松坂「代数系入門」

2023 年 3 月 2 日

主に問題の解答．価値があると思った補足も少し．

1　整数

2　群

2.1　写像

略．

2.2　群とその例

2. まず右逆元も存在して，それが左逆元と一致することを示す．$ba = e$，$cb = e$ とすると，
$$ab = eab = cbab = ceb = cb = e$$
従って
$$\forall a \in G, \exists b \in G, ab = ba = e$$
がわかる．次に左単位元が右単位元でもあることを示す．
$$ae = aba = ea = a$$
これで単位元，逆元の存在が言えたので G は群である．
3. まず単位元の存在を示す．ある元 $a_0 \in G$ について，$a_0 x = a_0$ とする．このとき $\forall a \in G$ について，
$$\exists v \in G, a = va_0 = va_0 x = ax$$
がわかる．$ya_0 = a_0$ についても同様で，これより
$$\forall a \in G, a = ax = ya$$
特に $a = x, y$ としたときに $x = y$ がわかる．これは単位元なので e と表す．次に逆元の存在を示す．
$$\exists x, y \in G, ax = ya = e$$
より，
$$y = ye = yax = ex = x$$
従って逆元が一意に定まる．これより G は群である．
4. $a \in G$ を固定して得られる G から G への写像 $x \mapsto ax$，$x \mapsto xa$ は条件より単射である．G は有限集合なのでこれらは全射でもある．従って，前問の結果より G は群である．

5. a を固定して得られる写像は単射だが，G が無限集合の場合全射とは限らなくなる．例えば $\mathbb{Z}$ に乗法を与えたものがある (この場合逆元が存在しないことがある)．
6. $o(G) = n$ とすると，$\{e, a, a^2, \cdots a^n\}$ の各要素はいずれも G の元だが，どこかに被りがある．$a^k = a^l (k < l)$ とすると，$a^{l-k} = e$．したがってある $m \in \mathbb{N}$ で $a^m = e$ が成り立つ．
7. $a = a^{-1}$ より，$ab = a^{-1}b^{-1} = (ba)^{-1} = ba$.
8. (a) は $abab = a^2b^2$ より $ba = ab$．(b) は
$$\begin{aligned}(ab)^{n+2} &= a^{n+2}b^{n+2}\\ a(ba)^{n+1}b &= a(a^{n+1}b^{n+1})b\\ (ba)^{n+1} &= a^{n+1}b^{n+1} = (ab)^{n+1} = (ab)^n ab\end{aligned}$$
ここで左辺は
$$(ba)^{n+1} = a^{-1}abab\cdots aba = a^{-1}(ab)^{n+1}a = a^n b^{n+1}a = (ab)^n ba$$
より，
$$(ab)^n ab = (ab)^n ba \quad \therefore ab = ba$$
9. 明らかに $\triangle$ は可換で，結合的．空集合 $\emptyset$ が単位元，逆元は A 自身として，$P(S)$ は可換群をなす．

2.3 部分群と生成系

1. 明らか．
2. m と n の最小公倍数を l として $l\mathbb{Z}$.
3. ある $a \in H \subset G$ を固定すれば，$H \to H$ の写像 $x \mapsto ax$ は全単射．簡約律が成り立つことと単射であることは同値なので，2 節問題 4 の結果が使えて，$H < G$ が成り立つ．
4. 置換であること ($\mathbb{R} \to \mathbb{R}$ の全単射であること) は明らか．この形の置換全体は $S(X)$ の部分群をなすことは，
$$\sigma_{a,b}(\sigma_{a',b'}(x)) = a(a'x + b') + b = aa'x + (ab' + b)$$
と，単位元が $\sigma_{1,0}$，$\sigma_{a,b}$ の逆元が $\sigma_{1/a,-b/a}$ で与えられることからわかる．
5. G が有限群だから，$\forall x \in S$ について，ある $n \in \mathbb{N}$ で $x^n = e, x^{n-1} = x^{-1}$ となる．したがって S^{-1} の任意の元は S の元の有限個の積で表されるから，S によって生成される G も S の元の有限個の積で表される．
6. S^{-1} の元と S'^{-1} の元も可換であるから，$S \cup S^{-1}$ の元の積で表される H と $S' \cup S'^{-1}$ の元の積で表される H' の任意の元も可換である．
7. 明らか．
8. 2 次元平面上で，x 軸と y 軸に関する鏡映操作
$$\sigma = \begin{bmatrix}-1 & 0\\ 0 & 1\end{bmatrix}, \quad \tau = \begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}, \quad e = \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$$
は条件を満たす．このとき自明でない部分群は
$$\{e, \sigma\}, \{e, \tau\}, \{e, \sigma\tau\}$$
9. σ を正 n 角形の $2\pi/n$ 回転，τ をある対称軸に関する鏡映操作とすると，これは条件を満たす．別の対称軸に関する鏡映操作 τ' は，図形的な考察により $\tau' = \sigma^{2m}\tau$ のように表せる．したがってこの正 n 角

