Lecture XVIII: Towards a classification of finite groups

GOAL: Use Sylow p-subgroups to classify finite groups (up to isomorphism)

§18.1 Groups of order 45

Let G be a finite group with $|G| = 45 = 3^2 \cdot 5$ ⤳ only Sylow p-subgroups are for $p = 3, 5$

- $n_3 \equiv 1 \pmod 3$ & $n_3 \mid 5$ $\Rightarrow$ $n_3 = 1$
- $n_5 \equiv 1 \pmod 5$ & $n_5 \mid 3^2$ $\Rightarrow$ $n_5 = 1$

Conclusion: In an group with 45 elements, there is a unique subgroup of size 9, say P, and a unique subgroup of size 9, say Q. In particular $P \trianglelefteq G$ & $Q \trianglelefteq G$.

Observations: (1) If $H \leq G$ is the subgroup generated by P and Q, then both 9 and 5 divides $|H|$ so $45 \leq |H|$. Since $H \subseteq G$ & $|G| = 45$, we get $H = G$.

(2) $P \cap Q = \{e\}$ Because if $\sigma \in P \cap Q$ $\left.\begin{array}{l} \mathrm{ord}(\sigma) \mid |P| = 9 \\ \mathrm{ord}(\sigma) \mid |Q| = 5 \end{array}\right\} \Rightarrow \mathrm{ord}(\sigma) = 1$, ie $\sigma = e$.

These 2 facts will allow us to build G from P and Q. First, a general fact:

Lemma: Let G be a group, and N_1, N_2 be 2 subgroups of G. Assume that

(1) $N_1, N_2 \trianglelefteq G$

(2) $N_1 \cap N_2 = \{e\}$.

Then, $ab = ba$ $\forall a \in N_1, b \in N_2$.

Proof: $[a:b] = aba^{-1}b^{-1} = (aba^{-1})\,b^{-1} \in aN_2a^{-1}N_2 = N_2 a a^{-1} N_2 = N_2$ ($N_2 \trianglelefteq G$)

$= a(ba^{-1}b^{-1}) \in N_1 b N_1 b^{-1} = N_1 b b^{-1} N_1 = N_1$ ($N_1 \trianglelefteq G$).

$\Rightarrow aba^{-1}b^{-1} \in N_1 \cap N_2 = \{e\}$, so $ab = ba$ □

- Now, we go back to G with $|G| = 45$.

Claim: G is generated by P, Q two normal "mutually commuting" subgroups with trivial intersection. More precisely

$$G = \{ p \cdot q \mid p \in P, q \in Q \}$$

group operation $(pq)(p'q') \underset{\substack{\uparrow \\ qp' = p'q \text{ by Lemma}}}{=} (pp')(qq')$ $\qquad (pq)^{-1} = q^{-1}p^{-1} \underset{\substack{\downarrow \\ \text{by Lemma}}}{=} p^{-1}q^{-1}$

Consequence: $G \simeq P \times Q$ (coordinatewise group operation)
$pq \longleftarrow\!\shortmid (p,q)$

So, to completely describe G, we need full description of $Q \simeq \mathbb{Z}/5\mathbb{Z}$ & P.

P has order 9.

Claim: $P \simeq \mathbb{Z}/9\mathbb{Z}$ or $P \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

Pf/ See Proposition §18.2 below.

Note: These 2 groups are not isomorphic because $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ has no element of order 9.

Corollary: $G \simeq \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ or $G \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$.

§18.2 Groups of order p^2:

Lemma: Assume H is a group with $|H| = p^2$ and p is prime. Then, H is abelian.

Proof: From Corollary §14.2, we know $Z(H)$ is non-trivial because H is a p-group.
Then, either $|Z(H)| = p$ or p^2.
So $\left|H/Z(H)\right| = p$ or 1. In both case $H/Z(H)$ is cyclic. By HW2, H is abelian. $\square$

Proposition: Assume H is a group with $|H| = p^2$ and p is prime. Then,

$$H \simeq \mathbb{Z}/p^2\mathbb{Z} \quad \text{or} \quad H \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$$

Furthermore, these groups are not isomorphic.

