$\tau=(i\,j\,k)$ として一般性を失わない [17]．このとき，補題 16.7 から $\tau(i\,j)(k\,l)\tau^{-1}=(\tau(i)\,\tau(j))(\tau(k)\,\tau(l))=(\tau(j)\,\tau(k))(\tau(i)\,\tau(l))$ となるので，H は $\mathfrak{V}_4$ の非自明な 2 元を含むこととなり，したがって，$\mathfrak{V}_4$ 全体を含む．すると，$\mathfrak{A}_4=\mathfrak{V}_4\langle(i\,j\,k)\rangle$ であることから $H=\mathfrak{A}_4$ となってしまい，$\#H=6$ と矛盾する．

p.310 上から 4 行目　まず，$X\in\widetilde{\mathcal{S}}_{p^k}(G)$ に対して $X\to g*X\,;x\mapsto g*x$ および $g*X\to X\,;y\mapsto g'*y$ は互いに他の逆写像となる（したがって，全単射である）ので，$\#g*X=\#X=p^k$ であり $g\bullet_l X=g*X\in\widetilde{\mathcal{S}}_{p^k}(G)$ となることに気をつけよう．さて，$X\in\widetilde{\mathcal{S}}_{p^k}(G)$ に対して，

$$e_G\bullet_l X=e_G*X=\{g*x\mid x\in X\}=\{x\mid x\in X\}=X$$

であるから，(LA1) がなりたち，任意の $g_1,g_2\in G$ および $X\in\widetilde{\mathcal{S}}_{p^k}(G)$ に対して，

$$\begin{aligned}(g_1*g_2)\bullet_l X &= (g_1*g_2)*X \overset{\because\text{定義}}{=} \{(g_1*g_2)*x\mid x\in X\} \\ &\overset{\because\text{(G3)}}{=} \{g_1*(g_2*x)\mid x\in X\} \overset{\because\text{定義}}{=} g_1\bullet_l \underbrace{\{g_2*X\mid x\in X\}}_{=g_2\bullet_l X} \\ &\overset{\because\text{定義}}{=} g_1\bullet_l(g_2\bullet_l X)\end{aligned}$$

より，(LA2) もなりたつ．したがって，$\bullet_l$ は $(G,*)$ の $\widetilde{\mathcal{S}}_{p^k}(G)$ への左作用を定めている．

p.310 下から 3 行目　実際，(ア) より G の位数 p^k の部分群は，$\mathrm{Stab}_G(X_i)=X_i$ を

---

[17] H は τ で生成される部分群を含むので，τ が $(j\,i\,k)$ の形であったら $\tau^2=(i\,j\,k)$ に取り換えればよい．

みたす $w_{G,k}$ 個の X_i が属する G-軌道 $\mathrm{Orb}_G(X_i)$ にしか現れず，さらに，(イ) より各 $\mathrm{Orb}_G(X_i)$ には位数 p^k の部分群がちょうど 1 つ存在することがわかる．したがって，$w_{G,k}$ 個の軌道 $\mathrm{Orb}_G(X_i)$ に属する部分群を 1 つずつ取り出したものが，G の位数 p^k の部分群の総数となるので，前半の主張が従う．

p.311 下から 2 行目 まず，任意の $h \in H$ に対して $h \bullet_l H = h * H = H$ がなりたつ［⇨ **例題 10.13**］ので $h \in \mathrm{Stab}_G(H)$ であり，$H \subset \mathrm{Stab}_G(H)$ がなりたつ．逆に，$g \in \mathrm{Stab}_G(H)$ を任意にとると，固定部分群の定義より $g \bullet_l H = g * H = H$ がなりたつ．したがって，とくに $e_G \overset{\because\,(\mathrm{H1})}{\in} H$ に対して $g = g * e_G \in g * H = H$ となるため，$\mathrm{Stab}_G(H) \subseteq H$ もなりたつ．以上より，$\mathrm{Stab}_G(H) = H$ であることが家訓できた．

p.312 上から 5 行目 $\mathrm{Stab}_G(X_i) = X_i$ がなりたたないときは，$\mathrm{Stab}_G(X_i) \subsetneq X_i$ となるので，ラグランジュの定理［⇨ **定理 10.23**］より，$\mathrm{Stab}_G(X_i)$ は $\#X_i = p^k$ の真の約数となる．つまり，$\#\mathrm{Stab}_G(X_i) = p^l$ と表したときに，$1 \leq l \leq k-1$ がなりたつ．このとき，軌道・固定部分群定理［⇨ **定理 15.11**］より $\#\mathrm{Orb}_G(X_i) = (G : \mathrm{Stab}_G(X_i)) = \dfrac{mp^e}{p^l} = mp^{e-l}$ となるので，$e - l \geq e - k + 1$ より $p^{e-k+1} \mid \#\mathrm{Orb}_G(X_i)$ が従う．

p.314 上から 3 行目 実際，2 つのシロー p 部分群 $P_1, P_2 \in \mathrm{Syl}_p(G)$ に対し，シローの第 2 定理［⇨ **定理 18.12**］より $P_2 = g_0 * P_1 * g_0'$ をみたす $g_0 \in G$ が存在する．このとき $P_1 \to P_2\,;\, x \mapsto g_0 * x * g_0'$ および $P_2 \to P_1\,;\, y \mapsto g_0' * y * g_0$ は互いに他の逆写像であるような群準同型写像であるため，同型である．最後に，シローの第 1 定理［⇨ **定理 18.8**］より，G の位数 p^e の部分群 P_0 が存在し，G のシロー p 部分群となる［⇨ **注意 18.5**］ため，前半で確認したことによりすべてのシロー p 部分群の位数は p^e となる．

p.314 上から 11 行目 まず，$a_1 * Q_0 = a_2 * Q_0$ であるとき，$a_1 = a_2 * q$ $(q \in Q_0)$ と表せるので，任意の $h \in H$ に対して，

$$\begin{aligned} h \bullet_l (a_1 * Q_0) &\overset{\because\,\text{定義}}{=} (h * a_1) * Q_0 = (h * a_2 * q) * Q_0 \\ &= (h * a_2) * (q * Q_0) = (h * a_2) * Q_0 \overset{\because\,\text{定義}}{=} h \bullet_l (a_2 * Q_0) \end{aligned}$$

