Thur Sept 5

Current Goal: Jordan-Hölder.

Last Time: Isomorphism Theorems

- If $\varphi: G \to G'$ is a homomorphism then

$$G/\ker\varphi \cong \operatorname{im}\varphi.$$

- If $N \trianglelefteq H \trianglelefteq G$ then

$$\frac{G/N}{H/N} \cong G/H.$$

- If $H, K \leq G$ and $K \trianglelefteq G$ then $HK \leq G$ and we have

$$H/H\cap K \cong HK/K.$$

Today: Products of Groups.

Given subgroups $H, K \leq G$, when is

$$HK := \{hk : h \in H, k \in K\} \subseteq G$$

a subgroup of G?

Theorem: $HK \leq G \iff HK = KH$.

Assume $HK = KH$ and consider two elements h_1k_1 and $h_2k_2 \in HK$. We wish to show that $(h_1k_1)(h_2k_2)^{-1}$ $= h_1k_1k_2^{-1}h_2^{-1}$ is in HK.
So let $k_3 = k_1k_2^{-1} \in K$ and $h_3 = h_2^{-1} \in H$.
Since $k_3h_3 \in KH = HK$, $\exists\ h_4 \in H$ and $k_4 \in K$ such that $k_3h_3 = h_4k_4$.
Hence

$$(h_1k_1)(h_2k_2)^{-1} = h_1k_3h_3$$
$$= h_1h_4k_4 \in HK$$

and we conclude that $HK \leq G$ ///

Conversely, assume $HK \leq G$ and consider any $hk \in HK$. Since $(hk)^{-1} \in HK$ we have $(hk)(h'k') = 1$ for some $h' \in H$, $k' \in K$. But then

$$hk = (k')^{-1}(h')^{-1} \in KH,$$

hence $HK \subseteq KH$. The other direction is similar.

[Note: This always holds in abelian groups and we write

$$HK = H + K \quad]$$

Even when $HK \neq KH$ we can still define a surjective function from the Cartesian product:

$$\mu : H \times K \twoheadrightarrow HK \subseteq G$$
$$(h, k) \longmapsto hk$$

Properties:

- μ is injective $\iff H \cap K = \{1\}$.

Proof: Assume $H \cap K \neq \{1\}$, and consider $1 \neq x \in H \cap K$. Then

$$\mu(x, x^{-1}) = xx^{-1} = 1 = \mu(1, 1),$$

so μ is not injective. ///.

Conversely, assume $H \cap K = \{1\}$, and suppose that

$$\mu(h_1, k_1) = h_1 k_1 = h_2 k_2 = \mu(h_2, k_2)$$

for some $h_1, h_2 \in H$, $k_1, k_2 \in K$. Then

$$h_2^{-1} h_1 = k_2 k_1^{-1} \in H \cap K.$$

$h_2^{-1} h_1 \in H$, $k_2 k_1^{-1} \in K$.

Hence $h_2^{-1} h_1 = k_2 k_1^{-1} = 1$

$\Longrightarrow h_1 = h_2$ and $k_1 = k_2$

$\Longleftrightarrow (h_1, k_1) = (h_2, k_2)$ ▨

In this case each $x \in HK$ has a unique expression $x = hk$.

Def: There is an obvious group structure on $H \times K$ called the direct product

$$(h_1, k_1) \cdot (h_2, k_2) := (h_1 h_2, k_1 k_2). \quad ///$$

- The map $\mu : H \times K \longrightarrow G$.
  $(h, k) \longmapsto hk$.
  is a group homomorphism
  $\Updownarrow$.
  we have $hk = kh \quad \forall h \in H, k \in K$.

Proof: Given $(h_1, k_1), (h_2, k_2) \in H \times K$ we have.

$$\mu((h_1, k_1) \cdot (h_1, k_2)) = \mu(h_1 h_2, k_2, k_2)$$
$$= h_1 h_2 k_2 k_2 .$$

and

$$\mu(h_1, k_1) \cdot \mu(h_2, k_2) = h_1 k_1 h_2 k_2 .$$

Note that $h_1 h_2 k_2 k_2 = h_1 k_1 h_2 k_2$

$$\Updownarrow$$

$$h_2 k_1 = k_1 h_2$$

□

- Finally, we have that

($\mu : H \times K \longrightarrow G$ is an isomorphism)

if and only if

($H \cap K = \{1\}$, $H \trianglelefteq G$, $K \trianglelefteq G$, $HK = G$.)

Proof: If $G \cong H \times K$ then we can identify H, K as the corresponding subgroups of $H \times K$:

$$H = \{(h, 1_K) : h \in H\} \leq H \times K$$
$$K = \{(1_H, k) : k \in K\} \leq H \times K$$

Certainly the desired properties hold.

Conversely, suppose that $H \cap K = \{1\}$, $H \trianglelefteq G$, $K \trianglelefteq G$, and $HK = G$, and consider the map $\mu : H \times K \to G$.

It is a hom because $\forall\, h \in H, k \in K$ we have

$$hkh^{-1}k^{-1} = \underbrace{(hkh^{-1})k^{-1}}_{\in K} = \underbrace{h(kh^{-1}k^{-1})}_{\in H} \in H \cap K.$$

$$\Rightarrow hkh^{-1}k^{-1} = 1$$
$$\Rightarrow hk = kh \qquad ///.$$

Then $H \cap K = \{1\} \Rightarrow \mu$ injective
and $HK = G \Rightarrow \mu$ surjective

[Note: When G is abelian we always have $H \trianglelefteq G$ and $K \trianglelefteq G$, and we use a different notation:

$G = H \oplus K \iff G = H + K$
"direct sum" and $H \cap K = \{0\}$.

Compare to vector spaces.]

Q: What if only one of H, K is normal, say $K \trianglelefteq G$?

A: If we have

$H \cap K = \{1\}$, $H \leq G$, $K \trianglelefteq G$, $HK = G$,

we still want to say that G is a "product" of H and K, but it is not the direct product.

We will call it a semi-direct product. (or a "twisted" direct product)

The group operation is

$$(h_1, k_1)(h_2 k_2) = \underbrace{[h_1 h_2]}_{H}\underbrace{[(h_2^{-1} k_1 h_2) k_2]}_{K}$$

and we can write this as a group operation on the set $H \times K$.

$$(h_1, k_1) \circ (h_2, k_2) := (h_1 h_2, (h_2^{-1} k_1 h_2) k_2)$$

To avoid confusion we call this group structure $H \rtimes K$.

