群とは3つ組 $(G,\cdot,e)$ で以下の公理をみたすもののことであった。

① $\forall a\in G\ \forall b\in G\ \forall c\in G\quad (ab)c=a(bc)$

② $\forall a\in G,\ ea=a=ae$

③ $\forall a\in G\ \exists b\in G,\ ab=e=ba$

ここで G：集合，$e\in G$：元，$\cdot: G\times G\to G$：写像（2項演算）である。

Def 群 $(G,\cdot,e)$ の部分集合 H は，3つ組 $(H,\cdot|_{H\times H},e)$ が①,②,③をみたすとき部分群と呼ばれる。

Remark 同値な条件として $H\neq\emptyset$ かつ $\forall a\in H\ \forall b\in H,\ ab^{-1}\in H$ は容易に分かる。

Def G：群，$H\subseteq G$：部分群について $g\sim g' \overset{\text{def}}{\Leftrightarrow} g^{-1}g'\in H$ $(g,g'\in G)$

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checkできる。

記法・$g\in G$ の同値類 $C_g=\{g'\in G\mid g\sim g'\}$ は $C_g=gH:=\{gh\mid h\in H\}$ であることが簡単に分かる。（$C_g=[g]$）

・同値関係による商集合を G/H と書く。（この講義では）

系 G：群，$H\subseteq G$：部分群について $G=\coprod_{[g]\in G/H} gH$ （集合としての等式）

系 G：有限群の部分群 H について $|H|$ は $|G|$ の約数

☺ $g\in G$ について $\varphi_g: G\to G$（$x\mapsto gx$）は $\varphi_{g^{-1}}\circ\varphi_g=\mathrm{id}$ で $\varphi_g(gH)=H$

より $|G|=|G/H|\cdot|H|$ が成立 //

Def G：有限群，$g \in G$について $\exists M \geq 1,\ g^M = e$ となる（$\because \exists a \neq b \geq 1,\ g^a = g^b$）
このMの最小値をgの位数と言い，$\mathrm{ord}_G(g)$と書く

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

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

応用 $\varphi(n) := \left|(\mathbb{Z}/n\mathbb{Z})^\times\right|$ $(n \geq 1)$ をオイラー関数という。

以下は易しい
- $(\mathbb{Z}/n\mathbb{Z})^\times = \{[a] \in \mathbb{Z}/n\mathbb{Z} \mid \gcd(a,n) = 1\}$
- $\varphi(n) = \left|\{1 \leq a \leq n \mid \gcd(a,n) = 1\}\right|$

系 $n \geq 1$，a：nと互いに素，$a^{\varphi(n)} \equiv 1 \pmod n$

例えば$p \geq 3$：奇素数について，$2^{p-1} \equiv 1 \pmod p$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。

prop 可換環$R_1, \cdots, R_s$について $(R_1 \times \cdots \times R_s)^\times = R_1^\times \times \cdots \times R_s^\times$ in $R_1 \times \cdots \times R_s$

☺ 明らか

系 $n = p_1^{e_1} \cdots p_s^{e_s}$ （$p_1 \sim p_s$は相異なる素数，$e_1, \cdots, e_s \geq 1$）について
$\varphi(n) = n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_s}\right)$

☺ CRTより $\mathbb{Z}/n\mathbb{Z} \simeq \left(\mathbb{Z}/p_1^{e_1}\mathbb{Z}\right) \times \cdots \times \left(\mathbb{Z}/p_s^{e_s}\mathbb{Z}\right)$。これと上のpropより
$\left|\left(\mathbb{Z}/p^e\mathbb{Z}\right)^\times\right| = p^e\left(1 - \frac{1}{p}\right)$ を言えばよいが（ここでp：素数，$e \geq 1$），易しい。 //

Remark 本当は上の議論で $R \simeq R'$（可換環の環同型）$\Rightarrow R^\times \simeq (R')^\times$（群同型，後述）を用いている。

Remark $g\sim g' \overset{\text{def}}{\iff} g'g'^{-1}\in H$ を $g\sim g' \overset{\text{def}}{\iff} g'g^{-1}\in H$ としても同様の議論が可能。このとき $g\in G$ の同値類 $[g]=C_g=Hg:=\{hg \mid h\in H\}$ となる。(この講義では) 商集合を $H\backslash G$ と書く。

