# Math 493
# Honors Algebra I

University of Michigan
Harrison Centner
Prof. Kartik Prasanna
November 13, 2023

# Contents

# INTRODUCTION & MOTIVATION

We will study

(a) Linear algebra

(b) Group Theory

(c) Finite Group Representations

In 494 we will study

(a) Ring Theory

(b) Fields

(c) Galois Theory

This class is good preparation for 575 or 676. The official textbook is Artin's Second edition. We will probably proceed in a different order than Artin. Other than Artin's look into Dummit & Foote, Lang, Hirstine. Pick the book that you like and read it. Sit four to a table.

Sometimes a polished proof will not be presented in class and you are expected to finish the proof at home.

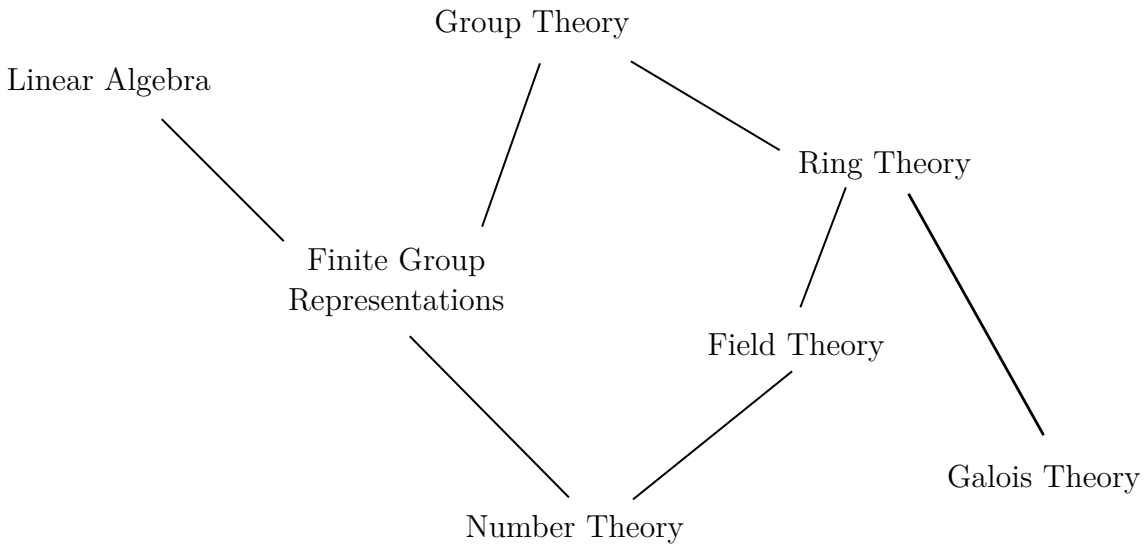



Figure 1: Partial Ordering of Course Topics

# GROUP THEORY

**Definition**. (Group)
A group is a set $G$ with a binary operation $\star : G \times G \to G$.

(i) $\exists e \in G$ such that $e \star a = a \star e = a$ for all $a \in G$ (existence of identity)

(ii) $\forall a, b, c \in G$ we have $(a \star b) \star c = a \star (b \star c)$ (associativity of $\star$)

(iii) $\forall a \in G,\ \exists a' \in G$ such that $a \star a' = a' \star a = e$ (existence of inverses)

Examples:

(a) The trivial group

(b) $(\mathbb{Z}, +)$

(c) $(\mathbb{Z}/2\mathbb{Z}, \oplus)$

(d) $(\mathbb{Z}/n\mathbb{Z}, +)$

(e) $(\mathbb{Q}^\times, \cdot)$ (nonzero rationals)

(f) $\mathrm{Aut}(S)$ for any set $S$, this is the symmetric group $S_n$ when $|S| = n \in \mathbb{N}$

(g) Rotations of a square

(h) Free group on $n$ elements

Consider $S_1, S_2, S_3, \ldots$
Already, $S_3$ is quite complex. Recall that $|S_n| = n!$.

Note that $S_2$ has one generator and $S_3$ has two generators:

$$\sigma = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \qquad \tau = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}$$

Every column and row in the Cayley Table of $S_n$ has every element exactly once.

| $S_1$ | $e$ |
|---|---|
| $e$ | $e$ |

| $S_2$ | $e$ | $\sigma$ |
|---|---|---|
| $e$ | $e$ | $\sigma$ |
| $\sigma$ | $\sigma$ | $e$ |

| $S_3$ | $e$ | $\tau$ | $\tau^2$ | $\sigma$ | $\sigma\tau$ | $\sigma\tau^2$ |
|---|---|---|---|---|---|---|
| $e$ | $e$ | $\tau$ | $\tau^2$ | $\sigma$ | $\sigma\tau$ | $\sigma\tau^2$ |
| $\tau$ | $\tau$ | $\tau^2$ | $e$ | $\sigma\tau^2$ | $\sigma$ | $\sigma\tau$ |
| $\tau^2$ | $\tau^2$ | $e$ | $\tau$ | $\sigma\tau$ | $\sigma\tau^2$ | $\sigma$ |
| $\sigma$ | $\sigma$ | $\sigma\tau$ | $\sigma\tau^2$ | $e$ | $\tau$ | $\tau^2$ |
| $\sigma\tau$ | $\sigma\tau$ | $\sigma\tau^2$ | $\sigma$ | $\tau^2$ | $e$ | $\tau$ |
| $\sigma\tau^2$ | $\sigma\tau^2$ | $\sigma$ | $\sigma\tau$ | $\tau$ | $\tau^2$ | $e$ |

Note that $\tau\sigma = \sigma\tau^2 \implies \tau^k\sigma = \sigma\tau^{2k}$ for $k \in \mathbb{N}$.

**Definition**. (Subgroup)
Suppose $G$ is a group and $H \subseteq G$ such that
(a) $e \in H$
(b) $\forall a, b \in H$ we have $a \star b \in H$
(c) $\forall a \in H$ we have $a^{-1} \in H$
$H$ is a group with the group law inherited from $G$. If $S \subseteq G$, then $\langle S \rangle$ is the subgroup generated by $S$ (note that $S$ may be a singleton).

Now we find all subgroups of $S_3$: $S_3, \{e\}, \{e, \tau, \tau^2\}, \{e, \sigma\}, \{e, \sigma\tau\}, \{e, \sigma\tau^2\}$. There are three subsets of $S_3$ that are isomorphic to $S_2$ and one isomorphic to $\mathbb{Z}/3\mathbb{Z}$. You can find subgroups by taking a single element and taking all powers of it (positive and negative). We obtain a lattice of subgroups.

**Definition**. (Order)
If $a \in G$, the **order** of $G$ is $\mu n \in \mathbb{N}$ such that $a^n = e$. If no such $n$ exists, then $a$ has **infinite order**. Note that the order of all elements in a finite group are finite (pigeon hole principal).

Note that $S_3 \cong D_3$, the rigid symmetries of an equilateral triangle. We have three reflections over each axis and rotations by $\frac{2\pi}{3}$ and $\frac{4\pi}{3}$.

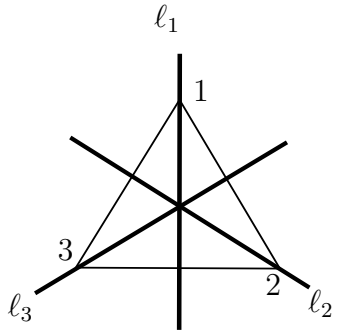



Figure 2: $D_3$

As isomorphisms of $\mathbb{R}^2$ we have

$$S_3 \cong D_3 \cong \left\{ I_2, \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}, \begin{bmatrix} -\frac{1}{2} & \frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & -\frac{1}{2} \end{bmatrix}, \begin{bmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{bmatrix} \right\}$$

Since rotations of $\mathbb{R}^2$ are parametrized by $\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$.

$D_n$ is the group of rigid rotations of a regular $n$-gon. Note that $D_n \hookrightarrow S_n$ and $|D_n| = 2n$. Explicitly $D_n$ is the group with presentation

$$D_n = \langle x, y : x^n = e = y^2, yxy^{-1} = x^{-1} \rangle.$$

Geometrically, it is clear that $y^{-1} = y$ and $x^{-1} = x^{n-1}$.

# Lagrange's Theorem & Quotient Groups

**Theorem**. (Lagrange's Theorem)
If $H \subseteq G$ a subgroup of a finite group $G$, then $|H|$ divides $|G|$.

*Proof.*
$P = \{gH : g \in G\}$ defines an equally sized partition on $G$. Since $G$ is finite, the partition is finite and it must be that $|P| \cdot |H| = |G|$. □

**Definition**. (Cosets)
Let $H \subseteq G$ be a subgroup.
A **left coset** of $H$ in $G$ is a subset of $G$ of the form $aH = \{ah : h \in H\}$.
Similarly, A **right coset** of $H$ in $G$ is a subset of $G$ of the form $Ha = \{ha : h \in H\}$.

Find all left and right cosets of all subgroups of $S_3$. Let $H = \{e, \tau, \tau^2\}$, then $eH \sqcup \sigma H \cong S_3$. Note that $eH = \tau H = \tau^2 H$ and $\sigma\tau H = \sigma H = \sigma\tau^2 H$. Similarly, for $K = \{e, \sigma\}$ we have $eK = \sigma K$, $\tau K = \sigma\tau^2 K$, and $\tau^2 K = \sigma\tau K$.

| Subgroup | Left Cosets | Right Cosets |
|---|---|---|
| $G$ | $G$ | $Gb$ |
| $\{e\}$ | $\{\{a\} : a \in G\}$ | $\{\{a\} : a \in G\}$ |
| $K = \{e, \tau, \tau^2\}$ | $K,\ \sigma K$ | $K,\ K\sigma$ |
| $H_1 = \{e, \sigma\}$ | $H_1,\ \tau H_1,\ \tau^2 H_1$ | $H_1,\ H_1\tau,\ H_1\tau^2$ |
| $H_2 = \{e, \sigma\tau\}$ | $H_2,\ \tau H_2,\ \tau^2 H_2$ | $H_2,\ H_2\tau,\ H_2\tau^2$ |
| $H_3 = \{e, \sigma\tau^2\}$ | $H_3,\ \tau H_3,\ \tau^2 H_3$ | $H_3,\ H_3\tau,\ H_3\tau^2$ |

But note that $\tau^m H_k \neq H_k \tau^m$ for $m \in [2]$ and $k \in [3]$.

Fix a subgroup $H \subseteq G$. We now prove **Lagrange's Theorem** via three statements.