Can we abstract this?
Given abstract groups H and K (not necessarily subgroups of anything). How should we define a "semi-direct product" of H and K?

Def: Consider groups H, K and a group hom $\theta : H \longrightarrow Aut(K)$.

$$h \longmapsto (\theta_h : K \to K)$$

We define a group operation on the set $H \times K$ by.

$$(h_1, k_1) \circ (h_2, k_2) := (h_1 h_2, \theta_{h_2^{-1}}(k_1) k_2).$$

We call this the semidirect product of H and K with respect to $\theta : H \to \mathrm{Aut}(K)$ and we denote it by.

$$\boxed{H \rtimes_\theta K}$$

Remarks:

- Note that $H \rtimes_\theta K \approx H \times K$ ("untwisted")

$\iff \theta : H \to \mathrm{Aut}(K)$ is the trivial map.
$h \to (\mathrm{id} : K \to K)$

- If $H \leq G$, $K \trianglelefteq G$, $H \cap K = \{1\}$, $HK = G$

Then $G \approx H \rtimes_\theta K$ where θ is defined by.

$$\theta : H \to \mathrm{Aut}(K).$$
$$h \mapsto \theta_h.$$

where $\theta_h(k) := hkh^{-1}$ $\forall h \in H, k \in K$.
conjugation.

Tues Sept 10

HW 2 due Tues Sept 24

Today: Semi-direct Products continued...

Definition: We say group G acts on X if we have a homomorphism

$$\theta : G \longrightarrow Aut(X)$$
$$g \longmapsto (\theta_g : X \to X)$$

We usually write $\theta_g(x) = "g(x)"$

Because θ is a hom we have

- $\theta_1 = id : X \to X$

  i.e. $1(x) = x$ for all $x \in X$.

- $\theta_g \circ \theta_h = \theta_{gh}$

  i.e. $g(h(x)) = (gh)(x) \quad \forall\, g, h \in G, x \in X$.

We may ask θ_g to preserve structure of X (if it has any).

Recall: Given groups H, K and an action

$$\theta : H \longrightarrow Aut(K)$$

We can define the semidirect product as the set $H \times K$ with operation.

$$(h_1, k_1) * (h_2, k_2) := (h_1 h_2, \theta_{h_2}^{-1}(k_1) k_2)$$

We call it $H \rtimes_\theta K$ or $K \rtimes_\theta H$

Define subgroups

$$H \approx \tilde{H} = \{(h, 1_K) : h \in H\}$$
$$K \approx \tilde{K} = \{(1_H, k) : k \in K\}$$

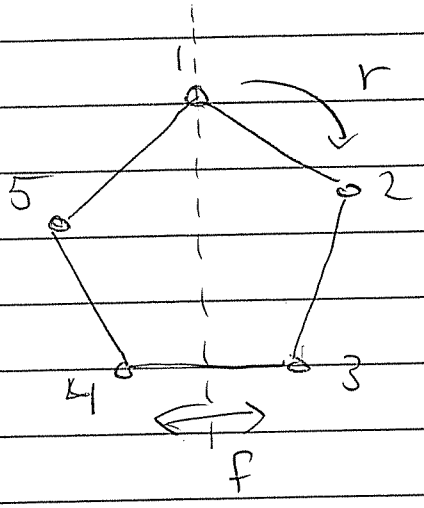
HW 2.3 asks you to show that

- $\tilde{H} \cap \tilde{K} = \{1\}$
- $\tilde{H}\tilde{K} = H \rtimes_\theta K$
- $\tilde{K} \trianglelefteq H \rtimes_\theta K$

Two important examples:

(1) Finite Example

Let D_n be group of symmetries of regular n-gon.



Let f be a flip
Let r be a rotation.

Observe:

$$rf = fr^{-1}$$

D_n is called a dihedral group

Claim: $D_n = \langle r \rangle \rtimes \langle f \rangle$

Proof: We need to check

$D_n = \langle r \rangle \langle f \rangle$, $\langle r \rangle \trianglelefteq D_n$, $\langle r \rangle \cap \langle f \rangle = \{1\}$.

$\langle r \rangle \cap \langle f \rangle = \{1\}$ is easy.

Consider any $g \in D_n$. Suppose it takes vertex 1 to vertex i. Then either

(1) $r^{-i}g = 1 \implies g = r^i \in \langle r \rangle \langle f \rangle$

OR

(2) $fr^{-i}g = 1 \implies g = r^i f \in \langle r \rangle \langle f \rangle$

We conclude $D_n = \langle r \rangle \langle f \rangle$.

Finally, for any $r^k \in \langle r \rangle$ we have

$$r^i r^k r^{-i} = r^k \in \langle r \rangle$$

OR

$$\begin{aligned}(r^i f) r^k (r^i f)^{-1} &= r^i f r^k f r^{-i} \\ &= r^i r^{-k} r^{-i} \\ &= r^{-k} \quad \in \langle r \rangle.\end{aligned}$$

Hence $\langle r \rangle \trianglelefteq D_n$ ∎

The action of $\langle f \rangle$ on $\langle r \rangle$ is

$$\theta_f(r) = frf^{-1} = frf = r^{-1}$$

inversion.

Note $D_n \cong \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$.

$\Rightarrow |D_n| = 2n$.

Dihedral groups are important.

Theorem (Prop 1.2.13 in Alperin):

Consider group G with elements $s, t \in G$ of order 2 (involutions). Then.

$\langle s, t \rangle$ is dihedral.

Proof: We'll show $\langle s,t \rangle = \langle s \rangle \rtimes \langle st \rangle$ where $\langle s \rangle$ acts on $\langle st \rangle$ by inversion:

$s(st)s = (ss)ts = ts = (st)^{-1} \in \langle st \rangle$.

$\Rightarrow s(st)^n s = (st)^{-n}$ for all n. ///

- Claim: $\langle s,t \rangle = \langle s \rangle \langle st \rangle$.