Def G:群, $H\subseteq G$:部分群 が正規部分群 $\overset{\text{def}}{\iff} \forall g\in G,\ gH=Hg$ in G
($\iff \forall g\in G,\ g^{-1}Hg\subseteq H$)
(このとき $H\trianglelefteq G$ と書く)

prop G:群, $N\subseteq G$:正規部分群について, 商集合 G/N は以下の構造で
$(G/N, \cdot, e)$ 群になることが check できる。これを G の N による商群という。

2項演算 $\cdot: G/N\times G/N\to G/N$, 単位元 $[e]\in G/N$
$([a],[b])\mapsto [ab]$

☺ routine work.

Def G_1, G_2:群, 写像 $\varphi: G_1\to G_2$ が群準同型写像
$\overset{\text{def}}{\iff}$ ① $\forall g\in G_1, \forall g'\in G_1,\ \varphi(gg')=\varphi(g)\varphi(g')$
② $\varphi(e_1)=e_2$ (e_i は G_i の単位元)
③ $\forall g\in G_1,\ \varphi(g^{-1})=\varphi(g)^{-1}$
$\overset{\text{容易}}{\iff} \forall g\in G_1\ \forall g'\in G_1,\ \varphi(gg')=\varphi(g)\varphi(g')$

prop G:群, $N\subseteq G$:正規部分群について 自然な全射 $G\overset{\pi}{\twoheadrightarrow} G/N$
$g\mapsto [g]_N=gN=Ng$
は群準同型写像

☺ routine work.

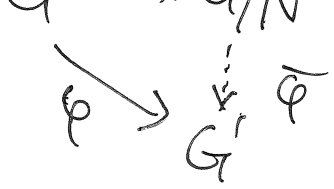
系 G:群 について 正規部分群と群準同型写像の核は同じ概念である。

☺ $\varphi: G\to G'$:群準同型の $\ker\varphi$ が正規であることは易しい。又, 上の π について
$\ker\pi=N$ //

prop (商群の普遍性) G: 群, $N \trianglelefteq G$: 正規部分群は以下の性質をもつ:

任意の群 G' と任意の群準同型写像 $\varphi: G \to G'$ 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 $\varphi = \overline{\varphi} \circ \pi$ なる群準同型 $\overline{\varphi}: G/N \to G'$ がただ1つ存在する。



☺ 商集合の普遍性より目的の写像 $\overline{\varphi}: G/N \to G'$ がただ1つ存在する。
これが群準同型であることは簡単にcheckできる。//

Thm (群の準同型定理) G, G': 群, $f: G \to G'$: 群準同型について
群同型 $G/\mathrm{Ker}\, f \xrightarrow{\sim} \mathrm{Im}\, f$ が成立。ここでおまけの以下のdefを用いている。

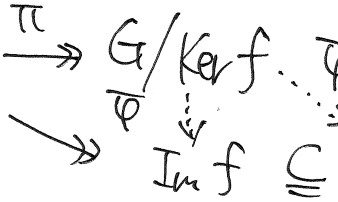
(**Def** $G \xrightarrow{\varphi} G'$: 群準同型が群同型 $\overset{\text{def}}{\iff} \exists \varphi: G' \to G$: 群準同型 s.t. $\varphi \circ \varphi = \mathrm{id}_G$, $\varphi \circ \varphi = \mathrm{id}_{G'}$
$\overset{\text{iff}}{\iff} \varphi$ は bij (環や加群のときと同様))

☺ $\mathrm{Im}\, f \subseteq G'$ が G' の部分群であることは簡単にcheckできる。

$\forall g_1 \in G\ \forall g_2 \in G,\ [g_1]_{\mathrm{Ker}\, f} = [g_2]_{\mathrm{Ker}\, f} \iff f(g_1) = f(g_2)$

(☺ $\Rightarrow$ $g_1^{-1} g_2 \in \mathrm{Ker}\, f$ より $f(g_1)^{-1} f(g_2) = e'$ $\therefore f(e_1) = f(e_2)$
$\Leftarrow$: 逆にたどる)