(a) Any two left cosets of $H$ in $G$ are either identical or disjoint.
*Proof.*
Suppose $aH \cap bH \neq \varnothing$ so then there exists

$$c = ah_1 = bh_2 \implies a = b\left(h_2 h_1^{-1}\right) \in bH \implies a \in bH.$$

Now for any element $ah_3$ of $aH$ we have

$$ah_3 = b(h_2 h_1^{-1})h_3 \in bH$$

Thus $aH \subseteq bH$. Interchanging the roles of $aH$ and $bH$ shows $bH \subseteq aH$. □

(b) All cosets have the same cardinality.
*Proof.*
Let $H \subseteq G$ be a subgroup and take $a \in G$. Define $f : H \to aH$ given by $f(x) = ax$. $f$ is surjective by construction and if $f(x) = ax = ay = f(y)$, then $x = y$ by cancellation. So $f$ is a bijection. Thus $|eH| = |aH|$ for all $a \in G$. □

(c) Finally, $G = \sqcup$(left cosets)
*Proof.*
Given (a) it suffices to show $G = \cup$(left cosets). Pick $a \in G$, then $a \in aH \in$ (left cosets). □

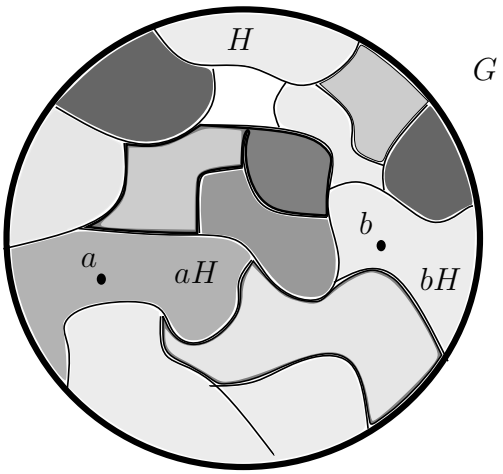



Figure 3: Cosets partition $G$

**Definition**. (Index)
The **index** of a subgroup $H \subseteq G$ is given by $[G : H]$ and gives the cardinality of the number of left cosets (which equals the number of right cosets).

Prove at home this holds for finite and infinite number of cosets.

**Definition**. (Cyclic Group)
A group $G$ is said to be **cyclic** provided that $G = \langle a \rangle$ for some $a \in G$. Therefore, every cyclic group is countable and isomorphic to either $\mathbb{Z}$ or—if finite—$\mathbb{Z}/n\mathbb{Z}$ for some $n \in \mathbb{N}$.

**Proposition**.
If $|G| = p$, a prime number, then $G$ is cyclic.

Note: For every $n \in \mathbb{N}$, $\exists$ a cyclic group of order $n$. We write this group $C_n$.

**Definition**. (Homomorphism)
A **homomorpism** is a map $\phi : G_1 \to G_2$ such that $\phi(ab) = \phi(a)\phi(b)$ and we call $\phi$ an **isomorphism** if $\phi$ is bijective.

Exercise: Classify groups of small order up to isomorphism.

**Definition**. (Direct Product)
Suppose $G_1, G_2$ are groups. Then $G_1 \times G_2$ with componentwise multiplication and inverses is a group of order $|G_1| \cdot |G_2|$. Note the direct product of cyclic groups is cyclic.

We prove that we have exhausted all groups of order four. Suppose there is an element of order four, then $G \cong C_4$. Suppose there is no element of order four, then every nontrivial element has order 2. The very cute fact about groups which have this property is that $\forall a, b \in G$ we have $(ab)^{-1} = b^{-1}a^{-1} = ba = ab$. Another way to prove this is $(ab)^2 = e = a^2b^2$.

| Order | Groups |
|---|---|
| 1 | $C_1$ |
| 2 | $C_2$ |
| 3 | $C_2$ |
| 4 | $C_4, C_2 \times C_2$ |
| 5 | $C_5$ |
| 6 | $C_6, S_3$ |
| 7 | $C_7$ |
| 8 | $C_8, (C_2)^3, D_4$ |

We prove that we have exhausted all groups of order six. Let $G$ be an arbitrary group of order six. If there is an element of order six then $G \cong C_6$. Suppose there are no elements of order six ...

**Definition**. (Normal Subgroup)
Let $N \subseteq G$ be a subgroup. The following are equivalent
(i) $aN = Na$ for all $a \in G$.
(ii) $aNa^{-1} = N \ \forall a \in G$
(iii) $a^{-1}Na = N \ \forall a \in G$
(iv) $aNa^{-1} \subseteq N \ \forall a \in G$
(v) $N \subseteq aNa^{-1} \ \forall a \in G$
(vi) Every left coset of $N$ in $G$ is a right coset.
(vii) Every right coset of $N$ in $G$ is a left coset.
**Definition**
$N$ is said to be **normal** in $G$ if it satisfies any of the aforementioned conditions. We write $N \trianglelefteq G$ to denote that $N$ is normal in $G$.

*Proof.*
(i) $\implies$ (ii) $\implies$ (iii) $\implies$ (iv) $\implies$ (v) is clear.

Suppose every left coset of $N$ is a right coset this means that $\forall a \in G$, $aN = Nb$ for some $b \in G$. Certainly $a \in Nb$. Since right cosets are disjoint the only right coset that contains $a$ is $Na$ so $a$ and $b$ are representatives for the same right coset. □

Exercise: Identify all $N_1 \subseteq S_3$ and $N_2 \subseteq D_4$ such that $N_1 \trianglelefteq S_3$ and $N_2 \trianglelefteq D_4$.

The moment you find one conjugate that is different you know it is not normal. Note that all $H \subseteq S_3$ such that $H \cong S_2$ are conjugate to each other.

| Group | Normal Subgroups |
|---|---|
| $S_3$ | $\{e\}, \{e, \tau, \tau^2\}, S_3$ |
| $D_4$ | $\{e\}, \{e, x^2\}, \{e, x, x^2, x^3\}$, $\{e, yx, yx^3, x^2\}, \{e, y, yx^2, x^2\}$ |

A subgroup of order two is normal only when it is contained in the center. This follows since you need $ak = ka$ for the one nontrivial $k \in K \subseteq G$.

Cute Fact: Any subgroup of index two is normal. This follows since if $K \subseteq G$ has index two, then the right cosets are $K$ and $G - K$ (certainly the same thing holds of the left cosets).

Let $\phi : G \to \{K, G \setminus K\}$ be given by $\phi(g) = gK$. Now $\phi \in \text{Hom}(G, C_2)$ and $\ker(\phi) = K$. Since $\{K, G \setminus K\} \cong C_2$ we are done (WHY?).

**Definition**. (Quotient Group)
Let $N \subseteq G$ be a normal subgroup. Then we can define the **quotient group** $G/N$ which is as a set is the collection of left (resp. right) cosets and has group law $aN \star bN = abN$. This is well defined. $G/N$ has identity $eN = N$ and inverses $(aN)^{-1} = a^{-1}N$.

*Proof.*

$$aN \star bN = (aN)(bN) = a(Nb)N = (ab)NN = abN$$

were the third equality follows since $N$ is normal, shows that the product is well defined.

□

**Proposition**. (Normal Subgroups are Kernels of Homomorphism)
If $\varphi \in \mathrm{Hom}(G, H)$, then $\ker \varphi = \{g \in G : \varphi(g) = e\}$ is a normal subgroup.

*Proof.*
$aNa^{-1} \subseteq N \ \forall a \in G$. Given $n \in N$, $ana^{-1}$ is annihilated by $\varphi$. Meaning,

$$\varphi(ana^{-1}) = \varphi(a)\varphi(n)\varphi(a^{-1}) = aea^{-1} = e.$$

The converse is also true. So the normal subgroups are exactly the kernels of $\varphi \in \mathrm{Hom}(G, H)$.

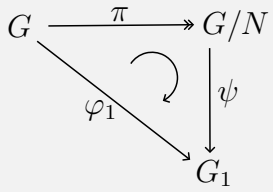
Now to prove the converse, Define a map $\psi : G \to G/N$ where $\psi(a) = aN$. Then $N = \ker(\psi)$ by construction.

□

We can now give a characterization of quotients. Taking successive quotients of a group leads to subsets of subsets and becomes cumbersome.

**Proposition**. (Universal Property of Quotient Map)

Let $\varphi_1 : G \to G_1$ be any homomorphism such that $N \subseteq \ker(\varphi_1)$.
In other words $\varphi_1$ annihilates $N$.
Then $\exists! \psi \in \mathrm{Hom}(G/N, G_1)$ such that $\varphi_1 = \psi \circ \pi$.
Moreover, $N = \ker(\varphi_1) \iff \psi$ is injective.




Uniqueness is easiest to check because we only need to check the diagram commutes. If $\psi$ exists, it must be unique and must be given by the formula $\psi(aN) = \varphi_1(a)$ since $\varphi$ is surjective.

Now we need to check that the map $\psi$ is well defined (since it is defined via coset representatives). Suppose $aN = bN$, so $a = bn$ for $n \in N$. This gives $\varphi_1(a) = \varphi_1(b)\varphi_1(n) = \varphi_1(b)$.

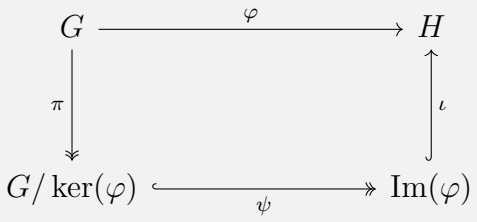
Now we show the second portion. Suppose $N = \ker(\varphi_1)$, then $\psi$ is injective because $\ker(\psi) = \{e\}$. This follows since $\psi(aN) = e \iff \varphi_1(a) = e \iff a \in N$.

Now suppose that $\psi$ is injective, so $\ker(\psi) = \{e\}$. This means that $\varphi_1(a) = e \iff a \in N$.

By prof: $\psi$ is injective $\iff \ker(\psi) = e \iff K/N = \{e\} \iff K = N$. □

**Theorem**. (First Isomorphism Theorem)

Let $\varphi \in \mathrm{Hom}(G, H)$. Then we can **factor** $\varphi$ through $\ker(\varphi)$. Meaning, $\exists! \psi \in \mathrm{Hom}(G/\ker(\varphi), H)$ such that $\varphi = \psi \circ \pi$ where $\pi$ is projection onto the kernel, $\psi$ is an isomorphism witnessing $G/\ker(\varphi) \cong \mathrm{Im}(\varphi)$, and $\iota$ denotes the inclusion map.




A natural question to ask arises. How are subgroups of $G/N$ related to subgroups of $G$?