形のシンメトリー全体からなる群は σ と τ により生成され，すべての元は $\sigma^i\tau^j$ と表される．

$$\sigma = R(2\pi/n), \quad \tau = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

と行列で表すとわかりやすい．

10. $o(D_4) = 8$ だから，真部分群の位数の候補は 2,4．位数が 2 の部分群は $\{e, \tau\}$，$\{e, \sigma^2\}$，$\{e, \sigma\tau\}$，$\{e, \sigma^2\tau\}$，$\{e, \sigma^3\tau\}$．位数が 4 の部分群は $\{e, \sigma, \sigma^2, \sigma^3\}$，$\{e, \tau, \sigma^2, \sigma^2\tau\}$，$\{e, \sigma\tau, \sigma^2, \sigma^3\tau\}$．
11. #(大変そうなため)
12. 四元数．

$$i = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, \quad j = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \quad k = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}, \quad e = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad m = -e$$

とすれば，与えられた関係式を全て満たす．このとき

$$ji = -k, \quad kj = -i, \quad ik = -j$$

である．e, m は全ての元と可換なので，e, m をそれぞれ $1, -1$ で表すと，i, j, k の逆元は $-i, -j, -k$ になる．真部分群は $\{\pm 1\}$，$\{\pm 1, \pm i\}$，$\{\pm 1, \pm j\}$，$\{\pm 1, \pm k\}$．

2.4 剰余類分解

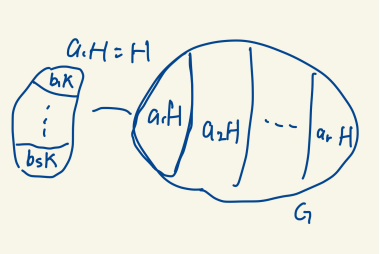
1. $Q_l \to Q_r$ の写像 $aH \mapsto Ha^{-1}$ の well-defined 性を確認する．

$$aH = bH \Leftrightarrow \forall h \in H, \exists h' \in H, ah = bh' \Leftrightarrow \forall h \in H, \exists h' \in H, ha^{-1} = h'b^{-1} \Leftrightarrow Ha^{-1} = Hb^{-1}$$

全単射であることは明らか．

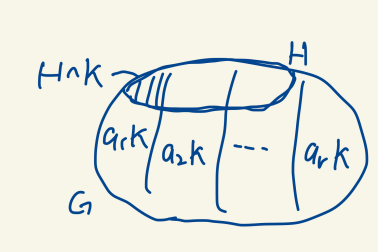
2. G の H に関する左剰余類を $\{a_1H, \cdots, a_rH\}$，H の K に関する左剰余類を $\{b_1K, \cdots, b_sK\}$ とする．このとき任意の $x \in G$ は，まずある $a_i (i = 1, \cdots, r)$ と $h \in H$ によって $x = a_ih$ と書かれる．次に h はある $b_j (j = 1, \cdots, s)$ と $k \in K$ によって $h = b_jk$ と書かれる．従って $x = a_ib_jk$．これより G の K に関する左剰余類は $\{a_ib_jK\} (1 \le i \le r, 1 \le j \le s)$ である．

図 1　2-4-2



3. 任意の $a, b \in H$ について，$a^{-1}b \in H \cap K \subset K$ より，$a \equiv b (\mathrm{mod}\ H \cap K) \Rightarrow a \equiv b (\mathrm{mod}\ K)$．#また，$a \not\equiv b (\mathrm{mod}\ H \cap K)$ のとき $a^{-1}b \notin H \cap K$ だが，$a, b \in H$ なので，$a^{-1}b \notin K$，つまり $a \not\equiv b (\mathrm{mod}\ K)$．従って H の $H \cap K$ による異なる剰余類は必ず G の K による異なる剰余類の中に含まれるから，$(H : H \cap K) \le (G : K)$．
4. 2，3 問で得られた結果を用いていく．$H^{(n)} = H_1 \cap \cdots \cap H_n$ とすると，$(G : H^{(n)}) = (G : H_n)(H_n : H^{(n)}) \le (G : H_n)(G : H^{(n-1)})$．これを繰り返し適用すれば得られる．

