Tues Sept 24

HW 2 due now
(only problems 1–3).

Today: The Hölder Program

Recall the Jordan-Hölder Theorem

Every finite group G is built from its simple composition factors

Q: What do I mean by "built from"?

Consider a composition series of length 2

$$\underset{G/N}{G \rhd} N \underset{N}{\rhd} 1.$$

Then G is "built from" the simple groups N and G/N. We can express this with a short exact sequence

$$1 \to N \to G \to G/N \to 1.$$

"Exact" means that at each step we have

$$\xrightarrow{\varphi_i} C \xrightarrow{\varphi_{i+1}} \qquad \operatorname{im}\varphi_i = \ker\varphi_{i+1}$$

Let $\iota : N \hookrightarrow G$ be the inclusion map and let $\varphi : G \twoheadrightarrow G/N$ be the canonical surjection. Then

$$1 \longrightarrow N \overset{\iota}{\hookrightarrow} G \overset{\varphi}{\twoheadrightarrow} G/N \longrightarrow 1$$

is exact.

More generally, let N and H be simple groups. Find all G with comp factors N and H. Such a G will satisfy a short exact sequence

$$1 \longrightarrow N \overset{\iota}{\hookrightarrow} G \overset{\varphi}{\twoheadrightarrow} H \longrightarrow 1.$$

where $N \approx \operatorname{im} \iota = \ker \varphi \triangleleft G$.

hence $H = \operatorname{im} \varphi \approx G/\ker\varphi \approx G/N$.

In this case we say that G is an extension of N by H.

Problem: Classify all extensions of N by H.

Example: For any groups N, H and any hom $\theta : H \to \mathrm{Aut}(N)$, the semidirect product $N \rtimes_\theta H$ is an extension of N by H:

$$\begin{tikzcd}
1 \arrow[r] & N \arrow[r, hook, "\iota"'] & N \rtimes_\theta H \arrow[r, two heads, "\varphi"'] & H \arrow[r] \arrow[ll, bend right, "\beta"'] & 1 .
\end{tikzcd}$$

In this case there is an extra map $\beta : H \hookrightarrow N \rtimes_\theta H$ called a "splitting map" such that $\varphi(\beta(h)) = h \ \forall \ h \in H$

Theorem: Consider an extension G of N by H

$$\begin{tikzcd}
1 \arrow[r] & N \arrow[r, hook, "\iota"'] & G \arrow[r, two heads, "\varphi"'] & H \arrow[r] \arrow[l, bend right, "\beta"'] & 1 .
\end{tikzcd}$$

Then $G \cong N \rtimes_\theta H$ for some θ
$\iff$ the s.e.s. splits, i.e., $\exists \ \beta : H \to G$ with $\varphi \circ \beta = id$.

Proof omitted. ///

Fact: Not every s.e.s. splits.

Smallest Example: Consider the "quaternion" group Q_8 of order 8.

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

with $i^2 = j^2 = k^2 = ijk = -1$

Lemma: $-1 \in Q_8$ is the only element of order 2.

Now assume Q_8 can be written as

$$Q_8 = N \rtimes H$$

where $|N| = 2$, $|H| = 4$
or $|N| = 4$, $|H| = 2$

In either case, both N, H contain elements of order 2 $\Longrightarrow$ Q_8 contains ≥ 2 elements of order 2. Contradiction

$\Rightarrow$ Q_8 is not a semidirect product.

The composition factors of Q_8 are $\mathbb{Z}/2$, $\mathbb{Z}/2$, $\mathbb{Z}/2$ but Q_8 cannot be constructed from them using semidirect products ☹

This leads to the Hölder Program:

In order to classify finite groups we should

(1) Classify finite simple groups.

(2) Classify all group extensions

Part (2) has been deemed "too hard" but part (1), amazingly, has been solved (~1980)

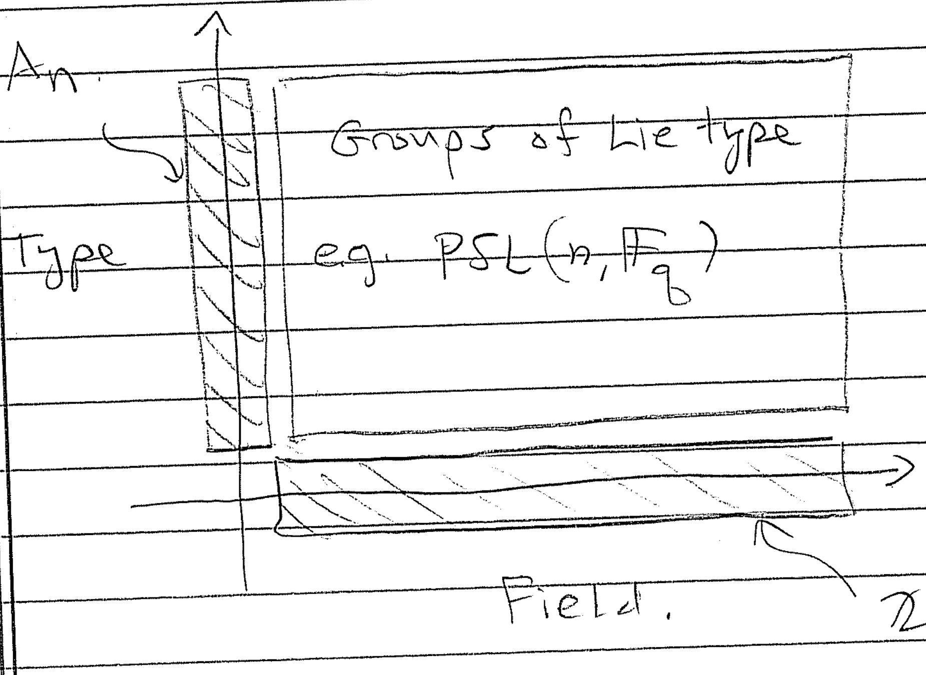
HUGE THEOREM (~1980):

There are 18 infinite families of simple groups and 26 sporadic ("exceptional") simple groups.

