Recall G_1, G_2：群 $\rightsquigarrow$ $G_1 \times G_2$：直積群

prop G：群 $\triangleright$ G_1, G_2：正規部分群 s.t. $G_1 \cap G_2 = \{e\}$
$G = G_1 G_2 := \{ g_1 g_2 \mid \begin{matrix} g_1 \in G_1 \\ g_2 \in G_2 \end{matrix} \}$

このとき $G_1 \times G_2 \longrightarrow G$ は同型
$(g_1, g_2) \longmapsto g_1 g_2$

(:) 問題の写像をφとする。仮定よりφは全射。又, $\varphi(g_1, g_2) = e$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, $\forall g_1 \in G_1$, $\forall g_2 \in G_2$, $g_1 g_2 = g_2 g_1$ を示す。
これは $g_1 g_2 g_1^{-1} g_2^{-1} \in G_1 \cap G_2$ から従う //

Def H, N：群, $f : H \to Aut(N)$：群準同型について
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 による半直積と言って $N \underset{f}{\times} H$ と書く。
$(n, h) \cdot (n', h') := (n f(h)(n'), hh')$
(注) $\forall h \in H, f(h) = id_N$ なら $N \underset{f}{\times} H = N \times H$ (群として)

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

prop G：群, $N \triangleleft G$, $H \subseteq G$：正規部分群と部分群 s.t. $H \cap N = \{e\}$
$G = NH$
について $N \underset{f}{\times} H \longrightarrow G$ は同型。ここで $f : H \to Aut(N)$
$(n, h) \longmapsto nh$
$h \mapsto f(h) : N \to N$
$n \mapsto hnh^{-1}$

(:) 問題の写像φが群準同型であることを示せばよい。//

例 $A \in GL_n(\mathbb{R})$, $\vec{b} \in \mathbb{R}^n$ について, $\left(\begin{array}{l} Aff(\vec{b}, A) : \mathbb{R}^n \to \mathbb{R}^n \\ \qquad\qquad \vec{x} \mapsto A\vec{x} + \vec{b} \end{array} \right) \in Bij(\mathbb{R}^n)$ を考える。

$Aff(\vec{b_1}, A_1) \circ Aff(\vec{b_2}, A_2) = Aff(\vec{b_1} + A\vec{b_2}, A_1A_2)$ は簡単にcheckできるので

$Aff := \{ Aff(\vec{b}, A) \mid \begin{array}{l} A \in GL_n(\mathbb{R}) \\ \vec{b} \in \mathbb{R}^n \end{array} \}$ は $Aff \cong \mathbb{R}^n \rtimes_T GL_n(\mathbb{R})$ が分かる。

ここで $T : GL_n(\mathbb{R}) \to Aut(\mathbb{R}^n)$

$$A \longmapsto T(A) : \begin{array}{l} \mathbb{R}^n \to \mathbb{R}^n \\ \vec{x} \mapsto A\vec{x} \end{array}$$

以下, 位数の小さな有限群の分類を考える。

記法 $n \geq 1$ について 加法群 $\mathbb{Z}/n\mathbb{Z}$ を C_n と書く。

prop $n \geq 1$ について, 有限群 G が $|G| = n$ かつ $\exists g \in G$ s.t. $ord_G(g) = n$ ならば $G \cong C_n$

☺ 明らか (群準同型 $\begin{array}{l} \mathbb{Z} \twoheadrightarrow G \\ n \mapsto g^n \end{array}$ に準同型定理を適用する)

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

☺ $\forall g \in G \setminus \{e\}$ について $ord_G(g) \mid p$ より $ord_G(g) = p$ //

Lemma G : 有限群 $\supseteq A, B$: 部分群 について $|AB| = \dfrac{|A| \cdot |B|}{|A \cap B|}$

☺ $A \times B$ は $(a,b) \cdot g := agb^{-1}$ によって G に作用する。e の orb 群が AB で $Stab_{A \times B}(e) \cong A \cap B$ はやさしい //

BA
=

(注) A, Bの少なくともどちらかが正規ならABはGの部分群なのだった。

Prop $p \geq 2$: 素数 について, $|G| = p^2 \Rightarrow G \cong C_{p^2}$ or $C_p \times C_p$
G: 有限群