図 2　2-4-3



2.5　正規部分群と商群

1. 明らか.
2. HK の任意の元は $hk(h \in H, k \in K)$ と表されるが，これの逆元は $k^{-1}h^{-1} \in KH$ である．したがって，HK が部分群になることの必要十分条件は $HK = KH$ になることである.
3. #
4. 前問を使えばすぐわかる.
5. aHa^{-1} の任意の元は $\sigma_a(x)$(共役) の形に表される．したがって $\sigma_a(x)\sigma_a(y) = \sigma_a(xy) \in aHa^{-1}$, $\sigma_a(e) = e$，$\sigma_a(x)^{-1} = \sigma_a(x^{-1})$ より aHa^{-1} は部分群.
6. N が正規だから $HN = NH$ である．したがって問題 2 から $HN < G$．また $\sigma_a(hn) = \sigma_a(h)\sigma_a(n)$ だから，H が正規ならば HN も正規になる.
7. 明らか.
8. 左剰余類と右剰余類の数はどちらも 2 で，そのうちの一つは N なので，任意の $a \notin N$ をとれば $aN = Na \neq N$．したがって N は正規.
9. 任意の $x \in N$ について，$a \sim a$ を $e \sim x$ の左辺からかけて $a \sim ax$．$a^{-1} \sim a^{-1}$ を右辺からかけて $e \sim axa^{-1}$ より，$axa^{-1} \in N$．したがって N は正規．このとき $a \sim b \Leftrightarrow a^{-1}b \sim e \Leftrightarrow a^{-1}b \in N$ より，$a \sim b \Leftrightarrow a \equiv b (\mathrm{mod}\ N)$.
10. 四元数群がその例.
11. $a, b \notin H$ をとる．$(aH)(bH) = cH$ とすると，任意の $h, h' \in H$ についてある $h'' \in H$ が存在し，$ahbh' = ch''$．ここで $h = h' = e$ ととると $ab = ch''$ より $c^{-1}ab \in H$．つまり $ab \equiv c (\mathrm{mod}\ H)$ なので，$(aH)(bH) = abH$．したがって $ahbh' = abh''$ で，これを整理すると，任意の $h \in H$ について $hb = bh'$ をみたす $h' \in H$ が存在することがわかる．つまり $bH = Hb$．これより H は正規である.
14. 任意の $x \in N_1, y \in N_2$ の交換子は，$[x, y] = xyx^{-1}y^{-1} = (xyx^{-1})y^{-1} = x(yx^{-1}y^{-1})$ より，$[x, y] \in N_1 \cap N_2 = \{e\}$．したがって $xy = yx$.

2.6　準同型写像

1. 全射であることに注意するとできる.
2. 単位元が $\sigma_{1,0}$，$\sigma_{a,b}\sigma_{c,d} = \sigma_{ac,ad+b}$ より，$\sigma_{a,b}^{-1} = \sigma_{1/a,-b/a}$ であることに注意すると確認できる.
3. $f : \mathbb{C}^* \to \mathbb{T}$ を $z \mapsto z/|z|$ で定義すると，全射準同型になっている．$\mathrm{Ker}\ f = \mathbb{R}^+$ だから，準同型定理より $\mathbb{C}^*/\mathbb{R}^+ \simeq \mathbb{T}$.

4. $f : X \to X'$(全単射) として，$\phi : S(X) \to S(X')$ を $\varphi \mapsto f \circ \varphi \circ f^{-1}$ で定義する．これは同型写像.
5. #
6. #$g : G/N \to G'$ を $aN \mapsto f(a)$ と定義する．$aN = bN \Leftrightarrow a^{-1}b \in N \Rightarrow a^{-1}b \in N_0 \Leftrightarrow a \equiv b (\mathrm{mod}\ N_0) \Rightarrow g(a) = g(b)$ より，well-defined である．準同型になっていることもすぐ確かめられる．これより $f = g \circ \varphi$ なる g が存在する．一意性は，$g' : G/N \to G'$ で，ある $aN \in G/N$ について $g(aN) \neq g'(aN)$ とすると，$g \circ \varphi(a) \neq f(a)$ となって矛盾．したがって $g = g'$.
7 まず G' が可換群だから $f(aba^{-1}b^{-1}) = f(a)f(b)f(a^{-1})f(b^{-1}) = e'$ である．つまり $D \subset \mathrm{Ker}\ f$．したがって前問より $f = g \circ \varphi$ なる準同型 g が一意的に存在する.
8.