The largest sporadic group is called the Monster. It has order

$$|M| \approx 8 \cdot 10^{53}$$

The 18 infinite families can be visualized as follows:



The classification of finite groups of Lie type depends on the classification of compact Lie groups over $\mathbb{C}$.

(It's a big topic).

Next we will examine two aspects of the classification

Ⓐ The Sylow Theorems

Ⓑ Groups of Lie type

After that we will discuss representations of groups.

The Sylow Theorems (Alperin Chap. 3)

Recall Lagrange's Theorem:

Let G be a finite group. If $H \leq G$ then $|H|$ divides $|G|$.

Proof: G is partitioned into left cosets $G/H = \{gH : g \in G\}$, all of the same size $|H|$. Hence

$$|G| = |G/H| \cdot |H|$$

▨

Q: To what extent is the converse true?

i.e. If $n \mid |G|$, does there exist a subgroup $H \leq G$ with $|H| = n$?

Prop: Converse Lagrange holds for cyclic groups

Proof: Recall $\mathcal{L}(\mathbb{Z}/n) \approx D(n)$.

Prop: Converse Lagrange holds for dihedral groups.

Proof: Let $D_{2n} = \langle r, f : r^n = f^2 = 1, frf = r^{-1} \rangle$

$\langle f \rangle \leq D_{2n}$ has order 2

$\langle r \rangle \leq D_{2n}$ has order n

$\langle r \rangle$ has a subgroup of each order dividing n

∎

To find a counterexample to converse Lagrange we can eliminate groups of order p (cyclic) and order 2p (cyclic or dihedral).

~~1~~, ~~2~~, ~~3~~, ~~4~~, ~~5~~, ~~6~~, ~~7~~, 8, 9, ~~10~~, ~~11~~, 12

<u>Prop</u>: If $|G| = p^2$ then

$G \approx \mathbb{Z}/p^2$ or $\mathbb{Z}/p \times \mathbb{Z}/p$

In either case converse Lagrange holds.

<u>Proof</u> Postponed.

8, ~~9~~, 12, 18, 20

<u>Prop</u>: Any $|G| = 8 = 2^3$ satisfies converse Lagrange

<u>Proof</u>: Elements $a \in G$ have order 1, 2, 4, 8.

If $\exists$ elt order 8, done.

If $\exists$ elt order 4, done.

$$\begin{array}{cccc} G, & \langle a\rangle, & \langle a^2\rangle, & 1 \\ 8 & 4 & 2 & 1. \end{array}$$

Otherwise we have $|\langle a\rangle| = 2 \ \forall\ 1 \neq a \in G$.

Consider $a, b \in G$ of order 2. Then ab has order 2, hence

$$ab = (ab)^{-1} = b^{-1}a^{-1} = ba.$$

So $\{1, a, b, ab\}$ is a subgroup order 4

∎

$$\cancel{8}, \textcircled{12}, 18, 20$$

Next: Groups of order 12

Claim: $|A_4| = 12$ has NO subgroup of order 6.

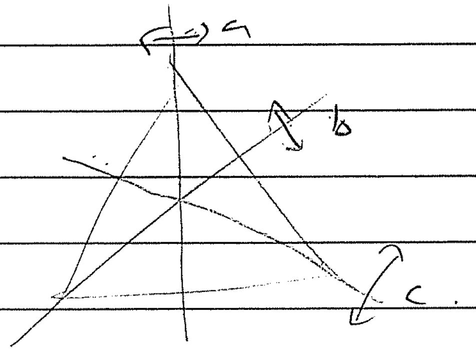
$A_4 = \{ 1, (12)(34), (13)(24), (14)(23),$
$(123), (132), (124), (142), (134), (143), (234), (243) \}$

Proof: Suppose $H \leq A_4$ has order $6 = 2 \cdot 3$
Then H is cyclic or dihedral

But A_4 has no elt order 6
$\Longrightarrow H \approx D_6$.
Note D_6 has three elements order 2

$\Longrightarrow \{(12)(34), (13)(24), (14)(23)\} \subseteq H$.

The elts of order 2 in D_6 don't commute



$$\left.\begin{array}{l} ba = (ab)^{-1} \\ ac = (ca)^{-1} \\ cb = (bc)^{-1} \end{array}\right\} = \text{rotate } + \pi/3$$

But the elements $(12)(34), (13)(24), (14)(23)$ **DO** commute.

Contradiction ∎

The converse to Lagrange is FALSE.

Thurs Sept 26

Today: Sylow Theory

Recall that the converse of Lagrange's Theorem

$\circledast$ "$n \mid |G| \Rightarrow G$ has a subgroup of order n"

is NOT true.
The smallest counterexample is the alternating group A_4.

$|A_4| = 12$ but A_4 has no subgroup of order 6.

Today we will try to find a weaker statement than $\circledast$ that is true.

First Try:

Let A be an abelian group and let $p \in \mathbb{Z}$ be prime.

If $p \mid |A|$ then A has an element of order p.

Proof: If A is cyclic we're done.
So suppose A is not cyclic.

Choose $1 \neq x \in A$ such that $H = \langle x \rangle \neq A$
If $p \mid |H|$ then H has an elt order p
and so does A, done.

So assume $p \nmid |H|$. Since $H \lhd A$ (abelian),
consider the quotient A/H.

$$|A/H| = |A| / |H|.$$

$$p \mid |A| \text{ and } p \nmid |H| \Rightarrow p \mid |A/H|$$

By induction, A/H has an element
of order p, say aH.

i.e. $aH \neq H$ $(a \notin H)$
$(aH)^p = a^p H = H$ $(a^p \in H)$

Now let $m = |H|$. By Lagrange
we have,

$$a^p \in H \Rightarrow (a^p)^m = 1$$

But $(a^m)^p = (a^p)^m = 1$

$\Longrightarrow$ a^m has order dividing p.

If the order of a^m is p we're done, so assume that $a^m = 1$.

i.e. $(aH)^m = a^m H = H$.