(:) $\exists g \in G$, $\mathrm{ord}_G(g) = p^2$ を仮定する。$a \in G \setminus \{e\}$ について $\mathrm{ord}_G(a) = p$ である。
$\forall b \in G \setminus \langle a \rangle := \{a^n \mid n \in \mathbb{Z}\} \left(= \{a^0, \cdots, a^{p-1}\} \cong C_p\right)$ についてもそう。
$G_1 := \langle a \rangle$, $G_2 := \langle b \rangle$ とすると, $G_1 \cap G_2 = \{e\}$ から $G_1 G_2 = G$ が分かる。
これと以下より $G_1, G_2 \trianglelefteq G$。よって $G \cong G_1 \times G_2 \left(\cong C_p \times C_p\right)$ //

Lemma $p \geq 2$: 素数, G: 有限群 が $|G| = p^2 \Rightarrow G = Z(G)$

(:) 類等式 $|G| = |Z(G)| + \sum_{[x] \in (G \setminus Z(G))/\text{共役}} |\mathrm{Conj}_G(x)|$ と $|\mathrm{Conj}_G(x)| = \dfrac{|G|}{|C_G(x)|}$ より
$p \mid |Z(G)|$。$|Z(G)| = p$ なら $G/Z(G) \cong C_p$。これは以下に矛盾する。//

Lemma G: 群, $N \subseteq Z(G)$: 正規部分群。$\exists n$, $G/N \cong C_n \Rightarrow G$: 可換群

(:) $[a] \in G/N$ が位数 n とすると, $g \in G$ は $a^i z \left(\begin{smallmatrix} 0 \leq i < n \\ z \in N \end{smallmatrix}\right)$ の形に書ける //

Lemma $p > q \geq 2$: 素数, G: 有限群 s.t. $|G| = pq$ について $|\mathrm{Syl}_p(G)| = 1$

(:) $k_p = |\mathrm{Syl}_p(G)|$ とすると $k_p \equiv 1 \pmod p$ かつ, 全ての p-Sylow 群は互いに共役だったので
$k_p \mid |G|$ $(\text{i.e. } k_p = 1, q, p, pq)$ これから $k_p = 1$ //

系 前のLemmaで、さらに $p \not\equiv 1 \bmod q$ とすると、$G \cong C_{pq}$

(!) 同様に $n_q := Syl_q(G)$ は $n_q = 1$ である。$Syl_p(G) = \{P\}$, $Syl_q(G) = \{Q\}$ としたとき、$G \supset P, Q$ で $P \cap Q = \{e\}$ より $G = PQ$ $\therefore G \cong P \times Q$ //

Def $n \geq 2$ について、$D_n = \left\{ \underbrace{\begin{pmatrix} \cos k\theta_n & \sin k\theta_n \\ \sin k\theta_n & \cos k\theta_n \end{pmatrix}}_{=: R_k}, \underbrace{\begin{pmatrix} \cos k\theta_n & \sin k\theta_n \\ \sin k\theta_n & -\cos k\theta_n \end{pmatrix}}_{=: S_k} \middle| 0 \leq k < n \right\} \subseteq GL_2(\mathbb{R})$

を二面体群という。

(注) 交換関係 $R_i R_j = R_{i+j}$, $R_i S_j = S_{i+j}$, $S_i R_j = S_{i-j}$, $S_i S_j = R_{i-j}$ が成立。
ただし添字は $\bmod n$ でみる。

prop $p \geq 3$: 奇素数, G : 有限群 s.t. $|G| = 2p \Rightarrow G \cong C_{2p}$ or D_p

(!) $Syl_p(G) = \{P\}$ となっている。$\forall C \in Syl_2(G)$ をとる。$P \cap C = \{e\}$, $PC = G$
$P \trianglelefteq G$ より、$G \cong P \underset{f}{\times} C$ $(\exists f : C \to Aut(P))$ となっている。
以下より $C = \{e, g\}$ について $f(g) = id_P$ 又は $f(g)(h) = h^{-1}$ でなければならない。前者が C_{2p} に後者が D_p に対応する //
(ここで $P = \{e, h, \cdots, h^{p-1}\}$ とした)