**Proposition**. (The Correspondence Theorem)
Let $N \subseteq G$ be a subgroup. There is a bijection $g$ between subgroups of $G$ containing $N$ and subgroups of $G/N$. $h(K) = K/N$ and $h(K/N) = h^{-1}(K)$ (or the fibres of $K$ under $h$). The normality of a subgroup is preserved under the map $h$.

*Proof.*
See homework. □

We should interpret this as saying that the lattice of subgroups of $G/N$ describes the lattice of subgroups of $G$ at the "top".

# Cauchy's Theorem

**Lemma**. (Order Lemma)
Let $h : G \to G_1$ be a homomorphism. Take $x \in G_1$, $o(g)$ for $g \in h^{-1}(x)$ is a multiple of $o(x)$.

**Definition**. (Conjugates)
Let $x, y \in G$. We say $x$ and $y$ are **conjugate** in $G$ provided that $\exists g \in G$ such that $y = gxg^{-1}$.

So $C_x = \{y \in G : \exists g \text{ s.t. } y = gxg^{-1}\}$

Note that conjugacy is an equivalence relation. Let's take a look at the equivalence classes produced by conjugation in $S_3$. $C_e = \{e\}$, $C_\tau = \{\tau, \tau^2\}$, and $C_\sigma = \{\sigma, \sigma\tau, \sigma\tau^2\}$.

Note: In an abelian group all conjugacy classes are singletons.

Note: Elements of the same conjugacy class have the same order because

$$(gxg^{-1})^n = gx^n g^{-1}.$$

Think about how when we want to take powers of a matrix, we first try to diagonalize the matrix.

Notation: Let $H \subseteq G$ be a subgroup.
Then $G/H$ is the set of left cosets $H$ in $G$ and $G\ H$ is the set of right cosets of $H$ in $G$.

**Theorem**. (Size of Conjugacy Class)
Let $G$ be a finite group. Let $x \in G$, then the cardinality of the conjugacy class of $x$ divides the order of $G$.

Take $x, g_1, g_2 \in G$. Then,

$$g_1 x g_1^{-1} = g_2 x g_2^{-1} \iff (g_2^{-1} g_1)x = x(g_2^{-1} g_1) \iff g_2^{-1} g_1 \text{ commutes with } x \iff g_2^{-1} g_1 \in \mathcal{Z}_G(x)$$

Exercise: Write $\mathcal{Z}_G(x) = \{g \in G : gx = xg\}$.

(i) Show that $\mathcal{Z}_G(x)$ is a subgroup of $G$.

(ii) Furthermore, show there is a bijection $C_x \leftrightarrow G/\mathcal{Z}_G(x)$.

*Proof.*
Certainly $e \in \mathcal{Z}_G(x)$ and suppose $a, b \in \mathcal{Z}_G(x)$. Then, $ax = xa \implies bax = bxa \implies bax = xab$ since $bx = xb$. Also $ax = xa \implies xa^{-1} = a^{-1}x$.

Now we show there is a bijection. Let $\gamma : G \to C_x$ be given by $\gamma(g) = gxg^{-1}$. This map is surjective by definition. Now

$$\gamma(g_1) = \gamma(g_2) \iff g_2^{-1} g_1 \in \mathcal{Z}_G(x) \iff g_1 \in g_2 \mathcal{Z}_G(x) \iff g_1 \mathcal{Z}_G(x) = g_2 \mathcal{Z}_G(x).$$

Which shows that $\gamma$ gives a bijection $G/\mathcal{Z}_G(x) \to C_x$.

□

The center of a group consists of exactly the elements which have singleton conjugacy classes.

**Theorem**. (Class Equation)
Let $G$ be a finite group. Then

$$|G| = \sum_{x \in G} |C_x| = |\mathcal{Z}(G)| + \sum_{x \in G \setminus \mathcal{Z}(G)} |C_x| = |\mathcal{Z}(G)| + \sum_{x \in G \setminus \mathcal{Z}(G)} \frac{|G|}{|\mathcal{Z}_G(x)|}$$

**Theorem**. (Cauchy's Theorem)
Let $G$ be a finite group. Let $p$ be a prime number such that $p$ divides $|G|$, then $G$ contains an element of order $p$.

*Proof.*
Case I: Suppose $G$ is cyclic, then there is an element $x$ such that $\langle x \rangle = G$ and $x$ has order $|G| = n$. If $p$ is prime and divides $n$, then $n = pm$ and $x^m$ has order $p$.

Case II: Suppose $G$ is abelian. If $|G| = 2$, then we know $G \cong C_2$ which satisfies the theorem. Assume inductively that the theorem holds for all $G$ such that $|G| < k$ for $k \in \mathbb{N}$. Take nontrivial $x \in G$ and consider $H = \langle x \rangle$, which is cyclic. If $p$ divides the order of $H$ we are done by Case I, if not then consider $G/H$ ($H$ is normal since $G$ is abelian). $|G/H| = |G|/|H|$ which is less than $k$ (and divisible by $p$), so the inductive hypothesis guarantees that $G/H$ has an element of order $p$. Call this element $aH$.

Now we can lift this to an element of order $p$ in $G$ by the natural isomorphism between $G/H$ and subgroups of $G$ containing $H$.

Case III:
Here are the hints. (i) Use the class equation, (ii) use the abelian case, and (iii) induct on $|G|$.

If $p$ divides $|\mathcal{Z}(G)|$ then we are done by Case II since the center of a group is abelian. Suppose not, then at least one summand is not divisible by $p$ (i.e. $\exists x$ such that $p$ does not divide $\frac{|G|}{|\mathcal{Z}_G(x)|}$). This follows since if every summand was divisible by $p$ then $|G|$ would not be divisible by $p$.

So if $p$ does not dive the ratio (which is the summand), then $p$ must divide the denominator $|\mathcal{Z}_G(x)|$ which is less than $|G|$. By induction, we are done. □

**Proposition**. (Groups of Prime Order have Nontrivial Centers)
If $|G| = p^n$ for $p$ prime, then $\mathcal{Z}(G) \neq (e)$.

**Corollary**.
Any group of order $p^2$ is abelian.

*Proof.*
If $G$ is abelian we are done. Suppose not. Take $x \notin \mathcal{Z}(G)$, then since $\mathcal{Z}_G(x) \subseteq G$ by Lagrange's Theorem $|\mathcal{Z}_G(x)| = p^i$ for $i < n$. Since $|G| = p^n$ we know $p \mid \frac{|G|}{|\mathcal{Z}_G(x)|}$. Now the Class Equation ensures that $p \mid |\mathcal{Z}(G)|$ which shows $|\mathcal{Z}(G)| \geq p$.
$\therefore$ the center of $G$ is nontrivial.

Now we prove the Corollary.
Let $|G| = p^2$ for a prime $p$. We know that $|\mathcal{Z}(G)| \in \{p, p^2\}$. Suppose $|\mathcal{Z}(G)| = p$. Take $y \notin \mathcal{Z}(G)$. Note that $\mathcal{Z}_G(y) \supset \mathcal{Z}(G)$. But both of these are subgroups, so since $|\mathcal{Z}(G)| = p$ it must be that $|\mathcal{Z}_G(y)| = p^2 = |G|$. Contradiction! Thus every group of order $p^2$ is abelian.

□

# The Sylow Theorems

**Definition**. ($p$-Sylow Subgroup)
Let $G$ be a finite group such that $|G| = p^r \cdot m$ where $p$ is prime, $r \geq 1$, and $p$ does not divide $m$. A $p$-Sylow subgroup of $G$ is a subgroup $H \subseteq G$ such that $|H| = p^r$.

**Theorem**. (Sylow Theorems)
Let $G$ be a finite group with $|G| = p^r \cdot m$ where $p$ is prime, $r \geq 1$, and $p$ does not divide $m$.

(1) $G$ contains a $p$-Sylow subgroup $H$.
(2) (Weak version) Any two $p$-Sylow subgroups are conjugate in $G$. Meaning, if $H_1, H_2 \subseteq G$ are $p$-Sylow then $\exists g \in G$ such that $H_2 = gH_1g^{-1}$.
(3) The number of $p$-Sylow subgroups
    - divides $m$ and
    - is congruent to 1 mod $p$.

Exercise: Classify all groups of order 15.

Note that $15 = 5 \cdot 3$. Take $p = 5$ and $m = 3$, this makes $r = 1$. By (3) any group of order 15 has exactly one 5-Sylow subgroup and exactly one 3-Sylow subgroup. These subgroups must be cyclic because they have prime order. Furthermore their intersection must be trivial.

Take an element not in the union of the aforementioned subgroups. Its order must be 15 because (a) it cannot be the identity, (b) its order cannot be 3 since that would generate a new 3-Sylow subgroup, (c) cannot have order 5 for the same reason.

$C_{15} \cong C_5 \times C_3$ by the internal direct product construction. Both $C_5$ and $C_3$ are normal in $G$ because conjugation produces another 5-Sylow and 3-Sylow respectively. But $C_5$ and $C_3$ are the unique Sylow subgroups. This gives us the conditions to satisfy the internal direct product construction. Thus we have determined all groups of order 15 up to isomorphism.

Exercise: Classify all groups of order 21. This one is trickier because $7 \mod 3 \equiv 1$.

There is a unique 7-Sylow subgroup which is cyclic. If there is only one 3-Sylow subgroup then the group is isomorphic to $C_{21}$ since $C_{21}$ is the internal direct product of $C_3$ and $C_7$ (by the same argument as the previous exercise).

Now suppose there are seven 3-Sylow subgroups. They have trivial intersection because they are cyclic. So these give $2 \cdot 7 + 1 + 6$ elements accounted for so far. Fix a 3-Sylow $K$ and a generator $y$. Take a generator $x$ for the 7-Sylow $H$. Note that $H$ is normal because it is the unique 7-Sylow. So now we know that $HK$ is a group because $HK = KH$ since $hk = kk^{-1}hk$ and $k^{-1}hk \in H$ since $H$ is normal in $G$. But this now gives us that $G \cong HK = \{x^i y^j : 0 \leq i \leq 6 \wedge 0 \leq j \leq 2\}$ so $G$ is cyclic. Because $H$ is normal, $yxy^{-1} \in H$ so it is of the form $x^i$ for some $i \in [6]$. Note that $i = 0 \implies x = e$ which is not possible. Also $i \neq 1$ since this gives us the abelian case and $G \cong C_{21}$ again. Recall that $y$ has order three, so

$$y^2xy^{-2} = yx^iy^{-1} = (yxy^{-1})^i = x^{i^2} \implies x = y^3xy^{-3} = yx^{i^2}y^{-1} = (yxy^{-1})^{i^2} = x^{i^3}$$

So now $x^1 = x^{i^3}$ so $i^3 \equiv 1 \mod 7$. So $1, 2, 4$ are the only values of $i$ that work.