This impies that the order of aH (i.e. p) divides m. But $p \nmid m$.
Contradiction.

▨

Theorem:
Finite abelian A and $p \mid |A|$
$\Longrightarrow$ A has an element of order p.

Second Try:

Is the same true for abitrary groups?

$p \mid |G| \Longrightarrow \exists$ elt order p ?

Yes! But we need a tool.

Let G be a finite group and consider the action $G \curvearrowright G$ by conjugation:

$$\varphi : G \longrightarrow \mathrm{Aut}(G)$$
$$g \longmapsto \varphi_g$$

where $\varphi_g(h) := ghg^{-1} \quad \forall\ h \in G$.

The orbits are called "conjugacy classes"

$$\mathrm{Orb}(h) = \{ k \in G : \exists\, g \in G \text{ with } k = ghg^{-1} \}$$

The stabilizers are called "centralizers"

$$\begin{aligned} \mathrm{Stab}(h) &= \{ g \in G : ghg^{-1} = h \} \\ &= \{ g \in G : gh = hg \} \\ &=: C_G(h). \end{aligned}$$

Recall that for any $h \in G$ we have a bijection

$$\mathrm{Orb}(h) \longleftrightarrow G / \mathrm{Stab}(h)$$

Hence

$$|\mathrm{Orb}(h)| = |G| / |C_G(h)|$$

Now let $x_1, x_2, \dots, x_m \in G$ be representatives for the orbits, we have a disjoint union

$$G = \bigsqcup_i \mathrm{Orb}(x_i)$$

$$|G| = \sum_i |\mathrm{Orb}(x_i)|$$

$$= \sum_i |G| / |C_G(x_i)|$$

Q: When is $|\mathrm{Orb}(x_i)| = 1$?

Define the <u>center</u> (Zentrum) of the group

$$Z(G) := \{ g \in G : gh = hg \ \forall h \in G \}.$$

Note that

- $Z(G) \trianglelefteq G$
- $Z(G)$ is abelian.

For all $x \in Z(G)$ we have $\mathrm{Orb}(x) = \{x\}$.

Thus we can pull these "singleton" classes out of the sum

$$|G| = \sum_i |G|/|C_G(x_i)|$$

$$\boxed{|G| = |Z(G)| + \sum_{\substack{i \\ \cancel{C_G(x_i) \neq G}}} |G|/|C_G(x_i)|}$$

This is called the class equation of G

Finally, we can use this to prove

☆ Cauchy's Theorem (~1815):

Consider finite group G and prime $p \in \mathbb{Z}$.

If $p \mid |G|$ then G has an element of order p.

Proof (induction on $|G|$):

Suppose $p \mid |G|$ and assume the theorem holds for groups of size $< |G|$.

If $p \mid |C_G(x)|$ for some centralizer $C_G(x) \lneqq G$. Then we're done by induction. So suppose

$$p \nmid |C_G(x)| \text{ for all } C_G(x) \neq G,$$

in which case $p \mid |G|/|C_G(x)|$.

Now consider the class equation

$$\underset{\textcircled{1}}{|G|} = \underset{\textcircled{3}}{|Z(G)|} + \underset{\textcircled{2}}{\sum_{\substack{i \\ C_G(x_i) \neq G}} |G|/|C_G(x_i)|}$$

Since $p \mid \textcircled{1}$ and $p \mid \textcircled{2}$ we have

$$p \mid \textcircled{3} = \textcircled{1} - \textcircled{2}, \text{ i.e. } p \mid |Z(G)|$$

If $Z(G) \neq G$ then we're done by induction. If $Z(G) = G$ then G is *abelian* and we're done by the previous theorem. ∎

So we have the following partial converse to Lagrange:

Consider finite group G and prime p.

If $p \mid |G|$ then G has an element $x \in G$ of order p, hence a <u>subgroup</u> $\langle x \rangle$ of order p.

[Remark: If $G = A_4$ then $|G| = 12 = 2 \cdot 2 \cdot 3$. Then $6 \mid 12$ but 6 is <u>not</u> prime. In fact, A_4 has no subgroup of order 6.

Does it have a subgroup of order $4 = 2 \cdot 2$?]

Third Step:

If $p^n \mid |G|$ then G has subgroups of orders p^m for all $1 \leq m \leq n$.

↓

Proof (induction on $|G|$):

Let $p^n \mid |G|$ and suppose the result holds for all groups of size $< |G|$.

Look at the class equation

$$|G| = |Z(G)| + \sum_i |G|/|C(x_i)|.$$

If $p^n \mid |C(x_i)|$ then we're done by induction. So sp. $p^n \nmid |C(x_i)|$ $\forall i$.