Proof: By Lemma, we know H is abelian.

Pick $\sigma \in H \setminus \{e\}$. Then $\operatorname{ord}(\sigma) = p$ or p^2.

If $\operatorname{ord}(\sigma) = p^2$, then $H = \langle \sigma \rangle \simeq \mathbb{Z}/p^2\mathbb{Z}$

If $\operatorname{ord}(\sigma) = p$, then $\langle \sigma \rangle \trianglelefteq H$ has order $\mathbb{Z}/p\mathbb{Z}$.

Thus, either $H \simeq \mathbb{Z}/p^2\mathbb{Z}$ or $\exists\, H_1 \trianglelefteq H$ with $|H_1| = p$.

If H has no element of order p^2, then any $\tau \in H \setminus H_1$ has order p and $N = \langle \tau \rangle$ satisfies $N \cap H_1 = \{e\}$, $N, H_1 \triangleleft H$. As in §17.1 we have $H \simeq H_1 \times N$, $\sigma^i \tau^j \longleftarrow (\sigma^i, \tau^j)$

Since $H_1 \simeq N \simeq \mathbb{Z}/p\mathbb{Z}$, the result follows.

Finally, since $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ has no element of order p^2, then $\mathbb{Z}/p^2\mathbb{Z} \not\simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ $\square$

§18.3 Groups of order 8:

We aim to classify groups of order 8. We already know one group of order 8 which is not abelian, namely $D_8 = \langle s, r \mid s^2 = r^4 = e,\ srs = r^{-1} \rangle$

$$\underset{Z(D_8) = \langle r^2 \rangle = \{e, r^2\}}{\triangledown\!\!\mid} \quad \text{by HW 1.}$$

Now $D_8/Z(D_8)$ has order $4 = 2^2$, so it is abelian.

By Proposition §18.2: $D_8/Z(D_8) \simeq \mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

But $D_8/Z(D_8) \simeq D_4$ by proof of Proposition §16.2. is not cyclic, so $D_8/Z(D_8) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

$\langle \bar{s}, \bar{r} \mid \bar{s}^2 = \bar{r}^2 = 1,\ \bar{s}\bar{r}\bar{s} = \bar{r}^{-1} \rangle$

Note: $\bar{r}\bar{s} = \bar{s}\bar{r}$ So $D_8/Z(D_8) \simeq \underset{\langle \bar{r} \rangle}{\mathbb{Z}/2\mathbb{Z}} \times \underset{\langle \bar{s} \rangle}{\mathbb{Z}/2\mathbb{Z}}$

- Another non-abelian group of order 8 is the Quaternion group Q_8

$$Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$$

has 8 elements.

Group operation: $(\pm i)^2 = (\pm j)^2 = (\pm k)^2 = -1$, $(-1)^2 = 1$

$i \cdot j = k$; $j \cdot i = -k$

$j \cdot k = i$; $k \cdot j = -i$

$k \cdot i = j$; $i \cdot k = -j$

$\Rightarrow Z(Q_8) = \{+1, -1\} \simeq \mathbb{Z}/2\mathbb{Z}$

$Q_8/Z(Q_8) = \{1, i, j, k\}$ $\quad i^2 = j^2 = k^2 = 1$ and they all commute.
$(k = i \cdot j)$

$\simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

⚠ D_8 and Q_8 are <u>not</u> isomorphic because

- # elements of order 2 in $D_8 = 5$ $\quad (s, sr, sr^2, sr^3, r^2)$
- # ————————— $Q_8 = 1$ $\quad (-1)$.

However, $Z(D_8) \trianglelefteq D_8$ and $Z(Q_8) \trianglelefteq Q_8$ satisfy

$$Z(D_8) \simeq Z(Q_8) \simeq \mathbb{Z}/2\mathbb{Z} \quad \text{and} \quad D_8/Z(D_8) \simeq Q_8/Z(D_8) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

This means the isomorphism type of a p-group need not be determined by its chain of relatively normal subgroups with abelian successive quotients seen in Proposition §14.2.

<u>Note</u>: If G is not abelian and has size 8, then $|Z(G)| = 2$.
(Otherwise $|Z(G)| = 4$ would say $G/Z(G)$ is cyclic (of order 2), hence G would be abelian.)