なので, $\Rightarrow$ と商群の普遍性より



全射群準同型 $G/\mathrm{Ker}\, f \xrightarrow{\overline{\varphi}} \mathrm{Im}\, f$ が存在し, $\Leftrightarrow$ なので $\overline{\varphi}$ は集合論的単射//
(よって bij)

Def 群Gの集合Xへの(左)作用とは以下をみたす写像$a: G\times X\to X$のことである。

① $\forall g_1\in G\ \forall g_2\in G\ \forall x\in X\quad a(g_1,g_2,x)=a(g_1,g_2x)$

② $\forall x\in X,\ a(e,x)=x$

記法 普通 $a(g,x)=gx$ のように書く

Ex 集合Xについて $\mathfrak{S}_X=Bij(X):=\{f: X\overset{\text{全}}{\to}X\}$ は合成に関して群をなす

$\mathfrak{S}_X\times X\to X$ は作用である

$(f,x)\mapsto f(x)$

Ex $GL_n(\mathbb{C})\times M_n(\mathbb{C})\to M_n(\mathbb{C})$ は作用である

$(P,M)\mapsto PMP^{-1}$

Ex $(GL_m(\mathbb{C})\times GL_n(\mathbb{C}))\times M_{m,n}(\mathbb{C})\to M_{m,n}(\mathbb{C})$ は作用である。

$((P,Q),M)\mapsto PMQ^{-1}$

ここで群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。

Ex G:群，H:部分群について，$G\times G/H\to G/H$ は作用である。

$(g,[g'])\mapsto[gg']$

Ex $M_n(\mathbb{C})\times\mathbb{C}^n\to\mathbb{C}^n$ は①②をみたすが，$(M_n(\mathbb{C}),\cdot,E_n)$ は群では

$(M,\vec{v})\mapsto M\vec{v}$

ないので群ではない。ただしこの写像で$\mathbb{C}^n$は$M_n(\mathbb{C})$加群となる。

軌道

記法① 群作用 $G \times X \to X$ $(g, x) \mapsto gx$ において, $Gx := \{gx \mid g \in G\}$ を $x \in X$ の軌道という。

② $Stab_G(x) := \{g \in G \mid gx = x\}$ を x の固定(化)部分群という。($Stab_G(x) = G$ のとき x は固定点と呼ばれる)

Ex $\widetilde{G_X} \times X \to X$ $(f, x) \mapsto f(x)$ において $\forall x \in X$, $\widetilde{G_X} \cdot x = X$

Ex $GL_n(\mathbb{C}) \times M_n(\mathbb{C}) \to M_n(\mathbb{C})$ $(P, M) \mapsto PMP^{-1}$ において, $\forall M \in M_n(\mathbb{C})$ の軌道の代表として $JNF(M)$ をとることが出来る

(注: $JNF(M)$ は存在を前回示した。一意性はまだ扱っていない)

Ex $(GL_m(\mathbb{C}) \times GL_n(\mathbb{C})) \times M_{m,n}(\mathbb{C}) \to M_{m,n}(\mathbb{C})$ $((P, Q), M) \mapsto PMQ^{-1}$ において,

$\forall M \in M_n(\mathbb{C})$ $\exists! r \geq 0$ s.t. $\exists P \in GL_m(\mathbb{C})$ $\exists Q \in GL_n(\mathbb{C})$ $PMQ^{-1} = \begin{pmatrix} E_r & O \\ O & O \end{pmatrix}$

Ex $G \times G/H \to G/H$ $(g, [g']) \mapsto [gg']$ において, $\forall [g] \in G/H$, $G[g] = G/H$ かつ $Stab_G([e]) = H$

prop 群作用 $G \times X \to X$ において

① $x \sim x' \overset{def}{\iff} Gx = Gx'$ ($x, x' \in X$) は X 上の同値関係である。

② $\forall x \in X$, $G/Stab_G(x) \xrightarrow{\sim} G \cdot x$ は全単射 $[g] \mapsto gx$

(ヒント) ① 容易 ② 集合の準同型定理を用いる。$gx = g'x \iff g^{-1}g' \in Stab_G(x)$ をcheckすればよいが、易しい。

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

① $x\in G$の軌道 $Gx=:Conj_G(x)=\{gxg^{-1}\mid g\in G\}$ をxの共役類 (conjugacy classes)