↓

Every element of $\langle s,t \rangle$ looks like

$s, st, sts, stst, \cdots$

$t, ts, tst, tsts, \cdots$

4 cases
(1) $s(ts)^n = s(st)^{-n} \in \langle s \rangle \langle st \rangle$
(2) $(st)^n \in \langle s \rangle \langle st \rangle$
(3) $(ts)^n = (st)^{-n} \in \langle s \rangle \langle st \rangle$
(4) $(ts)^n t = ss(ts)^n t$
$= s(st)^{n+1} \in \langle s \rangle \langle st \rangle$

///

- Claim: $\langle s \rangle \cap \langle st \rangle = \{1\}$.

If $s = (st)^n$ then

$$1 = \underbrace{tsts \cdots st}_{n-1}$$

Conjugating by t gives

$$1 = \underbrace{stst \cdots ts}_{n-3}.$$

Continue until $1 = s$

///

• Claim: $\langle st \rangle \trianglelefteq \langle s, t \rangle$.

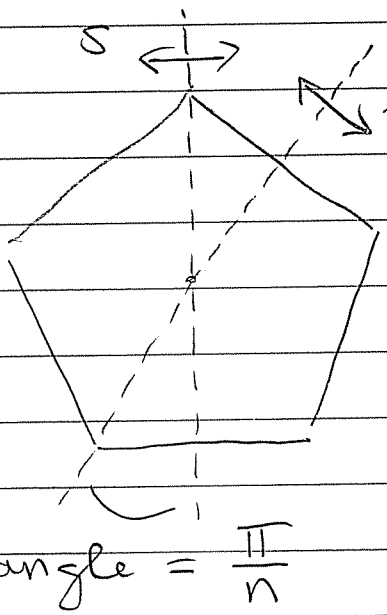
Indeed, $s(st)s = ts = (st)^{-1} \in \langle st \rangle$

$t(st)t = ts = (st)^{-1} \in \langle st \rangle$ ///

Hence $\langle s, t \rangle = \langle s \rangle \rtimes \langle st \rangle$

$\cong$ dihedral of order $2|\langle st \rangle|$

Picture: D_n is generated by two adjacent reflections



st is a rotation of order n.

$D_n = \langle s \rangle \rtimes \langle st \rangle$.

(2) Matrix Example

Let $\mathrm{Isom}(\mathbb{R}^n) = \{\text{isometries } f : \mathbb{R}^n \to \mathbb{R}^n\}$

$\mathrm{Isom}_0(\mathbb{R}^n) = \{\varphi \in \mathrm{Isom}(\mathbb{R}^n) : \varphi(0) = 0\}$.

[Remark: It happens that

$$\mathrm{Isom}_0(\mathbb{R}^n) = O(n) \leq GL(n, \mathbb{R})$$

Proof omitted.]

Given $\alpha \in \mathbb{R}^n$ define the "translation" $t_\alpha : \mathbb{R}^n \to \mathbb{R}^n$ by $t_\alpha(x) := x + \alpha$.

Note:
- $t_\alpha \circ t_\beta = t_{\alpha+\beta}$
- $t_\alpha \in \mathrm{Isom}(\mathbb{R}^n)$.

We get a subgroup

$$\mathbb{R}^n_+ := \{t_\alpha : \alpha \in \mathbb{R}^n\} \leq \mathrm{Isom}(\mathbb{R}^n)$$

isomorphic to $(\mathbb{R}^n, +, 0)$.

Claim: $\mathrm{Isom}(\mathbb{R}^n) = \mathbb{R}^n_+ \rtimes O(n)$.

Proof:

- Note $\mathbb{R}^n_+ \cap O(n) = \{1\}$.

- Consider $f \in \mathrm{Isom}(\mathbb{R}^n)$ and let $a := f(0)$. Then $\varphi := t_{-a} \circ f \in O(n)$ because

$$t_{-a} \circ f(0) = t_{-a}(f(0)) = t_{-a}(a) = a - a = 0.$$

Hence $f = t_a \circ \varphi$ and

$$\mathrm{Isom}(\mathbb{R}^n) = \mathbb{R}^n_+ O(n).$$

- Given $t_a \in \mathbb{R}^n_+$ and $\varphi \in O(n)$ we have.

$\forall x \in \mathbb{R}^n$,

$$\varphi \circ t_a(x) = \varphi(x+a) = \varphi(x) + \varphi(a) = t_{\varphi(a)}(\varphi(x)) = t_{\varphi(a)} \circ \varphi\,(x).$$

(φ linear)

Hence $\varphi \circ t_a = t_{\varphi(a)} \circ \varphi$

OR $\boxed{\varphi \circ t_\alpha \circ \varphi^{-1} = t_{\varphi(\alpha)}}$

Finally, for any $t_\beta \circ \varphi \in \mathrm{Isom}(\mathbb{R}^n)$ and any $t_\alpha \in \mathbb{R}^n_+$ we have

$$(t_\beta \circ \varphi) \circ t_\alpha \circ (t_\beta \circ \varphi)^{-1}$$

$$= t_\beta \circ \boxed{\varphi \circ t_\alpha \circ \varphi^{-1}} \circ t_{-\beta}$$

$$= t_\beta \circ t_{\varphi(\alpha)} \circ t_{-\beta} = t_{\varphi(\alpha)} \in \mathbb{R}^n_+ .$$

Hence $\mathbb{R}^n_+ \trianglelefteq \mathrm{Isom}(\mathbb{R}^n)$.

We conclude that

$$\mathrm{Isom}(\mathbb{R}^n) = \mathbb{R}^n_+ \rtimes O(n).$$

the natural action ☺

Thurs Sept 12

HW 2 due Tues Sept 24.

Today: Jordan-Hölder.

Def: We say group G is simple if the existence of a surjective hom

$$\varphi : G \twoheadrightarrow G'$$

implies that $G' \simeq 1$ or $G' \simeq G$.

Equivalently, G has no nontrivial normal subgroups. Indeed, every normal subgroup is the kernel of a surjective hom

$$\varphi : G \twoheadrightarrow G'$$

with

$$G' \simeq G/\ker\varphi \begin{cases} \simeq 1 \iff \ker\varphi = G \\ \simeq G \iff \ker\varphi = 1 \end{cases}$$

Simple groups are the "prime numbers" of group theory.

