

既習事項のまとめ

- (1) 群の定義：集合 G に演算 $G \times G \rightarrow G : (a, b) \mapsto ab$ が与えられていて、次の 3 条件を全て満たすとき G を群と呼ぶ；
(G1) この演算は結合法則をみたす、
(G2) 単位元 e を持つ、
(G3) 各元 $g \in G$ に対して逆元 g^{-1} が存在する。
- (2) 群 G の部分集合 $H \subset G$ が 部分群 であるとは、 G の演算について H 自身が群になっていることである。
- (3) 記号 $H < G$ または $G > H$ は、 G が群であり、 H はその部分群であることを表すものとする。
- (4) 群 G が アーベル群 とは任意の $a, b \in G$ について $ab = ba$ が成り立つものをいう。アーベル群の演算を $+$ で表して、そのアーベル群を 加群 と呼ぶことがある。
- (5) 群 G の 位数 とは集合としての G の元の個数のことで $|G|$ と書かれる。
- (6) 群 G の要素 g の 位数 とは $g^m = e$ となる最小の正の整数 m のことである。そのような m が存在しないとき g の位数は ∞ であるという。
- (7) G の部分群 H による 右剰余類 とは、同値関係 $g_1 \sim g_2 \iff g_1 g_2^{-1} \in H$ で分類した類のことである。左剰余類も同様。
- (8) $H < G$ のとき、指数 $[G : H]$ とはこの右剰余類の類の個数である。
- (9) ラグランジュの定理：群 G の部分群 H による右剰余類は Hg ($g \in G$) の形にかける。また $|G| = [G : H]|H|$ が成り立つ。
- (10) $G = \bigsqcup_j Hg_j$ から $G = \bigsqcup_j g_j^{-1}H$ が導かれるから、右剰余類と左剰余類の“個数は”等しい。
- (11) 群 G の 正規部分群 とは、任意の $g \in G$ に対して $gNg^{-1} \subset N$ なる部分群 $N < G$ のことである。(これは $gNg^{-1} = N$ とも $gN = Ng$ とも同値)
記号 $N \triangleleft G$ もしくは $G \triangleright H$ で、 G が群であり、 N がその正規部分群であることを表すものとする。
- (12) $N \triangleleft G$ のとき $H \setminus G$ と G/H は完全に一致し (つまり $Hg = gH$)、自然な演算 $(Hg_1)(Hg_2) = Hg_1g_2$ で群になる。それゆえ $H \setminus G = G/H$ を G の H による 剰余群 と呼ぶ。
- (13) H_1, H_2 が $H_2 < H_1 < G$ なるとき、 $[G : H_2] = [G : H_1][H_1 : H_2]$ が成り立つ。
- (14) 群 G_1 から群 G_2 への写像 $\varphi : G_1 \rightarrow G_2$ が $\varphi(ab) = \varphi(a)\varphi(b)$ を満たすとき、 φ を 準同型 であるという。
- (15) 単射であり全射である準同型を 同型 といい、 $\varphi : G_1 \rightarrow G_2$ が同型写像であることを $\varphi : G_1 \xrightarrow{\sim} G_2$ または $G_1 \cong G_2$ で表す。
- (16) 準同型 $\varphi : G_1 \rightarrow G_2$ について
 $\text{Ker}(\varphi) = \{g \in G_1 \mid \varphi(g) = e\}$,
 $\text{Im}(\varphi) = \{\varphi(g) \mid g \in G_1\}$,
と定め、それぞれ φ の 核, 像 と呼ぶ。
- (17) 準同型定理 I. 準同型 $\varphi : G_1 \rightarrow G_2$ について
 $\text{Ker}(\varphi)$ は G_1 の正規部分群であり、 $G/\text{Ker}(\varphi) \ni g\text{Ker}(\varphi) \mapsto \varphi(g)$ なる写像は $G/\text{Ker}(\varphi)$ から $\text{Im}(\varphi)$ への同型写像である。つまり $G/\text{Ker}(\varphi) \xrightarrow{\sim} \text{Im}(\varphi)$ 。
- (18) 群 G からそれ自身への同型を G の自己同型といい、それらの全体を $\text{Aut}(G)$ と書く。2 つの同型の合成は同型であるし、同型の逆写像も同型であるから、 $\text{Aut}(G)$ は写像の合成に関して群になる。それゆえ $\text{Aut}(G)$ を 自己同型群 と呼ぶ。