となる．つまり，$\bullet_l$ は左剰余類の代表元の取り方によらず矛盾なく定まっている．さらに，

$$e \bullet_l (a * Q_0) \overset{\because\,\text{定義}}{=} (e * a) * Q_0 = a * Q_0$$

より，(LA1) がなりたち，$h_1, h_2 \in H$ に対して，

$$(h_1 * h_2) \bullet_l (a * Q_0) \overset{\because\ \text{定義と}}{=} {}^{(\mathrm{G3})} (h_1 * (h_2 * a)) * Q_0$$
$$= h_1 \bullet_l ((h_2 * a) * Q_0) = h_1 \bullet_l (h_2 \bullet_l (a * Q_0))$$

より，(LA2) もなりたつので，$\bullet_l$ は H の G/Q_0 への左作用となる．

p.314 下から 5 行目　条件 $\#\mathrm{Orb}_H(g_0 * Q_0) = 1$ より，$\mathrm{Orb}_H(g_0 * Q_0) = \{g_0 * Q_0\}$ である．したがって，任意の $h \in H$ に対して，

$$h \bullet_l (g_0 * Q_0) = h * (g_0 * Q_0) \in \mathrm{Orb}_H(g_0 * Q_0) = \{g_0 * Q_0\}$$

より，$h * (g_0 * Q_0) = g_0 * Q_0$ がなりたつ．

p.315 上から 1 行目　実際，2 つの任意のシロー p 部分群 P_1, P_2 が Q_0 と共役であるならば，共役関係 $\sim_{\mathrm{c}}$ が同値関係だったこと［⇨【p.272 下から 7 行目】の ✍］[18]から，$P_1 \sim_{\mathrm{c}} Q_0 \sim_{\mathrm{c}} P_2$ と推移律 (E3) により，P_1 と P_2 が共役であることが従う．

p.316 上から 3 行目　$\#P = p^e$ $(e \in \mathbb{N})$ とおくと，$\#P \mid \#N_G(P)$ であったので $\#N_G(P) = m_0 p^e$ $(m_0 \in \mathbb{N})$ と表せる．さらに $(G : N_G(P)) = k_0$ $(k_0 \in \mathbb{N})$ とおくと，$\#G = (G : N_G(P))\#N_G(P) = k_0 m_0 p^e$ より $m = \#G/\#P = (k_0 m_0 p^e)/p^e = k_0 m_0$ となるので，確かに $(G : N_G(P)) = m_0$ は m の約数である．

p.316 上から 10 行目　$\#\mathrm{Syl}_p(G) \equiv 1 \pmod{p}$ より $\#\mathrm{Syl}_p(G) = 1 + kp$ $(k \in \mathbb{Z}_{\geq 0})$ と表せる（$\#\mathrm{Syl}_p(G) > 0$ に注意）．一方で $\#\mathrm{Syl}_p(G) \mid m$ より $\#\mathrm{Syl}_p(G) = 1 + kp \leq m$ がなりたつ．$k \geq 1$ と仮定すると $1 + kp \geq 1 + p \overset{\because\ \text{仮定}}{>} m$ となり矛盾するので，$k = 0$ でなければならず，したがって，$\#\mathrm{Syl}_p(G) = 1$ である．

§19 の ✍ のマーク

p.323 上から 2 行目　まず，$e_G^{*p_i^{f_i}} = e_G$ より $e_G \in G(p_i)$ であり，(H1) がなりたつ．続いて，任意の $a \in G(p_i)$ に対して $(a')^{*p_i^{f_i}} = \left(a^{*p_i^{f_i}}\right)' = e_G$ より，$a' \in G(p_i)$ であるから，(H2) もなりたつ．最後に，任意の $a, b \in G(p_i)$ に対して，

---

18) ここでは群の元に対する共役作用が同値関係であることを確認しているが，部分群の集合に対する共役作用が同値関係であることもまったく同様に確認できる．

$$(a*b)^{*p_i^{f_i}} \overset{(\mathrm{Ab})}{\overset{\because}{=}} a^{*p_i^{f_i}} * b^{p_i^{f_i}} = e_G * e_G = e_G \qquad \cdots (*)$$

