- 群に関する基本的なこと（部分群，正規部分群，商群，準同形定理）
- 部分群による剰余類の応用として「p が奇素数なら $2^{p-1} \equiv 1 \pmod{p}$」.
- 群の集合への作用（共役類，シローの定理）.

注意：群とは 3 つ組 $(G, \cdot, e)$ で，以下の公理を満たすもののことであった.

(1) $\forall a \in G, \forall b \in G, \forall c \in G, (ab)c = a(bc)$.
(2) $\forall a \in G, ea = a = ae$.
(3) $\forall a \in G, \exists b \in G, ab = e = ba$.

ここで G は集合，$e \in G$ は元，$\cdot : G \times G \to G$ は写像（2 項演算）である.

定義：群 $(G, \cdot, e)$ の部分集合 H は，3 つ組 $(H, \cdot|_{H \times H}, e)$ が群であるとき部分群と呼ばれる.

注意：同値な条件として「$H \neq \emptyset$ かつ $\forall a \in H, \forall b \in H, ab^{-1} \in H$」は容易にわかる.

定義：群 G と部分群 $H \subseteq G$ について

$$g \sim g' \Leftrightarrow g^{-1}g' \in H$$

とすると，これは G の同値関係になっていることが簡単に確認できる.

記法：$g \in G$ の同値類 $[g] = C_g = \{g' \in G \mid g \sim g'\}$ は

$$C_g = gH := \{gh \mid h \in H\}$$

であることが簡単にわかる．同値関係による商集合を G/H と書く（この講義では）.

系：群 G と部分群 $H \subseteq G$ について，集合として

$$G = \bigsqcup_{[g] \in G/H} gH.$$

系：有限群 G の部分群 H について，$|H|$ は $|G|$ の約数.

証明：$g \in G$ について，$\varphi_g : G \to G, x \mapsto gx$ とすると，$\varphi_{g^{-1}} \circ \varphi_g = \mathrm{id}$ で，$\varphi_{g^{-1}}(gH) = H$ より，$|G| = |G/H| \cdot |H|$ が成立.

定義：有限群 G の元 $g \in G$ について（鳩の巣原理より $\exists a \neq \exists b \geq 1, g^a = g^b$ であるから）

$$\exists M \geq 1, g^M = e.$$

この $M \geq 1$ の最小値を g の位数といい，$\mathrm{ord}_G(g)$ と書く（この講義では）.

系：有限群 G の元 $g \in G$ について，$\mathrm{ord}_G(g)$ は $|G|$ の約数.

証明：$H := \{g^n \mid n \in \mathbb{Z}\}$ は G の部分群で，$|H| = \mathrm{ord}_G(g)$.

応用：$\varphi(m) := |(\mathbb{Z}/n\mathbb{Z})^\times|$ をオイラー関数という（$n \geq 1$）．以下は簡単に確認できる.

1. $(\mathbb{Z}/n\mathbb{Z})^\times = \{[a] \in \mathbb{Z}/n\mathbb{Z} \mid \gcd(a,n) = 1\}$.
2. $\varphi(n) = |\{1 \le a \le n \mid \gcd(a,n) = 1\}|$.

系：$a, n \ge 1$ が $\gcd(a,n) = 1$ ならば，$a^{\varphi(n)} \equiv 1 \pmod{n}$.

注意：例えば奇素数 $p \ge 3$ について，$2^{p-1} \equiv 1 \pmod{p}$ が成り立つ．これが奇数 p について不成立ならば p は合成数であると分かる．

命題：可換環 $R_1, \cdots, R_s$ について

$$(R_1 \times \cdots \times R_s)^\times = R_1^\times \times \cdots \times R_s^\times.$$

証明：明らか.

系：$n = p_1^{e_1} \cdots p_s^{e_s}$（ここで $p_1, \cdots, p_e$ は相異なる素数で，$e_1, \cdots, e_s \ge 1$）について

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_s}\right).$$

証明：CRT より以下の環同型が成り立つ.

$$\mathbb{Z}/n\mathbb{Z} \cong (\mathbb{Z}/p_1^{e_1}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p_s^{e_s}\mathbb{Z}).$$

上の命題より，素数 p と $e \ge 1$ について $|(\mathbb{Z}/p^e\mathbb{Z})^\times| = p^e(1 - 1/p)$ を言えばよいが，易しい.

注意：本当は上の議論で，可換環の環同型 $R \cong R'$ が群同型（後述．しかし定義は推測できるべきである）$R^\times \cong (R')^\times$ を誘導することを用いている.

注意：$g \sim g' \Leftrightarrow g^{-1}g' \in H$ を

$$g \sim g' \Leftrightarrow g'g^{-1} \in H$$

に変えても同様の議論が可能である．このとき $g \in G$ の同値類 $[g] = C_g = Hg := \{hg \mid h \in H\}$ となる．商集合を $H \backslash G$ と書く（この講義では）.