So now $yxy^{-1} \in \{x, x^2, x^4\}$ so there are at most three groups of order 21. The guess is that both the $x^2$ and $x^4$ case are isomorphic.

Wait until the next homework to find out !

**Definition**. (Group Actions)
Let $G$ be a group and $S$ a set. A **group action** is a map $G \times S \to S$ given by $(g, s) \mapsto g \cdot s = gs$. The map should satisfy

(i) $e \cdot s = s$ for all $s \in S$,
(ii) $(g_1g_2) \cdot s = g_1 \cdot (g_2 \cdot s)$

Examples:

(a) Forget the group structure on $G$ to obtain a set $S$ and have the action be standard group product (but right multiplication would not work).

(b) Forget the group structure on $G$ to obtain a set $S$ and have the action be right multiplication by the inverse of $g$.

(c) Forget the group structure on $G$ to obtain a set $S$ and have the action be conjugation.

(d) Forget the group structure on $G$ to obtain a set $S$ and

(e) $S$ is a compact polytope and $G$ is its set of symmetries.

(f) $D_n$ acting on $\mathbb{R}^2$ as linear maps.

This gives us a preview into **group representations** where we will ask about $G \times V \to V$ where $v \mapsto gv$ is a linear transformation.

**Definition**. (Orbit and Stabilizer)
The **orbit** of $s$ is $O(s) = \{gs : g \in G\}$ and the **stabilizer** of $s$ is $\text{Stab}(s) = \{g \in G : gs = s\}$.

So when the group action is conjugation, $O(s) = C_s$ and $\text{Stab}(s) = \mathcal{Z}_G(s)$ the centralizer of $s$.

**Proposition**. ()
$G_s \trianglelefteq G$ and as sets $O(s) \cong G/G_s$.

**Corollary**.
$|O(s)| = [G : G_s]$ which equals $\frac{|G|}{|G_s|}$ when $G$ is finite.

Note that $O(s)$ may not be a group.

Clearly $e \in G_s$. Now suppose $a, b \in G_s$ then $abs = as = s$. $as = s \implies s = a^{-1}s$. $G_s \trianglelefteq G$ by definition.

Let $\gamma_s : G \to O(s)$ be given by the group action. So $\gamma_s(g) = g \cdot s$ is surjective. Now

$$g_1 \cdot s = g_2 \cdot s \iff g_2^{-1} g_1 \in G_s \iff g_1 \in g_s G_s \iff g_1 G_s = g_s G_s.$$

This gives a bijection $G/G_s \longleftrightarrow O(s)$.

**Theorem**. (General Class Equation)

$$|S| = \sum_{[s]} |O(s)|$$

**Theorem**. (First Sylow Theorem)
Let $|G| = g^r \cdot m$ with $r \geq 1$ and $p \nmid m$ then $G$ contains a subgroup of order $p^r$.

*Proof.*
Step I: Let $S = \{M \in \mathcal{P}(G) : |M| = p^r\}$. Let $G$ act on $S$ by left multiplication so $g \cdot s = gs$.

First we claim that $p \nmid |s|$.

$$|S| = \binom{p^r \cdot m}{p^r} a = \frac{p^r m(p^r m - 1) \cdots (p^r m - (p^r - 1))}{p^r (p^r - 1) \cdots (p^r - (p^r - 1))} = \frac{p^r m - i}{p^r - i}$$

where $i = p^j \cdot k$ with $j < r$ and $p \nmid k$.

$$\frac{p^r m - i}{p^r - i} = \frac{p^r m - p^j k}{p^r - p^j k} == \frac{p^r m - p^j k}{p^r - p^j k} =$$

THINK ABOUT AT HOME

From this claim we obtain some $s \in S$ such that $|O(s)|$ is prime to $p$. But we know

$$p^r \cdot m = |G| = |G_s| \cdot |O(s)| \implies p^r \mid |G_s|.$$

So $s = \{g_1, g_2, \ldots, g_{p^r}\}$ and $G_s g_1 \subseteq s$ because $G_s$ stabilizes the set $s$ (we could have used any element in $s$). This gives us that $|G_s| \leq |s| = p^r$ but since $|G_s| \mid p^r$ we conclude that $|G_s| = p^r$.

You never need to remember the proof of this theorem. □

"You are one of the most on brand people I know" -Nikki

"Today we are doing a worksheet but if anyone comes let tell them theres a quiz going on."

**Theorem**. (Strong Second Sylow)
Let $G$ be a finite group with $p \mid |G|$. Let $H$ be a $P$-Sylow subgroup of $G$. Let $K$ be any subgroup of $G$. Then there exists an element $a \in G$ such that $K \cap aHa^{-1}$ is a $p$-Sylow subgroup of $K$.

The following theorem follows from the above.

**Theorem**. (Consequences of Strong Second Sylow)
Let $G$ be a finite group. Any two $p$-Sylow subgroups of $G$ are conjugate in $G$.
If $K \subseteq G$ is a subgroup that is a $p$-group (i.e. one whose order is a power of $p$), then $K$ is contained in a $p$-Sylow subgroup of $G$.

*Proof.*
Let $H_1, H_2$ be $p$-Sylow subgroups of $G$. Let $|G| = p^r m$ where $p \nmid m$. Then $|H_1| = p^r = |H_2|$. Then take $K = H_1$ and the Second Sylow Theorem gives an element $a$ such that $H_1 \cap aH_2a^{-1}$ is $p$-Sylow in $H_1$. Note that $|H_2| = |aH_2a^{-1}|$. This means that $|H_1 \cap aH_2a^{-1}| = p^r$. This implies that $|H_1| = |H_1 \cap aH_2a^{-1}|$ Consequently, $H_1 = aH_2a^{-1}$ since $H_1 \supseteq H_1 \cap aH_2a^{-1}$.

Suppose $|G| = p^r m$ and $|K| = p^\ell$ for $\ell < r$. The only $p$-Sylow subgroups of $K$ is $K$ itself. Suppose that $H$ is a $p$-Sylow subgroup, then from Strong Second Sylow $\exists g \in G$ such that $gHg^{-1}$ is a $p$-Sylow in $K$. So $K \subseteq gHg^{-1}$.

Consider the group action $G \times G/H \to G/H$ given by left multiplicatoin. This group action is transitive (has a single orbit) because $ba^{-1} \cdot aH \to bH$. Note that $\text{Stab}(aH) = aHa^{-1}$. Now take $g \in \text{Stab}(aH)$. Then

$$gaH = aH \iff a^{-1}gaH = H \iff g \in H \iff g = aha^{-1}$$

for some $h \in H$.

Consider the restriction of the group action to $K$. Then $\text{Stab}(aH) = K \cap aHa^{-1} \cap K$.

Let's use the fact that $H$ is $p$-Sylow in $G$. So $|G/H|$ is prime to $p$. The size of the full set is the sum of the sizes of the orbits. There must exist some orbit $O(aH)$ which has cardinality prime to $p$. Now the Orbit Stabilizer Theorem tells us

$$|O(aH)| \cdot |\operatorname{Stab}(aH)| = |K| \implies |O(aH)| = |aHa^{-1} \cap K| = |K|.$$

The powers of $p$ that divide $|K|$ and $|aHa^{-1} \cap K|$ are the same. So $K$ is a $p$-Sylow subgroup.

Be ready to work through 5 and 6 on the board next time.

**Problem 5 on the worksheet** Take $g \in \operatorname{Stab}(s)$. Then $g \cdot s = gsg^{-1}$.

**Theorem**. (Third Sylow)
Suppose $|G| = p^r m$ with $p \nmid m$. The number of $p$-Sylow subgroups of $G$ divides $m$ and is congruent to 1 mod $p$.

Step I: Let $S$ be the set of $p$-Sylow subgroups of $G$ and consider the action of $G$ on $S$ by conjugation:

$$G \times S \to S, \quad (g, H) \mapsto gHg^{-1}.$$

Since the action is transitive (by the previous theorem), we get

$$|S||\operatorname{Stab}(H)| = |G|.$$

We show that $\operatorname{Stab}(H) = N_G(H)$, and conclude that $|S|$ divides $m$.

$\operatorname{Stab}(H) = N_G(H)$ be definition. Since this group action is transitive then $O(s) = S$ for $s \in S$. Now the Orbit Stabilizer Theorem gives $|S||\operatorname{Stab}(H)| = |G|$. This tells us that $|S| = \frac{|G|}{|N_G(H)|} = [G : N_G(H)]$. Since $[N_G(H) : H] \cdot [G : N_G(H)] = [G : H]$ we obtain that $|S|$ divides $s$. It may be useful to use $|S| = [G : N_G(H)]$.

Step II: Now fix a $p$-Sylow subgroup $H$ and restrict the last action to an action $H \times S \to S$. If $K$ is a $p$-Sylow subgroup of $G$, we show that $|O(K)| = 1 \iff K = H$, and otherwise $|O(K)|$ is divisible by $p$.

Suppose $H = K$ then for all $h \in H$, $hKh^{-1} = k \implies O(K) = K$. Now suppose $|O(K)| = 1$. Then $O(K) = K$ which gives $H \subseteq \operatorname{Stab}(K) = N_G(K)$. Now $K \trianglelefteq N_G(K)$ which gives that $K$ is $p$-Sylow in $N_G(K)$. Since $H$ is also $p$-Sylow in $N_G(K)$ but there is a unique $p$-Sylow inside the normalizer by the Second Sylow Theorem, so $H = K$. This is a good trick to apply the second Sylow to the normalizer of $K$.

Now we conclude that $|S| \equiv 1 \bmod p$, thus finishing the proof of Theorem the Third Sylow.

Now $|O(K)| > 1 \implies p \mid |O(K)|$ and by the Orbit Stabilizer theorem $|O(K)| \cdot |\operatorname{Stab}(K)| = |H| = p^r$. So $|O(K)| = p^\ell$ for some $\ell \in \mathbb{N}$. We know that

$$|S| = \sum_{[k]} |O(K)| = |O(H)| + \sum_{[k] \neq [H]} |O(K)| \equiv 1 \bmod p$$

This completes the proof. $\square$

# Group Actions on Sets

As we have seen that classifying finite groups becomes increasingly hard. Classifying groups of order only 16 is very difficult. This leads us to a new approach. We will study groups by studying their normal subgroups and their quotients.