より，$a*b \in G(p_i)$ であるから，(H3) もなりたつ．以上より，$G(p_i)$ が $(G,*)$ の部分群であることが確認できた．

※ $(*)$ 式の最初の等式は，**アーベル群でないとなりたたない**ことに注意（理由を考えてみよう）．

p.324 下から 5 行目 問 7.6 より従う．あるいは，$(x_0^{*p^{d-1}})^* p = x_0^{*p^d} = e_G$ より，$x_0^{*p^{d-1}}$ の位数は p の約数であり［⇨ **命題 7.25** (3)］，$x_0^{*p^{d-1}} \neq e_G$ であるので，$x_0^{*p^{d-1}}$ の位数は（1 ではなく）p となる．

p.325 下から 9 行目 $\tilde{y}^{*p} = y_0^{*p} * x^{*(-pk_0)} = x_0^{*k} * x_0^{*(-k)} = e_G$ より，$\tilde{y}$ の位数は p の約数であり［⇨ **命題 7.25** (3)］，さらに，$\tilde{y} * \langle x_0 \rangle = \overline{y} \neq e_{G/\langle x_0 \rangle}$ より $\tilde{y} \neq e_G$ なので，$\tilde{y}$ の位数は（1 ではなく）p となる．

p.326 上から 5 行目 $f\colon \langle e_G \rangle \times \langle e_G \rangle \to \langle e_G \rangle\,;(e_G, e_G) \mapsto e_G$ は自明な準同型写像［⇨ **例 8.8**］である．また，$\langle e_G \rangle \times \langle e_G \rangle$ および $\langle e_G \rangle$ はどちらも 1 つしか元をもたない集合であるため，f は全単射である．したがって，f は群同型写像であり，$\langle e_G \rangle \times \langle e_G \rangle \cong \langle e_G \rangle$ が従う．

p.326 下から 7 行目 $\overline{x}_0$ の位数を k_0 とすると $\overline{x}_0^{\overline{*}k_0} = e_{G/\langle y_0 \rangle}$ がなりたつ．このとき剰余群の演算の定義から $x_0^{*k_0} \in \langle y_0 \rangle$ がなりたつ．しかし，$\langle x_0 \rangle \langle y_0 \rangle = \{e_G\}$ であったから，$x_0^{*k_0} = e_G$ となるので k_0 は x_0 の位数 p^d の倍数である［⇨ **命題 7.25** (3)］．k_0 は $\overline{x}_0$ の位数であったから，p^d の正の倍数で最小のものである p^d となる．

p.327 上から 2 行目 まず，$(G,*)$ はアーベル群なので，その部分群 $\langle x_0 \rangle$ および K は G の正規部分群となる［⇨ **例 11.6**］．また，直積分解 $G/\langle y_0 \rangle \cong \langle \overline{x}_0 \rangle \times \overline{K}$ より，G の任意の元 $\overline{g}$ に対して，$\overline{g} = \overline{x}_0^{*a} \overline{*} \overline{k}$ をみたす $a \in \mathbb{Z}$ および $k \in K$ が存在する．とくに，$g' * x_0^{*a} * k \in \langle y_0 \rangle$ より，$g' * x_0^{*a} * k = y_0^{*b}$ をみたす $b \in \mathbb{Z}$ が存在し，$g = x_0^{*a} * (k * y_0^{*(-b)}) \in \langle x_0 \rangle * K$ がなりたつので，$G = \langle x_0 \rangle * K$ が従う（K の定義から K は $\langle y_0 \rangle$ を含むことに注意しよう）．最後に，任意の $h \in \langle x_0 \rangle \cap K$ に対し，その $G/\langle y_0 \rangle$ での像 $\overline{h}$ は $\langle \overline{x}_0 \rangle$ と $\overline{K}$ の共通部分の元となるが，$G/\langle y_0 \rangle \cong \langle \overline{x}_0 \rangle \times \overline{K}$ は直積分解であったため $\langle \overline{x}_0 \rangle \cap \overline{K} = \{e_{G/\langle y_0 \rangle}\}$ であり，したがって，$\overline{h} = e_{G/\langle y_0 \rangle}$ である．つまり，$h \in \langle y_0 \rangle$ であるが，構成から $\langle x_0 \rangle \cap \langle y_0 \rangle = \{e_G\}$ であったので $h = e_G$ となり，$\langle x_0 \rangle \cap K = \{e_G\}$ であることも確認できた．以上より，$\langle x_0 \rangle$

と K は命題 13.1 の仮定をすべてみたすので，直積分解 $G \cong \langle x_0 \rangle \times K$ を得る．

p.327 上から 3 行目　$f = 1$ のときは $(G, *)$ は巡回群なので［⇨ **系 10.25**］，(19.5) の同型 $(G, *) \xrightarrow{\sim} C_p$ が存在する．以下では $f > 1$ と仮定しよう．まず，G の元の中で位数が最大のもの x_0（位数を p^{a_1} とする）を 1 つ選ぶと，命題 19.10 より G の部分群 K で $\langle x_0 \rangle \times K \xrightarrow{\sim} G\,; (x_0^{*a}, k) \mapsto x_0^{*a} * k$ が同型写像となるものが存在する．ここで，K は位数が $p^{f-a_i}\ (< p^f)$ のアーベル p 群であるから [19]，帰納法の仮定により巡回群の直積 $C_{p^{a_2}} \times \cdots \times C_{p^{a_t}}$ と同型となる（$a_2, \ldots, a_t$ は $f - a_1$ の分割）．$\langle x_0 \rangle \cong C_{p^{a_1}}$ であったので，最終的に同型

$$(G, *) \xrightarrow{\sim} \langle x_0 \rangle \times K \xrightarrow{\sim} C_{p^{a_1}} \times C_{p^{a_2}} \times \cdots \times C_{p^{a_t}} \quad (a_1, a_2, \ldots, a_t \text{ は } f \text{ の分割})$$