定義：群 G の部分群 $H \subseteq G$ が正規部分群 $\Leftrightarrow \forall g \in G, gH = Hg$．このとき $H \trianglelefteq G$ と書く．この条件は以下とも同値である.

$$\forall g \in G, g^{-1}Hg \subseteq H.$$

命題：群 $G = (G, \cdot, e)$ の正規部分群 $N \trianglelefteq G$ について，$(G/N, \cdot', [e])$ は以下の構造で群になることが確認できる．これを G の N による商群という.

$$\cdot' : G/N \times G/N \to G/N, \quad ([a], [b]) \mapsto [ab].$$

証明：環のときと同様.

定義：群 G_1, G_2 について，写像 $\varphi : G_1 \to G_2$ が群準同形写像とは

(1) $\forall g \in G_1, \forall g' \in G_1, \varphi(gg') = \varphi(g)\varphi(g')$.
(2) $\varphi(e_1) = e_2$.
(3) $\forall g, \in G_1, \varphi(g^{-1}) = \varphi(g)^{-1}$.

注意：条件 (1),(2),(3) は

$$\forall g \in G_1, \forall g' \in G_1, \varphi(gg') = \varphi(g)\varphi(g')$$

とも同値で，教科書にはよくこちらが採用される．

命題：群 $G = (G, \cdot, e)$ の正規部分群 $N \trianglelefteq G$ について，自然な全射 π は群準同型写像．ここで

$$\pi : G \twoheadrightarrow G/N, \quad g \mapsto [g]_N = gN = Ng.$$

証明：環のときと同様.

系：群 G について，正規部分群と群準同型写像の核は同じ概念である．

証明：群準同型 $\varphi : G \to G'$ の Ker が G の正規部分群であることは易しい．逆に，上の π について $\operatorname{Ker} \pi = N$ である．

命題（商群の普遍性）：群 G の正規部分群 N による商群 G/N は以下の性質を持つ：

任意の群 G' と任意の群準同型 $\varphi : G \to G'$ について，

$$\forall g_1 \in G, \forall g_2 \in G, [g_1]_N = [g_2]_N \Rightarrow \varphi(g_1) = \varphi(g_2)$$

ならば，$\varphi = \bar{\varphi} \circ \pi$ なる群準同型 $\bar{\varphi} : G/N \to G'$ がただ 1 つ存在する．

$$\begin{tikzcd} G \arrow[r, "\pi"] \arrow[dr, "\varphi"'] & G/N \arrow[d, dotted, "\bar{\varphi}"] \\ & G'. \end{tikzcd}$$

証明：商集合の普遍性より，目的の写像 $\bar{\varphi} : G/N \to G'$ がただ 1 つ存在する．これが群準同型であることは，$\bar{\varphi}([g]) = \varphi(g)$ から簡単に確認できる（ここで $g \in G$）．

定理（群の群準同型定理）：群準同型 $f : G \to G'$ について，以下の群同型が成り立つ．

$$G/\operatorname{Ker} f \xrightarrow{\sim} \operatorname{Im} f.$$

注意：ここでおきまりの以下の定義を用いている．群準同型 $\varphi : G \to G'$ が群同型とは，

$$\exists \varphi' : G' \to G, \varphi' \circ \varphi = \mathrm{id}_G, \varphi \circ \varphi' = \mathrm{id}_{G'}.$$

これは（環や加群のときと同様に）φ が全単射であることと同値である．

証明：$\mathrm{Im}\, f \subseteq G'$ が G' の部分群であることは簡単に確認できる．

以下の $\Leftrightarrow$ の $\Rightarrow$ と商群の普遍性より全射群準同型 $\bar{\varphi} : G/\mathrm{Ker}\, f \xrightarrow{\sim} \mathrm{Im}\, f$ が存在する．$\Leftrightarrow$ なので，集合の準同形定理より $\bar{\varphi}$ は単射（よって全単射）．

> 主張：$\forall g_1 \in G, \forall g_2 \in G, [g_1]_{\mathrm{Ker}\, f} = [g_2]_{\mathrm{Ker}\, f} \Leftrightarrow f(g_1) = f(g_2)$
> 証明：$(\Rightarrow)$：$g_1^{-1} g_2 \in \mathrm{Ker}\, f$ より $f(g_1)^{-1} f(g_2) = e'$．よって $f(g_1) = f(g_2)$.
> $(\Leftarrow)$：上の議論を逆にたどる．

定義：群 G の集合 X への左作用とは，以下を満たす写像 $a : G \times X \to X$ のことである．

(1) $\forall g_1 \in G, \forall g_2 \in G, \forall x \in X, a(g_1 g_2, x) = a(g_1, a(g_2, x))$.
(2) $\forall x \in X, a(e, x) = x$.

