

代数と幾何D (第4回小テスト (リベンジテスト) 解答・2008/1/9)

各小問 10 点 (150 点満点)

[1] < 5+5 点 >

- (i) 群 G の部分群 H が, $gH = Hg$ ($\forall g \in G$) を満たすとき, H を G の正規部分群という.
 (ii) 群 G が自明群 $\{1\}$ と G 自身以外に正規部分群を持たないとき, G を単純群という.

[2] < 4+3+3 点 > $H = \{(1), (1\ 2)\}$ に対し, まず次が分かる:

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

- (i) 左剰余類分解: $S_3 = H \cup (1\ 3)H \cup (2\ 3)H$, 右剰余類分解: $S_3 = H \cup H(1\ 3) \cup H(2\ 3)$.
 (ii) S_3/H の完全代表系 $\{(1), (1\ 3), (2\ 3)\}$. $H \backslash S_3$ の完全代表系 $\{(1), (1\ 3), (2\ 3)\}$.
 (iii) $(1\ 3)H \neq H(1\ 3)$ より, H は G の正規部分群ではない.

[解説] (ii) の完全代表系の取り方は色々ある. 例えば $\{(1\ 2), (1\ 2\ 3), (1\ 3\ 2)\}$ でもよい.

[3] < 5+5 点 > (i) $S_n = A_n \cup (1\ 2)A_n$. また, $\#A_n = n!/2$.

(ii) $\#A_4 = 12$. A_4 の各元とそれぞれの位数を表にしてみると:

A_4 の元	(1)	(1 2)(3 4)	(1 3)(2 4)	(1 4)(2 3)	(1 2 3)	(1 2 4)	(1 3 4)	(2 3 4)
					(1 3 2)	(1 4 2)	(1 4 3)	(2 4 3)
位数	1	2	2	2	3	3	3	3

[4] < 10 点 > $g \in G$ に対し, $g \in H$ ならば $gH = H = Hg$ である. $g \notin H$ のとき, G の H による左 (右) 剰余類分解を考えると, $G = H \cup gH$, $G = H \cup Hg$ となる. よって $gH = Hg$.

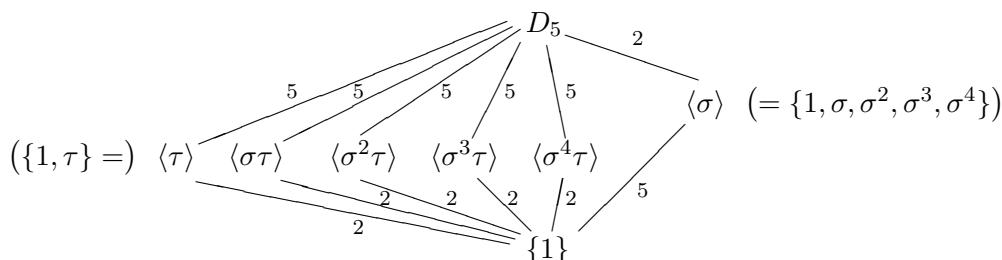
[5] < 4+3+3 点 > (i) $\text{ord}(\sigma) = n$, $\text{ord}(\tau) = 2$, $\text{ord}(\sigma\tau) = 2$.

(ii) D_5 の元のうち, $\{\sigma, \sigma^2, \sigma^3, \sigma^4\}$ は回転, $\{\tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau, \sigma^4\tau\}$ は (ある軸に対する) 裏返しに対応してはならない. よって

D_5 の元	1	σ	σ^2	σ^3	σ^4	τ	$\sigma\tau$	$\sigma^2\tau$	$\sigma^3\tau$	$\sigma^4\tau$
位数	1	5	5	5	5	2	2	2	2	2

[注意] 一般には, $\text{ord}(xy) \neq \text{ord}(x) \cdot \text{ord}(y)$ である (積 xy の位数は位数の積ではない!).

(iii) (ラグランジュの定理から) D_5 の部分群の位数は 1, 2, 5, 10 であり, 位数 1, 10 はそれぞれ $\{1\}, D_5$. よって, 位数 2, 5 の部分群がどの位あるか調べればよい. 位数が素数の群は巡回群 $\langle a \rangle$ であり, $\text{ord}(a) = \#\langle a \rangle$. D_5 の (単位元ではない) 全ての元に対し, それらが生成する巡回群を考えて, D_5 の全ての部分群が得られる. また, Hasse 図は以下の様になる.



[6] < 4+3+3 点 > (i) aHa^{-1} の任意の元 $X = axa^{-1}, Y = aya^{-1}$ に対し, $X \cdot Y = (axa^{-1})(aya^{-1}) = a(xy)a^{-1} \in aHa^{-1}$ かつ $X^{-1} = (axa^{-1})^{-1} = ax^{-1}a^{-1} \in aHa^{-1}$. よって (部分群の判定条件より) aHa^{-1} は G の部分群である.