が導かれた．

p.327 上から 9 行目　実際，$G(p_i)$ に定理 19.11 を適用して得られる同型

$$G(p_i) \xrightarrow{\sim} C_{p_i^{a_{i1}}} \times C_{p_i^{a_{i2}}} \times \cdots \times C_{p_i^{a_{it_i}}} = \prod_{j=1}^{t_i} C_{p_i^{a_{ij}}}$$

を命題 19.7 の同型

$$(G, *) \cong G(p_1) \times G(p_2) \times \cdots \times G(p_s) = \prod_{i=1}^{s} G(p_i)$$

の右辺に現れる各 $G(p_i)$ に適用したものが，定理 19.1 の同型 (19.2) に他ならない．

p.327 下から 6 行目　命題 19.7 の直積分解 (19.3) に現れる直積因子（シロー p_i 部分群）に，定理 19.11 と定理 19.12 を適用すればよい．

p.328 上から 6 行目　$g\colon \mathcal{X} \to \{f \text{ の分割}\}$ を

$$(b_1, b_2, \ldots, b_k) \mapsto (\underbrace{k, \ldots, k}_{b_k \text{個}}, \underbrace{k-1, \ldots, k-1}_{b_{k-1} \text{ 個}}, \ldots\ldots, \underbrace{2, \ldots, 2}_{b_2 \text{個}}, \underbrace{1, \ldots, 1}_{b_1 \text{個}})$$

と定めると [20]，g は f の逆写像となる．実際，f の分割 $\boldsymbol{a} = (a_1, a_2, \ldots, a_t)$ に対して，

---

[19] $a_1 = 0$ と仮定すると G の位数の最大値が 1 ということとなり，$G = \{e\}$（自明な群）となってしまい，$\#G > p$ と矛盾するため，$a_1 \geq 1$ である．

[20] 実際に $g((b_1, b_2, \ldots, b_k))$ が f の分割となることは，集合 $\mathcal{X}$ の定義でもある関係式 $kb_k + (k-1)b_{k-1} + \cdots + 2b_2 + 1b_1 = f$ から従う．

$$\begin{aligned} g \circ f(\boldsymbol{a}) &= g\big((\boldsymbol{a} \text{ の中の } 1 \text{ の個数}, \ldots, \boldsymbol{a} \text{ の中の } k \text{ の個数})\big) \\ &= (\underbrace{k, \ldots, k}_{\boldsymbol{a} \text{ の中の } k \text{ の個数}}, \ldots\ldots, \underbrace{1, \ldots, 1}_{\boldsymbol{a} \text{ の中の } 1 \text{ の個数}}) = \boldsymbol{a} \end{aligned}$$

がなりたち，$b_1 + 2b_2 + \cdots + kb_k = f$ をみたす $\boldsymbol{b} = (b_1, b_2, \ldots, b_k) \in \mathcal{X}$ に対して，

$$f \circ g(\boldsymbol{b}) = g\big((\underbrace{k, \ldots, k}_{b_k \text{ 個}}, \ldots\ldots, \underbrace{1, \ldots, 1}_{b_1 \text{ 個}})\big) = (b_1, b_2, \ldots, b_k) = \boldsymbol{b}$$

がなりたつので，確かに g は f の逆写像である．

§20 の ✍ のマーク

p.332 上から 4 行目　$H = \langle x \rangle \cap \langle t \rangle$ は G の部分群である［⇨ **問 7.4** (1)］．また，H は位数 5 の群 $\langle x \rangle$ の部分群であるため，ラグランジュの定理［⇨ **定理 10.23**］より $\#H \mid 5$ がなりたち，かつ H は位数 2 の群 $\langle t \rangle$ の部分群でもあるため，$\#H \mid 2$ もなりたつ．したがって，$\#H = 1$ となるので，$H = \langle x \rangle \cap \langle t \rangle = \{e_G\}$ がなりたつ．

p.332 上から 10 行目　$\langle x \rangle * \langle t \rangle$ は，$\langle x \rangle$ の 5 つの元と t を含むので，$\#\langle x \rangle * \langle t \rangle \geq 6$ がなりたつ．一方で，ラグランジュの定理［⇨ **定理 10.23**］より，$\#\langle x \rangle * \langle t \rangle \mid \#G = 10$ であるから，$\#\langle x \rangle * \langle t \rangle = 10$ がなりたたねばならない．したがって，$G = \langle x \rangle * \langle t \rangle$ がなりたつ．

p.333 上から 7 行目　(ア) のケースでは C_{10} はアーベル群なので，その（唯一の）位数 2 の部分群は正規部分群である［⇨ **例 11.6**］．(イ) のケースでは，1 つのシロー 2 部分群はそれぞれ $\langle t \rangle$, $\langle x * t \rangle$, $\langle x^{*2} * t \rangle$, $\langle x^{*3} * t \rangle$, $\langle x^{*4} * t \rangle$ である（ただし，例題 20.1 の解答の記号を用いた）．詳細は次の ✍ の解説にて．

p.333 上から 10 行目　2 面体群の基本関係式 $t * x * t = x'$ ［⇨ **補題 9.5** (2)］ より，

$$(x^{*i} * t)^{*2} = x^{*i} * \underbrace{t * x^{*i} * t}_{=(x')^{*i}} = x^{*i} * (x')^{*i} = e_G \qquad (i = 0, 1, 2, 3, 4)$$

であるから，$x^{*i} * t$ の位数は 2 である．シローの第 2 定理［⇨ **定理 18.12**］を直接適用すると，注意 20.2 にも書かれている通り，$\langle t \rangle$ の共役 $\langle x^k * t * x^{*(-k)} \rangle$ を計算することになるが，$x^{*k} * t * x^{*(-k)} = x^{*k} * \underbrace{(t * x^{*(-k)} * t)}_{=x^{*k}} * t = x^{*(2k)} * t$ より，計算結果は結局