Since $p^n \mid |G|$ and $p^n \nmid |C(x_i)|$ we have

$$p \mid |G|/|C(x_i)| \quad \forall i.$$

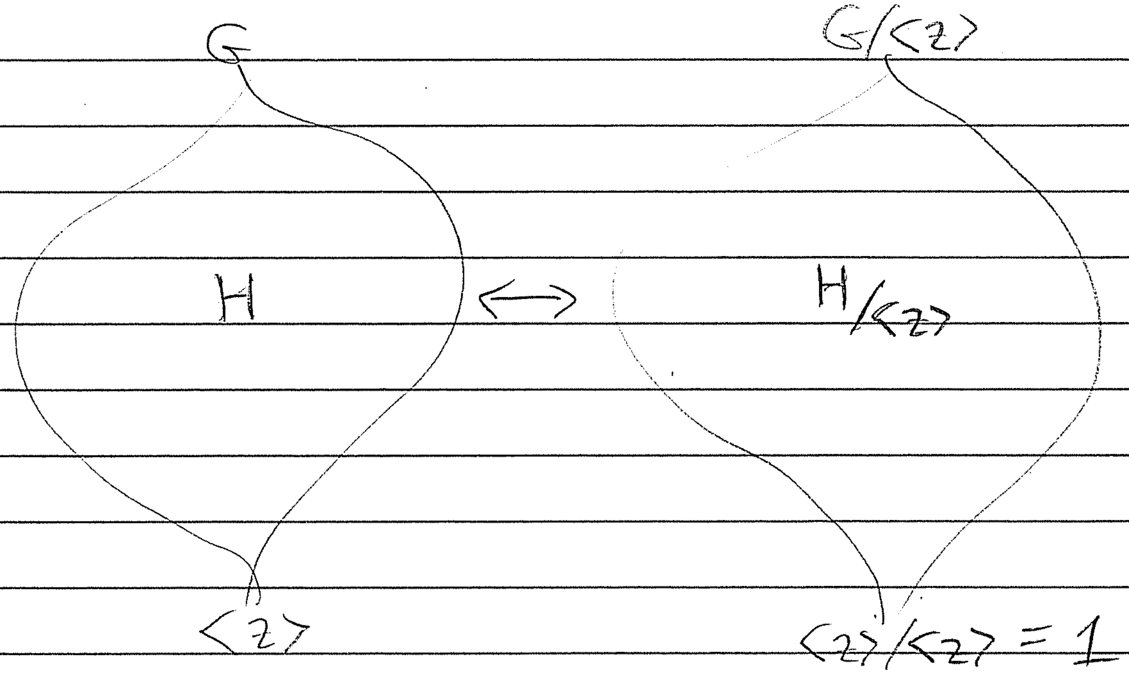
Hence $p \mid |Z(G)|$. Thus $Z(G)$ has an element $z \in Z(G)$ of order p.

We have $\langle z \rangle \lhd G$ and $|\langle z \rangle| = p$.

$$\Longrightarrow \quad p^{n-1} \mid |G/\langle z \rangle| = |G|/p.$$

By induction, $G/\langle z \rangle$ has subgroups of order p^m for all $1 \leq m \leq n-1$.

By correspondence, each subgroup of $G/\langle z \rangle$ looks like $H/\langle z \rangle$ for some $\langle z \rangle \leq H \leq G$.



Finally, note that

$$p^m = \left|\frac{H}{\langle z \rangle}\right| = \frac{|H|}{p} \implies |H| = p^{m+1}.$$

Hence G has subgroups of order p^{m+1} for all $1 \leq m \leq n-1$.

▨

Fourth Step : Sylow's Theorems

Let G be finite and let p be prime. Suppose $p^n \mid |G|$ and $p^{n+1} \nmid |G|$. (concisely : $p^n \| |G|$)

A "Sylow p-subgroup" is a <u>maximal</u> p-subgroup of G

Theorem:

1. Every Sylow p-subgroup has size p^n

2. All Sylow p-subgroups are conjugate

3. Let n_p = # Sylow p-subgroups. Then

- $n_p \mid |G|/p^n$

- $n_p = 1 \mod p$

- $n_p = |G|/|N_G(P)|$

where $N_G(P)$ is the normalizer of any Sylow p-subgroup P .

Tues Oct 1.

HW 2.5 due next Tues Oct 8

HW 3 postponed.

Today: Sylow Theory.

But First: G-sets

Given group G, set X, consider a homomorphism $\alpha : G \to \mathrm{Aut}(X)$.

Def: The pair (X, α) is called a "G-set"

Consider two G-sets (X, α) and (Y, β). We say $\varphi : X \to Y$ is a morphism of G-sets if $\forall g \in G$ the following square commutes:

$$\begin{tikzcd}
X \arrow[r, "\varphi"] \arrow[d, "\alpha_g"'] & Y \arrow[d, "\beta_g"] \\
X \arrow[r, "\varphi"] & Y
\end{tikzcd}$$

[We also say φ is "G-equivariant".]

i.e. for all $x \in X$ and $g \in G$ we have

$$\varphi(\alpha_g(x)) = \beta_g(\varphi(x))$$

$$\text{"}\ \varphi(g(x)) = g(\varphi(x))\ \text{"}$$

Given a G-set X, let $\mathrm{Aut}_G(X)$ denote the group of G-set automorphisms.

HW 2.5 examines the structure of $\mathrm{Aut}_G(X)$ (and corrects the old Problem 4)

☆ The Fundamental Theorem of G-sets ☆
(Orbit-Stabilizer Theorem).

Consider a G-set X. For all $x \in X$ we have an isomorphism of G-sets

$$\mathrm{Orb}(x) \approx G/\mathrm{Stab}(x).$$

$$g(x) \underset{\varphi}{\longmapsto} g\,\mathrm{Stab}(x).$$

↓

Proof: We already know that φ is a bijection. We must show it is G-equivariant. Indeed, for all $h(x) \in \mathrm{Orb}(x)$ and $g \in G$ we have

$$\begin{aligned} g(\varphi(h(x))) &= g\big(h\,\mathrm{Stab}(x)\big) \\ &= (gh)\,\mathrm{Stab}(x) \\ &= \varphi((gh)(x)) \\ &= \varphi(g(h(x))) \end{aligned}$$

i.e. $g \circ \varphi = \varphi \circ g$. ∎

Application: Let G be finite group and let $H, K \leq G$ be subgroups (possibly both non-normal)

Then we have

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|}$$

Proof: Let $X = G/K$ and consider X as an H-set under left multiplication.