**Definition**. (Simple)
A group $G$ is a said to be **simple** if it contains no normal subgroups other than $(e)$ and $G$.

Examples:

(i) Any group of prime order.

(ii) Finite abelian groups if and only if it has prime order. This follows since if $p \mid |G|$, by Cauchy's Theorem, $G$ contains an element of order $p$ called $x$ and $\langle x \rangle \trianglelefteq G$.

(iii)

Exercise: Show that if $G$ is non-abelian, $|G| < 60$, then $G$ is not simple. There is a unique non-abelian group which is simple but we will.

Recall that we have shown that the center of a group is normal and group of order $p^n$ has nontrivial center.

After removing groups of these orders we have

$$6, 10, 12, 15, 20, 21, 22, 24, 26, 28, 30, 33, 34, 35, 39, 40, 42, 44, 45, 46, 48, 51, 52, 54, 56, 57$$

Let $p$ and $q$ be primes with $p < q$.

Suppose $G$ is a group of order $2p$.

Suppose $G$ is order $p \cdot q$. Then the number of $q$-Sylows $n_q$ is congruent to 1 mod $q$ and divides $p$, $p$ does not satisfy this since $p < q$ so then there is a unique $q$-Sylow (which is normal) so $G$ cannot be simple.

Suppose $G$ is order $p \cdot q^2$. If $c_q = 1$ then the unique $q$-Sylow is normal and $G$ is not simple. Suppose $C_q = 1$ or $C_q = p^2$. Ten $p^2(q-1)$ elements of $G$ are of order $q$. Exactly $p^2$ elements are left. So there is a unique $p$-Sylow.

We are left with

$$24, 36, 40, 48, 56, 60$$

So $24 = 2^3 \cdot 3$. The number of 2-Sylows $C_2$ divides 3 and is congruent to 1 mod 2. We cannot have $C_2 = 3$ and $C_3 = 4$, so either $C_2 = 1$ or $C_3 = 1$. Each 2-Sylow has order eight.

Suppose $C_3 = 3$ and $C_3 = 4$. We can make a homomorphism to another group with a non-trivial kernel which will give a normal a subgroup of $G$. A group action $G \times S \to S$ induces a homomorphism $G \to \mathrm{Aut}(S)$.

Call the 2-Sylows $S = \{K_1, K_2, K_3\}$. We know by the Second Sylow Theorem these sets are conjugate. Let $G$ act on $S$ by conjugation. Then We obtain a map $\varphi : G \to \mathrm{Aut}(S) \cong S_3$. This

map is transitive, so $\ker(\varphi) \neq G$ and $\ker(\varphi) \neq (e)$ since $\varphi$ cannot be injective. We conclude that $\ker(\varphi)$ is a nontrivial normal subgroup. We conclude that $G$ is not simple.

We can eliminate 40 by seeing there is only 1 5-Sylow.

We can also eliminate 56 by seeing there is either $C_7 \in \{1, 8\}$ Because if there are 8 7-Sylows, then $8 \cdot 6 = 48$ elements of order 7. But this means that there is a unique 2-Sylow. So groups of order 56 are not simple.

Now we consider $|G| = 36 = 2^2 \cdot 3^2$. So $C_2 \in \{1, 3, 9\}$ and $C_3 \in \{1, 4\}$. First suppose $C_3 = 4$. Then put $S$ to be the four 3-Sylows. Let $G$ act on $S$ by conjugation. This induces a map $\varphi : G \to \mathrm{Aut}(S)$. $\ker(\varphi) \neq G$ because elements of $S$ are conjugate (the group action is transitive) and $|\mathrm{Aut}(S)| = |S_4| = 24 < 36$ so $\varphi$ cannot be injective.

For 48 we look at the 2-Sylows which are either 1 or 3 and the same argument as above suffices.

□

# Simple Groups

Now we move on to the initial results of the important program: **the classification of finite simple groups**.

**Definition**. (Alternating Group)
Consider the homomorphism $\mathrm{sgn} : S_n \to \{\pm 1\}$ defined by

$$f(x) = \prod_{i<j}(x_i - x_j) \quad \mathrm{sgn}(\pi) f(x) = \prod_{i<j}(x_{\pi(i)} - x_{\pi(j)})$$

Now we can use cycle notation to describe elements of $S_3$ for example $(123)(45) \in S_5$ written with disjoint cycles. Then

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

Then,

| $\pi \in S_n$ | $\mathrm{sgn}(\pi)$ |
|---|---|
| $e$ | +1 |
| (12) | -1 |
| (13) | -1 |
| (23) | -1 |
| (123) | +1 |
| (132) | +1 |

The sgn(transposition) $= -1$.

**Fact**. (Permutation's are Products of Transpositions)
Any element of $S_n$ is a product of transpositions. The number of such transpositions is invariant under automorphism.

*Proof.*
The first statement follows from inspection.

$$\pi = \prod_{i\in[\ell]} \tau_i \implies \operatorname{sgn}(\pi) = \prod_{i\in[\ell]} \operatorname{sgn}(\tau_i) = (-1)^{\ell}$$

□

Note that $S_n$ is not simple since ker(sgn) gives a nontrivial normal subgroup.

**Theorem**. (Simplicity of $A_n$)
$A_n$ is simple for $n \geq 5$.

**Proposition**. ($A_5$ is Simple)
The group $A_5$ has order 60, is simple, and non-abelian. If $|G| = 60$ and is simple then $G \cong A_5$.

*Proof.*
Let $P \trianglelefteq H \trianglelefteq G$ and suppose $P$ is a $p$-Sylow subgroup of $H$. We show that $P \trianglelefteq G$. So $P$ is the unique $p$-Sylow in $H$. If $x \in H$, then $xPx^{-1} = P$ so we are done. Suppose $x \in G \setminus H$, then consider $xPx^{-1} \subseteq xHx^{-1} = H$, so now that $xPx^{-1}$ has the same order as $P$, so it must be the unique $p$-Sylow.

Now if $|G| \in \{15, 20, 30\}$ then $G$ has a unique 5-Sylow. This follows immediately from the Third Sylow for 15 and 20. Now from the homework we know that groups of order 30 contain a normal subgroup of order 15 isomorphic to $C_{15}$ which is cyclic (so its center is the whole subgroup). Now the previous paragraph shows that $C_5 \trianglelefteq G$ since $C_5$ is the unique 5-Sylow in $C_{15}$.

Let $G$ be a group of order 60. Then $\text{Syl}_5 \in \{1, 6\}$ by the Third Sylow. Now suppose $\text{Syl}_5 = 6$ (these are all cyclic), and $G$ contains a nontrivial proper normal subgroup $H$. If $|H| \in \{5, 10, 15, 20, 30\}$ then $H$ contains a normal 5-Sylow and by two paragraphs ago there is a unique 5-Sylow in $G$ but we assumed this was not the case. So now $|H| \in \{2, 3, 4, 6, 12\}$.

Now suppose there exists an $H$ or order 6 or 12. If $|H| = 6$, then $H$ has a unique 3-Sylow. If $|H| = 12$ then $H$ might have four 3-Sylows, if this is the case then there is a unique 2-Sylow which has order four. So now if $|H| = 6$, then there is a nontrivial proper normal subgroup $H'$ with order in $\{2, 3, 4\}$.

Now consider the quotient $G/H'$ which must have order 15,20, or 30 by Lagrange's Theorem. Then by the argument above $G/H'$ has a unique 5-Sylow which can be lifted to a subgroup $K$ which is normal in $G$ and contains a group of order 5. So $5 \mid |K|$.

The conclusion from all of this is that if $\text{Syl}_5 = 6$ there is no such nontrivial, proper, normal subgroup in $G$. Checking that in $A_5$ it is the case that $\text{Syl}_5 = 6$. □

**Proposition**. (There is a Unique Simple Group of Order 60)
Up to isomorphism, $A_5$ is the unique simple group of order 60.

*Proof.*
Suppose $G$ is a simple group of order 60. We will show that $G$ cannot have a subset $H \subset G$ such

that $[H : G] < 5$. $G$ is not simple so there cannot be subsets with index 1, 2 (since these subgroups will be normal) since this does not divide 60. Suppose $G$ has a subgroup of index 3 (resp. 4). Take $n \in \{3, 4\}$. Consider the group action given by left multiplication acting on $G/H$. Then the group action induces a homomorphism $h : G/H \to \mathbb{S}_n$. This map cannot be trivial since the map is surjective. Now if $n < 5$, then $n! < 60$ so the map cannot be an injection.

Now suppose $G$ has a subgroup $H$ of index 5, show that $G$ is isomorphic to $A_5$. Use the same map as above to obtain a homomorphism $h : G \to S_5$, we know this map is injective (since it is not a trivial map and $G$ is simple). Compose with the quotient map to obtain $G \to S_5 \to S_5/A_5$ and we want to show this is trivial. Since if everything in $G$ is annihilated by this map, then the image of $G$ is contained in $A_5$. The size of the map of this kernel is at least 30, but it cannot be between 30 and 60 since $G$ is simple (and the kernel is a normal subgroup). So, now we know that $G$ must size 30, and so the composed map is trivial.

$$G \xhookrightarrow{\iota} S_n \xrightarrow{\pi} C_2$$

Figure 4: Composed Homomorphism

We know that $\text{Syl}_2 \in \{1, 3, 5, 15\}$. Suppose $\text{Syl}_2 \notin \{1, 3\}$. It cannot be one since then $G$ would not be normal. Similarly, cannot be three since then we can induce a homomorphism by the group action of conjugation acting on the set of two Sylows into $S_3$. We can also frame this in terms of cosets, since the orbit of this group action is in bijection with the cosets of the normalizer of a 2-Sylow. Now the same argument as above works to show $G \cong A_5$.

Now we need to rule out that $\text{Syl}_2 \neq 15$. If all the Note that there are at least $\text{Syl}_5 \geq 6$ and all elements in these groups have order five. It cannot be the case that all the 2-Sylows are disjoint since then we would have accounted for at least $4 \cdot 6 + 3 \cdot 15$ elements.

Let $P$ and $Q$ be 2-Sylows with nontrivial intersection. Consider $N_G(P \cap Q)$. $|P| = 4 = |Q|$ and $P, Q \subset N_G(P \cap Q)$.

FINISH AT HOME □

**Theorem**. ($A_n$ is simple for $n \geq 5$)
$A_n$ is simple for $n \geq 5$ and is the unique simple group of this order.

Product of permutations $(132)(45)(1452) = (15)(23)$.