2.7 自己同型写像，共役類

1. 任意の $x, y \in G$ について $(xy)^{-1} = x^{-1}y^{-1} = (yx)^{-1}$ より，G は可換.
2. $\sigma_a\sigma_b = \sigma_{ab}$，単位元は σ_e，σ_a の逆元は $\sigma_{a^{-1}}$ で部分群になる．任意の $f \in \mathrm{Aut}(G)$ について $f\sigma_a f^{-1}(x) = f(af^{-1}(x)a^{-1}) = f(a)xf(a)^{-1} = \sigma_{f(a)}(x)$ より正規.
3. 内部自己同型群を H として $\varphi : G \to H$ を $a \mapsto \sigma_a$ とすると，これは準同型．$\sigma_a = I_G \Leftrightarrow \forall x \in G, \sigma_a(x) = axa^{-1} = x$ より $ax = xa$．つまり $a \in Z$．したがって $\mathrm{Ker}\ \varphi = Z$ で，準同型定理より $G/Z \simeq H$.
4. $f \in \mathrm{Aut}(\mathbb{Z})$ は $f(n) = nf(1)$ をみたす．$f(1) = m$ とすると $f(n) = mn$．これが全単射になるには $m = \pm 1$ でなければならない．したがって $\mathrm{Aut}(\mathbb{Z}) = \{I_{\mathbb{Z}}, -I_{\mathbb{Z}}\}$.
5. $f \in \mathrm{Aut}(\mathbb{Q})$ は $a, b \in \mathbb{Z}$ について $f(a/b) = af(1/b)$ をみたすから，任意の $n \in \mathbb{Z}$ について $f(1/n)$ を求めればよい．$f(1 + 1/n) = f(1) + f(1/n) = (n+1)f(1/n)$ より，$f(1/n) = f(1)/n$．したがって $f(1) = \alpha$ とすれば $f(1/n) = \alpha/n$ と表される．これより $\mathrm{Aut}(\mathbb{Q}) = \{(x \mapsto \alpha x) | \alpha \in \mathbb{Q}\}$.
6. $aSa^{-1} = bSb^{-1} \Leftrightarrow Sa^{-1}b = a^{-1}bS \Leftrightarrow a^{-1}b \in N(S) \Leftrightarrow a \equiv b (\mathrm{mod}\ N(S))$．最後は左合同．したがって S に共役な G の異なる部分集合の個数は $(G : N(S))$.
7. H の共役部分群は位数が $o(H)$ と変わらないから，仮定より任意の $a \in G$ について $\sigma_a(H) = H$．したがって H は正規.
8. 任意の $x, y \in N$ は任意の $a \in G$ とある $h, h' \in H$ によって $x = \sigma_a(h), y = \sigma_a(h')$ と表されるから，$xy = \sigma_a(h)\sigma_a(h') = \sigma_a(hh')$．当然 $e \in N$ かつ任意の $a, b \in G$ について $\sigma_a(h) = \sigma_b(h') \Leftrightarrow \sigma_a(h^{-1}) = \sigma_b(h'^{-1})$ より，$\sigma_a(h) \in N \Leftrightarrow \sigma_a(h)^{-1} = \sigma_a(h^{-1}) \in N$．これで N は部分群．次に N が正規であることは，$N = \bigcap_{a \in G} \sigma_a(H)$ から $\sigma_b(N) = \bigcap_{a \in G} \sigma_{ba}(H)$ となるが，ba は a が動けば G 全体を尽くすから，$\sigma_b(N) = N$ より示される．H に含まれる任意の G の正規部分群を S とすると $S = \bigcap_{a \in G} \sigma_a(S)$ で，各 $a \in G$ について $\sigma_a(S) \subset \sigma_a(H)$ だから $S \subset N$.

2.8 巡回群

1. a を生成元とすると $f(a^k) = f(a)^k$ より準同型像は $f(a)$ を生成元とする巡回群.
2. $a^{n/d}$ を生成元とする巡回群.
3. $(k, n) = d$，$m = n/d$ とすると mk は n の倍数になるから，$a^{mk} = e$ より a^k によって生成される部分