Lemma $n \geq 1$ について $Aut(C_n) \cong (\mathbb{Z}/n\mathbb{Z})^\times$

(!) $C_n = \mathbb{Z}/n\mathbb{Z} \xrightarrow{\varphi} C_n$: 群準同型は $\varphi([1])$ 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) 同様にして奇素数 $p > q \geq 3$ についても $|G| = pq$ なる G を $p \equiv 1 \bmod q$ の条件下で分類でき、2種類あることが分かる。$(\mathbb{Z}/p\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$ を用いるがこれは後に報う。
(原始根の存在定理)

有限アーベル群について分類結果を述べる（証明はJNFと同時に最後で扱う）

Thm 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 $G \cong C_{d_1} \times \cdots \times C_{d_s}$

Rk この $(d_1, \cdots, d_s)$ を G のねじれ不変量と言う。

Ex G：位数8のアーベル群のねじれ不変量は (8) 又は $(2,4)$ 又は $(2,2,2)$ 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, $C_2 \times C_4$, $C_2 \times C_2 \times C_2$

Rk 位数8の非アーベル群は D_4，又は $\{\pm 1, \pm i, \pm j, \pm k\} \subseteq \mathbb{H}$（四元数群）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。

Rk 位数が2のべ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。このうち前者が位数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られている。

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

(:) $(\mathbb{Z}/p\mathbb{Z})^\times \sim C_{d_1} \times \cdots \times C_{d_s}$ $(s \geq 1, 2 \leq d_1 | \cdots | d_s)$ とする，$\mathbb{Z}/p\mathbb{Z}$ には位数 d_1 の
元が少なくとも d_1 コある。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 コ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） //

Cor（ウィルソンの定理） $p \geq 2$：素数
$\Rightarrow (p-1)! \equiv -1 \pmod p$

(:) $(\mathbb{Z}/p\mathbb{Z})^\times = \{g^0, \cdots, g^{p-1}\}$ とすると，$(p-1)! \equiv g^{\frac{p(p-1)}{2}} \equiv g^{\frac{p-1}{2}} \pmod p$。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 $g^{\frac{p-1}{2}} \equiv -1 \pmod p$ でなければならない //

実は次が知られている(この講義では多分扱わない)

Fact ① $e \geq 3$ ならば $(\mathbb{Z}/2^e\mathbb{Z})^\times \simeq C_2 \times C_{2^{e-2}}$

② $p \geq 3$: 奇素数, $e \geq 1$ について $(\mathbb{Z}/p^e\mathbb{Z})^\times \simeq C_{\varphi(p^e)}$

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えられる。

Cor $n \geq 2$ について $\prod_{\substack{1 \leq m < n \\ (m,n)=1}} m \equiv \pm 1 \pmod{n}$。さらに -1 になる $\Leftrightarrow n = 2, 4, p^e, 2p^e$ ($p \geq 3$: 奇素数, $e \geq 1$)

Rk $\mathbb{Z}/6\mathbb{Z}$ で $2 \cdot 3 = 0$ なので $(X-1)(X-2)=0$ は $X=4,5$ も解にもつ。

Rk $\mathbb{H}$ で X^2+1 は $i\cos\theta + j\sin\theta$ を"解にもつ"。しかし $\mathbb{H}$ は非可換なので多項式や代入の意味を正確にしなければならない。又, 共役を考えてみること。

以下, 特別な群として対称群を扱う。

Def $n \geq 0$ について $\mathfrak{S}_n := \mathrm{Bij}(\{1, \cdots, n\})$ ($n=0$ なら $\mathfrak{S}_0 = \{id_\phi : \phi \to \phi\}$ である)

Thm (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。

(!) $G = \{g_1, \cdots, g_n\}$ 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, $i \leftrightarrow j$ となる互換($\mathfrak{S}_n$ の元)を $(i\ j)$ と書く。$(i\ j) = (j\ i)$ である。

又, 互いに相異なる $1 \leq i_1, \cdots, i_k \leq n$ について $i_1 \to i_2 \to \cdots \to i_k \to i_1$ 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。

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、線形代数の行列式でやったように知られている。

Ex. $\mathfrak{S}_3 = \left\{ \begin{pmatrix} 1&2&3 \\ 1&2&3 \end{pmatrix}, \begin{pmatrix} 1&2&3 \\ 1&3&2 \end{pmatrix}, \begin{pmatrix} 1&2&3 \\ 2&1&3 \end{pmatrix}, \begin{pmatrix} 1&2&3 \\ 2&3&1 \end{pmatrix}, \begin{pmatrix} 1&2&3 \\ 3&1&2 \end{pmatrix}, \begin{pmatrix} 1&2&3 \\ 3&2&1 \end{pmatrix} \right\}$