We'll see in a future lecture that such a group is either isomorphic to D_8 or Q_8.
The abelian ones are isomorphic to either $\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ or $(\mathbb{Z}/2\mathbb{Z})^3$ (with standard products).

§18.4 Sylow subgroups of $GL_n(\mathbb{F}_p)$: (OPTIONAL)

<u>Recall</u>: $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ with usual $+$ and $\cdot$ of $\mathbb{Z}$ performed modulo p, a fixed prime.

<u>Lemma</u>: $G = GL_n(\mathbb{F}_p)$ has order $(p^n-1)(p^n-p)\cdots\cdots(p^n-p^{n-1})$

<u>Proof</u>: We count the possibilities for each column

Column 1 : $\mathbb{F}_p^n \smallsetminus \left\{\begin{bmatrix}0\\ \vdots \\ 0\end{bmatrix}\right\} \to (p^n-1)$ choices

Column 2 : $\mathbb{F}_p^n \smallsetminus \underbrace{\text{Span}(\text{Column } 1)}_{\simeq\, \mathbb{F}_p} = p^n - p$

Column 3 : $\mathbb{F}_p^n \smallsetminus \underbrace{\text{Span}(\text{column } 1, \text{Column } 2)}_{\simeq\, \mathbb{F}_p^2} = p^n - p \cdot p = p^n - p^2$

$\vdots$

Column n : $\mathbb{F}_p^n \smallsetminus \underbrace{\text{Span}(\text{Column } 1, \ldots, \text{Column } n-1)}_{\simeq\, \mathbb{F}_p^{n-1}} = p^n - \underbrace{p \cdot p \cdots p}_{n-1 \text{ many}} = p^n - p^{n-1}$

$\square$

$$\Rightarrow |G| = (p^n-1)(p^n-p)\cdots(p^n-p^{n-1}) = p^{1+\cdots+n-1}(p^n-1)(p^{n-1}-1)\cdots(p^2-1)(p-1)$$
$$= p^{\frac{n(n+1)}{2}}(p^n-1)(p^{n-1}-1)\cdots\cdots(p-1)$$

$\Rightarrow$ The order of a Sylow p-subgroup is $p^{\frac{n(n+1)}{2}}$.

Proposition 1: $U := \left\{ \begin{bmatrix} 1 & & * \\ & \ddots & \\ 0 & & 1 \end{bmatrix} \in GL_n(\mathbb{F}_p) \right\} \in Syl_p(GL_n(\mathbb{F}_p))$

Proof: By construction $I_n \in U$, U is closed under multiplication. It remains to show U is closed under inverses. Recall $U^{-1} = Adj(U)$ because $\det U = 1$. Now, $Adj(U)_{ij} = 0$ if $i > j$ because $\det(A^{ji}) = 0$ if $j < i$

$\hookrightarrow$ remove row j & column i

so U^{-1} is also upper triangular, and $\det(A^{ii}) = 1$ $\forall i$.

$|U| = p^{\frac{n(n-1)}{2}}$ because there are $\frac{n(n-1)}{2}$ spots above the diagonal for these matrices. □

Remark: Similarly $U' = \left\{ \begin{bmatrix} 1 & & 0 \\ & \ddots & \\ * & & 1 \end{bmatrix} \in GL_n(\mathbb{F}_p) \right\} \in Syl_p(GL_n(\mathbb{F}_p))$

Q: How many Sylow p-subgroups does G have?

A: We need to conjugate U' by the Sylow Thm (2).

The answer is simple when $n = 2$.

Proposition 2: $|Syl_p(GL_2(\mathbb{F}_p))| = p+1$.