群の位数は m になる．したがって a^k が G の生成元になるのは $m = n$，つまり $(k, n) = 1$ のときで，その逆も然り．

4. $a = e$ または $b = e$ のときや，$a = b$ のときは明らかなので，$a \neq b, a \neq e, b \neq e$ を考える．$o(ab) = n$ とすると，$(ab)^n = e$．$(ba)^n = a^{-1}(ab)^{n+1}b^{-1} = a^{-1}abb^{-1} = e$ より，$o(ba) \leq n$．ここで $(ab)^m \neq e (1 \leq m \leq n-1)$ より，$(ba)^m = a^{-1}(ab)^{m+1}b^{-1} = e$ とすると $(ab)^{m+1} = ab$，つまり $(ab)^m = e$ となって矛盾．したがって $o(ba) = o(ab)$.
5. k, l を自然数とし，$a^k = b^l$ とすると，$e = a^{mk} = b^{ml}$ だが，$n|ml$ となるので，$(m, n) = 1$ より $n|l$．このとき $b^l = e$ だから $a^k = e$．つまり $n|k$．これより $a^k = b^l$ をみたす最小の k, l は n, m．したがって $(ab)^k = a^k b^k = e$ をみたす k は $a^k = b^k = e$ をみたし，このうち最小なものは mn となる．
6.
7. 部分群の位数は 1 か p なので真部分群は持たない．したがって G はある $a \in G$ によって生成される群そのもので，それは a の巡回群である．
8. 可換群の部分群は常に正規なので，ここでは単純群を真部分群を持たない群とする．このとき任意の $a \in G (a \neq e)$ は G の生成元になるので，G は巡回群．一つ $a \in G$ を固定して $o(G) = n$ とすると，どの $k = 1, 2, \cdots, n-1$ についても a^k が G の生成元になる必要があるが，これは問題 3 より $(k, n) = 1$ と同値である．したがって n は素数.
9.

2.9 置換群

1. S_3 の部分群は $\{e\}, \{e, (1\ 2)\}, \{e, (1\ 3)\}, \{e, (2\ 3)\}, \{e, (1\ 2\ 3), (1\ 3\ 2)\}, S_3$ の 6 つで，このうち正規なのは $\{e\}, \{e, (1\ 2\ 3), (1\ 3\ 2)\}, S_3$ である．(一般論として $(G : H) = 2$ ならば H は正規)
2. (a)r．(b)$\sigma = (i_1\ i_r)(i_1\ i_{r-1}) \cdots (i_1\ i_2)$ より，$\varepsilon(\sigma) = (-1)^{r-1}$.
3. (a)$r_1, \cdots, r_k$ の最小公倍数．(b)$(-1)^{r_1 + \cdots + r_k - k}$.
4.
5.(a) $(1\ 3\ 6\ 7\ 2)(4\ 5)$.
5.(b) $(1\ 3\ 5\ 6)(2\ 4)$.
6.(a,b) $[1,1,1,1] : e$．$[2,1,1] : (1\ 2), (1\ 3), (1\ 4), (2\ 3), (2\ 4), (3\ 4)$．$[2,2] : (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)$.
$[3,1] : (1\ 2\ 3), (1\ 3\ 2), (1\ 2\ 4), (1\ 4\ 2), (1\ 3\ 4), (1\ 4\ 3), (2\ 3\ 4), (2\ 4\ 3)$.
$[4] : (1\ 2\ 3\ 4), (1\ 2\ 4\ 3), (1\ 3\ 2\ 4), (1\ 3\ 4\ 2), (1\ 4\ 2\ 3), (1\ 4\ 3\ 2)$.
6.(c) $o(S_4) = 24$ より，部分群の位数としてあり得るのは 24 の約数のうち，共役類の元の数 $1, 6, 3, 8, 6$ をたかだか一つずつ使う和で表現できるもの．これに従って確かめると，$\{e\}, \{e, [2,2]\}, A_4 = \{e, [2,2], [3,1]\}, S_4$ が正規.

2.10 置換表現，群の集合への作用

1. $(ab) \cdot Hx = Hxb^{-1}a^{-1} = a \cdot (b \cdot H)$，$e \cdot Hx = Hx$ より.
2. $aH \mapsto Ha^{-1}$ は G 同型写像で，G の G/H における表現と $G\backslash H$ における表現は同値になる (well-defined 性などを確認すること).