Examples:

(1) For each $n \in \mathbb{N}$ there is a unique cyclic group of order n. We call it $\mathbb{Z}/n\mathbb{Z}$. Since a cyclic group is abelian, every subgroup is normal. Recall that

$$\mathcal{L}(\mathbb{Z}/n\mathbb{Z}) \simeq D(n) = \text{lattice of divisors of } n.$$

We conclude that

$\mathbb{Z}/n\mathbb{Z}$ is simple $\iff$ n is prime.

Furthermore, let G be any group of prime order p and choose $1 \neq g \in G$. Since $|\langle g \rangle|$ divides $|G|$ we conclude that

$$G = \langle g \rangle \simeq \mathbb{Z}/p\mathbb{Z}.$$

Fact: These are the only finite abelian simple groups

Proof: Postponed.

(2) The smallest non-abelian simple group is.

I = rotational symmetries of the regular icosahedron.

It has order $60 = 2 \cdot 2 \cdot 3 \cdot 5$

(3) The second smallest non-abelian simple group has order 168. It is the group of automorphisms of the "Klein quartic curve"

i.e. the zero set in $\mathbb{CP}^2 \left(= Gr(1, \mathbb{C}^3)\right)$ of the polynomial

$$x^3y + y^3z + z^3x$$

It is isomorphic to

$$PSL(3, \mathbb{F}_2) = \frac{SL(3, \mathbb{F}_2)}{Z(SL(3, \mathbb{F}_2))}.$$

(4) Define the special orthogonal group

$$SO(n) := \{ A \in GL(n, \mathbb{R}) : A^t A = I, \det(A) = 1 \}$$

Then $SO(2m+1)$ is simple for $m \geq 1$

The center of $SO(2m)$ for $m \geq 2$ equals $\{\pm I\}$ and

$SO(2m+1)/\{\pm I\}$ is simple. ///

==

Today we will prove the

Jordan-Hölder Theorem (~1869):

Every finite group (and some infinite) has an essentially unique "factorization" into simple groups.

First define "factorization"

Def: Given a group, we say that a chain

$$G = G_0 \rhd G_1 \rhd G_2 \rhd \cdots \rhd G_r = 1$$

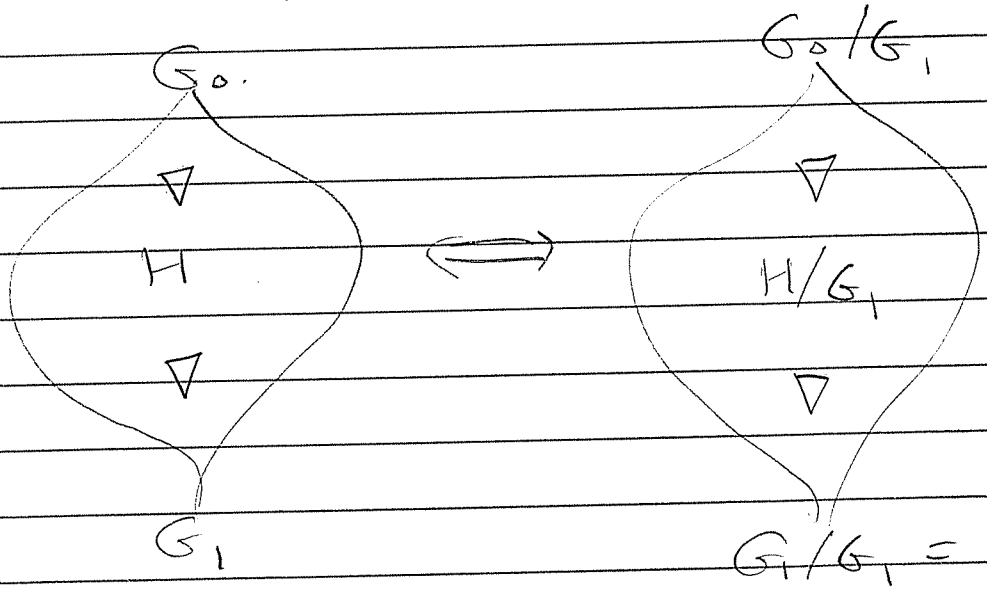
is a composition series if G_i/G_{i+1} is simple for all i. These simple groups are the "composition factors" of the series.

Prop (10.1 in Alperin):
Finite groups have composition series.

Proof: If G is simple, done.
If G is not simple, choose a maximal normal subgroup $G_1 \triangleleft G$.
By induction G_1 has a comp series

$$G_1 \triangleright G_2 \triangleright \cdots \triangleright G_r = 1$$

We obtain $G = G_0 \triangleright G_1 \triangleright G_2 \triangleright \cdots \triangleright G_r = 1$
and note that G_0/G_1 is simple because G_1 is maximal:



Exercise: Show that $(\mathbb{Z}, +, 0)$ has no composition series.

Lemma (10.2 in Alperin): Consider $N \trianglelefteq G$. If G has a comp series then so does N.

Proof: Let $G = G_0 \rhd G_1 \rhd \cdots \rhd G_r = 1$ be a comp series and define $N_i = N \cap G_i \ \forall i$. Check that

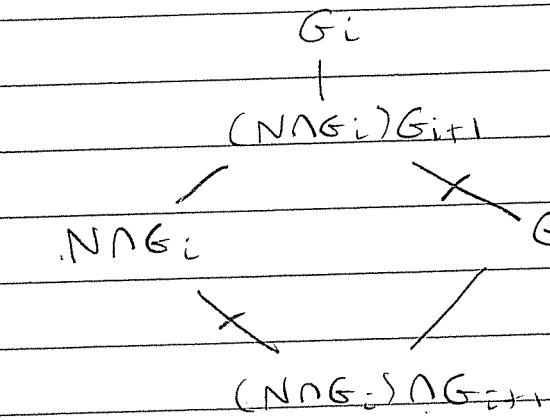
$$N = N_0 \trianglerighteq N_1 \trianglerighteq \cdots \trianglerighteq N_r = 1$$

with possible repetition.

Claim: N_i / N_{i+1} is $\cong$ to a normal subgroup of $G_i / G_{i+1} \quad \forall i$.

Proof of claim: Note that

$$N_{i+1} = N \cap G_{i+1} = N \cap (G_i \cap G_{i+1}) = (N \cap G_i) \cap G_{i+1}.$$



Diamond Isomorphism:

$$\frac{N_i}{N_{i+1}} = \frac{N \cap G_i}{(N \cap G_i) \cap G_{i+1}} \cong \frac{(N \cap G_i) G_{i+1}}{G_{i+1}}$$

Consider the canonical map $\varphi : G_i \to G_i / G_{i+1}$.