記法：普通，$a(g, x) = gx$ とか $a(g, x) = g \cdot x$ と書く．以下，左という形容詞を省略する．

例：集合 X について

$$\mathfrak{S}_X = \mathrm{Bij}(X) := \{ f : X \xrightarrow{\sim} X \mid f \text{ は全単射 } \}$$

は，合成に関して群をなす．このとき，以下は作用である．

$$\mathfrak{S}_X \times X \to X, (f, x) \mapsto f(x).$$

例：$\mathrm{GL}_n(\mathbb{C}) \times \mathrm{M}_n(\mathbb{C}) \to \mathrm{M}_n(\mathbb{C}), (P, M) \mapsto PMP^{-1}$ は作用である．

例：$(\mathrm{GL}_m(\mathbb{C}) \times \mathrm{GL}_n(\mathbb{C})) \times \mathrm{M}_{m,n}(\mathbb{C}) \to \mathrm{M}_{m,n}(\mathbb{C}), ((P, Q), M) \mapsto PMQ^{-1}$ は作用である．

注意：群 G, H について，直積群 $G \times H$ がいつもの方法で定義され，いつもの普遍性をもつ．

例：群 G の部分群 H について，$G \times (G/H) \to G/H, (g, [g']) \mapsto [gg']$ は作用である．

例：$\mathrm{M}_n(\mathbb{C}) \times \mathbb{C}^n \to \mathbb{C}^n$ は (1),(2) を満たすが，$(\mathrm{M}_n(\mathbb{C}), \cdot, E_n)$ は群ではないので，作用ではない．ただしこの写像で $\mathbb{C}^n$ は左 $\mathrm{M}_n(\mathbb{C})$ 加群となる．

記法：群作用 $G \times X \to X$ において，

(1) $Gx := \{ gx \mid g \in G \}$ を $x \in X$ の G 軌道という．
(2) $\mathrm{Stab}_G(x) := \{ g \in G \mid gx = x \}$ を x の固定（化）部分群という．
(3) $x \in X$ が固定点とは，$\mathrm{Stab}_G(x) = G$ となること（i.e.,$\forall g \in G, gx = x$）．

命題：群作用 $G \times X \to X$ において，

(1) $x \sim x' \Leftrightarrow Gx = Gx'$（ここで $x, x' \in X$）は X 上の同値関係である．
(2) 任意の $x \in X$ について，$G/\mathrm{Stab}_G(x) \xrightarrow{\sim} Gx, [g] \mapsto gx$ は全単射．

証明：(1) は容易．(2) は集合の準同型定理を用いる．$gx = g'x \Leftrightarrow g^{-1}g' \in \mathrm{Stab}_G(x)$ を確認すればよいが，易しい．

例：$\mathfrak{S}_X \times X \to X, (f, x) \mapsto f(x)$ において，$\forall x \in X, \mathfrak{S}_X x = X$.

例：$\mathrm{GL}_n(\mathbb{C}) \times \mathrm{M}_n(\mathbb{C}) \to \mathrm{M}_n(\mathbb{C}), (P, M) \mapsto PMP^{-1}$ において，$M \in \mathrm{M}_n(\mathbb{C})$ の軌道の代表として $\mathrm{JNF}(M)$ を取ることができる．

例：$(\mathrm{GL}_m(\mathbb{C}) \times \mathrm{GL}_n(\mathbb{C})) \times \mathrm{M}_{m,n}(\mathbb{C}) \to \mathrm{M}_{m,n}(\mathbb{C}), ((P, Q), M) \mapsto PMQ^{-1}$ において，$M \in \mathrm{M}_{m,n}(\mathbb{C})$ 軌道の代表としてランク標準形を取ることができる．

例：$G \times (G/H) \to G/H, (g, [g']) \mapsto [gg']$ において，$\forall [g] \in G/H, G[g] = G/H$ で $\mathrm{Stab}_G([e]) = H$.

記法：群 G について，$G \times G \to G, (g, x) \mapsto gxg^{-1}$ は作用である（共役作用）．

(1) $x \in G$ の軌道 $Gx =: \mathrm{Conj}_G(x) = \{gxg^{-1} \mid g \in G\}$ を x の共役類.
(2) $x \in G$ の固定部分群 $\mathrm{Stab}_G(x) =: C_G(x) = \{g \in G \mid gx = xg\}$ を x の中心化部分群.
(3) $\bigcap_{x \in G} \mathrm{Stab}_G(x) =: Z(G) = \{g \in G \mid \forall h \in G, gh = hg\}$ を G の中心.

例：$\mathfrak{S}_3 := \mathfrak{S}_{\{1,2,3\}} = \mathrm{Bij}(\{1, 2, 3\})$ を考える（3 次対称群）．$f \in \mathfrak{S}_3$ を $\begin{pmatrix} 1 & 2 & 3 \\ f(1) & f(2) & f(3) \end{pmatrix}$ と書く（2 行表示）．共役類は以下の 3 つである．

- $\mathrm{Conj}_{\mathfrak{S}_3}\left(\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}\right) = \left\{\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}\right\}$（単位元）．
- $\mathrm{Conj}_{\mathfrak{S}_3}\left(\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\right) = \left\{\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}\right\}$，（互換）．
- $\mathrm{Conj}_{\mathfrak{S}_3}\left(\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\right) = \left\{\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}\right\}$（巡回置換）