3. #定理 16 を使う．$aH \in G/H$ の安定部分群は $\{x \in G | xaH = aH\}$ で $xaH = aH \Leftrightarrow x \in aHa^{-1}$．したがって $K = aHa^{-1}$ と表されるならば (つまり H, K が共役ならば) 定理 16 より G/H と G/K における表現は同値になる．逆は難しい．G 同型写像を φ として，$\varphi(K) = aH$ とする．このとき $\varphi(xK) = xaH$ で，$x \in K$ のときに限り $\varphi(xK) = \varphi(K) = aH$．したがって $x \in K \Leftrightarrow aH = xaH \Leftrightarrow x \in aHa^{-1}$ より，$K = aHa^{-1}$．
4. X を推移的 G 集合とする．ある $x \in X$ についての安定部分群を H とする．このとき X と G/H における表現は同値．X における表現が忠実なので，G/H における表現も忠実．これは定理 17 の系により H が単位群以外に G の正規部分群を含まないことと同値だが，G は可換群なので任意の部分群は正規．したがって H は単位群以外の部分群を含まない，つまり H は単位群である．これより G/H における表現は G の左正則表現であり，X における表現と同値．
5. $H < G, o(H) = p$ とする．H は真部分群をもたない巡回群である．また $(G : H) = m$ で，$m!$ は p で割り切れないので，H は単位群以外の G の正規部分群を含む．つまり H 自身が G の正規部分群である．
6. #まず次の補題を示す:$H < G$ として，$N \triangleleft G, N \triangleleft H$ とする．このとき $H/N \triangleleft G/N \Leftrightarrow H \triangleleft G$．(証明):$aNxN(aN)^{-1} = axa^{-1}N$ より，$aNxN(aN)^{-1} \in H/N$ が成り立つのは $axa^{-1} \in H$ が成り立つとき，またそのときに限る．
   まず $n = 1$ のときは明らか．$n > 1$ で，$o(G) = p^n, o(H) = p^{n-1}$ とすると $(G : H) = p$．$p!$ は p^n で割り切れないので，H は単位群以外の G の正規部分群を含む．これは当然 H の正規部分群でもある．これを N として $o(N) = p^m$ とすると，$H/N, G/N$ はそれぞれ位数 $o(H/N) = p^{n-m-1}, o(G/N) = p^{n-m}$ だから，帰納法の仮定により $H/N \triangleleft G/N$．したがって補題より $H \triangleleft G$．

2.11 直積

1.(a) $\mathbb{R}^* = \pm\mathbb{R}^*_>$．$\mathbb{R}^*$ は可換群で，$\mathbb{R}^*_>$ と $\{\pm 1\}$ はどちらも $\mathbb{R}^*$ の部分群なので正規．$\mathbb{R}^*_> \cap \{\pm 1\} = \{1\}$ なので，$\mathbb{R}^*$ はこれらの直積に分解される．

1.(b) $\mathbb{C}^*$ の任意の元が $re^{i\theta}$ と表されることから $\mathbb{C}^* = \mathbb{R}^*_> \mathbb{T}$．$\mathbb{C}^*$ は可換群で，$\mathbb{R}^*_>$ と $\mathbb{T}$ はどちらも $\mathbb{C}$ の部分群なので正規．$\mathbb{R}^*_> \cap \mathbb{T} = \{1\}$ なので，$\mathbb{C}^*$ はこれらの直積に分解される．

2. $\varphi_1 : G \to N_1$ を $xy \mapsto x (x \in N_1, y \in N_2)$ とすれば，φ_1 は全射準同型で，$\mathrm{Ker}\ \varphi_1 = N_2$．したがって準同型定理より $G/N_2 \simeq N_1$．
3. 明らか．
4. G は位数 pq の巡回群．真部分群の位数は p, q で，それぞれ G_1, G_2 のみが対応する．
5. $G \times G$ の位数は p^2 だから，真部分群の位数としてあり得るのは p．a を G の生成元とする．このとき $\langle (a, e) \rangle, \langle (a, a) \rangle, \langle (a, a^2) \rangle, \cdots, \langle (a, a^{p-1}) \rangle, \langle (e, a) \rangle$ は部分群になる．部分群は $p + 1$ 個存在する．$\langle (a^n, a) \rangle$ は，$\langle (a, a^m) \rangle$ と同じになってしまうので重複に注意．
6. 「G が $N_1, \cdots, N_n$ の直積に分解される $\Leftrightarrow N_i \triangleleft G$ で (1),(2) をみたす」を示す．まず $(\Rightarrow)$ を示す．(1) が成り立つのは明らか．まず $N_i \triangleleft G$ を示す．任意の $x \in G$ は $x = x_1 x_2 \cdots x_n (x_i \in N_i)$ と一意に表されるから，任意の $y \in N_i$ について $xyx^{-1} = x_1 \cdots x_{i-1} x_{i+1} \cdots x_n x_i y x_i^{-1} x_n^{-1} \cdots x_{i+1}^{-1} x_{i-1}^{-1} \cdots x_1^{-1} = x_i y x_i^{-1} \in N_i$．したがって $N_i \triangleleft G$．次に (2) を示す．$x \in (N_1 \cdots N_{i-1} N_{i+1} \cdots N_n) \cap N_i$ とすると，$x \in N_i$ より $x = e \cdots x \cdots e (i$ 番目が $x)$，$x \in N_1 \cdots N_{i-1} N_{i+1} \cdots N_n$ より $x = x_1 \cdots x_{i-1} x_{i+1} \cdots x_n$