Proof: For every fixed $\alpha \in \mathbb{F}_p$, we conjugate elements of U' by $\begin{bmatrix} 1 & \alpha \\ 0 & 1 \end{bmatrix}$

$$\begin{bmatrix} 1 & \alpha \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ y & 1 \end{bmatrix} \begin{bmatrix} 1 & \alpha \\ 0 & 1 \end{bmatrix}^{-1} = \begin{bmatrix} 1 & \alpha \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ y & 1 \end{bmatrix} \begin{bmatrix} 1 & -\alpha \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1+\alpha y & \alpha \\ y & 1 \end{bmatrix} \begin{bmatrix} 1 & -\alpha \\ 0 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 1+\alpha y & -\alpha^2 \\ y & 1-\alpha y \end{bmatrix}$$

$\Rightarrow Q_\alpha := \left\{ \begin{bmatrix} 1+\alpha y & -\alpha^2 y \\ y & 1-\alpha y \end{bmatrix} : y \in \mathbb{F}_p \right\} \in Syl_p(GL_2(\mathbb{F}_p))$ for each fixed $\alpha \in \mathbb{F}_p$

Claim: $Q_\alpha \cap Q_\beta = \{I_2\}$ if $\alpha \neq \beta$, $U \cap Q_\alpha = \{I_2\}$

Pf/ $A \in Q_\alpha \cap Q_\beta$ satisfies $\begin{bmatrix} 1+\alpha y & -\alpha^2 y \\ y & 1-\alpha y \end{bmatrix} = \begin{bmatrix} 1+\beta y' & -\beta^2 y' \\ y' & 1-\beta y' \end{bmatrix}$ for $y, y' \in \mathbb{F}_p$.

$\Rightarrow y = y'$

- If $y = y' = 0$, then $A = I_2$.
- If $y = y' \neq 0$, then $1 + \alpha y = 1 + \beta y' \Rightarrow \alpha y = \beta y'$ gives $\alpha = \beta$ Contr!

• Now $A \in Q_\alpha \cap U$ forces $y=0$ so $A = I_2$ $\square$

$\Rightarrow |Syl_p(GL_2(\mathbb{F}_p))| \geq p+1$. $\left(\{Q_\alpha : \alpha \in \mathbb{F}_p\} \cup \{U\} \subseteq Syl_p(GL_2(\mathbb{F}_p))\right)$

$n_p \equiv 1 \mod p$ and $n_p \mid (p^2-1)(p-1) = (p+1)(p-1)^2$

To show $n_p = p+1$, we need some cool fact from Linear Algebra.

Lemma: Given $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ 2x2 matrix with $\Delta = ad-bc \neq 0$. Then,

either $c=0$ or $\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 1 & a/c \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} c & d \\ 0 & -\frac{\Delta}{c} \end{bmatrix}$

Proof: Assume $c \neq 0$, then $\Delta \neq 0$ gives $b = \frac{ad-(ad-bc)}{c} = \frac{ad-\Delta}{c}$

Check $\begin{bmatrix} 1 & a/c \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} c & d \\ 0 & -\frac{\Delta}{c} \end{bmatrix} = \begin{bmatrix} a/c & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} c & d \\ 0 & -\frac{\Delta}{c} \end{bmatrix} = \begin{bmatrix} a & \frac{ad-\Delta}{c} \\ c & d \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ ✓

$\square$

Corollary: $GL_2(\mathbb{F}_p) = B \sqcup B \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} B$ with $B = \left\{ \begin{matrix} \text{Upper Triangular} \\ \text{Matrices with } \Delta \neq 0 \end{matrix} \right\}$

Proof: Check $B \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} B = \left\{ A = \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} f & g \\ 0 & h \end{bmatrix} \quad ad \neq 0, fh \neq 0 \right\}$

$A = \begin{bmatrix} b & a \\ d & 0 \end{bmatrix} \begin{bmatrix} f & g \\ 0 & h \end{bmatrix} = \begin{bmatrix} bf & bg+ah \\ df & dg \end{bmatrix}$ so $A \notin B$.

$\neq 0$

By the Lemma, if $M \notin B \Rightarrow M \in B \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} B$. $\square$

• Now, back to the proof of Proposition 2.

$\Rightarrow$ To get the Sylow p-subgroups of $GL_2(\mathbb{F}_p)$, we need to conjugate U by any $M \in GL_2(\mathbb{F}_p)$.