「群の構造」期末試験問題兼解答用紙

(2010年度, 月曜V時限, 数学教育専修, 数理情報コース, 各2年)

試験時間 80分, 教科書: 三宅著「入門代数学」

- 注意 1. 最終的な答に至る途中の説明をできるだけ詳しく書くこと. 最終結果だけでは得点できない.
注意 2. 学生証, 記名用のペン, 鉛筆またはシャープペンシル, 消しゴム以外は机の上に置かないこと.
注意 3. 試験場の静粛を保つために, 退場は 17:30 の時点の一回限りとする.

A, B, C, D の各群から 1 問ずつ, 計 4 問を解答せよ. (各 25 点)

- A1** 巡回群の部分群は巡回群であることを示せ.
A2 巡回群の剰余群は巡回群であることを示せ.
A3 群 G の任意の元 g が $g^2 = e$ をみたすならば, G はアーベル群であることを示せ.

- B1** 加群 \mathbb{Z} の部分加群はある整数 m を用いて $m\mathbb{Z} = \{ma \mid a \in \mathbb{Z}\}$ と書けることを示せ.
B2 $a \in \mathbb{Z}$ を含む $\mathbb{Z}/m\mathbb{Z}$ の剰余類を \bar{a} と書く. \bar{a} が $\mathbb{Z}/m\mathbb{Z}$ の生成元であるための必要十分条件は $\gcd(a, m) = 1$ であることを示せ.

学籍番号	氏名	点
------	----	---

C1 群 $G \neq \{e\}$ が $\{e\}$ 以外に真の部分群を持たなければ, G は位数が素数の巡回群であることを示せ.

((Hint) $g \neq e, \in G$ の生成する部分群 $\langle g \rangle$ が G 全体と一致しないとすると, これは真の部分となる. つまり $G = \langle g \rangle$ となる. これは G が であることを意味する. さて, もし $G = \langle g \rangle$ が無限巡回群であれば $\langle g^2 \rangle$ が真の部分群となってしまう. よって $\langle g \rangle$ は有限位数の巡回群でなければならない. いま, その位数 n が素数でないとして $n = ab$ ($a > 1, b > 1$) とすると, は $\langle g \rangle$ の真の部分群をとるので, それは有り得ない.)

C2 群 G が 2 つの部分群 H と K の和集合であるならば, $G = H$ または $G = K$ であることを示せ.

(Hint: 背理法で示すために, $G \neq H$ かつ $G \neq K$ だとする. このとき, $h \in H, \notin K$ なる h と, $k \in K, \notin H$ なる k が存在する [確認せよ]. このとき hk が H か K に属することができるか考察せよ.)

C3 有限群 G の部分集合 S の元の個数について $2|S| > |G|$ であるとき $G = SS$ であることを示せ.

(Hint: 任意の $g \in G$ に対して $|gS^{-1}| = |S| > |G|/2$ ゆえ, $S \cap gS^{-1} \neq \emptyset$ でなければならない [なぜか]. そこで $s_1 = gs_2^{-1} \in S \cap gS^{-1}$ とすれば ...)

D1 加群 $\mathbb{Z}/5\mathbb{Z}$ の自己同型群 $\text{Aut}(\mathbb{Z}/5\mathbb{Z})$ を記述せよ.

D2 加群 $\mathbb{Z}/8\mathbb{Z}$ の自己同型群 $\text{Aut}(\mathbb{Z}/8\mathbb{Z})$ を記述せよ.

3 次対称群 S_3 の自己同型群 $\text{Aut}(S_3)$ を求めよ.

解答. 関係式 $(1\ 3\ 2)^{-1} = (1\ 2\ 3)$ と $(1\ 3\ 2)(1\ 2)(1\ 2\ 3) = (1\ 3)$, $(1\ 3\ 2)(1\ 3)(1\ 2\ 3) = (2\ 3)$ より, ひとつの同型写像 $\varphi: S_3 \rightarrow S_3$ は 2 元 $(1\ 2\ 3)$ と $(1\ 2)$ の写る先 $\varphi((1\ 2\ 3))$ と $\varphi((1\ 2))$ だけで決定される.