(ii) $|H| < \infty$ の場合, $H = \{a_1, \dots, a_n\}, \#H = n$ とすると, $aHa^{-1} = \{aa_1a^{-1}, \dots, aa_na^{-1}\}$ であり, $a_i \neq a_j \implies aa_ia^{-1} \neq aa_ja^{-1}, (1 \leq i < j \leq n)$ が成り立つ (なぜなら, 消去律より $aa_ia^{-1} = aa_ja^{-1} \implies a_i = a_j$). よって $|H| = |aHa^{-1}|$.

$|H| = \infty$ の場合, H の元 x, y ($x \neq y$) に対して $axa^{-1} \neq aya^{-1}$ であり, $|aHa^{-1}| = \infty$. よって, $|H| = |aHa^{-1}| = \infty$ を得る.

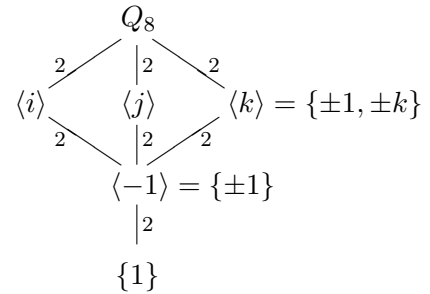
(iii) $H \triangleleft G \iff gH = Hg$ ($\forall g \in G$) $\iff gHg^{-1} = H$ ($\forall g \in G$) $\iff H$ の共役部分群は H のみ.

[7] <4+3+3点>

(i) (ラグランジュの定理より) 位数2, 4の部分群を求めればよい. 各元の位数を求めると

Hasse 図

Q_8 の元	1	i	j	k	-1	$-i$	$-j$	$-k$
位数	1	4	4	4	2	4	4	4



よって, Q_8 の位数2の部分群は $\langle -1 \rangle = \{1, -1\}$ のみ. また位数4の部分群は, 必ず位数4の元を1つ以上含む. これより, 位数4の巡回群 $\langle a \rangle$ となる (← なぜか? 分からない場合は, 少しの時間考える!). よって, 位数4の部分群は $\langle i \rangle, \langle j \rangle, \langle k \rangle$ の3つのみである. Hasse 図は右のようになる.

(ii) Q_8 の部分群のうち, $\{1\}, Q_8$ は正規部分群である. また, 3つの部分群 $\langle i \rangle, \langle j \rangle, \langle k \rangle$ は指数が2なので, 正規部分群である (問[6] 参照). 残りの1つの部分群を $H = \langle -1 \rangle = \{1, -1\}$ とする. H の元は任意の Q_8 の元と可換であることから, $gH = Hg (\forall g \in Q_8)$ となる. よって, $H = \{\pm 1\} \triangleleft Q_8$. これより, Q_8 の全ての部分群は正規部分群である.

解説 G が可換群 $\implies G$ の全ての部分群は正規部分群, であった. (ii) はこの逆が成り立たないことを示している. それでも, Q_8 の部分群は全て正規部分群であることから, 非可換群の中でも, 可換群に近い性質を持っていることが期待できる(?).

(iii) 剰余群 $Q_8/\{\pm 1\}$ は4つのクラス (類) $H = \{\pm 1\}, iH = \{\pm i\}, jH = \{\pm j\}, kH = \{\pm k\}$ からなる位数4の群であり, 単位元は $H = \{\pm 1\}$ である. 各剰余類の $Q_8/\{\pm 1\}$ における位数を求めると:

$Q_8/\{\pm 1\}$ の元	$H = \{\pm 1\}$	$iH = \{\pm i\}$	$jH = \{\pm j\}$	$kH = \{\pm k\}$
位数	1	2	2	2

実際, $(iH)^2 = (iH)(iH) = i^2H = (-1)H = H$ の様に, 位数2が確かめられる. 一方, Q_8 には位数2の元は1つしかない. よって, $Q_8/\{\pm 1\}$ は Q_8 のどの部分群とも同型ではない.

解説 $H \triangleleft G$ に対し, 剰余類群 $G/H = \{gH \mid g \in G\} = \{\overline{g_1}, \dots, \overline{g_n}\} (g_i \in G)$ に対し, $\overline{g_i} \cdot \overline{g_j} = \overline{g_i \cdot g_j}$ であるが, G/H は G の部分群と見なせるとは限らない.

[8] <3+3+2+2点> (i) $f(1_G) = f(1_G \cdot 1_G) = f(1_G)f(1_G)$ より, 両辺を $f(1_G)$ で割れば, $f(1_G) = 1_{G'}$.

(ii) $1_{G'} = f(1_G) = f(gg^{-1}) = f(g)f(g^{-1})$ より, $f(g)^{-1} = f(g^{-1})$.