Then
- $\varphi(G_i) = G_i / G_{i+1}$
- $\varphi(N \cap G_i) = (N \cap G_i) G_{i+1} / G_{i+1}$
- $\varphi(N \cap G_i) \trianglelefteq \varphi(G_i)$.

Hence $N_i / N_{i+1} \cong \varphi(N \cap G_i) \trianglelefteq \varphi(G_i) = G_i / G_{i+1}$ ///

But we assumed that G_i / G_{i+1} is simple.

Hence either $N_i / N_{i+1} \cong G_i / G_{i+1}$ (and is simple) or $N_i = N_{i+1}$. By removing repetition in

$$N = N_0 \trianglerighteq N_1 \trianglerighteq \cdots \trianglerighteq N_r = 1$$

we obtain a composition series

∎

We say two composition series

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_r = 1$$
$$G = H_0 \rhd H_1 \rhd \cdots \rhd H_s = 1$$

are equivalent if

- $r = s$
- the composition factors are the same (up to reordering)

Theorem (Jordan-Hölder, 1869 $\rightarrow$).

If G has a composition series, then any two comp. series are equivalent (and we can speak of "the composition factors of G").

Proof: Suppose G has two comp series

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_r = 1$$
$$G = H_0 \rhd H_1 \rhd \cdots \rhd H_s = 1.$$

Induction on r. If $r = 1$ then $G/1$ is simple $\Longrightarrow$ $s = 1$ and the series are equivalent.

Let $r > 1$. If $G_1 = H_1$ then G_1 has two comp series of lengths $r-1$ and $s-1$. By induction, $r-1 = s-1$ ($\Rightarrow r = s$) and we have that

$$\begin{array}{ccccccccc} G = G_0 & \triangleright & G_1 & \triangleright & G_2 & \triangleright & \cdots & \triangleright & G_r = 1 \\ \updownarrow & & \| & \{ & \text{matching} & & & \} & \\ G = H_0 & \triangleright & H_1 & \triangleright & H_2 & \triangleright & \cdots & \triangleright & H_r = 1 \end{array}$$

are equivalent.

Now assume $G_1 \neq H_1$. Since $G_1 \trianglelefteq G$ and $H_1 \trianglelefteq G$ we know that $G_1 H_1 \trianglelefteq G$.
[Proof: $g(ab)g^{-1} = (gag^{-1})(gbg^{-1})$.]

Claim: In fact, $G_1 H_1 = G$.

Proof of Claim: If $G_1 < H_1 \trianglelefteq G$, then $H_1/G_1 \trianglelefteq G/G_1$. But we assumed G/G_1 simple. Hence $G_1 \not\trianglelefteq H_1$.

Then $H_1 < G_1 H_1 \trianglelefteq G$. If $G_1 H_1 \trianglelefteq G$ then $G_1 H_1 / H_1 \trianglelefteq G/H_1$. But we assumed G/H_1 simple. Hence $G_1 H_1 = G$. ///

Now let $K := G_1 \cap H_1$. By Diamond Isom. we have simple groups

$$\frac{H_1}{K} \cong \frac{G}{G_1} \quad \text{and} \quad \frac{G_1}{K} \cong \frac{G}{H_1}.$$

By the Lemma, K has a comp series.

$$K = K_0 \rhd K_1 \rhd \cdots \rhd K_t = 1.$$

Thus G_1 has two comp series.

$$G_1 \rhd G_2 \rhd G_3 \rhd \cdots \rhd G_r = 1$$
$$G_1 \rhd K \rhd K_1 \rhd \cdots \rhd K_t = 1$$

By induction, $r-1 = t+1$ and the series are equivalent. Similarly, the series

$$H_1 \rhd H_2 \rhd H_3 \rhd \cdots \rhd H_s = 1$$
$$\& \quad H_1 \rhd K \rhd K_1 \rhd \cdots \rhd K_{r-2} = 1.$$

are equivalent, with $s-1 = r-1$ (i.e. $r = s$).

Finally, we have equivalences

$$G = G_0 \rhd G_1 \rhd G_2 \rhd G_3 \rhd \cdots \rhd G_r = 1$$
$$\Big| \wr \text{ matching } \wr$$
$$G = G_0 \rhd G_1 \rhd K \rhd K_1 \rhd \cdots \rhd K_{r-2} = 1$$
$$\Big| \quad \Big| \quad \Big|$$
$$G = H_0 \rhd H_1 \rhd K \rhd K_1 \rhd \cdots \rhd K_{r-2} = 1$$
$$\Big| \wr \text{ matching } \wr$$
$$G = H_0 \rhd H_1 \rhd H_2 \rhd H_3 \rhd \cdots \rhd H_r = 1.$$

∎

Why do we care?

Def: We say G is solvable if its composition factors are all cyclic (i.e. of the form $\mathbb{Z}/p\mathbb{Z}$).

Theorem (Galois, before 1830).

A polynomial is "solvable by radicals" if and only if its Galois group is solvable.

Tues Sept 17

HW 2 due Tues Sept 24

Next Topic:
Classification of Finite Groups

Recall: Jordan-Hölder

A sub-normal series

$$G = G_0 \triangleright G_1 \triangleright G_2 \triangleright \cdots \triangleright G_r = 1$$