The orbit of $K \in G/K$ is

$$\text{Orb}(K) = \{hK : h \in H\}.$$

Note that $HK = \bigcup_{C \in \text{Orb}(K)} C$, hence

$$|HK| = |\text{Orb}(K)| \cdot |K|.$$

The stabilizer of K is

$$\text{Stab}(K) = \{h \in H : hK = K\} = H \cap K.$$

By orbit-stabilizer we have

$$\begin{aligned} |HK| &= |\text{Orb}(K)| \cdot |K| \\ &= \left(\frac{|H|}{|H \cap K|}\right) \cdot |K|. \end{aligned}$$

$\blacksquare$

↓

Corollary: Consider finite group G, subgroups $H, K \leq G$ and $x \in G$. Define the double coset

$$HxK = \{hxk : h \in H, k \in K\}.$$

Then we have.

$$|HxK| = \frac{|H||K|}{|H \cap xKx^{-1}|} = \frac{|H||K|}{|x^{-1}Hx \cap K|}.$$

Proof: By the above result we have

$$|HxK| = |HxKx^{-1}|$$

$$= \frac{|H||xKx^{-1}|}{|H \cap xKx^{-1}|} = \frac{|H| \cdot |K|}{|H \cap xKx^{-1}|}$$

$$= \frac{|H||K|}{|x^{-1}(H \cap xKx^{-1})x|}$$

$$= \frac{|H||K|}{|x^{-1}Hx \cap K|}$$

∎

The Sylow Theorems (1872)

Let $|G| = p^\alpha m$ with p prime, $p \nmid m$. We say $H \leq G$ is a Sylow p-subgroup if $|H| = p^\alpha$. Let $\mathrm{Syl}_p(G)$ be the set of Sylow p-subgroups.

① Sylow p-subgroups exist, i.e. $\mathrm{Syl}_p(G) \neq \emptyset$.

② If $P \in \mathrm{Syl}_p(G)$ and $Q \leq G$ is any p-subgroup, $\exists\, g \in G$ such that

$$Q \leq gPg^{-1}.$$

In particular all Sylow p-subgroups are conjugate

③ We have

$$|\mathrm{Syl}_p(G)| = 1 \mod p$$

and $|\mathrm{Syl}_p(G)| \;\Big|\; m$.

Proof: We proved ① last time, using the Class Equation and induction on $|G|$.

For ② consider $P \in Syl_p(G)$, i.e. $|P| = p^\alpha$ and $Q \leq G$ with $|Q| = p^r$, $r \leq \alpha$.

Decompose G into double cosets

$$G = \bigsqcup_i Q x_i P$$

$$(*) \quad |G| = \sum_i |Q x_i P| = \sum_i \frac{|Q||P|}{|Q \cap x_i P x_i^{-1}|}$$

Suppose that $Q \cap x_i P x^{-1} \lneqq Q \quad \forall i$.

Then $|Q \cap x_i P x_i^{-1}| = p^s$ for $s < r$.

and
$$\frac{|Q||P|}{|Q \cap x_i P x_i^{-1}|} = \frac{p^{\alpha + r}}{p^s} = p^{\alpha + r - s}$$
$$= p^n \text{ for } n > \alpha.$$

But then $p^{\alpha+1}$ divides all summands in $(*)$, hence divides $|G|$.

Contradiction.

We conclude that

$$Q \cap x_i P x_i^{-1} = Q, \quad \text{i.e.} \quad Q \leq x_i P x_i^{-1}$$

for some i. //

For ③, consider the action of G on $Syl_p(G)$ by conjugation: $P \xmapsto{g} gPg^{-1}$.

By ② we know the action is transitive. The stabilizer of $P \in Syl_p(G)$ is

$$Stab(P) = \{ g \in G : gPg^{-1} = P \} = N_G(P).$$

Hence Orbit-Stabilizer says.

$$|Syl_p(G)| = |G| / |N_G(P)|$$

Note that $p^\alpha = |P| \mid |N_G(P)|$,

say $|N_G(P)| = p^\alpha n$. Then

$$|Syl_p(G)| = \frac{\cancel{p^\alpha} m}{\cancel{p^\alpha} n} = \frac{m}{n} \mid m.$$

Finally we will prove $|\mathrm{Syl}_p(G)| = 1 \bmod p$.

<u>Lemma</u>: Given $P, Q \in \mathrm{Syl}_p(G)$ we have

$$P \leq N(Q) \iff P = Q$$

Indeed, suppose $P \leq N(Q)$. Then since $Q \triangleleft N(Q)$, $PQ \leq N(Q)$. and $|PQ|$ divides $|N(Q)|$. But

$$|PQ| = \frac{|P||Q|}{|P \cap Q|} = \frac{p^{2\alpha}}{p^{s}}$$

is divisible by $p^{\alpha+1}$ unless $|P \cap Q| = p^{\alpha}$, i.e. $P = Q$. ///

Now given $P \in \mathrm{Syl}_p(G)$, let P act on $\mathrm{Syl}_p(G)$ by conjugation. We have

$$\mathrm{Syl}_p(G) = \bigsqcup_i \mathrm{Orb}_P(Q_i)$$

But note that

$$|\mathrm{Orb}_P(Q_i)| = |P| \big/ |\mathrm{Stab}_P(Q_i)| \;\Big|\; p^{\alpha}.$$

and

$$\begin{aligned} |\mathrm{Orb}_p(Q_i)| = 1 &\iff xQ_ix^{-1} = Q_i \quad \forall x \in P \\ &\iff P \leq N(Q_i) \\ &\iff P = Q_i \end{aligned}$$

Hence we have

$$\begin{aligned} |\mathrm{Syl}_p(G)| &= 1 + \sum_{Q_i \neq p} |\mathrm{Orb}_p(Q_i)| \\ &= 1 \mod p \end{aligned}$$

▨

Thurs Oct 3

HW 2.5 due Tues Oct 8

Today: Applications of Sylow.

Look at groups of small order.

Order 1: Trivial Group

Order 2: $\mathbb{Z}/2$.

[Order prime p: Only $\mathbb{Z}/p$.

Proof: Let $|G| = p$ and consider $1 \neq x \in G$. Then since $|\langle x \rangle| \neq 1$ and divides p, we have

$$|\langle x \rangle| = p \implies \langle x \rangle = G.]$$

Order 3: $\mathbb{Z}/3$.

Order 4: We have $\mathbb{Z}/4$ and the "Klein Viergruppe" $V = \mathbb{Z}/2 \times \mathbb{Z}/2$

Is that all? Yes.

[Proof: Let $|G| = 4$ and let $1 \neq x \in G$.
If $|\langle x \rangle| = 4$ then $G = \mathbb{Z}/4$.
So suppose all $1 \neq x \in G$ have order 2.