(iii) $n = \text{ord}(g)$ とすると, $f(g)^n = f(g^n) = f(1_G) = 1_{G'}$. よって, $\text{ord}(f(g)) \mid n$.

(iv) $m = \text{ord}(f(g))$ とする. $f(1_G) = 1_{G'} = f(g)^m = f(g^m)$ より, f が単射であれば, $1_G = g^m$ を得る. よって, $\text{ord}(g) \mid m$. (iii) と合わせると, $m = n$ を得る.

[9] <4+3+3点> (i) $(\implies) f(1_G) = 1_{G'}$ より OK. $(\impliedby) f(x) = f(y), (x, y \in G)$ とすると, $f(xy^{-1}) = f(x)f(y)^{-1} = f(x)f(x)^{-1} = 1_{G'}$ より, $xy^{-1} = 1_G$ つまり $x = y$ を得る. よって f は単射.

(ii) $f(x), f(y) \in \text{Im} f$ に対し, $f(x)f(y)^{-1} = f(xy^{-1}) \in \text{Im} f$. よって, (部分群の判定条件より) $\text{Im} f$ は G' の部分群.

(iii) $x, y \in \text{Ker} f$ とする. $f(xy^{-1}) = f(x)f(y)^{-1} = 1_{G'}$ より, $xy^{-1} \in \text{Ker} f$. よって, よって, (部分群の判定条件より) $\text{Ker} f$ は G の部分群. さらに, 正規部分群を示す. $\forall x \in \text{Ker} f, \forall g \in G$ に対し, $f(gxg^{-1}) = f(g)f(x)f(g)^{-1} = f(g)f(g)^{-1} = 1_{G'}$. よって, $gxg^{-1} \in \text{Ker} f$. つまり, $g \text{Ker} f g^{-1} \subset \text{Ker} f (\iff g \text{Ker} f = \text{Ker} f g)$ であり, $\text{Ker} f$ は G の正規部分群.

[10] <4+3+3点> (i) 行列式の性質 $\det(AB) = \det(A) \cdot \det(B)$ より, $\det$ は準同型写像であり, 任意の $a \in \mathbb{R}$ に対し, $\det \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} = a$ より, 全射である.

(ii) $\text{SL}_2(\mathbb{R}) = \text{Ker} \det$ である. よって, (問[9] (iii) より) $\text{SL}_2(\mathbb{R})$ は $\text{GL}_2(\mathbb{R})$ の正規部分群.

(iii) $\text{GL}_2(\mathbb{R})/\text{SL}_2(\mathbb{R}) \cong \mathbb{R}^\times$.

- [11] <10点> $C_2 = \langle \sigma \rangle = \{1, \sigma\}$, $C_3 = \langle \tau \rangle = \{1, \tau, \tau^2\}$ とする. 直積の定義から $C_2 \times C_3 = \{(1, 1), (1, \tau), (1, \tau^2), (\sigma, 1), (\sigma, \tau), (\sigma, \tau^2)\}$ であり, 位数6の可換群となる. もし, $C_3 \times C_2$ に位数6の元 a が存在すれば, $C_3 \times C_2 \supset \langle a \rangle$ かつ $\# \langle a \rangle = 6$ より $C_3 \times C_2 = \langle a \rangle \cong C_6$ となる. ここで (σ, τ) の位数を計算すると, $(\sigma, \tau)^2 = (1, \tau^2) \neq (1, 1)$, $(\sigma, \tau)^3 = (\sigma, 1) \neq (1, 1)$ より (σ, τ) の位数は6である. よって $C_3 \times C_2 = \langle (\sigma, \tau) \rangle \cong C_6$.

[解説] より一般に, **中国の剰余定理** $(m, n) = 1$ ならば, $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, $(C_{mn} \cong C_m \times C_n)$ が成り立つのであった.

- [12] <5+5点> (i) A_4 に位数6の部分群 H が存在したとすると, $|A_4 : H| = 2$ より $H \triangleleft A_4$ (正規部分群) とならなくてはならない(問[4]). 正規部分群 H は単位元1といくつかの共役類の和集合からなるが, A_4 の類等式は $12 = 1 + 3 + 4 + 4$ であり, いくつかの共役類の和集合が位数6になるのは不可能である.