$= e$, $= (2,3)$, $= (1,2)$, $= (1,2,3) = (1,2)(2,3)$, $= (1,3,2) = (2,3)(1,2)$, $= (1,3)$

系 $\mathrm{sgn} : \mathfrak{S}_n \to \{\pm 1\} (\subseteq \mathbb{C}^\times)$ は群準同型

$g \mapsto \begin{cases} 1 & (g\text{を表すのに必要な互換は偶数個}) \\ -1 & (\quad\text{〃}\quad\text{奇数〃}) \end{cases}$

Def $A_n := \mathrm{Ker}(\mathrm{sgn} : \mathfrak{S}_n \to \{\pm 1\})$ 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。

Ex $g = \begin{pmatrix} 1&2&3&4&5&6&7&8 \\ 3&4&5&2&1&6&8&7 \end{pmatrix} \in \mathfrak{S}_8$ 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 $\mathrm{Par} := \{ \lambda = (\lambda_1 \geq \cdots \geq \lambda_\ell \geq 1) \mid \forall i,\ \lambda_i \in \mathbb{Z} \}$ の元を整数の分割

$\mathrm{Par}(n) := \{ \lambda = (\lambda_1, \cdots, \lambda_\ell) \in \mathrm{Par} \mid \sum_{i=1}^{\ell} \lambda_i = n \}$ の元を n の分割

又、同じ部分をまとめて $(5,4,2,2,1,1,1,1) = (5,4,2^2,1^4) \in \mathrm{Par}(17)$ とも書く。

prop $g, g' \in \mathfrak{S}_n$ が共役 $\Leftrightarrow$ cycletype(g) = cycletype(g')

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

prop $\lambda = (1^{m_1}, 2^{m_2}, \cdots, n^{m_n}) \in \mathrm{Par}(n)$ (ここで $m_i \geq 0$) について

$$\left|\{ g \in \mathfrak{S}_n \mid \text{cycletype}(g) = \lambda \}\right| = n!/z_\lambda \quad \text{ここで } z_\lambda := \prod_{i=1}^{n} i^{m_i} \cdot m_i!$$

(!) $g_0 = \begin{pmatrix} 1 & \cdots & m_1 & m_1+1 & m_1+2 & \cdots \\ 1 & \cdots & m_1 & m_1+2 & m_1+1 & \cdots \end{pmatrix}$ について $\left|\mathrm{Stab}_{\mathfrak{S}_n}(g_0)\right| = z_\lambda$ //

(m_1 コ, m_2 コ)

Ex $\mathfrak{S}_5$ 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、それぞれの型の共役類は

24, 30, 20, 20, 15, 10, 1 個ある。

Ex 詳しくは述べないが 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、$C_\lambda \subseteq A_5$ 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 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 $(12345), (12354)$ がとれることが確認できる。

系 $N \trianglelefteq A_5 \Rightarrow N = \{e\}$ or $N = A_5$

(!) A_5 の類等式は $60 = 1+15+20+12+12$ である。1をふくむ和で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。//

Def G: 有限群が単純群とは $N \trianglelefteq G \Leftrightarrow G = \{e\}$ or $G = N$

$\Downarrow$

$\{e\}$

$\{e\} \trianglelefteq N \trianglelefteq G$ 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た（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。

Fact $n \geq 5$ について A_n は単純群である。

証明はちょっとしたパズルである。$n=5$ のときのみ，類等式にもとづくものを述べた。

Rk $p \geq 2$：素数について 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（M と書かれる）は，

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

であり，$GL_n(\mathbb{C})$ の部分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

$$J(q) = \frac{1}{q} + 744 + 196884q + 21493760q^2 + \cdots \qquad q = e^{2\pi i \tau}$$

の係数の類似は偶然ではない（ムーンシャイン現象）。

A_5 は正20面体を保つ群である（パズル）。このように群に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（たとえばリー4格子の存在）などと関係していると考えられる。最大限誇張して言うなら，M は"場の理論の対称性"として理解される。

Rk 位数 2^n の有限群のうち，単純群の2-Sylow群になれるのは11コであることが知られている。
（500億程度存在するのだった）