上記の 5 つの部分群と一致する [21].

p.334 上から 7 行目　$(G,*)$ の中心 $Z(G)$ の任意の元 g は，G のすべての元と可換であるため，とくに $x \in G$ とも可換である（つまり，$g*x = x*g$ をみたす）．したがって，中心化群の定義より $g \in Z_G(x)$ なので，$Z(G) \subseteq Z_G(x)$ が従う．

p.335 上から 6 行目　共役により x_0 は位数 4 の元に移されるので［⇨ **問 16.4** (2)］，$y \odot_{\mathrm{c}} x_0$ は x_0 または x_0' に移される（e_G は位数 1，x_0^{*2} は位数 2 なので不適）．したがって，$\odot_{\mathrm{c}}$ は $\odot_{\mathrm{triv}}$ または $\odot_{\mathrm{inv}}$ と一致する．

p.335 上から 8 行目　$\overline{y}^{\overline{*}2} = e_{G/\langle x_0\rangle}$ より $y^{*2} \in \langle x_0\rangle$ がなりたつので，$y^{*2} = x_0^{*k}$ $(k = 0,1,2,3)$ と表される．ここで，y の位数は高々 4 であるので，y^{*2} の位数は高々 2 である．したがって，$y^{*2} = e_G$（位数 1）または $y^{*2} = x_0^{*2}$（位数 2）のいずれかがなりたつ．

p.335 上から 10 行目　$\langle x_0\rangle \cap \langle y\rangle \neq \{e\}$ とすると，$\langle y\rangle = \{e, y\}$ なので $\langle x_0\rangle \supset \langle y\rangle$ とならねばならないが，これは y の選び方 $(y \in G \smallsetminus \langle x_0\rangle)$ に反する．

p.335 下から 12 行目　$\overline{y} = y * \langle x_0\rangle$ が $G/\langle x_0\rangle$ を生成するので，任意の $g \in G$ に対して $g * \langle x_0\rangle = y^{*k} * \langle x_0\rangle$ をみたす整数 $k \in \mathbb{Z}$ が存在する．とくに，$g \in y^{*k} * \langle x_0\rangle$ であるから，整数 l が存在して $g = y^{*k} * x_0^{*l}$ と表される．とくに，$g \in \langle x_0, y\rangle$ である．

p.335 下から 9 行目　まず，アーベル群 C_8, $C_4 \times C_2$, $C_2 \times C_2 \times C_2$ がいずれも同型でないことは，有限アーベル群の構造定理における分解の一意性［⇨ **定理 19.1** (3)］の帰結である．また，D_8, Q_8 は非可換群であるので，どちらも C_8, $C_4 \times C_2$, $C_2 \times C_2 \times C_2 \times C_2$ とは同型でない．残った D_8 と Q_8 が同型でないことは問 9.7 から従う．

p.336 上から 6 行目　【p.332 上から 4 行目】の ✍ とほぼ同様．まず，$H = G(2) \cap G(3)$ は G の部分群である［⇨ **問 7.4** (1)］．また，H は位数 4 の群 $G(2)$ の部分群であるため，ラグランジュの定理［⇨ **定理 10.23**］より $\#H \mid 4$ がなりたち，かつ，H は位数 3 の群 $G(3)$ の部分群でもあるため $\#H \mid 3$ もなりたつ．したがって，$\#H = 1$ となるので，$H = G(2) \cap G(3) = \{e_G\}$ がなりたつ．

---

[21] $x^{*k} * t * (x')^{*k}$ の方が，位数が 2 であることは見やすい．実際，$(x^{*k} * t * (x')^{*k})^{*2}$ は $x^{*k} * t * \underbrace{(x')^{*k} * x^{*k}}_{=e_G} * t * (x')^{*k} = x^{*k} * \underbrace{t * t}_{=e_G} * (x')^{*k} = x^{*k} * (x')^{*k} = e_G$ と計算される．

p.336 下から 7 行目　$H \cap H'$ は G の部分群なので［⇨ **問 7.4** (1)］，単位元 e_G を含む (H1)．一方でラグランジュの定理［⇨ **定理 10.23**］ より $\#(H \cap H') \mid \#H = 3$ であるから $\#(H \cap H') = 1$ または 3 である．$H \cap H' = \{e_G\}$ のときは結論がなりたつので，$H \cap H' \neq \{e_G\}$，つまり，$H \cap H'$ が単位元以外の元をもつと仮定すると，$\#(H \cap H') \geq 2$ より $\#(H \cap H') = 3$ であるから，$H = H \cap H'$，つまり，$H \subseteq H'$ が導かれる．さらに，$\#H = \#H' = 3$ であることをあわせると，$H = H'$ がなりたつことが従う．

p.337 上から 8 行目　$\#\mathrm{Syl}_2(G) = \#\mathrm{Syl}_3(G) = 1$ のときは，$G(2)$ も $G(3)$ も $(G, *)$ の正規部分群であり［⇨ **系 18.15**］，$G(2) \cap G(3) = \{e\}$ かつ $G = G(2) * G(3)$ がなりたつので，命題 13.1 より G は直積分解 $G \cong G(2) \times G(3)$ をもつ．命題 20.4 より $G(2)$ はアーベル群であり，系 10.25 より $G(3)$ は巡回群であるので，それらの直積である G もアーベル群となる．