のように表されるが，一意性より両者は一致しなければならないので，$x = x_j = e$．したがって (2) も成り立つ．次に ($\Leftarrow$) を示す．(1) より $G = N_1 \cdots N_n$ は明らかなので，N_i, N_j が可換なことと，表示が一意なことが言えればよい．まず可換であることは問題 2.5.14 と同様にしてわかる．一意性を示す．$x = x_1 \cdots x_n = y_1 \cdots y_n$ とすると，$(x_1^{-1}y_1) \cdots (x_n^{-1}y_n) = e$ より $(x_1^{-1}y_1) \cdots (x_{i-1}^{-1}y_{i-1})(x_{i+1}^{-1}y_{i+1}) \cdots (x_n^{-1}y_n) = x_i y_i^{-1}$．これより両辺は e に等しく，これが任意の i で成り立つので $x_i = y_i$，つまり表示は一意である．

2.12 Sylow の定理

3 環と多項式

3.1 環とその例

非可換環の例 1 加法群 $\mathbb{Z}^2$ は可換群で，自己準同型写像全体は要素が整数の 2 次正方行列で表せる．つまり $\mathrm{End}(\mathbb{Z}^2) = M(2, \mathbb{Z})$ である．これは一般に非可換である．$\mathrm{End}(\mathbb{Z}^2) = M(2, \mathbb{Z})$ となることを示す．任意の $x \in \mathbb{Z}^2$ は $m, n \in \mathbb{Z}$ によって

$$x = m\begin{bmatrix}1\\0\end{bmatrix} + n\begin{bmatrix}0\\1\end{bmatrix}$$

と表せる．[*1] したがって任意の自己準同型写像 f による像は

$$f(x) = mf\left(\begin{bmatrix}1\\0\end{bmatrix}\right) + nf\left(\begin{bmatrix}0\\1\end{bmatrix}\right)$$

のようになる．ここで

$$\left[f\left(\begin{bmatrix}1\\0\end{bmatrix}\right) \quad f\left(\begin{bmatrix}0\\1\end{bmatrix}\right)\right] = \left[\begin{bmatrix}1\\0\end{bmatrix} \quad \begin{bmatrix}0\\1\end{bmatrix}\right]\begin{bmatrix}a_{11} & a_{12}\\ a_{21} & a_{22}\end{bmatrix} \quad (a_{ij} \in \mathbb{Z})$$

のように基底が移り変わるとすると，右辺の行列を A として

$$f(x) = A\begin{bmatrix}m\\n\end{bmatrix}$$

と表せる．従って任意の自己準同型写像は $M(2, \mathbb{Z})$ の元で表せる．逆は明らかなので，$\mathrm{End}(\mathbb{Z}^2) = M(2, \mathbb{Z})$ が示された．

1. 単位元は R の単位元への定値写像．$M(S, R)$ が可換なとき，任意の $f, g \in M(S, R)$ について，
$$\forall x \in S, (fg)(x) = (gf)(x) \therefore f(x)g(x) = g(x)f(x)$$
ここで $f(x), g(x)$ は，f, g を動かすと R の元全体を取りうるので，$M(S, R)$ が可換になるのは R が可換なときのみ．
2. 明らか．
3. 明らか．
4. 前問の結果を使えばすぐわかる．
5. 公式
$$\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$$

[*1] $\mathbb{Z}^2$ だから基底を整数回足し合わせて任意の元を作れるが，$\mathbb{R}^2$ ではそれができないことに注意．

を用いて，数学的帰納法によって示せる (可換環なので特に気にすることもない).

6. 明らか.
7. 任意の $x, y \in R$ について
$$(x+y)^2 = (x+y)(x+y) = x^2 + xy + yx + y^2$$
$$x + y = x + y + xy + yx$$
$$xy = -yx$$
特に $y = 1$ としたら $x = -x$ だから，$xy = -yx = yx$ より，R は可換環．$n \in \mathbb{Z}$ について $nx = (n \bmod 2)x$ となり，たしかに Boole らしい.
8. 環になることを示す．積に関して，結合律・単位元 S の存在はすぐわかる．分配法則に関しては，
$$A \cap (B \triangle C) = (A \cap B) \triangle (A \cap C)$$
などがわかる (図を描くと良い)．これより $P(S)$ は環になって，$A \cap A = A$ なので Boole 環である.

3.2 整域，体

整域の性質についての補足

- $$ab = 1 \Rightarrow ba = 1$$
証明：
$$ab = 1 \Rightarrow b = bab \quad \therefore (1 - ba)b = 0 \quad \therefore 1 = ba$$
- $a \in R (a \neq 0)$ を固定した写像 $x \mapsto ax$ は単射である：
$$ax = ay \Leftrightarrow a(x - y) = 0 \quad \therefore x = y$$

問題解答.