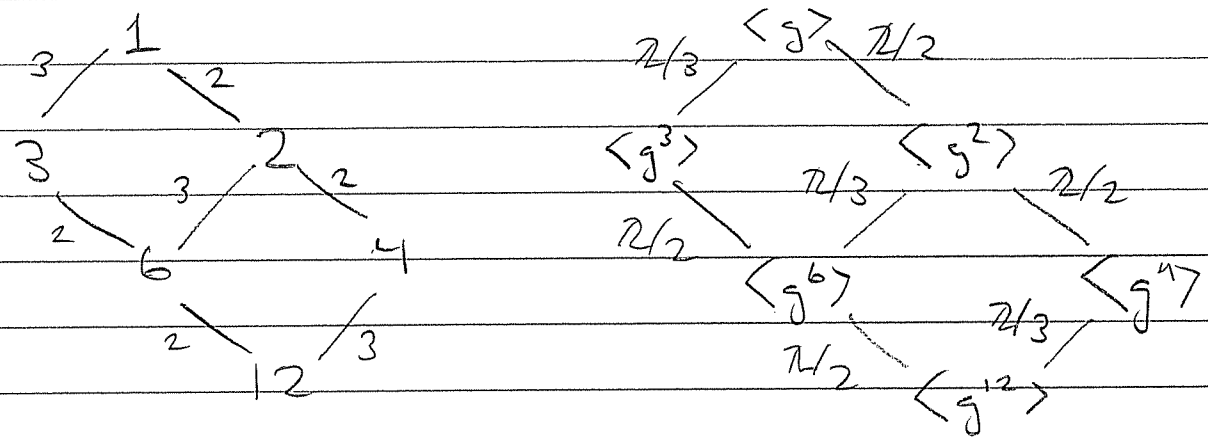
is called a composition series if G_i/G_{i+1} is simple $\forall\, i$.

Theorem (J-H): If G has a composition series then any two such are equivalent.

The groups G_i/G_{i+1} are called the "composition factors" of G.

For abelian groups, J-H is just the fundamental theorem of arithmetic.

Example: $G = \langle g \rangle$ of order 12.



There are three composition series.

$3 \cdot 2 \cdot 2$	$\mathbb{Z}/3, \mathbb{Z}/2, \mathbb{Z}/2$
$2 \cdot 3 \cdot 2$	$\mathbb{Z}/2, \mathbb{Z}/3, \mathbb{Z}/2$
$2 \cdot 2 \cdot 3$	$\mathbb{Z}/2, \mathbb{Z}/2, \mathbb{Z}/3$

Q: Why do we care about composition factors?

A: Def: A finite group is called solvable if its composition factors are abelian.
(i.e. of the form $\mathbb{Z}/p$ for some prime p)

Now consider a polynomial $f(x) \in k[x]$ over field k and let $k \subseteq K$ be the splitting field. Recall the definition of the Galois group

$$\mathrm{Gal}(K,k) := \{ \varphi \in \mathrm{Aut}(K) : \varphi(a) = a \ \forall a \in k \}.$$

Here is why we care.

Theorem (Galois, pre-1830):

The roots of $f(x)$ can be expressed in terms of the coefficients using $+, -, \times, \div, \sqrt[n]{\ }$ for various n.

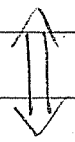
(we say $f(x) = 0$ is "solvable by radicals").

$\Updownarrow$

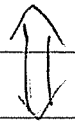
The group $\mathrm{Gal}(K,k)$ is solvable

Special case:

The roots of $f(x)$ are "constructible" from the coefficients using straightedge and compass (i.e. $+, -, \times, \div, \sqrt[2]{\ }$)



The comp. factors of $Gal(K,k)$ are all $\mathbb{Z}/2$.



$|Gal(K,k)|$ is a power of 2.
(we call it a "2-group")

Example: The roots of $ax^2 + bx + c = 0$ are

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

These are constructible and the Galois group is $\mathbb{Z}/2$. ///

If $f(x) \in k[x]$ has splitting field K, not that each $\varphi \in Gal(K,k)$ permutes the roots of $f(x)$ because.

$$f(\alpha) = 0 \iff \varphi(f(\alpha)) = 0$$
$$\iff f(\varphi(\alpha)) = 0.$$

If $f(x)$ has degree n, then.

$Gal(K,k) \leq S_n$ = group of permutations of n things

$$|Gal(K,k)| \leq |S_n| = n!$$

We know that every group of order < 60 is solvable, hence:

polynomials of degree 3 & 4 are solvable.
(as was known to Cardano, 1545).

Q: Is the general quintic solvable?

Theorem (Abel-Galois, pre-1830):

No!

Proof: The general quintic has Galois group S_5, and S_5 is not solvable. ∎

Let me explain.

Given a set X of size n, let

$$S_n := \mathrm{Aut}(X)$$
$$= \text{the group of permutations } X \to X$$

Note: $|S_n| = n!$

Think of $S_n \leq GL(n, \mathbb{Z})$ as permutation matrices.

e.g.

$$S_3 = \left\{ \begin{pmatrix} 1 & & \\ & 1 & \\ & & 1 \end{pmatrix}, \begin{pmatrix} 1 & & \\ & & 1 \\ & 1 & \end{pmatrix}, \right.$$

$$\begin{pmatrix} & 1 & \\ 1 & & \\ & & 1 \end{pmatrix}, \begin{pmatrix} & & 1 \\ & 1 & \\ 1 & & \end{pmatrix},$$

$$\left. \begin{pmatrix} & 1 & \\ & & 1 \\ 1 & & \end{pmatrix}, \begin{pmatrix} & & 1 \\ 1 & & \\ & 1 & \end{pmatrix} \right\}$$

There is a homomorphism

$$\det : S_n \longrightarrow \mathbb{Z}^\times = \{\pm 1\}$$

The kernel is called the "alternating group".

$$A_n := \ker(\det).$$

e.g. $A_3 = \left\{ \begin{pmatrix} 1 & & \\ & 1 & \\ & & 1 \end{pmatrix}, \begin{pmatrix} & 1 & \\ & & 1 \\ 1 & & \end{pmatrix}, \begin{pmatrix} & & 1 \\ 1 & & \\ & 1 & \end{pmatrix} \right\}$

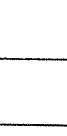
By the Fundamental Iso. Theorem,

$$S_n / A_n \cong \{\pm 1\}$$

$$\Longrightarrow |A_n| = \frac{|S_n|}{|\{\pm 1\}|} = \frac{n!}{2}$$

We could alternatively see that $A_n \triangleleft S_n$ because it has index 2

Theorem: If $H < G$ has index 2 then $H \triangleleft G$.



Proof: H has 2 left and 2 right cosets.
Consider $g \in G$.

If $g \in H$ then $gH = H = Hg$.

If $g \in G - H$ then $gH = G - H = Hg$.

In either case, $gHg^{-1} = H$ ∎

It follows that S_n is never simple.
But it is almost simple.

Theorem: A_n is simple for $n \geq 5$.

Proof: Postponed.

For now we'll just prove that A_5 is simple, in two steps.