記法：有限群 G について

$$G = \bigsqcup_{x \in Y} \mathrm{Conj}_G(x)$$

となるように，共役類から代表を集めた集合 $Y \subseteq G$ を取る．このうち $\mathrm{Conj}_G(y) = \{y\} \Leftrightarrow y \in Z(G)$ より（ここで $y \in G$），以下が成り立つ（類等式）．

$$|G| = |Z(G)| + \sum_{y \in Y \setminus Z(G)} |\mathrm{Conj}_G(y)|.$$

系：$\mathfrak{S}_3$ に位数 2 の正規部分群は存在しない（注：もちろん何も使わずに簡単に確認可能）．

証明：類等式 $6 = 1 + 3 + 2$ で 1 と他を使って 2 を作ることができないから（正規部分群が共役類の和集合であることを用いた）．

定義：p を素数とする．

(1) 有限群 P が p 群 $\Leftrightarrow \exists n \geq 0, |P| = p^n$.
(2) 有限群 G の p 部分群 $P \subseteq G$ が p シロー部分群 $\Leftrightarrow |G|/|P| \notin p\mathbb{Z}$.

定理：p を素数，G を有限群，$\mathrm{Syl}_p(G) := \{P \subseteq G \mid P$ は G の p シロー部分群 $\}$ とする．

(1) $\forall H \subseteq G$：p 部分群, $\exists P \in \mathrm{Syl}_p(G), H \subseteq P$.
(2) $\forall P_1 \in \mathrm{Syl}_p(G), \forall P_2 \in \mathrm{Syl}_p(G), \exists g \in G, gP_1g^{-1} = P_2$.
(3) $|\mathrm{Syl}_p(G)| \equiv 1 \pmod p$.

証明:$|G| = p^n m$ とする$(n \geq 0, m \notin p\mathbb{Z})$．$X := \{S \subseteq G \mid |S| = p^n\}$ について, $|X| = \binom{p^n m}{p^n} \notin p\mathbb{Z}$ は難しくない初等整数論の問題である．

よって $G \times X \to X, (g, S) \mapsto gS$ という作用で，$|GS| \notin p\mathbb{Z}$ となる軌道が取れる．今，$\mathrm{Stab}_G(S) =: P_0 \in \mathrm{Syl}_p(G)$ を示そう．$|GS| = |G|/|P_0|$ より，$|P_0| \geq p^n$．また $P_0S = S$ なので，$s \in S$ について $P_0s \subseteq S$．s を右からかける写像 $\cdot s : G \to G$ は単射なので $|P_0| \leq p^n$.

以上で $\mathrm{Syl}_p(G) \neq \emptyset$ が分かった．$Y := \{gP_0g^{-1} \mid g \in G\}$ とし，作用

$$H \times Y \to Y, \quad (h, Q) \mapsto hQh^{-1}$$

を考える．$|Y| = |G|/|\mathrm{Stab}_G(P_0)|$ は $|G|/|P_0|(\notin p\mathbb{Z})$ を割り切るので，$|Y| \notin p\mathbb{Z}$ である．したがって Y のある H 軌道は $p^0 = 1$ 個の元からなる．これを $Q \in Y$ とすると $HQ = QH$ なので，HQ は G の部分群で $Q \trianglelefteq HQ$．今，合成 $H \hookrightarrow HQ \twoheadrightarrow HQ/Q$ に準同型定理を適用して $H/(H \cap Q) \xrightarrow{\sim} HQ/Q$. よって $|H||Q| = |HQ||H \cap Q|$ で，左辺は p のべきなので $|HQ|$ もそうである．$Q \subseteq HQ$ と $Q \in Y \subseteq \mathrm{Syl}_p(G)$ より $HQ = Q$．特に $H \subseteq Q$．よって (1) が示された．

(2) を示す．$H \in \mathrm{Syl}_p(G)$ なら $\exists g \in G, H = Q = gP_0g^{-1}$.

(3) を示す．(2) より $Y = \mathrm{Syl}_p(G)$ で，固定した $I \in \mathrm{Syl}_p(G)$ について，Y の I 軌道が 1 つの元からなるものは I 自身．よって $|Y| \equiv 1 \pmod p$.

注意：群 G_1, G_2 について，直積群 $G_1 \times G_2$ が構成できた．

命題：群 G の正規部分群 $G_1, G_2 \trianglelefteq G$ が

$$G_1 \cap G_2 = \{e\}, \quad G = G_1G_2 := \{g_1g_2 \mid g_1 \in G_1, g_2 \in G_2\}$$

ならば，$G_1 \times G_2 \to G, (g_1, g_2) \mapsto g_1g_2$ は同型．

証明：問題の写像を φ とする．仮定より φ は全射．また $\varphi(g_1g_2) = e$ とすると，$g_1^{-1} = g_2 \in G_1 \cap G_2$ より $g_1 = g_2 = e$．よって φ は単射である．φ が群準同型であることを示すため，$\forall g_1 \in G_1, \forall g_2 \in G_2, g_1g_2 = g_2g_1$ を示す．これは $g_1g_2g_1^{-1}g_2^{-1} \in G_1 \cap G_2$ から従う．

定義：群 H, N と群準同型 $f : H \to \mathrm{Aut}(N)$ について，直積集合 $N \times H$ は，次の演算によって群になることが確認できる．これを H と N の f による半直積といって，$N \rtimes_f H$ と書く．

$$(n, h)(n', h') = (nf(h)(n'), hh').$$

注意：$\forall h \in H, f(h) = \mathrm{id}_N$ なら $N \rtimes_f H = N \times H$（群として）．

記法：群 G について，$\mathrm{Aut}(G) := \{\varphi : G \xrightarrow{\sim} G \mid G$ は群同型 $\}$ は合成で群になる．

命題：群 G の正規部分群 N と部分群 H について，$H \cap N = \{e\}, G = NH$ ならば

$$N \rtimes_f H \to G, \quad (n, h) \mapsto nh$$

は同型．ここで $f : H \to \mathrm{Aut}(N), h \mapsto (f(h) : N \to N, n \mapsto hnh^{-1})$.