1. $a \in R$ を単元とする．a が零因子でもあると仮定すると，ある $b \in R, b \neq 0$ が存在して，$ab = 0$．この両辺に a^{-1} を左からかければ $b = 0$ となり，矛盾．したがって a は零因子ではない.
2. $f \in M(S, R)$ で，ある $c \in S$ について $f(c) = 0$ となるとき，
$$g(x) = \begin{cases} 0 & (x \neq c) \\ 1 & (x = c) \end{cases}$$
とすれば $fg = 0$ となる．したがって f は零因子である．一方全ての $x \in S$ で $f(x) \neq 0$ ならば，R が体だから $f(x)$ の逆元が存在するので，$f^{-1}(x) = f(x)^{-1}$ とすれば $f^{-1}f = ff^{-1} = 1$.
3. 例えば $f(m, n) = (m + n, m + n)$，$g(m, n) = (m + n, -(m + n))$ とすれば，$fg = 0$ になる (3.1 節で与えた例のように行列で考えるとよい).
4. #a が左右どちらの零因子でないとする．このとき写像 $x \mapsto ax$ は単射である:$ax = ay \Leftrightarrow a(x-y) = 0$ のとき，a は零因子でないから $x = y$．同様に $x \mapsto xa$ も単射．R が有限集合だからどちらも全射でもあるので，逆写像，つまり逆元が存在する.
5. (i) $\Rightarrow$ (ii):$b \neq b', ab' = 1$ とすると $1 = ab = ab' \Leftrightarrow a(b - b') = 0$ より，a は左零因子．(ii) $\Rightarrow$ (i):単元だとすると矛盾 (1 でやった)．(iii) $\Rightarrow$ (i):a が単元でないとすると $ba \neq 1$ なので，#$ba = 1 + u (u \neq 0)$ と表せる．この両辺に a を左からかけると $aba = a + au$ となるが，$aba = a$ なので $au = 0$．したがっ

て，$b' = b + u$ ととれば $ab' = a(b + u) = 1$.

6. 零元は 0．逆元は $-(a+bi)$．単位元は 1．$a+bi$ に乗法の逆元が存在すれば，それは $(a-bi)/(a^2+b^2)$ の形．整数範囲ならば $a = 0, b = \pm 1$，$a = \pm 1, b = 0$ のときのみ逆元が存在する．つまり単元は $\pm 1, \pm i$ のみ．
7. たとえば $\sqrt{2}$ は単元ではない．
8.

3.3 イデアルと商環

1〜4. 容易に確認できる．
5. #
6〜8. 容易に確認できる．
9,10. $x^m = 0, y^n = 0 (m \leq n)$ とする．このとき $(x+y)^{2n} = 0$，$\forall r \in R, (rx)^n = r^n x^n = 0$ より N はイデアル．R/N の元で $\bar{a}$ をべき零元とすると，$\bar{a}^n \Leftrightarrow a^n \equiv 0 (\mathrm{mod}\ N) \Leftrightarrow a \in N$ より，$\bar{a} = \bar{0}$.
11. 容易に確認できる．

3.4 $\mathbb{Z}$ の商環

1. $\mathbb{Z}_p$ は真部分群を持たないので，取りうるイデアルは $\{0\}, \mathbb{Z}_p$ のいずれか．したがって $\mathbb{Z}_p$ は体である．
2. a を G の生成元とする．任意の $f \in \mathrm{Aut}(G)$ について，$f(a^m) = f(a)^m$ だから，$f(a)$ は G の生成元になっていなければならない．2 章 8 節問題 3 により，これは $(k, n) = 1$ なる自然数 k によって $f_k(a) = a^k$ と表されることを意味する．したがって $\mathrm{Aut}(G)$ は n と互いに素な n 未満の自然数 k によって f_k と表される自己同型写像全体で位数は $\varphi(n)$．これは法 n に関する $\mathbb{Z}$ の既約剰余類群と同型．
3. #$m = a^n - 1$ とする．$(a, m) = 1$ だから $\bar{a}$ は法を m とする既約剰余類群に含まれる．また $a^n \equiv 1 (\mathrm{mod}\ m)$ だから $\bar{a}^n = \bar{1}$ で，$a^n = m + 1$ だから n が $\bar{a}^k = 1$ をみたす k のうちで最小である．したがって $\bar{a}$ を生成元とする巡回群の位数は n だから，$n | \varphi(m)$.
4. #問題は，法を n とする既約剰余類群から位数 p の部分群を取り出せるか，に言い換えられる．素数位数の部分群は巡回群である．したがってその生成元を $\bar{a}$ とすれば $\bar{a}^p = 1$ となる．そしてこれは Sylow の定理により肯定される．