Claim 1: If $M \in B \Rightarrow M U M^{-1} = U$

Proof: $\begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} \frac{1}{\Delta} \begin{bmatrix} d & -b \\ 0 & a \end{bmatrix} = \frac{1}{\Delta} \begin{bmatrix} a & ax+b \\ 0 & d \end{bmatrix} \begin{bmatrix} d & -b \\ 0 & a \end{bmatrix} = \frac{1}{\Delta} \begin{bmatrix} ad & ax \\ 0 & da \end{bmatrix} = \begin{bmatrix} 1 & x/d \\ 0 & 1 \end{bmatrix} \in U$

for all $x \in \mathbb{F}_p$.

Claim 2: If $M \in B \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} B \Rightarrow M U M^{-1} = Q_\alpha$ for some α

Proof: Write $M = A_1 \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} A_2$ where A_1, A_2 are upper triangular

$$\Rightarrow \Pi U \Pi^{-1} = A_1 \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} A_2 U A_2^{-1} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}^{-1} A_1^{-1} = A_1 \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \underbrace{\boxed{A_2 U A_2^{-1}}}_{= U \text{ by Claim 1}} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} A_1^{-1}$$

Now $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} U \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \left\{ \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} : x \in \mathbb{F}_p \right\}$

$$= \left\{ \begin{bmatrix} 0 & 1 \\ 1 & x \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ x & 1 \end{bmatrix} \quad x \in \mathbb{F}_p \right\} = U'$$

$$\Rightarrow \Pi U \Pi^{-1} = A_1 U' A_1^{-1} \qquad \text{with} \qquad A_1 = \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \qquad ad \neq 0.$$

Need to check we can assume $a = d = 1$. If so, $A_1 U' A_1^{-1} = Q_\alpha$.

<u>Claim:</u> $\begin{bmatrix} a & b \\ 0 & d \end{bmatrix} U' \begin{bmatrix} a & b \\ 0 & d \end{bmatrix}^{-1} = \begin{bmatrix} 1 & b/d \\ 0 & 1 \end{bmatrix} U' \begin{bmatrix} 1 & b/d \\ 0 & 1 \end{bmatrix}^{-1}$

Pf/ $\begin{bmatrix} 1 & b' \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ y' & 1 \end{bmatrix} \begin{bmatrix} 1 & -b' \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1+b'y' & -(b')^2 y' \\ y' & 1-b'y' \end{bmatrix}$

$$\begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \begin{bmatrix} 1 & 0 \\ y & 1 \end{bmatrix} \frac{1}{\Delta} \begin{bmatrix} d & -b \\ 0 & a \end{bmatrix} = \frac{1}{\Delta} \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \underbrace{\begin{bmatrix} 1 & 0 \\ y & 1 \end{bmatrix} \begin{bmatrix} d & -b \\ 0 & a \end{bmatrix}}_{\begin{bmatrix} d & -b \\ dy & a-by \end{bmatrix}} = \frac{1}{\Delta} \begin{bmatrix} d(a+by) & -b^2 y \\ d^2 y & d(a-by) \end{bmatrix}$$

$$= \begin{bmatrix} 1+\frac{b}{a}y & -\frac{b^2 y}{\Delta} \\ \frac{d^2}{\Delta} y & 1-\frac{b}{a}y \end{bmatrix} = \begin{bmatrix} 1+\frac{b\Delta}{ad^2}\left(\frac{d^2 y}{\Delta}\right) & -\left(\frac{b}{d}\right)^2 \frac{d^2 y}{\Delta} \\ d^2 \frac{y}{\Delta} & 1-\frac{b\Delta}{d^2 a} \frac{d^2 y}{\Delta} \end{bmatrix}$$

But $\frac{b\Delta}{ad^2} = \frac{bad}{ad^2} = \frac{b}{d}$ $\qquad y' = \frac{d^2 y}{\Delta}$ sweeps $\mathbb{F}_p$ because $d, \Delta \neq 0$ are fixed.

The claim follows from this. $\square$

<u>Conclusion:</u> $\mathrm{Syl}_p(GL_2(\mathbb{F}_p)) = \{ g U g^{-1} \; g \in GL_2(\mathbb{F}_p) \} \subseteq \{U\} \cup \{Q_\alpha \; \alpha \in \mathbb{F}_p\}$