p.337 下から 10 行目　【p.335 上から 6 行目】の ✍ とほぼ同様である．共役により s は位数 3 の元にうつされるので［⇨ **問 16.4** (2)］，$t \odot s$ は s または s' にうつされる（e は位数 1 なので不適）．したがって，$\odot$ は $\odot_{\mathrm{triv}}$ または $\odot_{\mathrm{inv}}$ と一致する．

p.338 上から 3 行目　実際，$\phi_{x,y}((x^{*k}, y^{*l})) = (x^{*l}, y^{*k})$ $(k, l \in \mathbb{Z})$ で定義される写像 $\phi_{x,y}$ は，

$$\begin{aligned}
\phi_{x,y}((x^{*k_1}, y^{*l_1})(x^{*k_2}, y^{*l_2})) &= \phi_{x,y}((x^{*(k_1+k_2)}, y^{*(l_1+l_2)})) \\
&\overset{\text{定義}}{=} (x^{*(l_1+l_2)}, y^{*(k_1+k_2)}) \\
&= (x^{*l_1}, y^{*k_1})(x^{*l_2}, y^{*k_2}) \\
&\overset{\text{定義}}{=} \phi_{x,y}((x^{*k_1}, y^{*l_1}))\phi_{x,y}((x^{*k_2}, y^{*l_2}))
\end{aligned}$$

より，群準同型写像であり，$\phi_{x,y} \circ \phi_{x,y}((x^{*k}, y^{*l})) = \phi_{x,y}((x^{*l}, y^{*k})) = (x^{*k}, y^{*l})$ となることから全単射でもあるので（つまり，$\phi_{x,y}^{-1} = \phi_{x,y}$ である），$\phi_{x,y} \in \mathrm{Aut}(G(2))$ であり，$\phi_{x,y}((x, e)) = \phi_{x,y}((x^{*1}, y^{*0})) = (x^{*0}, y^{*1}) = (e, y)$ をみたす．

同様に，$\phi_{xy,y}((x^{*k}, y^{*l})) = (x^{*(k+l)}, y^{*l})$ $(k, l \in \mathbb{Z})$ で定義される写像 $\phi_{xy,y}$ は，

$$\begin{aligned}
\phi_{x,y}((x^{*k_1}, y^{*l_1})(x^{*k_2}, y^{*l_2})) &= \phi_{x,y}((x^{*(k_1+k_2)}, y^{*(l_1+l_2)})) \\
&\overset{\text{定義}}{=} (x^{*(k_1+k_2+l_1+l_2)}, y^{*(l_1+l_2)}) \\
&= (x^{*(k_1+l_1)}, y^{*l_1})(x^{*(k_2+l_2)}, y^{*l_2}) \\
&\overset{\text{定義}}{=} \phi_{xy,y}((x^{*k_1}, y^{*l_1}))\phi_{xy,y}((x^{*k_2}, y^{*l_2}))
\end{aligned}$$

より，群準同型写像であり，

$$\phi_{xy,y} \circ \phi_{xy,y}((x^{*k}, y^{*l})) = \phi_{xy,y}((x^{*k+l}, y^{*l})) = (x^{*(k+2l)}, y^{*l}) = (x^{*k}, y^{*l})$$

となることから全単射でもあるので（つまり，$\phi_{x,y}^{-1} = \phi_{x,y}$ である．x の位数が 2 であることに注意），$\phi_{xy,y} \in \mathrm{Aut}(G(2))$ であり，

$$\phi_{xy,y}((x,y)) = \phi_{x,y}((x^{*1}, y^{*1})) = (x^{*2}, y^{*1}) = (e, y)$$

をみたす．

$\boxed{\text{p.338 上から 7 行目}}$　写像（C_6 の生成元 t を s, x にうつす写像）

$$\Phi\colon C_6 \rtimes_{\odot_{\mathrm{inv}}} C_2 \to C_3 \rtimes_{\odot_{\mathrm{inv},y}} (C_2 \times C_2)\,;\, (t^a, y^b) \mapsto (s^a, (x^a, y^b))$$

は単射群準同型写像である．実際，

$$\begin{aligned}
&\Phi\big((t^{a_1}, y^{b_1}) \diamond_{\odot_{\mathrm{inv}}} (t^{a_2}, y^{b_2})\big) \overset{\text{◌}\ \diamond_{\odot_{\mathrm{inv}}}\ \text{定義}}{=} \Phi\big((t^{a_1}(y^{b_1} \odot_{\mathrm{inv}} t^{a_2}), y^{b_1+b_2})\big) \\
&= \Phi\big((t^{a_1+(-1)^{b_1}a_2}, y^{b_1+b_2})\big) \overset{\text{◌}\ \Phi\ \text{の定義}}{=} (s^{a_1+(-1)^{b_1}a_2}, (x^{a_1+(-1)^{b_1}a_2}, y^{b_1+b_2})) \\
&= (s^{a_1+(-1)^{b_1}a_1}, (x^{a_1+a_2}, y^{b_1+b_2}))\qquad (\text{◌}\ x\ \text{の位数は 2 なので}\ x' = x) \\
&\overset{\text{◌}\ \odot_{\mathrm{inv},y}\ \text{の定義}}{=} \big(s^{a_1}((x^{a_1}, y^{b_1}) \odot_{\mathrm{inv},y} s^{a_2}), y^{b_1}y^{b_2}\big) \\
&\overset{\text{◌}\ \diamond_{\odot_{\mathrm{inv},y}}\ \text{の定義}}{=} (s^{a_1}, (a^{a_1}, y^{b_1})) \diamond_{\odot_{\mathrm{inv},y}} (s^{a_2}, (x^{a_2}, y^{b_2})) \\
&\overset{\text{◌}\ \Phi\ \text{の定義}}{=} \Phi\big((t^{a_1}, y^{b_1})\big) \diamond_{\odot_{\mathrm{inv},y}} \Phi\big((t^{a_2}, y^{b_2})\big)
\end{aligned}$$