証明：問題の写像 φ が群準同型であることを示せばよい．

例：$A \in \mathrm{GL}_n(\mathbb{R}), \boldsymbol{b} \in \mathbb{R}^n$ について，

$$\mathrm{Aff}(\boldsymbol{b}, A) : \mathbb{R}^n \to \mathbb{R}^n, \quad \boldsymbol{x} \mapsto A\boldsymbol{x} + \boldsymbol{b}$$

を考える．$\mathrm{Aff}(\boldsymbol{b}_1, A_1) \circ \mathrm{Aff}(\boldsymbol{b}_2, A_2) = \mathrm{Aff}(\boldsymbol{b}_1 + A_1\boldsymbol{b}_2, A_1A_2)$ は簡単に確認できるので，

$$\mathrm{Aff} := \{\mathrm{Aff}(\boldsymbol{b}, A) \mid A \in \mathrm{GL}_n(\mathbb{R}), \boldsymbol{b} \in \mathbb{R}^n\}$$

は $\mathrm{Aff} \cong \mathbb{R}^n \rtimes_T \mathrm{GL}_n(\mathbb{R})$ が分かる．ここで

$$T : \mathrm{GL}_n(\mathbb{R}) \to \mathrm{Aut}(\mathbb{R}^n), \quad A \mapsto (T(A) : \mathbb{R}^n \to \mathbb{R}^n, \boldsymbol{x} \mapsto A\boldsymbol{x}).$$

記法：以下，位数の小さな有限群の分類を考える．$n \geq 1$ について，加法群 $\mathbb{Z}/n\mathbb{Z}$ を C_n と書く．

命題：$n \geq 1$ について，有限群 G が $|G| = n$ かつ $\exists g \in G, \mathrm{ord}_G(g) = n$ ならば $G \cong C_n$.

証明：明らか（全射群準同型 $\mathbb{Z} \twoheadrightarrow G, m \mapsto g^m$ に準同型定理を適用する）．

系：素数 $p \geq 2$ について，有限群 G が $|G| = p$ ならば $G \cong C_p$.

証明：$e \neq g \in G$ について，$\mathrm{ord}_G(g) \mid p$ より，$\mathrm{ord}_G(g) = p$.

補題：有限群 G の部分群 A, B について，$|AB||A \cap B| = |A||B|$.

証明:$A \times B$ は $(a, b)g := agb^{-1}$ によって G に作用する．$(A \times B)e = AB$ かつ $\mathrm{Stab}_{A \times B}(e) \cong A \cap B$.

注意：A, B の少なくともどちらかが正規なら $AB = BA$ は G の部分群なのだった．

命題：素数 $p \geq 2$ と有限群 G について，$|G| = p^2$ ならば，$G \cong C_{p^2}$ または $G \cong C_p \times C_p$.

証明：$\forall g \in G, \mathrm{ord}_G(g) < p^2$ を仮定すると，$e \neq a \in G$ について $\mathrm{ord}_G(a) = p$ である．また $b \in G \setminus \langle a \rangle$ についてもそうである．ここで $\langle a \rangle := \{a^n \mid n \in \mathbb{Z}\}$．$G_1 := \langle a \rangle, G_2 := \langle b \rangle$ とす

ると，$G_1 \cap G_2 = \{e\}$ から $G_1G_2 = G$ が分かる．これと以下の補題より $G_1, G_2 \trianglelefteq G$．よって $G \cong G_1 \times G_2 (\cong C_p \times C_p)$.

補題：素数 $p \geq 2$ と有限群 G について，$|G| = p^2$ ならば $G = Z(G)$.

証明：類等式 $|G| = |Z(G)| + \sum_{[x] \in (G \setminus Z(G))/\text{共役}} |\operatorname{Conj}_G(x)|$ と，$|\operatorname{Conj}_G(x)| = |G|/|C_G(x)| (> 1)$ より，$|Z(G)| \in p\mathbb{Z}$．$|Z(G)| = p$ なら $G/Z(G) \cong C_p$．これは以下の補題に矛盾する．

補題：群 G の正規部分群 N が $N \subseteq Z(G)$ と仮定する．$\exists n \geq 1, G/N \cong C_n$ ならば G は可換群.

証明：$[a] \in G/N$ が位数 n とすると，$g \in G$ は $a^i z$ の形に書ける（ここで $0 \leq i < n, z \in N$）.