Conjugation in $S_n$: $\sigma(i_1 i_2 \cdots i_r)\sigma^{-1}$. For example $\sigma = (132)$ and $\tau = (14)(523)$ then $\sigma\tau\sigma^{-1} = (125)(34) = (34)(512) = (\sigma(1)\sigma(4))(\sigma(5)\sigma(2)\sigma(3))$. In general, $\sigma(i_1 i_2 \cdots i_r)\sigma^{-1} = (\sigma(i_1)\sigma(i_2) \cdots \sigma(i_r))$.

First we show that the product of two transpositions can be written as the product of two three cycles. $(i_1 i_2)(i_3 i_4) = (i_3 i_2 i_4)(i_1 i_3 i_2)$ if they have nothing in common. And if they have an element in common then $(i_1 i_2)(i_2 i_3) = (i_1 i_2 i_3)$ as a singleton product. Since $A_n$ can is generated by even permutations, and even permutations are a product of an even number of transpositions. We can group these into pairs, which becomes tuples of three cycles. Three cycles are contained in $A_n$, so thus $A_n$ is generated by three-cycles.

Now we show that three cycles are conjugate in $S_n$. Let $\sigma(x) = x'$. Note that $\sigma(abc)\sigma^{-1} = (a'b'c')$. Now pick $r, s \notin \{a, b, c\}$. Now $\sigma(rs)(abc)(rs)\sigma^{-1} = (a'b'c')$.

Suppose $N \trianglelefteq A_n$. We will show that $n = (e)$ or $N$ contains a 3-cycle. Since $N$ is finite, there is a nontrivial element $\sigma \in N$ that has maximal element with respect to number of fixed points. Suppose $\sigma$ can be written as a product of disjoint transpositions. So $\sigma = \prod_{i=1}^{t}(a_i b_i)$ where $t \geq 2$ since $\sigma \in A_n$. Now we take $r \in \{1, \ldots, n\}$ such that $r \notin \{a_i b_i : i \in [t]\}$. Put $\tau = (a_1 b_1 r)$. Now show that the **commutator** $\tau\sigma\tau^{-1}\sigma^{-1}$ lies in $N$ since $N$ is normal. In this case the commutator is not trivial. Then $\tau^{-1} = (a_1 r b_1)$ and $\sigma^{-1} = \sigma$ then we have

$$\tau\sigma\tau^{-1}\sigma^{-1} = \tau(\sigma(a_1)\sigma(r)\sigma(b_1)) = \tau(b_1\sigma(r)a_1) = (a_1 r)(b_1\sigma(r)).$$

So in our proof this forces $r$ and $\sigma(r)$ to be in the set.

In the class proof we contradicted the maximality.

□

**Definition**. (Normal Series)
Let $G$ be a group. A **normal series** for $G$ is a sequence of nested subgroups

$$G = G_0 \trianglerighteq G_1 \cdots \trianglerighteq G_r = (e).$$

Two normal series $\{G_i\}_{i\in[r]}$ and $\{H_j\}_{j\in[s]}$ are said to be **equivalent** provided that the collection of quotients $\{G_i/G_{i+1}\}$ is the same as the quotients $\{H_j/H_{j+1}\}$ up to isomorphism. In particular if each are distinct then $r = s$ is a necessary condition for equivalence.

**Definition**. (Composition Series)
A **composition series** for $G$ is a normal series in which each quotient $G_i/G_{i+1}$ is nontrivial and simple.

**Theorem**. (Jordan-Holder)
If $G$ has a composition series, then any two composition series are equivalent.

**Proposition**. (Finite Groups Admit Composition Series)
If $G$ is a finite group, then $G$ has a composition series.

*Proof.*
Suppose $G$ is finite. Suppose $G$ has no composition series.

Consider all paths through the

If $G$ is simple then we are done, since $(G, (e))$ is a composition series for $G$. We induct on the order of $G$. If $|G| = 1$ then $G$ is simple and $((e))$ is a composition series. Now assume inductively that all groups with $|G| < k$ have a composition series. If $G$ is not simple, then $G$ has a maximal nontrivial normal subgroup $N_1$. Then $G/N_1$ has order strictly less than $G$. By the inductive hypothesis $G/N_1$ has a composition series $(\overline{G_2}, \ldots, \overline{G_r})$. The correspondence theorem lifts this sequence to a series$(G_2, \ldots, G_r)$ of subgroups in $G$. Lifting preserves normality. Then $(G_1, G_2, \ldots, G_r)$ is a composition series for $G$. □

Exercise: Find composition series for the following groups

(i) $S_3$. $S_3$ has the normal subgroup $T = \{e, \tau, \tau^2\}$. So then $(S_3, T, (e))$ is a composition series for $S_3$.

(ii) $D_4$. Put $N = \{e, x, x^2, x^3\}$ then $(D_4, N, \{e, x^2\}, (e))$ is a composition series. Any subgroup of index two is

For any $p$-group, every composition series looks like $(G, C_p, \ldots, C_p, (e))$. Any path through the subgroup lattice generates a $p$-group. We can also reverse $N$ and $\{e, x^2\}$ to get a new composition series.A

(iii) $Q$ the quaternions. Let $I = \{e, \pm\mathbf{i}\}$ and define $J$, $K$ similarly. Then $(Q, I, J, (e))$ is a composition series. The composition series look like $(Q, N_1, N_2, (e))$ where $N_1, N_2 \in \{I, J, K\}$ are distinct.

(iv) $C_3 \times C_3$. This is a simple group so $(C_3 \times C_3, (e), (e))$ is the only composition series.

(v) $C_9$. This group is abelian, so every subgroup is normal. So the only composition series is $(C_9, \{e, x^3, x^6\}, (e))$.

I WAS SICK HERE

**Definition**. (Commutator)
Let $G$ be a group with $x, y \in G$. Define the **commutator** of $x$ and $y$ as $[x, y] = xyx^{-1}y^{-1}$. Then $[x, y] = e \iff xy = yx$.

**Definition**. (Commutator Subgroup)
The **commutator subgroup** or (derived subgroup) of $G$ is the subgroup of $G$ generated by all commutators $[x, y]$ with $x, y \in G$. We denote this $G', G^{(1)}$, or $[G, G]$.

A subgroup generated by a set $S$ is the

(a) smallest subgroup of $G$ containing $S$,

(b) intersection of all subgroups containing $S$, and

(c) $S^*$ where $*$ is the Kleene star operator.

Now we show that $G' \trianglelefteq G$. Take $g, x, y \in G$ and then $gxyx^{-1}y^{-1}g^{-1}\ g[x, y]g^{-1} = gxygxg^{-1} = [gxg^{-1}, gyg^{-1}]$.

Now we compute $G'$ for $S_3, D_4, Q, D_5$.

(a) $[S_3, S - 3] = \{e, x, x^2\}$

(b) $[D_4, D_4] = \{e, x^2\}$

(c) $[Q, Q] = \{\pm I_2\}$

(d) $[D_5, D_5] = \{e, x, x^2, x^3\}$

**Theorem**. (Universal Property of Commutator Subgroup)
$G/G'$ is abelian. Moreover if $\psi \in \mathrm{Hom}(G, A)$ where $A$ is abelian, then $G' \subseteq \ker(\psi)$ and there is a unique homomorphism $\overline{\psi} \in \mathrm{Hom}(G/G', A)$ then the following diagram commutes.
DIAGRAM
So the commutator is the $\subset$-smallest $H \subseteq G$ such that $G/H$ is abelian.

Take $[x], [y] \in G/G'$ and compute $[[x], [y]] = [x][y][x]^{-1}[y]^{-1} = [xyx^{-1}y^{-1}] = [e]$.

**Definition**. (Commutator Series)
Iteratively take commutators of $G$. The **derived series** or **commutator series** of $G$ is

$$G = G^{(0)} \supseteq G^{(1)} \supseteq \cdots$$

It might be that if we keep taking commutators then we eventually get $(e)$.

**Definition**. (Solvable)
$G$ is said to be **solvable** if it admits a normal series in which every successive quotient is abelian. We will use this definition when we study Galois Theory.

**Theorem**. (Characterization of Solvability)
$G$ is solvable when the commutator series is a normal series. So we eventually get $(e)$ when we take successive commutators.

*Proof.*
If $G$ is solvable then it has a normal series. By definition of solvable, $G^{(1)} \subseteq G_1$ and similarly, $G^{(k)} \subseteq G_k$. Eventually some $k$ gives $G_k = (e)$ which shows the commutator series is a normal series.

Now for the other direction. □

# Group Presentation

**Definition**. (Universal Property of Free Groups)
The **free group** on $S$ (a set) is a group $f(S)$ together with an injection $\iota : S \hookrightarrow f(S)$ with the property that the following diagram commutes.

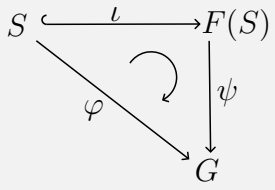
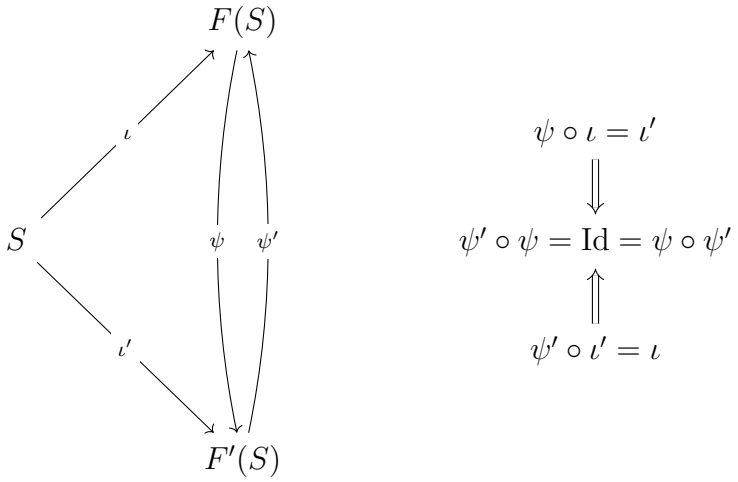



Figure 5: Universal property of free groups.

Furthermore $\psi$ is unique.

Taking $G$ to be $f'(S)$




So all that is left is to argue uniqueness of the map $\psi$.

**Definition**. (Construction of Free Group)
The free group on $S$ is the set of all reduced words on $S$ (where no cancellations are possible). Every word can be simplified to a unique reduced word. The free group $F(S) = S^*/\sim$ where $*$ is the Kleene star operator and the group product is given by concatenation where $\sim$ is the equivalence relation that identifies words of the same reduced word.

Exercise: Show that in fact this gives a construction of the free group.