より，Φ は群準同型写像であり，また，$\Phi\big((t^a, y^b)\big) = (s^a, (x^a, y^b)) = (e, (e, e))$ がなりたつのは $3 \mid a$ かつ $2 \mid a$ かつ $2 \mid b$ がなりたつとき，すなわち，$6 \mid a$ かつ $2 \mid b$ がなりたつときのみで，このとき $(t^a, y^b) = (e, e)$ であるから，$\mathrm{Ker}\,\Phi = \{(e, e)\}$ より Φ は単射である．$C_3 \rtimes_{\odot_{\mathrm{inv},y}} (C_2 \times C_2)$ は位数が高々 12 であり，Φ の単射性より

$$\#\mathrm{Im}\,\Phi = \#D_{12} = 12 \leq \#C_3 \rtimes_{\odot_{\mathrm{inv},y}} (C_2 \times C_2)$$

がなりたつので，$\#C_3 \rtimes_{\odot_{\mathrm{inv},y}} (C_2 \times C_2) = \#\mathrm{Im}\,\Phi = 12$ がなりたち，Φ が同型写像であることが従う．

$\boxed{\text{p.338 下から 11 行目}}$　共役により t は位数 4 の元に移されるので［⇨ **問 16.4** (2)］，$s \odot t$ は t または t' しかし，$s \odot t = t'$ であるとすると，

$$t \overset{\text{(LA1)}}{\overset{\circlearrowleft}{=}} e \odot t = s^3 \odot e \overset{\text{(LA2)}}{\overset{\circlearrowleft}{=}} s \odot (s \odot (s \odot t)) = s \odot (s \odot t') = s \odot t = t'$$

となり，$t' = t^2 \neq t$ と矛盾するので，$\odot$ として考えられるものは $\odot_{\mathrm{triv}}$ のみとなる．

p.338 下から 4 行目　シローの第 3 定理［⇨ **定理 18.16**］より，

$$\#\mathrm{Syl}_3(\mathrm{GL}_2(\mathbb{F}_2)) \equiv 1 \pmod 3 \quad \text{かつ} \quad \#\mathrm{Syl}_3(\mathrm{GL}_2(\mathbb{F}_2)) \mid 2$$

がなりたつが，これらをみたすのは $\#\mathrm{Syl}_3(\mathrm{GL}_2(\mathbb{F}_3)) = 1$ のみである．

p.339 上から 1 行目　クラインの 4 元群 $\mathfrak{V}_4$ は $\mathfrak{S}_4$ の正規部分群であり［⇨ **問 11.6** (3)］，$\mathfrak{V}_4 \cap \langle (1\,2\,3) \rangle = 1$ がなりたつ [22]．さらに，$(1\,2\,3)$ は剰余群 $\mathfrak{S}_4/\mathfrak{S}_3 \cong C_3$ の生成元となることから，$\mathfrak{S}_4 = \mathfrak{V}_4 * \langle (1\,2\,3) \rangle$ であることもわかり，したがって，命題 14.25 より，半直積分解 $\mathfrak{S}_4 \cong \mathfrak{V}_4 \rtimes_{\odot} \langle (1\,2\,3) \rangle$ を得る．

p.339 下から 1 行目　$C_2 = \langle t \rangle$, $D_{12} = \langle r, s \rangle$ と表記することにすると，写像

$$\Psi\colon D_{12} \to \mathfrak{S}_3 \times C_2\,;\, r^a s^b \mapsto \bigl((1\,2\,3)^a (1\,2)^b, t^a\bigr)$$

が求める群同型写像となる．実際，

$$\begin{aligned}
\Psi\bigl((r^{a_1} s^{b_1})(r^{a_2} s^{b_2})\bigr) &\overset{\circlearrowleft\ srs=r'}{=} \Psi(r^{a_1+(-1)^{b_1} a_2} s^{b_1+b_2}) \\
&\overset{\circlearrowleft\ \Psi\text{の定義}}{=} \bigl((1\,2\,3)^{a_1+(-1)^{b_1} a_2} (1\,2)^{b_1+b_2}, t^{a_1+(-1)^{b_1} a_2}\bigr) \\
&= \bigl((1\,2\,3)^{a_1} (1\,2)^{b_1} (1\,2\,3)^{a_2} (1\,2)^{b_1}, t^{a_1+(-1)^{b_1} a_2}\bigr) \quad (\circlearrowleft\ (1\,2)(1\,2\,3)(1\,2) = (1\,2\,3)^{-1}) \\
&= \bigl((1\,2\,3)^{a_1} (1\,2)^{b_1} (1\,2\,3)^{a_2} (1\,2)^{b_1}, t^{a_1+a_2}\bigr) \quad (\circlearrowleft\ t\ \text{の位数は 2 なので}\ t^{-1} = t) \\
&\overset{\circlearrowleft\ \text{直積の演算の定義}}{=} \bigl((1\,2\,3)^{a_1} (1\,2)^{b_1}, t^{a_1}\bigr)\bigl((1\,2\,3)^{a_2} (1\,2)^{b_2}, t^{a_2}\bigr) \\
&\overset{\circlearrowleft\ \Psi\text{の定義}}{=} \Psi\bigl(r^{a_1} t^{b_1}\bigr)\Psi\bigl(r^{a_2} s^{b_2}\bigr)
\end{aligned}$$