補題：素数 $p > q \geq 2$ と，有限群 G について，$|G| = pq$ ならば $|\operatorname{Syl}_p(G)| = 1$.

証明：$k_p = |\operatorname{Syl}_p(G)|$ とすると，$k_p \equiv 1 \pmod p$ かつ，すべての p シロー部分群は互いに共役だったので $|G| = pq \in k_p\mathbb{Z}$．これから $k_p = 1$.

系：前の補題で，さらに $p \not\equiv 1 \pmod q$ とすると，$G \cong C_{pq}$.

証明：同様に $k_q := |\operatorname{Syl}_q(G)|$ は $k_q = 1$ である．$\operatorname{Syl}_p(G) = \{P\}, \operatorname{Syl}_q(G) = \{Q\}$ としたとき，$P, Q \trianglelefteq G$ で，$P \cap Q = \{e\}$ より $G = PQ$．故に $G \cong P \times Q$.

定義：$n \geq 2$ について，以下を二面体群という．

$$D_n = \left\{ R_k := \begin{pmatrix} \cos k\theta_n & \sin k\theta_n \\ \sin k\theta_n & \cos k\theta_n \end{pmatrix}, S_k := \begin{pmatrix} \cos k\theta_n & \sin k\theta_n \\ \sin k\theta_n & -\cos k\theta_n \end{pmatrix} \mid 0 \leq k < n \right\} (\subseteq \mathrm{GL}_2(\mathbb{R})).$$

注意：以下の交換関係が成立（ただし添字は mod n で見る）.

$$R_iR_j = R_{i+j}, \quad R_iS_j = S_{i+j}, \quad S_iR_j = S_{i-j}, \quad S_iS_j = R_{i-j}.$$

命題：奇素数 $p \geq 3$ と有限群 G について，$|G| = 2p$ ならば $G \cong C_{2p}$ または $G \cong D_p$.

証明：$\operatorname{Syl}_p(G) = \{P\}$ となっている．また $C \in \operatorname{Syl}_2(G)$ を取る．$P \cap C = \{e\}, PC = G, P \trianglelefteq G$ より，$\exists f : C \to \operatorname{Aut}(P), G \cong P \rtimes_f C$ となっている．

以下より $C = \{e, g\}$ について，$f(g) = \mathrm{id}_P$ または $f(g)(h) = h^{-1}$ でなければならない．ただし $P = \{e, h, \cdots, h^{p-1}\}$ とした．前者が C_{2p} に，後者が D_p に対応する．

補題：$n \geq 1$ について，$\operatorname{Aut}(C_n) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.

証明：群準同型 $C_n = \mathbb{Z}/n\mathbb{Z} \xrightarrow{\varphi} C_n$ は，$\varphi([1])$ を決めると決まる．$\varphi([1]) = [x]$ のとき，$(x, n) = 1$ ならば φ は単射で逆も正しい.

注意：同様にして，奇素数 $p > q \geq 3$ についても $|G| = pq$ なる G を $p \equiv 1 \pmod q$ の条件下で分類でき，2 種類あることが分かる．$(\mathbb{Z}/p\mathbb{Z})^\times \cong C_{p-1}$（原始根の存在定理）を用いるが，これは以下で扱う．

定理（有限アーベル群の分類定理）：$\forall G$：有限アーベル群, $\exists! s \geq 1, \exists! d_1 \in \mathbb{Z}_{\geq 2}, \cdots, \exists! d_s \in \mathbb{Z}_{\geq 2}$, s.t.,

(1) $d_1 | d_2 | \cdots | d_s$.
(2) $G \cong C_{d_1} \times \cdots \times C_{d_s}$.

注意：この $(d_1, \cdots, d_s)$ を G のねじれ不変量という．証明は JNF と同時に最後で扱う．G の同型類はねじれ不変量で決まることも証明できる．

例：位数 8 のアーベル群 G のねじれ不変量は (8),(2,4),(2,2,2) がありえる．よって位数 8 のアーベル群の同型類は 3 つあり，代表は $C_8, C_2 \times C_4, C_2 \times C_2 \times C_2$.

注意：位数 8 の非アーベル群は D_4 または $\{\pm 1, \pm i, \pm j, \pm k\} \subseteq \mathbb{H}$（4 元数群）のどちらかに同型であることが，少し頭を使うと証明できる．

注意：位数が 2 のべきの有限群の同型類は特にたくさんあることが知られている．位数 2000 以下の有限群の同型類は全部で $49483365422 + 423164062$ 個あるらしい．このうち前者が 2^{10} の群だそうである．ちなみに位数 2^{11} の群は，1770 兆個程度と同型類の個数が見積もられている．

応用（原始根の存在定理）：素数 $p \geq 2$ について，$(\mathbb{Z}/p\mathbb{Z})^\times \cong C_{p-1}$.