Let $G = \{1, a, b, c\}$

Then $ab = 1 \Rightarrow a = b^{-1} = b$ ×
$ab = a \Rightarrow b = 1$ ×
$ab = b \Rightarrow a = 1$ ×,

hence $ab = c$.
Similarly, $ba = c$. It follows that

$$G = \{1, a\} \times \{1, b\} \approx \mathbb{Z}/2 \times \mathbb{Z}/2. \quad //$$

More generally, you will show on HW 3 that if

$$|G| = p^2 \quad \text{for prime } p$$

then $G = \mathbb{Z}/p^2$ or $G = \mathbb{Z}/p \times \mathbb{Z}/p$.]

Order 5: $\mathbb{Z}/5$.

Order 6 : We have $\mathbb{Z}/6$ and D_6

Is that all? Yes

[On HW 3 you will show that $|G| = 2p$
$\Rightarrow$ G is cyclic or dihedral.

Recall: We say G is dihedral if

$$G \cong \langle r \rangle \rtimes_\theta \langle f \rangle,$$

where $|\langle r \rangle| = n$, $|\langle f \rangle| = 2$, and

$$\theta : \langle f \rangle \longrightarrow \mathrm{Aut}(\langle r \rangle)$$

is defined by $\theta_f(r) = r^{-1}$.]

More generally, we will show that there are at most 2 groups of order pq for p, q prime.

We will use Sylow. Recall:

If $p \mid |G|$ then $\mathrm{Syl}_p(G)$ is transitive under G-conjugation, hence

$$|\mathrm{Syl}_p(G)| = |G| / |N_G(P)|$$

for any $P \in Syl_p(G)$. Furthermore we have

$$|Syl_p(G)| = 1 \mod p.$$

Note that if $|Syl_p(G)| = 1$, say $Syl_p(G) = \{P\}$, then we have

$$gPg^{-1} \in Syl_p(G) \quad \forall g \in G$$

$$\Longrightarrow \quad gPg^{-1} = P \quad \forall g \in G$$

$$\Longrightarrow \quad P \trianglelefteq G.$$

Now let $|G| = pq$ with $p < q$ prime.

Let $n_q = |Syl_q(G)|$.

We know $n_q = 1 \mod q$ and $n_q \mid p$.
(hence $n_q \leq p < q$)

$$\Longrightarrow \quad n_q = 1$$

i.e. $Syl_q(G) = \{Q\}$ with $Q \triangleleft G$.

Now let $P \in Syl_p(G)$.

Since $P \cap Q = 1$ [if $x \in P \cap Q$ then $|\langle x \rangle|$ divides p and q $\Rightarrow |\langle x \rangle| = 1$] we have

$$|PQ| = \frac{|P||Q|}{|P \cap Q|} = pq = |G|.$$

It follows that

$$G = Q \rtimes_\theta P$$

for some $\theta : P \to Aut(Q)$.

Lemma: For all $n \in \mathbb{N}$ we have

$$Aut(\mathbb{Z}/n) = (\mathbb{Z}/n)^\times$$
$$= \{ a \in \mathbb{Z}/n : a, n \text{ coprime} \}$$

Proof: Consider a group homomorphism

$$\varphi : \mathbb{Z}/n \to \mathbb{Z}/n$$

and let $\varphi(1) = a$. Then for all $x \in \mathbb{Z}/n$ we have

$$\varphi(x) = \varphi(\underbrace{1+1+\cdots+1}_{x \text{ times}}) = \underbrace{\varphi(1)+\varphi(1)+\cdots+\varphi(1)}_{x \text{ times}}$$

$$= a + a + \cdots + a = ax$$

The image is $\operatorname{im}\varphi = \langle a \rangle \leq \mathbb{Z}/n$. Thus
φ is surjective $\iff \langle a \rangle = \mathbb{Z}/n$
$\iff a, n$ are coprime

In this case we can invert a mod n and thus φ is invertible with

$$\varphi^{-1}(x) = a^{-1}x.$$

Let $\varphi_a : \mathbb{Z}/n \to \mathbb{Z}/n$ denote the map $\varphi_a(x) := ax$. Then we have seen

$$\begin{aligned} \varphi : (\mathbb{Z}/n)^\times &\to \operatorname{Aut}(\mathbb{Z}/n) \\ a &\longmapsto \varphi_a \end{aligned}$$

is a bijection. It is an isomorphism because $\forall\, a, b \in (\mathbb{Z}/n)^\times$, $x \in \mathbb{Z}/n$,

$$\varphi_a(\varphi_b(x)) = a(bx) = (ab)x = \varphi_{ab}(x)$$

$\blacksquare$

Recall $G = P \rtimes_\theta Q$ with $\theta : P \to \mathrm{Aut}(Q)$.

We have $|\ker\theta| = 1$ or p. If $|\ker\theta| = p$ then θ is trivial, hence

$$G = P \times Q \approx \mathbb{Z}/p \times \mathbb{Z}/q.$$

This is actually cyclic because for all $(h,k) \in H \times K$, we have

$$|\langle (h,k) \rangle| = \mathrm{lcm}\left(|\langle h \rangle|, |\langle k \rangle| \right)$$

$$\Longrightarrow \quad G \approx \mathbb{Z}/(pq). \qquad ///$$

Otherwise we have $|\ker\theta| = 1$

$\Longrightarrow \quad |\mathrm{im}\,\theta| = |P| / |\ker\theta| = p.$

But we also have

$$|\mathrm{im}\,\theta| \;\Big|\; |\mathrm{Aut}(Q)| = |(\mathbb{Z}/q)^\times| = q-1$$

which is impossible unless $p \mid q-1$.

So assume $p \mid q-1$ and consider two nontrivial $\theta, \theta' : P \to \mathrm{Aut}(Q)$.

Claim: Then $P \rtimes_\theta Q$ and $P \rtimes_{\theta'} Q$ are isomorphic nonabelian groups.

