既習事項のまとめ

(1) $n|m$ は整数 n が整数 m を割り切ること, つまり m が n の倍数であることを意味する.

(2) 群の定義 : 集合 G に演算 $G \times G \to G : (a, b) \mapsto ab$ 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 1 を持つ,
(G3) 各元 $a \in G$ に対して逆元 a^{-1} が存在する.

(3) 群 G の空でない部分集合 $H \subset G$ が 部分群 であるとは, G の演算について
(SG1) $a, b \in H \implies ab \in H$
(SG2) $a \in H \implies a^{-1} \in H$
が成り立つことである.

(4) 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.

(5) 群 G が アーベル群 とは任意の $a, b \in G$ について $ab = ba$ が成り立つことをいう. 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.

(6) 群 G 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.

(7) 群 G と $a \in G$ について, a^j $(j \in \mathbf{Z})$ の全体は G の部分群である. これを $\langle a \rangle$ で表す.
1 つの元 a でもって $\langle a \rangle$ と書かれる群を 巡回群 と呼ぶ.

(8) 群 G の要素 a の 位数 とは $\langle a \rangle$ の (群としての) 位数のことで, これを $o(a)$ と記す. これは $g^m = 1$ となる最小の正の整数 m のことである. その様な m が存在しないとき g の位数は ∞ であるといい, $o(a) = \infty$ と書く.

(9) G の部分群 H による 左剰余類 とは, 同値関係 $g_1 \equiv_\ell g_2 \bmod H$ ($g_1{}^{-1}g_2 \in H$ で定義) で分類した類のことで, g_1 の属する類は g_1H である.

(10) G の部分群 H による 右剰余類 とは, 同値関係 $g_1 \equiv_\mathrm{r} g_2 \bmod H$ ($g_1g_2{}^{-1} \in H$ で定義) で分類した類のことで, g_1 の属する右剰余類は Hg_1 である.

(11) 集合 X と, そのいくつかの部分集合 $\{X_i\}_{i\in I}$ (I は添字からなるある集合) が
$X = \bigcup_{i\in I} X_i$ かつ $X_i \cap X_j = \emptyset$ $(i \neq j)$ を満たしているとき, これを簡単に $X = \sum_{i\in I} X_i$ と書く.

(12) 群 G の部分群 H による右剰余類の全体を $H\backslash G$ と書く. それをいま $\{Ha_i\}_{i\in I}$ と書くとき, $G = \sum_{i\in I} Ha_i$ である. これを G の H による 右分解 と呼び, 集合 $\{a_i \,|\, i \in I\}$ を $H\backslash G$ の 右完全代表系 という. 左剰余類の全体は G/H と書かれる. 左分解, 左完全代表系 も同様である.

(13) $H < G$ のとき, 指数 $|G : H|$ とは G の H による左 (右) 剰余類の類の個数である.
つまり $|G : H| = |H\backslash G| = |G/H|$.

(14) ラグランジュの定理 : G が有限群で $H < G$ のとき $|G| = |G : H||H|$ が成り立つ.

(15) **定理 9.1** (i) 巡回群の部分群はまた巡回群である.
(ii) G が位数 n の有限巡回群のとき, n の任意の約数 m について, G の部分群で位数 m のものがただ 1 つ存在する. (この逆も成り立つ (= **例題 9.8**).)

(16) **例題 9.4** 位数 n の有限巡回群 $G = \langle a \rangle$ の元 a^r に対して, $\langle a^r \rangle = \langle a^{\gcd(n,r)} \rangle$ が成り立つ. ただし (n, r) は r と n の最大公約数. したがって a^r の位数は $n/\gcd(n, r)$ である.

(17) **例題 9.5** 巡回群 $G = \langle a \rangle$ の生成元について, 次が成り立つ.
(i) $|G| = \infty$ ならば G の生成元は a と a^{-1} のみである.
(ii) $|G| = n$ のとき, a^i が G の生成元であるための必要十分条件は $(i, n) = 1$ となることである.