(1) The icosahedral group I is simple

(2) $I \cong A_5$.

Note that I acts on itself by conjugation.

$$I \to \mathrm{Aut}(I)$$
$$g \to (h \mapsto ghg^{-1})$$

The orbits are called conjugacy classes. They are as follows:

Geometry	Size of Class
rotate 0	1
rotate $2\pi/5$	12
rotate $4\pi/5$	12
rotate $2\pi/3$	20
rotate π	15
	60.

Now suppose $N \triangleleft I$. Then N is a union of conjugacy classes, hence $|N|$ is a sum of numbers from

$$1, 12, 12, 20, 15$$

which must include the 1 (identity).

But $|N|$ also divides $|I| = 60$ by Lagrange.

There is no such number $|N|$.

Hence I is simple. ///

Now we consider the set of 5 cubes incribed in a dodecahedron.
(look at Zome; I can't draw it.)

Each elt. of I permutes the cubes so we get a homomorphism

$$\varphi : I \to S_5$$

Since I is simple we have $\ker\varphi = 1$ or $\ker\varphi = I$ which is impossible, hence $\ker\varphi = 1$ (φ is injective) and $I \cong \varphi(I) \leq S_5$.

In fact, $\varphi(I) \leq A_5$. To see this consider the homomorphism

$$\det \circ \varphi : I \to S_5 \to \{\pm 1\}.$$

If $\det\circ\varphi$ is surjective then $\ker(\det\circ\varphi) \trianglelefteq I$ has order 30. But I is simple, hence $\det\circ\varphi$ is not surj., i.e. $\operatorname{im}(\det\circ\varphi) = \{+1\}$.
Hence $\varphi(I) \leq \ker(\det) = A_5$.

Then $|I| = |A_5| = 60 \implies I \cong A_5$

Thurs Sept 19

HW 2 due next Tues.

Topic: Classification of Finite Groups

Recall (Galois):

A polynomial is solvable by radicals $\Longleftrightarrow$ its Galois group is solvable (i.e. has abelian composition factors)

Corollary (Abel-Galois):

Polynomials of degree ≥ 5 are not generally solvable by radicals

Proof: A general polynomial of degree n has Galois group $\cong S_n$, and S_n is not solvable for $n \geq 5$ ∎

Why is S_n not solvable?

Recall the determinant hom

$$\det : S_n \longrightarrow \{\pm 1\}$$

with kernel $A_n := \ker(\det) \lhd S_n$

We saw that $A_5 \cong I$ (the icosahedral group) is simple. Hence,

Theorem: S_5 is not solvable.

Proof: S_5 has composition series

$$S_5 \rhd A_5 \rhd 1.$$

with simple factors $\mathbb{Z}/2$ and A_5. But A_5 is not abelian. ∎

Next we will show that S_n is not solvable for $n \geq 5$. But first...

The cycle notation for permutations:

We can identify S_n with the group of permutations $\mathrm{Aut}(\{1, 2, \ldots, n\})$.

There are various ways to encode a permutation

(1) One-Line Notation.

Given $\pi \in S_n$ write it as a table.

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \pi(1) & \pi(2) & \pi(3) & & \pi(n). \end{pmatrix}$$

eg. $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 5 & 2 & 8 & 1 & 6 & 4 & 7 \end{pmatrix}$

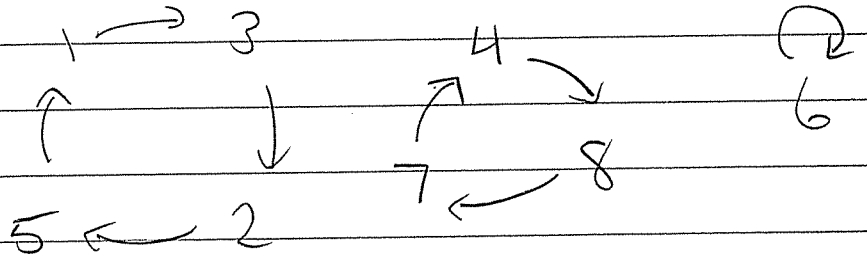
Sometimes we only write the second line

$$\pi = \pi(1)\,\pi(2)\,\pi(3) \cdots \pi(n).$$

eg. $\pi = 35281647 \in S_8$

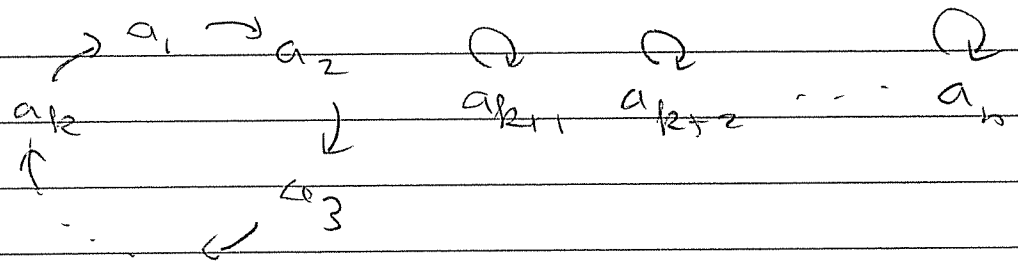
(2) Cycle notation.

Given $\pi \in S_n$ the set $\{1, 2, 3, \ldots, n\}$ breaks into π-orbits, called "cycles"



Suppose $\{a_1, a_2, \ldots, a_k\} \subseteq \{1, 2, \ldots, n\}$ and let $\{a_{k+1}, \ldots, a_n\} = \{1, \ldots, n\} - \{a_1, \ldots, a_k\}$.

We define $(a_1, a_2, \ldots, a_k) \in S_n$ by



Call this a k-cycle permutation.

Every $\pi \in S_n$ has a unique factorization into cycles

e.g. $\pi = 3528164 \in S_8$.

$$\pi = (1325)(487)(6)$$

$$\pi = (1325)(487)$$

We omit 1-cycles from the notation because $(a) = id. \in S_n$ for all a.

Example:

$$S_3 = \{ 1, (12), (13), (23), (123), (132) \}$$

$$= \{ 123, 213, 321, 132, 231, 312 \}$$

Theorem: Conjugacy classes in S_n are classified by "cycle type".

i.e. $\pi, \mu \in S_n$ are conjugate $\iff$ their cycles have the same sizes.