Proof: If $P \rtimes_\theta Q$ is abelian, then $P \triangleleft P \rtimes_\theta Q \implies \theta$ is trivial.

Now let $P = \langle x \rangle$ and consider nontrivial $\theta, \theta' : P \to \mathrm{Aut}(Q)$. We know $|\theta(P)| = |\theta'(P)| = p$. But since $\mathrm{Aut}(Q)$ is cyclic (Primitive Root Theorem) it has a unique subgroup of order p.

$$\implies \theta(P) = \theta'(P).$$

Since $\theta'(x)$ is a generator of $\theta(P)$ we have $\theta(x) = \theta'(x)^a$ for some a. Then since $\theta(x)$ is also a generator of $\theta(P) = \theta'(P)$ we conclude that a, p are coprime, hence

$$\varphi : P \to P$$
$$x^m \longmapsto (x^m)^a = x^{am}$$

is an automorphism.

Then for all $x^m \in P$ we have

$$\begin{aligned}\theta(x^m) = \theta(x)^m &= (\theta'(x)^a)^m \\ &= (\theta'(x^a))^m \\ &= (\theta'(\varphi(x))^m \\ &= \theta'(\varphi(x^m))\end{aligned}$$

$$\Rightarrow \quad \theta = \theta' \circ \varphi .$$

Finally we define a map

$$\begin{aligned} F : P \ltimes_{\theta} Q &\longrightarrow P \ltimes_{\theta'} Q \\ (x, y) &\longmapsto (\varphi(x), y) \end{aligned}$$

and note that

$$F[(x_1,y_1)(x_2,y_2)] = F[(x_1x_2, \theta_{x_2}^{-1}(y_1)y_2)]$$

$$= (\varphi(x_1x_2), \theta_{x_2}^{-1}(y_1)y_2)$$

$$= (\varphi(x_1)\varphi(x_2), (\theta'_{\varphi(x_2)})^{-1}(y_1)y_2)$$

$$= (\varphi(x_1), y_1)(\varphi(x_2), y_2)$$

$$= F[(x_1,y_1)]F[(x_2,y_2)] .$$

Since F is invertible with

$$F^{-1}(x,y) = (\varphi^{-1}(x), y)$$

we conclude that F is an isomorphism.

∎

In summary we have

<u>Theorem</u>: Let $p<q$ be prime.

If $p \nmid q-1$ then $|G|=pq \Rightarrow G$ cyclic.

If $p \mid q-1$ then there are exactly two groups of order pq:

$\mathbb{Z}/(pq)$ and one non-abelian group

Tues Oct 8

HW 2.5 due now.
HW 3 due Tues Oct 22

HW 2.5 Discussion:

Let $G \curvearrowright X$ and consider the group of G-set automorphisms:

$$\text{Aut}_G(X) := \{\varphi \in \text{Aut}(X) : \varphi(g(x)) = g(\varphi(x)) \ \forall x \in X\}.$$

Assume that $G \curvearrowright X$ is transitive, i.e. $\forall x, y \in X \ \exists g \in G$ such that $g(x) = y$. Then by Orbit-Stabilizer we have

$$\frac{G}{\text{Stab}(x)} \approx_G \text{Orb}(x) = X = \text{Orb}(y) \approx_G \frac{G}{\text{Stab}(y)}.$$

So fix a basepoint $x_0 \in X$ and let

$$H := \text{Stab}(x_0).$$

Then we have

$$X \approx_G G/H$$

as G-sets.

☆ Theorem: Every transitive G-set is isomorphic to G/H for some $H \leq G$. Furthermore, we have

$$G/H \cong_G G/K$$

if and only if $H = gKg^{-1}$ for some $g \in G$. Thus we get a bijection

$$\left\{\begin{array}{c}\text{transitive}\\ G\text{-sets}\end{array}\right\} \longleftrightarrow \left\{\begin{array}{c}\text{conjugacy classes}\\ \text{of subgroups of } G\end{array}\right\}$$

///

First a Lemma:

If $\varphi : X \to Y$ is an isomorphism of G-sets, then $\forall\, x \in X$ we have

$$\mathrm{Stab}(x) = \mathrm{Stab}(\varphi(x)).$$

Proof: Let $g \in \mathrm{Stab}(x)$. Then

$$\varphi(x) = \varphi(g(x)) = g(\varphi(x))$$

$\Longrightarrow g \in \mathrm{Stab}(\varphi(x))$. Hence $\mathrm{Stab}(x) \leq \mathrm{Stab}(\varphi(x))$.

Applying the same result to $\varphi^{-1}: Y \to X$ gives

$$\mathrm{Stab}(\varphi(x)) \leq \mathrm{Stab}(\varphi^{-1}(\varphi(x))) = \mathrm{Stab}(x).$$

Hence $\mathrm{Stab}(x) = \mathrm{Stab}(\varphi(x))$. ▨

<u>Proof</u> of Theorem:

Given $H \leq G$, note that G/H is a transitive G-set under left multiplication. We already saw that every trans. G-set X is $\cong$ to G/H for some $H \leq G$.

Suppose that $\varphi: G/H \to G/K$ is a G-isomorphism and let $\varphi(H) = gK$. By the Lemma,

$$\begin{aligned} H = \mathrm{Stab}(H) = \mathrm{Stab}(gK) &= g\,\mathrm{Stab}(K)g^{-1} \\ &= gKg^{-1}. \end{aligned}$$

Conversely, suppose $H = gKg^{-1}$ for some $g \in G$.

$$\begin{aligned} \text{Then } H &= gKg^{-1} \\ &= g\,\mathrm{Stab}(K)\,g^{-1} \\ &= \mathrm{Stab}(gK) \end{aligned}$$

Hence Orbit-Stabilizer implies.

$$G/K = \mathrm{Orb}(gK) \approx_G \frac{G}{\mathrm{Stab}(gK)} = G/H$$

▨

[Later, we will prove a similar theorem for <u>G-modules</u> of finite groups.