より，Ψ は群準同型写像であり，$\Psi\bigl(r^a s^b\bigr) = \bigl((1\,2\,3)^a (1\,2)^b, t^a\bigr) = (e, e)$ がなりたつのは $6 \mid a$, $2 \mid b$ がなりたつときで，このとき $r^a s^b = e$ である．したがって，$\mathrm{Ker}\,\Psi = \{e\}$ であり，Ψ は単射である．このことと，$\#D_{12} = \#(\mathfrak{S}_3 \times C_2) = 12$ から，Ψ が同型写像であることが示された．

---

22) $H = \mathfrak{V}_4 \cap \langle (1\,2\,3) \rangle$ は，位数 4 の群 $\mathfrak{V}_4$ と位数 3 の群 $\langle (1\,2\,3) \rangle$ の部分群であるため，ラグランジュの定理［⇨ **定理 10.23**］より $\#H$ は 4 と 3 の公約数 1 となる

※ $\mathfrak{S}_3$ の半直積分解 $\mathfrak{S}_3 \cong \langle(1\,2\,3)\rangle \rtimes_{\mathrm{c}} \langle(1\,2)\rangle$ ［⇨ **例 14.26**］に着目すると，上記の議論が【p.338 上から 7 行目】の ✍ の議論と極めて似通っていることにも納得しやすいだろう．

p.340 上から 9 行目　一般に巡回群は，その位数の約数を位数にもつ部分群を唯一つもつ［⇨ **命題 7.30** (2)］．したがって，位数が素数 p の巡回群 C_p は，位数 1 の部分群 $\{e\}$ と位数 p の部分群 C_p 以外に部分群をもたないため，単純群である．

p.340 下から 9 行目　対称群の共役類は巡回置換型で分類されるので［⇨ **命題 16.15**］，巡回置換型をすべて求めればよい．そのためには 5 の分割を数えればよいが，

$$5 = 4+1 = 3+2 = 3+1+1 = 2+1+1+1 = 1+1+1+1+1$$

の 5 個の分割があるので，対応して巡回置換型（共役類）が 5 つ存在する．

p.341 上から 10 行目　$\iota(\sigma)(k) = \begin{cases} \sigma(k) & 1 \le k \le n \text{ のとき} \\ n+1 & k = n+1 \text{ のとき} \end{cases}$ より，さらに τ を作用させると $\big(\iota(\tau)\iota(\sigma)\big)(k) = \begin{cases} \tau\sigma(k) & 1 \le k \le n \text{ のとき} \\ n+1 & k = n+1 \text{ のとき} \end{cases}$ となるが，これは $\iota(\tau\sigma)(k)$ とまったく変わらない．したがって，$\iota(\tau\sigma) = \iota(\tau)\iota(\sigma)$ がなりたつので ι は群準同型写像である．また，$\iota(\sigma) = e$ となるのは，すべての $1 \le k \le n$ に対して $\sigma(k) = k$ がなりたつときのみであるが，これは $\sigma = e$ であることを表している．したがって，ι は単射な群準同型写像である．

p.341 下から 6 行目　実際，置換 $(i\,j\,k)(j\,k\,l)$ は i, j, k, l と関係しない数字はまったく動かさず，i を j に，j を（k にうつしたのちに）i に，k を l に，l を（j にうつしたのちに）k にうつすので，結局，$(i\,j)(k\,l)$ と一致する．

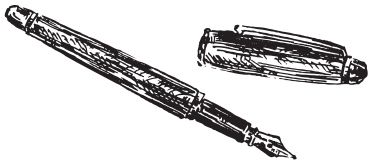
p.342 上から 7 行目　$n+1$ は l, x, y のいずれとも異なるので $\tau(n+1) = \sigma(n+1) = k$ がなりたつ．また，

$$\begin{aligned} \tau(l) &= (l\,x\,\big(\sigma^{-1}(l)\big)\sigma(l\,x\,\sigma^{-1}(l))^{-1}\big)(l) \\ &= \big((l\,x\,\sigma(l)^{-1}(l))\sigma\big)(\sigma^{-1}(l)) = (l\,x\,\sigma^{-1}(l))(l) = x \end{aligned}$$

である．x は $\{1, 2, \ldots, n+1\} \smallsetminus \{k, n+1, l, \sigma^{-1}(l)\}$ から選んでいたので，$\tau(l) = x \neq l$ がなりたつ．

p.342 下から 2 行目　$\mathfrak{S}_3/H$ は位数 2 の巡回群（とくに，アーベル群となる）ので，アーベル化の普遍性［⇨ **命題 13.8** (1)］ より $[\mathfrak{S}_n, \mathfrak{S}_n] \subset H$ を得る．

p.342 脚注 6)　$[\mathfrak{S}_4, \mathfrak{S}_4] = \mathfrak{V}_4$ であると仮定すると，$\mathfrak{S}_4/[\mathfrak{S}_4, \mathfrak{S}_4] = \mathfrak{S}_4/\mathfrak{V}_4 \cong \mathfrak{S}_3$ となり［⇨ **問 11.6** (5)］，商が非可換群となってしまうため矛盾する．



（お疲れさまでした）【終】