また, 実際これら $2 \times 3 = 6$ 種類の写像は同型写像であることが確かめられる. さらに, これらの同型写像はすべて内部自己同型として得られることがわかる. 実際,

$(1\ 2) \mapsto (1\ 3)$ 且つ $(1\ 2\ 3) \mapsto (1\ 2\ 3)$ なる同型は内部自己同型 $\sigma \mapsto (1\ 2\ 3)^{-1}\sigma(1\ 2\ 3)$ に他ならない. また

$(1\ 2) \mapsto (2\ 3)$ 且つ $(1\ 2\ 3) \mapsto (1\ 2\ 3)$ なる同型は内部自己同型 $\sigma \mapsto (1\ 3\ 2)^{-1}\sigma(1\ 3\ 2)$ であり,

$(1\ 2) \mapsto (1\ 2)$ 且つ $(1\ 2\ 3) \mapsto (1\ 3\ 2)$ なる同型は内部自己同型 $\sigma \mapsto (1\ 2)^{-1}\sigma(1\ 2)$,

$(1\ 2) \mapsto (1\ 3)$ 且つ $(1\ 2\ 3) \mapsto (1\ 3\ 2)$ なる同型は内部自己同型 $\sigma \mapsto (2\ 3)^{-1}\sigma(2\ 3)$,

$(1\ 2) \mapsto (2\ 3)$ 且つ $(1\ 2\ 3) \mapsto (1\ 3\ 2)$ なる同型は内部自己同型 $\sigma \mapsto (1\ 3)^{-1}\sigma(1\ 3)$ である.

以上の対応で

$$\text{Aut}(S_3) \cong S_3 \quad \dots\dots\dots (\text{答})$$

教科書の解答の訂正

問題 1.2 の問 12

☆ 有限群 G の部分群 H, K の指数 $[G : H]$ と $[G : K]$ が互いに素ならば $G = HK$ であることを示せ.

教科書の解答では HK が群になることが前提にされている様なので、それではマズイ！

これを証明するのに次を示しておく.

補題 Z $H < G, K < G$ で $[G : H]$ が有限のとき, $[K : H \cap K] \leq [G : H]$ である.

(証明). $H \cap K < K$ なので写像

$$\varphi : K/H \cap K \rightarrow G/H, \quad k(H \cap K) \mapsto kH$$

が定義される. これは単射である. 実際

$$\varphi(k(H \cap K)) = \varphi(k'(H \cap K)) \iff kH = k'H \implies kH \cap K = k'H \cap K$$

だからである. ゆえに

$$\begin{aligned} |K/H \cap K| &\leq |G/H|, \\ \therefore [K : H \cap K] &\leq [G : H] \end{aligned}$$

が示された

□

(☆ の証明)

いま集合としての直積 $H \times K$ を考えて, そこから集合 HK への写像

$$f : H \times K \rightarrow HK, \quad f(h, k) = hk$$

を調べる. $h_1, h_2 \in H$ と $k_1, k_2 \in K$ が $h_1k_1 = h_2k_2$ となったとすると $h_2^{-1}h_1 = k_2k_1^{-1}$ となる. これは $H \cap K$ の元である. これを x と書くことにすると $h_2^{-1}h_1 = x, k_2k_1^{-1} = x$ なので $h_2 = h_1x^{-1}, k_2 = xk_1$ である. つまり

$$h_1k_1 = h_2k_2 \iff \text{ある } x \in H \cap K \text{ について } h_2 = h_1x^{-1} \text{ かつ } k_2 = xk_1.$$

よって

$$(1) \quad |H| \times |K| = |H \times K| = |HK| \times |H \cap K|.$$

さて $[G : H]$ と $[G : K]$ は互いに素で, $[G : H \cap K] = [G : K][K : H \cap K] = [G : H][H : H \cap K]$ なので $[G : H][K : H \cap K]$. これと上記の補題 Z で得た $[K : H \cap K] \leq [G : H]$ を合わせると $[G : H] = [K : H \cap K]$ がわかる. これを上式の式に代入すれば

$$[G : H \cap K] = [G : K][G : H]$$

を得る. つまり

$$\begin{aligned} \frac{|G|}{|H \cap K|} &= \frac{|G|}{|K|} \times \frac{|G|}{|H|}, \\ \therefore |G| &= \frac{|H| \times |K|}{|H \cap K|} = |HK| \quad (\because (1)) \end{aligned}$$

よって $G = HK$.