Let $\varphi : S \to G$ be a set-theoretic map. Any such $\psi \in \mathrm{Hom}(S^*/\sim, G)$ is determined by $\varphi$ on the coset representatives of $x \in S$.

For example $F(\{x, y\})$ maps surjectively onto $D_n$ for all $n \in \mathbb{Z}^+ \cup \{\infty\}$.

Let $S = \{x, y\}$. Now take $N = N_{F(S)}(\langle x^n, y^2, xyxy^{-1}\rangle)$. Then $F(S)/N \cong D_n$.

# Coxeter Todd Algorithm

# SYMMETRY

We want to understand geometric symmetries. In $\mathbb{R}^n$ these are isometries or rigid motions.

**Definition**. (Isometry)
A **rigid motion** or **isometry** is a map $f : \mathbb{R}^n \to \mathbb{R}^n$ that preserves distances.

One can check that every isometry is a bijection. So the set of isometries $M_n$ on $\mathbb{R}^n$ forms a group.

For $n = 1$, this group is $\{x \mapsto x + r, x \mapsto -x + r : r \in \mathbb{R}\}$. Let $H$ be the set the set of translations on $\mathbb{R}$ and $K$ the set of reflections about any point in $\mathbb{R}$.

Note that $H$ is isomorphic to $\langle \mathbb{R}, + \rangle$. Then $K$ is isomorphic to $C_2$.

So then $K$ is normal in $M_1$.

This gives us $\mathbb{R} \rtimes C_2$ and conjugation gives a map $C_2 \to \mathrm{Aut}(\mathbb{R}, +)$.

Let $M_1$ be the set of reflections.

So $M_1/\mathbb{R} \cong C_2$. Any two subgroups of $M_1$ of order two are conjugate.

Now we should consider $M_2$. The set of translations is a subset of $M_2$ that is isomorphic to $\langle \mathbb{R}^2, + \rangle$, or $T$ the set of rotations. Now take $\mathcal{O}_2$ the set of isometries that fix the origin. Then $M_2 T \rtimes \mathcal{O}_2$. We can rotate by any $\theta \in \mathbb{R}/2\pi\mathbb{Z}$. The set of rotations in $\mathcal{O}_2$ has index two, so it is normal and its quotient is $C_2$. So $\mathcal{O}_2 \cong \{\text{rotations fixing } 0\} \ltimes C_2$.

**Proposition**. (Isometries are Affine)
Every isometry that fixes the origin is linear in $\mathbb{R}^n$.

*Proof.*
Choose $A$ an orthogonal matrix, so $A^T = A^{-1}$. $A$ induces an isometry on $\mathbb{R}^n$, because the columns of $A$ form an orthonormal basis of $\mathbb{R}^n$. This follows since $A$ fixes the dot product, so $A$ fixes distances too.

All isometries that fix the origin are induced by some orthonormal matrix. Let $L \in M_n$, an isometry. So $\|x\| = \|L(x)\| \implies \langle x, x \rangle = \langle L(x), L(x) \rangle$. Also $\|x - y\| = \|L(x) - L(y)\|$ which implies $\langle x - y, x - y \rangle = \langle L(x) - L(y), L(x) - L(y) \rangle$. Expanding this gives the equation $\langle x, y \rangle = \langle L(x), L(y) \rangle$. So now we know every isometry on $\mathbb{R}^n$ preserves the dot product. Put $A = (L(e_1), \ldots, L(e_n))$. Then the columns of $A$ must be orthogonal since $e_1, \ldots, e_n$ are orthogonal. Take $x \in \mathbb{R}^n$ are write $x = \sum_{i \in [n]} a_i e_i$ and $L(x) = \sum_{i \in [n]} b_i L(e_i)$. Now apply $A$ and $A^T$ to $x$ and we will get $x$.

To recap the set of translations $T$, we have $T \trianglelefteq M_n$ and $M_N/T \cong \mathcal{O}_n$.

Now take $A\mathcal{O}_2$. Suppose $\det(A) = 1$. Since $A$ is angle preserving $A$ must be a rotation and is thus given in the form

$$\begin{bmatrix} \cos(\theta) & \sin(\theta) \\ \sin(\theta) & -\cos(\theta) \end{bmatrix}$$

If instead $\det(A) = -1$. Then it must include a reflection so it is a reflection about the line. This is the reflection over the angle bisector of $e_1$ and $Ae_1$.

Now take $\rho_\theta \in \mathrm{SO}_2$. Then $r\rho_\theta^{-1} = \rho_{-\theta}$ where $r$ is rotation about the $x$-axis.

Let $t_\alpha$ be the translation by $\alpha \in \mathbb{R}^2$. Everything in $O_2$ is of the form $\rho_\theta$ or $\rho_\theta r$. Since $M_2 = T \rtimes O_2$ so we can write every element in the form $t_\alpha \rho_\theta r$.

(a) $\rho_\theta t_\alpha(x) = \rho_\theta(x+\alpha) = \rho_\theta(x) + \rho_\theta(\alpha) = \rho_\theta(x) t_{\rho_\theta(\alpha)}$

(b)

(c)

(d)

(e)

The projection map $\pi_1 : M_2 \to O_2$ commutes with change of coordinates if the change of coordinates map is translation.

Find a $b$ such that $t_b \cdot m t_b^{-1} = t_b \cdot t_a \rho_\theta \cdot t_{-b} = t_{a+b} t_{\rho_\theta(-b)} \rho_\theta = t_{a+b-\rho_\theta(b)} \rho_\theta = 0$

So we are going to solve for $\rho_\theta(b) - b = a$. We can check $\rho_{\theta(b)} - b$ is non-singular. Its determinant is $2(1-\cos(\theta))$. So if $\theta > 0$ with $\theta \in \mathbb{R}/2\pi\mathbb{Z}$.

Now for elements of the form $t_a \rho_\theta r$ we can write them as $t_a \ell$ for some line $\ell$. Then there is a (rotation) element in $\eta \in M_2$ whose conjugation gives the change of coordinates. So now $\eta^{-1}(\rho_\theta r)\eta = r$ and $\eta^{-1} t_a \eta = t_{a'}$ since the translations are normal in $M_2$. This gives that

$$t_{a'} r \begin{bmatrix} x \\ y \end{bmatrix} = t_{a'} \begin{bmatrix} x \\ -y \end{bmatrix} = \begin{bmatrix} a_1' \\ a_2' \end{bmatrix} + \begin{bmatrix} x \\ -y \end{bmatrix} +$$

Then $y = \frac{a_2'}{2}$ and $x$ is free.

Now we can ask

(a) What is the composite of two rotations (about two possibly different points)?

So what is $t_a \rho_\theta t_{a'} \rho_{\theta'} = t_{a+\rho_\theta(a')} \rho_{\theta+\theta'}$ This is a rotation around a point or a translation. This is a translations when $\theta + \theta'$ is zero in $\mathbb{R}/2\pi\mathbb{Z}$.

(b) What is the composite of two rotations and a glide? $t_a \rho_\theta r t_{a'} \rho_{\theta'} = t_a \rho_\theta t_{a'} r \rho_{\theta'} = t_{a+\rho_\theta(a')} + \rho_{-\theta'} r$ This is a glide. In either case it is a glide (since it is orientation reversing).

(c) What is the composite of two glides? Either a reflection or a translation.

Glides are orientation reversing and rotations and translations are orientation preserving. Recall we determine orientation by projecting to $O_2$ then taking the determinant.

**Definition**. (Discrete Group)
$\Gamma \subseteq M_2$ is said to be discrete if it does not contain arbitrarily small rotations or translations.

You might worry about why we did not impose any conditions on a glide. But the translation condition ensures that the product of a glide with itself is not arbitrarily small and also the product of two glides is not arbitrarily small.

We have $T \subseteq M_2 \to O_2$ So we can analyze a discrete $\Gamma$ by considering $\Gamma \cap T$ or the image $\bar{\Gamma}$ under the quotient map.

So $\Gamma \cap T$ is a discrete subgroup of $\mathbb{R}^2$.

Exercise: Describe all discrete subgroups of $\mathbb{R}^2$.

The simplest thing is $(\vec{0})$. If we take an element generated by one element then it is isomorphic to $\mathbb{Z}$. If you choose two directions well then you get a lattice. So the answer is $\mathbb{Z}^2$.

**Definition**. (Wallpaper Pattern)

$$T \to M_2 \to O_2$$
$$\Gamma \cap T \to \Gamma \to \bar{\Gamma}$$

Where there is containment. We want to understand $\Gamma \cap T$ and $\overline{\Gamma}$ separately.

Put $L \cong \Gamma \cap T$ then we have three possibilities for $L$,

$$L = \begin{cases} (e) \\ \mathbb{Z} \\ \mathbb{Z}^2 \end{cases}$$

*Proof.*
Suppose $L \neq 0$. Then suppose $L \subseteq \ell$ for $\ell$ a line through the origin. Then we can choose an element $\vec{v}$ of shortest length to zero. Then it must be that $L = \{m\vec{v} : m \in \mathbb{Z}\}$.

Now suppose $L$ is not contained on a line. Again we can choose a vector $\vec{v}_1$ of smallest length to the origin. Now there must be some vector $\vec{v}_2$ which is not contained in $\text{Span}(\vec{v}_1) = \ell$. Change coordinates so that $\ell$ is the $x$-axis. Pick $\vec{v}_2$ so that the height from the $x$-axis to $\vec{v}_2$ is minimized.

So we have found that $L$ is quite simple, it is a lattice.

Now let's consider the other group $\overline{\Gamma}$. Recall that everything in $M_2$ is of two kinds, those which are orientation performing $t_a\rho_\theta$ and those that are orientation reversing $t_a\rho_\theta r$. The former are either translations or rotations and the latter are glides.

When we analyzed glides we noted that $\rho_\theta r$ is some reflection about a line and the glide $t_a\rho_\theta r$ is a glide about a line $\ell'$ parallel to $\ell$. So the map $\Gamma \to \overline{\Gamma}$ takes rotations and translations to their rotational parts and it takes glides to reflections about the unique line $\ell$ which is parallel to the line $\ell'$.

The image $\overline{\gamma}$ is called the point set of $\Gamma$. Since $\Gamma \subseteq M_2$ is discrete, $\overline{\Gamma}$ is discrete in $O_2$. Let's consider what are the possibilities for $\overline{\Gamma}$. Translations are annihilated by the projection map. So rotations are taken to elements that generate groups isomorphic to $C_n$. And glides are taken to reflections.