Proof: Let $\pi \in S_n$ with cycles

$$\pi = (a_1 a_2 \cdots a_{k_1})(b_1 b_2 \cdots b_{k_2}) \cdots$$

Then for any $\sigma \in S_n$ we have

$$\sigma \pi \sigma^{-1} = (\sigma(a_1)\sigma(a_2)\cdots\sigma(a_{k_1}))(\sigma(b_1)\cdots\sigma(b_{k_2}))\cdots$$

Indeed, if $i \xrightarrow{\pi} j$ (i.e. $\pi(i) = j$) then

$$\sigma\pi\sigma^{-1}(\sigma(i)) = \sigma(\pi(i)) = \sigma(j),$$

i.e. $\sigma(i) \xrightarrow{\sigma\pi\sigma^{-1}} \sigma(j)$

Thinking Problem: How many conjugacy classes does S_n have?

Theorem: For $n \geq 5$, S_n is not solvable.

Proof: Suppose S_n is solvable with composition series

$$S_5 = H_0 \rhd H_1 \rhd H_2 \rhd \cdots \rhd H_r = 1$$

Let $X \subseteq S_n$ be the set of 3-cycles. We will show that $X \subseteq H_i \Rightarrow X \subseteq H_{i+1}$. By induction, $X \subseteq H_r = 1$. Contradiction. Hence S_n is not solvable.

So suppose that $X \subseteq H_i$. If $\alpha, \beta \in X$ then since H_i / H_{i+1} is abelian we have

$$(\alpha\beta\alpha^{-1}\beta^{-1})H_{i+1}$$

$$= (\alpha H_{i+1})(\beta H_{i+1})(\alpha H_{i+1})^{-1}(\beta H_{i+1})^{-1} = H_{i+1}$$

$$\Rightarrow \alpha\beta\alpha^{-1}\beta^{-1} \in H_{i+1}$$

Now if $n \geq 5$ then any 3-cycle (ijk) can be expressed as

$$(jkm)(ilj)(jkm)^{-1}(ilj)^{-1}$$

$$= (jkm)(ilj)(jmk)(ijl)$$

$$= (ijk)(l)(m) = (ijk)$$

Hence $(ijk) \in H_{i+1}$.
We conclude that $X \subseteq H_{i+1}$. ∎

Corollary: A general polynomical of degree $n \geq 5$ is not solvable.

But more is true.
In fact, S_n is almost simple.

Theorem: For $n \geq 5$, the alternating group A_n is simple

The proof is tricky (non-intuitive) but not hard.

First a

Lemma: Every $\pi \in A_n$ is a product of an even number of 2-cycles.

Proof: Every $\pi \in S_n$ is a product of 2-cycles because every cycle

$$(a_1, a_2, \dots, a_k) = (a_1 a_k)(a_1 a_{k-1}) \cdots (a_1 a_3)(a_1 a_2)$$

is a product of 2-cycles. Note that $\det((ij)) = -1$. Since $\det: S_n \to \{\pm 1\}$ is a homomorphism we have

$\det(\pi) = +1 \iff \pi$ is a product of an even # of 2-cycles

Proof that A_n is simple:

Induction on n. We already know A_5 is simple so assume $n \geq 6$.

Assume for contradiction we have

$$1 \lhd H \lhd A_n$$

For each $i \in \{1, 2, \dots, n\}$ let G_i be the stabilizer of i for the action $A_n \curvearrowright \{1, \dots, n\}$. Note that $G_i \cong A_{n-1}$ (which is simple) by induction.

(1) Suppose $\exists\ 1 \neq \pi \in H$ with $\pi(i) = i$ for some i. Since $\pi \in H \cap G_i$ and $H \cap G_i \leq G_i$ we have $H \cap G_i = G_i$ by simplicity of G_i, i.e.

$$G_i \leq H.$$

For any $\sigma \in A_n$ we have $\sigma G_i \sigma^{-1} = G_{\sigma(i)}$, so $G_{\sigma(i)} = \sigma G_i \sigma^{-1} \leq \sigma H \sigma^{-1} = H$, hence

$$G_j \leq H \text{ for all } j.$$

Any $\pi \in A_n$ can be written

$$\pi = \pi_1 \pi_2 \cdots \pi_t,$$

where each π_k is a product of two 2-cycles. Since $n \geq 5$, each π_k fixes some j, i.e. $\pi_k \in G_j$ for some j.

Hence

$$A_n \leq \langle G_1, G_2, \cdots, G_n \rangle \leq H \trianglelefteq A_n$$

Contradiction. Hence $\nexists\ 1 \neq \pi \in H$ with $\pi(i) = i$.
It follows that if $\pi_1, \pi_2 \in H$ with
$\pi_1(i) = \pi_2(i)$, then $\pi_1 \pi_2^{-1}(i) = i$
$\Rightarrow \pi_1 \pi_2^{-1} = 1 \Rightarrow \pi_1 = \pi_2$. ///

(2) Suppose $\exists\ \pi \in H$ whose cycle decomp. contains a cycle of length ≥ 3, say

$$\pi = (a_1 a_2 a_3 \cdots)(b_1 b_2 \cdots) \cdots$$

Choose $\sigma \in A_n$ with $\sigma(a_1) = a_1$, $\sigma(a_2) = a_2$ and $\sigma(a_3) \neq a_3$ (σ exists since $n \geq 5$), so that

$$\pi' := \sigma \pi \sigma^{-1} = (a_1 a_2 \sigma(a_3) \cdots)(\sigma(b_1) \sigma(b_2) \cdots) \cdots$$

Then $\pi \neq \pi'$ but $\pi(a_1) = \pi'(a_1) = a_2$.
Contradiction.

Thus only 2-cycles can appear in an element $\pi \in H$.

Finally, consider any $1 \neq \pi \in H$ with

$$\pi = (a_1 a_2)(a_3 a_4)(a_5 a_6) \cdots$$

[We require $n \geq 6$.] Let $\delta = (a_1 a_2)(a_3 a_5) \in A_n$. and define

$$\pi' := \delta \pi \delta^{-1} = (a_1 a_2)(a_5 a_4)(a_3 a_6) \cdots$$

We have $\pi \neq \pi'$ but $\pi(a_1) = \pi'(a_1) = a_2$. Contradiction.

Hence A_n is simple.