証明：$(\mathbb{Z}/p\mathbb{Z})^\times \cong C_{d_1} \times \cdots \times C_{d_s}$ とする（$s \geq 1$ で $2 \leq d_1 | \cdots | d_s$）．このとき $\mathbb{Z}/p\mathbb{Z}$ には，$x^{d_1} = 1$ の解が少なくとも d_1^s 個ある．これは $(\mathbb{Z}/p\mathbb{Z})[x]$ において，$x^{d_1} - 1 = 0$ の解が高々 d_1 個しかないことに矛盾する（多項式の除法と因数定理と $\mathbb{Z}/p\mathbb{Z}$ が整域であることを用いた）．

系（ウィルソンの定理）：素数 $p \geq 2$ について，$(p-1)! \equiv -1 \pmod{p}$.

証明：$(\mathbb{Z}/p\mathbb{Z})^\times = \{g^0, \cdots, g^{p-2}\}$ とすると，$p \geq 3$ なら $(p-1)! \equiv g^{(p-1)(p-2)/2} \equiv g^{-(p-1)/2} \pmod{p}$．再び $\mathbb{Z}/p\mathbb{Z}$ で $x^2 = 1$ の解は $x = \pm 1$ に限ることを用いると，$g^{-(p-1)/2} \equiv -1 \pmod{p}$ でなければならない．

注意：実は次が知られている（この講義では扱わない）．

(1) $e \geq 3$ ならば $(\mathbb{Z}/2^e\mathbb{Z})^\times \cong C_2 \times C_{2^{e-2}}$.
(2) 奇素数 $p \geq 3$ と $e \geq 1$ について，$(\mathbb{Z}/p^e\mathbb{Z})^\times \cong C_{\varphi(p^e)}$.

これを用いるとウィルソンの定理の次の一般化も容易に得られる．

系：$n \geq 2$ について，$\displaystyle\prod_{1 \leq m < n, \gcd(m,n)=1} m \equiv \pm 1 \pmod{n}$．さらに -1 になることと $n = 2, 4, p^e, 2p^e$ の形をしていることは同値（ここで $p \geq 3$ は奇素数で $e \geq 1$）．

注意：$\mathbb{Z}/6\mathbb{Z}$ で，$2 \cdot 3 = 0$ なので，$(x-1)(x-2) = 0$ は $x = 4, 5$ も解に持つ．

注意：$\mathbb{H}$ で $x^2 + 1$ は $i \cos\theta + j \sin\theta$ を「解に持つ」．しかし $\mathbb{H}$ は非可換なので，多項式や代入の意味を明確にしなければならない．また「共役」を考えることで，n 次多項式の解は共役を除いて高々 n 個である，という結果も導出できる．

定義：以下，特別な群として対称群を扱う．$n \geq 0$ について，$\mathfrak{S}_n := \mathrm{Bij}(\{1, \cdots, n\})$（$n = 0$ なら $\mathfrak{S}_0 = \{\mathrm{id}_\emptyset : \emptyset \to \emptyset\}$ である」）．

定理（ケーリー）：任意の有限群 G は，ある $\mathfrak{S}_n$ の部分群に同型である．

証明：$G = \{g_1, \cdots, g_n\}$ とし，$h \in G$ について $hg_i = g_{\varphi_h(i)}$ によって $\varphi_h \in \mathfrak{S}_n$ を定めると，$G \to \mathfrak{S}_n, h \mapsto \varphi_h$ は群準同型かつ単射が分かる．

記法：$1 \leq i \neq j \leq n$ について，$i \mapsto j, j \mapsto i$ となる互換（$\mathfrak{S}_n$ の元）を (i, j) と書く．$(i, j) = (j, i)$ である．また, 相異なる $1 \leq i_1, \cdots, i_k \leq n$ について, $i_1 \mapsto i_2 \mapsto i_3 \mapsto \cdots \mapsto i_{k-1} \mapsto i_k \mapsto i_1$ なる巡回置換を $(i_1, i_2, \cdots, i_k)$ と書く．$(i_1, i_2, \cdots, i_k) = (i_2, i_3, \cdots, i_k, i_1) = \cdots = (i_k, i_1, \cdots, i_{k-1})$ である．

例：任意の $g \in \mathfrak{S}_n$ は互換の積で書くことができる．このとき必要な互換の数の偶奇は，g のみに依ることが，線形代数の行列式の定義で行ったようによく知られている．

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1, 2, 3) = (1, 2)(2, 3), \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1, 3, 2) = (2, 3)(1, 2).$$

系：$\mathfrak{A}_n := \mathrm{Ker}(\mathrm{sign} : \mathfrak{S}_n \to \{\pm 1\})$ を n 次交代群という．

記法：$g \in \mathfrak{S}_n$ を互いに交わらない巡回置換の積で書くことができる．これは巡回置換の順序を除いてただ 1 通りであり，巡回置換の長さを並べて得られる n の分割を g のサイクル型と（この講義では）言って，$\mathrm{cycletype}(g)$ と書く．

例：$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 4 & 5 & 2 & 1 & 6 & 8 & 7 \end{pmatrix} \in \mathfrak{S}_8$ は $g = (1, 3, 5)(2, 4)(6)(7, 8)$ なので，$\mathrm{cycletype}(g) = (3, 2, 2, 1)$．これは 8 の分割である．