(ii) A_5 の正規部分群は自明群 $\{1\}$ と A_5 自身のみであることを示す. A_5 の類等式は $60 = 1 + 15 + 20 + 12 + 12$ であるから, $H \triangleleft A_5$, $(H \neq \{1\}, A_5)$ が存在すると, H はいくつかの共役類の和集合からなり, その位数は $\#A_5 = 60$ の約数である. しかし2つ, 3つ, 4つの共役類の和集合の位数を求めると,

2つ: $1 + 15 = 16$, $1 + 20 = 21$, $1 + 12 = 13$

3つ: $1 + 15 + 20 = 36$, $1 + 15 + 12 = 28$, $1 + 20 + 12 = 33$, $1 + 12 + 12 = 25$

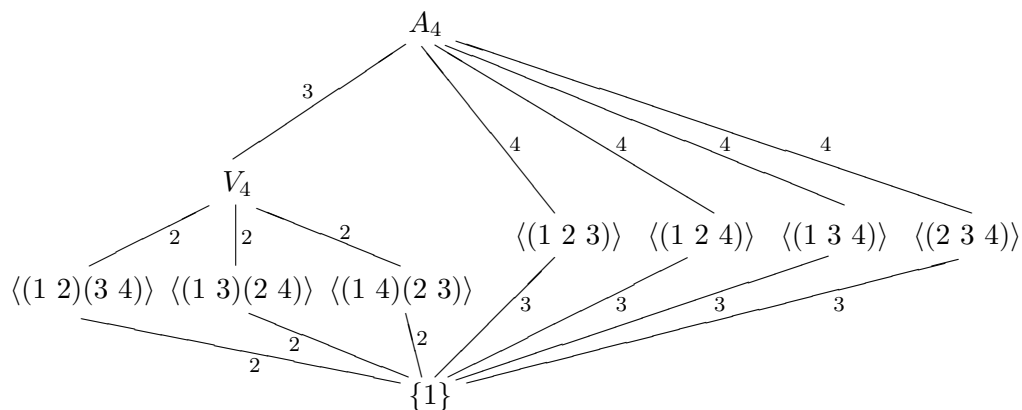
4つ: $1 + 15 + 20 + 12 = 48$, $1 + 15 + 12 + 12 = 40$, $1 + 20 + 12 + 12 = 45$

であり, $\#A_5 = 60$ の約数ではない. よって $\{1\}$ と A_5 以外の正規部分群は存在しない.

- [13] <10点> 問[12](i) とグランジュの定理より, A_4 の位数2, 3, 4の部分群を求めればよい. 位数2, 3の部分群は巡回群であり, それぞれ位数2, 3の元で生成される:

$$\begin{aligned} \langle (12)(23) \rangle &= \{(1), (12)(23)\}, & \langle (123) \rangle &= \{(1), (123), (132)\} = \langle (132) \rangle, \\ \langle (13)(24) \rangle &= \{(1), (13)(24)\}, & \langle (124) \rangle &= \{(1), (124), (142)\} = \langle (142) \rangle, \\ \langle (14)(23) \rangle &= \{(1), (14)(23)\}, & \langle (134) \rangle &= \{(1), (134), (143)\} = \langle (143) \rangle, \\ & & \langle (234) \rangle &= \{(1), (234), (243)\} = \langle (243) \rangle. \end{aligned}$$

位数4の部分群は巡回群 C_4 またはクラインの四元群 $V_4 (\cong C_2 \times C_2)$ に同型である. しかし, A_4 には位数4の元が存在しないので, C_4 と同型にはならない. よって, $V_4 = \{(1), g_1, g_2, g_3\}$ のみが位数4の部分群である. 以上により, Hasse 図は次の様になる.



- [14] <5+5点> (i) $(\mathbb{Z}/17\mathbb{Z})^\times$ は位数16の乗法群であり, $[10] \in (\mathbb{Z}/17\mathbb{Z})^\times$ に対して, $[10]^{16} = [1]$ である. つまり, $10^{16} \equiv 1 \pmod{17}$. $[10]$ の位数は16の約数であり, $10^2 \equiv 15 \pmod{17}$, $10^4 \equiv 4 \pmod{17}$, $10^8 \equiv 16 \pmod{17}$ より $[10]$ の位数は16. よって $k = 16$ が最小.
(ii) $109^{18} \equiv 1 \pmod{19}$ より, $109^{900} = (109^{18})^{50} \equiv 1^{50} = 1 \pmod{19}$. よって余りは1.

- [15] <5+5点> (i) $1, \dots, p, p+1, \dots, 2p, 2p+1, \dots, p^r$ のうち, p で割り切れる数は p 個ごとに1つ ($1/p$ の割合で) 存在する. よって, p と互いに素な数は $\frac{p-1}{p} p^r = p^{r-1}(p-1)$ 個.
(ii) $\varphi(19) = 18$, $\varphi(38) = \varphi(2)\varphi(19) = 1 \cdot 18 = 18$, $\varphi(60) = \varphi(2^2)\varphi(3)\varphi(5) = 2 \cdot 2 \cdot 4 = 16$, $\varphi(720) = \varphi(2^5)\varphi(3^2)\varphi(5) = 2^4 \cdot (3 \cdot 2) \cdot 4 = 192$.