② $x\in G$の固定部分群 $Stab_G(x)=:C_G(x)=\{g\in G\mid gx=xg\}$ を
xの中心化部分群 (centralizer subgroup)

③ $\bigcap_{x\in G} Stab_G(x)=:Z(G)=\{g\in G\mid \forall h\in G,\ gh=hg\}$ をGの中心 (center)

Ex $\tilde{S}_3:=\tilde{S}_{\{1,2,3\}}=Bij(\{1,2,3\})$ を考える (3次対称群)

$f\in\tilde{S}_3$ を $\begin{pmatrix}1&2&3\\f(1)&f(2)&f(3)\end{pmatrix}$ と書く (2行表示)

- 単位元 $\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$ の共役類はこれのみからなる。つまり $Conj_{\tilde{S}_3}\left(\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}\right)=\left\{\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}\right\}$

他は $Conj_{\tilde{S}_3}\left(\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\right)=\left\{\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix},\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix},\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\right\}$ (互換)

$Conj_{\tilde{S}_3}\left(\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\right)=\left\{\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\right\}$ (巡回置換)

記法 G: 有限群のとき $G=\coprod_{x\in X} Conj_G(x)$ となるように共役類から
代表を集めた集合 $X\subseteq G$ をとる。このうち $Conj_G(x)=\{x\}\Leftrightarrow x\in Z(G)$ より
$|G|=|Z(G)|+\sum_{x\in X\setminus Z(G)}|Conj_G(x)|$ が成り立つ (類等式)

系 $\tilde{S}_3$ に位数2の正規部分群はない (注: もちろん何も使わずに簡単にcheck可)

(:) 類等式 $6=1+3+2$ で1と他を使って2を作れない
(正規部分群が共役類の和集合であることを用いた) //

Def p：素数

① P：有限群が p-群 $\overset{\text{def}}{\iff} \exists n \geq 0$ s.t. $|P| = p^n$

② G：有限群，p-部分群 $P \subseteq G$ が p-Sylow 部分群 $\overset{\text{def}}{\iff} \frac{|G|}{|P|} \nmid p\mathbb{Z}$

Thm p：素数，G：有限群，$\mathrm{Syl}_p(G) := \{P \subseteq G \mid P \text{ は } G \text{ の } p\text{-Sylow 部分群}\}$

① $\forall H \subseteq G$：p-部分群，$\exists P \in \mathrm{Syl}_p(G)$ s.t. $H \subseteq P$

② $\forall P_1 \forall P_2 \in \mathrm{Syl}_p(G)$，$\exists g \in G$ s.t. $gP_1g^{-1} = P_2$

③ $|\mathrm{Syl}_p(G)| \equiv 1 \pmod p$

(:) $|G| = p^n \cdot m$，$n \geq 0$，$m \nmid p\mathbb{Z}$ とする。$X := \{S \subseteq G \mid |S| = p^n\}$ について

$|X| \nmid p\mathbb{Z}$ は易しい。よって $G \times X \to X$，$(g, S) \mapsto gS$ という作用で $|GS| \nmid p\mathbb{Z}$ なる軌道がとれる。今，$\mathrm{Stab}_G(S) =: P_0 \in \mathrm{Syl}_p(G)$ を示そう。$|GS| = \frac{|G|}{|P_0|}$ より $|P_0| \geq p^n$

又，$P_0 S = S$ なので $s \in S$ について $P_0 \cdot s \subseteq S$。$\cdot s$ 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。$|Y| = \frac{|G|}{\mathrm{Stab}_G(P_0)} \mid \frac{|G|}{|P_0|}$ なので Y のある H 軌道は $p' = 1$ コの元からなる。これを $Q \in Y$ とすると $HQ = QH$ なので

HQ は G の部分群で $HQ \rhd Q$。$H \hookrightarrow HQ \twoheadrightarrow HQ/Q$ に準同型定理を適用して $H/H \cap Q \simeq HQ/Q$

よって $|H|\cdot|Q| = |HQ|\cdot|H\cap Q|$ 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 $HQ = Q$。とくに $H \subseteq Q$。よって①が示された。

②を示す。$H \in \mathrm{Syl}_p(G)$ なら $H = Q = gP_0g^{-1}$ //

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