記法：$\mathrm{Par} := \{\lambda = (\lambda_1 \geq \cdots \geq \lambda_\ell \geq 1) | \forall i, \lambda_i \in \mathbb{Z}_{\geq 1}\}$ の元を整数の分割，$\mathrm{Par}(n) := \{\lambda = (\lambda_1, \cdots, \lambda_\ell) | \sum_{i=1}^{\ell} \lambda_i = n\}$ の元を n の分割という．また, 同じ部分をまとめて $(5, 4, 2, 2, 1, 1, 1, 1) = (5, 4, 2^2, 1^4) \in \mathrm{Par}(17)$ のようにも書く．

命題：$g, g' \in \mathfrak{S}_n$ が共役 $\Leftrightarrow \mathrm{cycletype}(g) = \mathrm{cycletype}(g')$.

証明：$\varphi \in \mathfrak{S}_n$ について，$\varphi(i_1, \cdots, i_k)\varphi^{-1} = (\varphi(i_1), \cdots, \varphi(i_k))$.

命題：$\lambda = (1^{m_1}, 2^{m_2}, \cdots, n^{m_n}) \in \mathrm{Par}(n)$（つまり $\sum_{i=1}^n i m_i = n$）について，$z_\lambda := \prod_{i=1}^n i^{m_i} m_i!$ とする．このとき $|\{g \in \mathfrak{S}_n \mid \mathrm{cycletype}(g) = \lambda\}| = n!/z_\lambda$.

証明：$g_0 = (1)(2) \cdots (m_1)(m_1 + 1, m_1 + 2) \cdots (m_1 + 2m_2 - 1, m_1 + 2m_2) \cdots (n - m_n + 1, \cdots, n)$ について，$|\mathrm{Stab}_{\mathfrak{S}_n}(g_0)| = z_\lambda$.

例：$\mathfrak{S}_5$ において，ありえるサイクル型は

$$\mathrm{Par}(5) = \{(5), (4, 1), (3, 2), (3, 1, 1), (2, 2, 1), (2, 1^3), (1^5)\}$$

それぞれ z_λ は 5,4,6,6,8,12,120 なので，それぞれのサイクル型の共役類は 24,30,20,20,15,10,1 個.

例：詳しくは述べないが，$\mathfrak{A}_n$ においても，共役類を分割の言葉で記述することができる．上の $\mathfrak{S}_5$ のサイクル型 λ の共役類を C_λ と書くと，$C_\lambda \subseteq \mathfrak{A}_5$ となる $\lambda \in \mathrm{Par}(5)$ は，$\lambda = (5), (3, 1^2), (2^2, 1), (1^5)$ に限る．このうち $C_{(5)}$ は $\mathfrak{A}_5$ の共役類としては 2 つに分かれ，それぞれの代表として $(1, 2, 3, 4, 5), (1, 2, 3, 5, 4)$ が取れることが確認できる．

系：$N \trianglelefteq \mathfrak{A}_5 \Rightarrow N = \{e\}, \mathfrak{A}_5$

証明：$\mathfrak{A}_5$ の類等式は $60 = 1 + 15 + 20 + 12 + 12$ である．1 を含む和で 60 の真の約数 2,3,4,5,6,10,12,15,20,30 を作ることはできない．

定義：単位群でない有限群 G が単純群とは：$N \trianglelefteq G \Leftrightarrow N = \{e\}, G$.

注意：$\{e\} \trianglelefteq N \trianglelefteq G$ なる N があれば，G は N と G/N から「構成されている」と考えることができ（群拡大），有限単純群は有限群の「原子」のようなものと思うことができる．

事実：$n \geq 5$ について，$\mathfrak{A}_n$ は単純群である（証明はちょっとしたパズルである．この講義では $n = 5$ のときのみ，類等式に基づくものを述べた）．

注意：素数 $p \geq 2$ について，C_p は単純群である．

1980 年代に，有限単純群が分類されたとされている．それによると，上記に加えて

- 線形代数に由来する無限系列（リー型有限群）
- 26 個の例外的な群（散在型）

とされる．このうち散在型で位数最大のもの（$\mathbb{M}$ と書かれる）は

$$|\mathbb{M}| = 2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^2 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71 = 8 \times 10^{53}$$

であり，$\mathrm{GL}_n(\mathbb{C})$ の部分群として実現しようとすると，可能な最小の n は $n = 196883$ であることが知られている．古典的に知られている j 関数

$$j(q) = \frac{1}{q} + 744 + 196884q + 21493760q^2 + \cdots$$

の係数との類似は偶然ではない（ムーンシャイン現象）．

$\mathfrak{A}_5$ は正 20 面体を保つ群である（パズル）．このように群は対称性の根拠となる深い対象と関連して理解できると望ましい．26 個の例外群は，数学における例外的な現象（例えば 24 次元におけるリーチ格子の存在）などと関係していると考えられる．最大限誇張していうならば，$\mathbb{M}$ は「場の理論の対称性」として理解される．

注意：位数 2^{10} の有限群（500 億程度存在するのだった）のうち，単純群の 2 シロー部分群になれるのは 11 個であることが知られている．