(18) 整数 $n > 0$ について, 加法群 $\mathbf{Z}$ の部分群 $n\mathbf{Z}$ による剰余類 $\mathbf{Z}$, $1+\mathbf{Z}$, $2+\mathbf{Z}$, $\cdots$, $(n-1)+\mathbf{Z}$ のうち, $\gcd(i, n) = 1$ (つまり $\{ai + bn \,|\, a, b \in \mathbf{Z}\}$=$\mathbf{Z}$) なる $i+\mathbf{Z}$ の個数を $\varphi(n)$ と表して, これを オイラーの関数 という. $\varphi(1) = 1$. 素数 p については $\varphi(p^m) = p^m - p^{m-1}$.

実施：2013 年 2 月 3 日 (月) 16:30-18:00, Y-32 室

「群 の 構 造」 期 末 試 験 問 題 兼 解 答 用 紙

(2012 年度, 後期, 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: 永尾 汎 著 「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, 退出は 17:30 の時点の一回限りとする.
注意 4. 4A と 4B は選択問題である.

1 (20 点) 群 G の任意の元 x に対して $x^2 = 1$ が成り立てば, G はアーベル群であることを証明せよ.

2 (20 点) 群 G の空でない部分集合 H が有限集合のとき $HH \subset H$ ならば H は G の部分群であることを証明せよ. (ちなみに G が無限集合なら $HH \subset H$ となる部分群でない無限部分集合 H を簡単に見出すことができる.)

3 (20 点) 位数が素数の群は巡回群であることを示せ.

学籍番号	氏名	点

4A (25 点) n 次対称群 S_n は $\{(1,2),\ (2,3),\cdots,(i,i+1),\cdots,\ (n-1,n)\}$ で生成されることを示せ. ただし, S_n が互換の全体で生成されることは既知としてよい.

4B (25 点) $G=\sum_{j\in I} Ha_j$ が $H<G$ による群 G の右分解のとき, $G=\sum_{j\in I} {a_j}^{-1}H$ は左分解を与えることを示せ.

5 (15 点) 正の整数 n について, 次の等式が成り立つことを示せ :

$$n=\sum_{m|n}\varphi(m).$$

(hint : 位数 n の巡回群を, その各元の位数によつて部分集合に分けよ)

解 (1) 位数 n の巡回群 $G=\langle a\rangle=\{1,\ a,\ a^2,\cdots a^{n-1}\}$ を考える. これの各元の位数は必ず n の約数になっている.
(なぜなら $1\leqq i\leqq n-1$ に対して $o(a^i)=m$ のとき, $\langle a^i\rangle=\{1,\ a^i,\ a^{2i},\cdots,\ a^{(m-1)i}\}<G$ であり,
Lagrange の定理より $m=|\langle a^i\rangle|$ は G の約数である.)
(2) さて, $m|n$ のとき, 位数 m の元はどれも $\langle a^{\frac{n}{m}}\rangle$ に属する.
(なぜなら, 位数 m の元は位数 m の巡回部分群の生成元であるが, 位数 m の部分群は 1 つしか存在しない (定理 9.1(2)) からである.)
(3) 従って, $m|n$ のとき位数 m の元は $\langle a^{\frac{n}{m}}\rangle$ の中の, $\gcd(i,m)=1$ なる $i\in\{0,1,\cdots,m-1\}$ でもって $a^{\frac{n}{m}i}$ と書かれる元に他ならず ($\because$ 例題 9.5(ii)), その様な元の個数は $\varphi(m)$ 個である (ちなみに, 位数 1 の元は単位元のみであり $\varphi(1)=1$).
(4) 以上から, 各 $m|n$ ごとに G の位数 m の元が $\varphi(m)$ 個あり, それらをすべて合せると G のすべての元が得られる筈だから

$$\sum_{m|n}\varphi(m)=n$$

でなければならない.

(ここより下には記入しないで下さい)