<u>Def</u>: Given a vector space V and a hom $\alpha : G \to \mathrm{Aut}(V) = GL(V)$, we say that (V, α) is a G-module.

Namely, we will have a bijection

$$\left\{ \begin{array}{c} \text{irreducible} \\ G\text{-modules}/\mathbb{C} \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{conjugacy classes} \\ \text{of elements in } G \end{array} \right\}$$]

Finally let $G \curvearrowright X$ be transitive, say $X \approx G/H$ and consider the group

$$\mathrm{Aut}_G(X) \approx \mathrm{Aut}_G(G/H).$$

Theorem:

$$\mathrm{Aut}_G(G/H) \approx N_G(H)/H$$

Proof: let $n \in N_G(H)$ so that $Hn^{-1} = n^{-1}H$. Define a function

$$\theta_n : G/H \longrightarrow G/H$$

by $\theta_n(gH) := (gH)n^{-1} = (gn^{-1})H \in G/H$. It's a bijection with inverse $\theta_n^{-1} = \theta_{n^{-1}}$ and its a G-hom since $\forall\, C \in G/H$ and $g \in G$ we have

$$g(\theta_n(C)) = g(Cn^{-1}) = (gC)n^{-1} = \theta_n(g(C)).$$

Thus we get a function

$$\begin{aligned} \theta : N_G(H) &\longrightarrow \mathrm{Aut}_G(G/H) \\ n &\longmapsto \theta_n \end{aligned}$$

Note that θ is a group hom since $\forall\, m,n \in N_G(H)$ and $C \in G/H$ we have

$$\begin{aligned} \theta_{mn}(C) = C(mn)^{-1} = C(n^{-1}m^{-1}) &= (Cn^{-1})m^{-1} \\ &= \theta_m \circ \theta_n(C). \end{aligned}$$

The kernel is $\ker\theta = H$ because

$$\theta_n = \mathrm{id} \iff gHn^{-1} = gH \quad \forall\, g \in G$$
$$\iff n \in H.$$

Finally we will show that θ is surjective. Consider any $\varphi \in \mathrm{Aut}_G(G/H)$ and let $\varphi(H) = n^{-1}H$ for some $n \in G$. We know from the Lemma that

$$H = \mathrm{Stab}(H) = \mathrm{Stab}(\varphi(H)) = \mathrm{Stab}(n^{-1}H)$$
$$= n^{-1}\mathrm{Stab}(H)\,n = n^{-1}Hn$$

$\Rightarrow n \in N_G(H)$. Then for all $gH \in G/H$ we have

$$\varphi(gH) = g(\varphi(H)) = g(n^{-1}H) = (gH)n^{-1}$$

$\Rightarrow \varphi = \theta_n$. We conclude that

$$\mathrm{Aut}_G(G/H) = \mathrm{im}\,\theta \approx \frac{N_G(H)}{\ker\theta} = \frac{N_G(H)}{H}.$$

▨

Special Case:

If $G \curvearrowright X$ is free and transitive then stabilizers are trivial and we get

$$\mathrm{Aut}_G(X) \approx \frac{N_G(1)}{1} = \frac{G}{1} \approx G.$$

Back to counting groups.

Order	# isomorphism classes
1	1
2	1
3	1
4	2
5	1
6	2
7	1
8	$\boxed{5}$
9	2
10	2
11	1
12	$\boxed{5}$
13	1
14	2
15	1
16	$\boxed{14}$

General Facts

Order	Groups .
p	$\mathbb{Z}/p$.
$2p$	$\mathbb{Z}/(2p)$ and D_{2p}
pq , $p<q$ $(p \nmid q-1)$	$\mathbb{Z}/(pq)$.
pq , $p<q$ $(p \mid q-1)$	$\mathbb{Z}/(pq)$ and one nonabelian
p^3	5 groups
$\vdots$	
p^k	# groups $\geq p^{\frac{2}{27}k^2(k-6)}$ (Theorem of Higman)

That's a lot !

What if we're looking for simple groups?

Theorem: If $|G| = p^\alpha$, $\alpha \geq 2$, then G is not simple.

Proof: Look at Class Equation:

$$|G| = |Z(G)| + \sum_{\substack{i \\ C(x_i) \neq G}} |G| / |C(x_i)|$$

If $C(x_i) \neq G$ (i.e. $x_i \notin Z(G)$) then p divides $|G| / |C(x_i)|$.

$\Longrightarrow \quad p \mid Z(G)$

$\Longrightarrow \quad 1 \underset{\neq}{\leq} Z(G) \trianglelefteq G$.

If $Z(G) \underset{\neq}{\trianglelefteq} G$ then G is not simple.

If $Z(G) = G$ then G is abelian and has lots of (normal) subgroups.

$\blacksquare$

Theorem: If $|G| = p^\alpha m$ with $p \nmid m$. and $m < p$, then G is not simple.

Proof: Let $n_p = |Syl_p(G)|$. Then we know that $n_p = 1 \mod p$ and $n_p \mid m$ hence $n_p \leq m < p$.

It follows that $n_p = 1$, so G has a unique (hence normal) Sylow p-subgroup. $\blacksquare$

Theorem (Burnside, 1904):

If $|G| = p^\alpha q^\beta$ for p, q prime then G is solvable.

If $\{\alpha, \beta\} \neq \{0, 1\}$ this means G is not simple.

Theorem (Feit-Thompson, 1962):

If $|G| =$ odd then G is solvable.

The smallest order not yet accounted for is $|G| = 30 = 2 \cdot 3 \cdot 5$

HW3 : $|G| = 30 \Rightarrow G$ not simple.

The smallest nonabelian simple groups are.

	order	names
$2^2 \cdot 3 \cdot 5 =$	60	$A_5 = PSL(2,4) = PSL(2,5)$
$2^3 \cdot 3 \cdot 7 =$	168	$PSL(2,7) = PSL(3,2)$
$2^3 \cdot 3^2 \cdot 5 =$	360	$A_6 = PSL(2,9)$
	⋮	⋮

It gets complicated