Since $\text{SO}_2 \trianglelefteq O_2$ we have $\overline{\Gamma}/(\overline{\Gamma} \cap \text{SO}_2) \hookrightarrow \mathcal{O}_2/\text{SO}_2 \cong \{\pm\}$. So $\overline{\Gamma} \cap \text{SO}_2$ is finite and semidirect product rules show that $\overline{\Gamma}$ must be $C_n$ or $D_n$.

$M_2$ acts on $T$ by conjugation. $O_2$ acts on $T$ by $\rho t_a \rho^{-1} = t_{\rho(a)}$ and in the same way $\overline{\Gamma}$ acts on $L$.

Now let's put all this information together to consider what are the possible forms of $\Gamma$. When $L = \mathbb{Z}$, this will require some work. Meaning, we want to study (classify[1]) $\Gamma$ such that $L \cong \mathbb{Z}^2$.

[1]Maybe this is too much at this point.

**Definition**. (Crystallographic Restriction)
$\overline{\Gamma} \cong C_2$ or $D_n$ then $n \in \{1, 2, 3, 4, 6\}$.

*Proof.*
Pick some nontrivial element $a \in L$ of smallest possible length. If $\overline{\Gamma} \subseteq D_n$ then $\rho_\theta \in \overline{\Gamma}$ where $\theta = \frac{2\pi}{n}$. This prevents $\theta$ from being very small. If $\theta < \pi/3$ then there is an element $b \in L$ such that $b - a$ is shorter than $a$. This restricts to $n \leq 6$. Now let's eliminate $n = 5$.

If we could rotate $a$ about a pentagon then we can obtain an element shorter than $a$, namely considering $a + \rho_{2\pi/3} a$.

If $\Gamma$ is the isometry group of a (proper ie not squares) rectangular lattice then we can only rotate by multiples of $\pi$ on points in the lattice or on the midpoints of the rectangles. But we can also reflect about many lines, so the point group is $D_2$.

If $\Gamma$ is the isometry group of a square lattice, then we can rotate by $\frac{\pi}{2}$ and this makes the point group $D_4$.

The point set is

(a) $C_1$

(b) $C_2$

(c) $C_3$

(d) $C_4$

(e) $C_6$

(f) $D_1$

(g) $D_1$ There is a glide.

(h) $D_1$

(i) $D_2$

(j) $D_2$ rotation about the middle of a rectangle, there is also a glide.

(k) $D_2$

(l) $D_2$

(m)

(n)

(o)

(p)

(q)

Theorem. These 17 wallpaper patterns give all possible isomorphism classes of discrete subgroups of $M_2$ with $L$ isomorphic to $\mathbb{Z}^2$. There are several of these groups with the same pointset. Why is that the case ?

**Definition**. (Exact Sequence)
Let $G_0, G_1, \dots$ be groups with maps

$$\cdots \to G_0 \to G_1 \to G_2 \to G_3 \to \cdots$$

The sequence is said to be **exact** at $G_i$ if $\Im(\phi_{i-1} = \ker(\phi_i)$.

**Definition**. (Short Exact Sequence)
A **short exact sequence** is an exact sequence of the form

$$1 \to H \to G \to K \to 1.$$

So $\ker(\varphi) = (1)$ and so $\varphi$ is injective. And $\Im(\psi) = K$, so $\psi$ surjective. Exactness in the middle means $\Im(\varphi) = \ker(\psi)$.

So we have a map $\psi : G \to K$ with $\ker \psi \Im(\varphi) = \varphi(H)$. The first isomorphism theorem says that $G/\varphi(H) \cong K$. So now we see that every short exact sequence is of the following form: take $N \trianglelefteq G$ then $1 \to N \to G \to G/N \to 1$.

Now here's what's interesting. Suppose you are given two groups $H, K$ (one for each end). How many ways are there for $1 \to H \to G \to K \to 1$ to be short exact. In general this is quite hard to answer.

We can always take $G = H \times K$. We can also take $G = H \rtimes_\varphi K$ for any $K \to \mathrm{Aut}(H)$. But these are not the only ways.

Let $H = C_2 = K$. We want $1 \to C_2 \to G \to C_2 \to 1$ to be short exact. Then $G$ must have size four, and there are only two groups of this order. In fact both of these possibilities work. But note that $C_4$ is not a semidirect product. This follows since there is only one map $C_2 \to \mathrm{Aut}(C_2)$ so every semidirect product $C_2 \rtimes C_2 \cong C_2 \times C_2$.

Exercise: Let $H = C_4$ and $K = C_2$.

Using our short exact sequences we will analyze all possible $\Gamma$.

To recall we have the exact sequence

$$0 \to T \to M_2 \to O_2 \to 1.$$

Now taking intersections of each of these groups with a discrete group $\Gamma \subseteq M_2$ gives a new short exact sequence

$$0 \to L \to \Gamma \to \overline{\Gamma} \to 1.$$

And we found the point group or $\bar{\Gamma}$ is isomorphic to one of $C_n$ or $D_n$ for $n \in \{1, 2, 3, 4, 6\}$.

This motivates the following problem.

**Problem**. (Extension Problem for Groups)
Given $H, K$, classify $G$ such that the following sequence is exact:

$$1 \to H \to G \to K \to 1.$$

We will identify $H$ with its image in $G$ (which is normal in $G$). Now $G/H \cong K$ by the First Isomorphism Theorem. So this is equivalent to (given $H$ and $K$ groups) find a $G$ such that $H \trianglelefteq G$ and $G/H \cong K$.

This is a horribly difficult problem. It is basically unsolvable.

Recall that there are two easy ways to find such a $G$ given an $H$ and $K$. For any $\Theta : K \to \mathrm{Aut}(H)$ then $G = H \rtimes_\Theta K$ works.

**Definition**. (Split Exact Sequence)

The map

$$1 \to C_4 \to C_4 \times C_2 \to C_2 \to 1$$

is split because you can always lift $C_2$ to a group isomorphic to $C_2$ in $C_4 \times C_2$ since there are three elements of order two in $C_4 \times C_2$ and only one in $C_2$.

$$1 \to C_4 \to C_8 \to C_2 \to 1$$

is not split since $C_8$ contains an element of order eight and $C_4 \rtimes_\phi C_2$ never has an element of order eight. Alternatively, there is a unique cyclic group of order four inside $C_8$, so there is no complement inside of $C_8$ isomorphic to $C_4$ which is different than the obvious one.

$$1 \to C_4 \to D_4 \to C_2 \to 1$$

is split because $D_4 \cong C_4 \rtimes C_2$. So this sequence is exact for the standard maps. But the sequence is exact for any maps since any reflection together with a rotation generates $D_4$ because there is only one choice for $C_4$ inside of $D_4$.

$$1 \to C_4 \to Q \to C_2 \to 1$$

is not split because any subgroup of order four contains $\{\pm 1\}$, so there is no way to find a complement.

We don't need to consider $(C_2)^3$ since it has no element of order four.

**Theorem**. (Classification of Wallpaper Groups)

We start by considering the cases $C_4 = \{e, \rho_{\pi/2}, \rho_\pi, \rho_{3\pi/2}\}$ and $D_4 = \langle C_4, \gamma \rangle$. We can look at what restriction having $\overline{\Gamma} = C_4$ places on $\Gamma$. This forces the basis elements of the lattice to be orthogonal

and the same magnitude. The only thing that can change now is scaling the lattice basis, but this does not affect the group structure, so we are done. This group is $\mathbb{Z}^2 \times C_4$.

More formally, consider a vector of minimal magnitude $v_1$ then $C_4$ acts on it and we get a $v_2 = \rho_{\pi/2} v_1$. Then we get $v_1 + v_2$ and its rotations will complete the lattice. Assume there is a $w$ which is not generated by $v_1$ and $v_2$, then we can find a $w - av_1 - bv_2$ for some $a, b \in \mathbb{Z}$ which lies in the convex hull of $0, v_1, v_2, v_1 + v_2$ which contradicts our minimality. This tells us that $L$ is a square lattice.

$\rho_{\pi/2}\mathbb{Z}^2\rho_{3\pi/2} = \gamma\mathbb{Z}^2 + 1$

Why does $\overline{\Gamma}$ act on $L$. It follows since $L$ is abelian, so we can lift an element of $\overline{\Gamma}$ to $\Gamma$ and then the conjugation action will have the $L$ portions cancel.

We know the map $0 \to L \to \Gamma \to \overline{\Gamma} \to 1$ is split because $\rho_{\pi/2}$ can be lifted to an element in $M_2$ which is a rotation by $\pi/2$ about some $x$.

So $\Gamma \cong \mathbb{Z}^2 \rtimes C_4$. So then the action is given by $e_1 \mapsto e_2$ and $e_2 \mapsto -e_1$.

Now lets consider $\overline{\Gamma} = D_4$. The element $r$, reflection across the standard axis will lift to an element $t_a r$ and we have $(t_a r)^2 = t_a r t_a r = t_{a'} t_{r(a')} = t_{a+r(a)}$ So $a + r(a) \in L$.

Furthermore, $(t_a r\rho)^2 = t_{a+r\rho(a)} \in L$. So if $a = (p, q)$ then $r(a) = (p, -q)$ and $r\rho(a) = (-q, -p)$ and their sums like $(2p, 0), (p - q, p - q)$ are in $L$. So this leaves us with two possibilities, $(p, q) \in \mathbb{Z}^2$ or $(p, q) \in \left(\frac{1}{2}, \frac{1}{2}\right) + \mathbb{Z}^2$. The first case corresponds to the semidirect product and a split exact sequence. The latter case gives an exact sequence that is not split.

# GROUP REPRESENTATIONS

We now turn to study group actions where the set $S$ is a vector space and the group acts on $S$ as a linear transformation on $S$.

**Definition**. (Group Representation)
Let $G$ be a finite group and $V$ a finite dimensional vector space over a field $k$ $(= \mathbb{C})$. A **representation** of $G$ on $V$ is an action of $G$ on $V$ $G \times V \to V$ such that every element $g \in G$ acts on $V$ as a linear transformation $\rho_g : V \to V$.

We can also think of a representation as a map $\rho : G \to \mathrm{GL}(V)$ since a group action is a homomorphism $G \to \mathrm{Perm}(S)$.

If we pick a basis $v_1, \cdots, v_n$ for $V$, then $\mathrm{GL}(V) \cong \mathrm{GL}_n(\mathbb{C})$. So any representation is a map $\rho \in \mathrm{Hom}(G, \mathrm{GL}_n(\mathbb{C}))$. Choosing a different basis leads to a map which is conjugate to $rho$.

Examples:

(a) Trivial representation. Let $V = \mathbb{C}$ Then $\mathrm{GL}(V) \cong \mathrm{GL}_1(\mathbb{C}) \cong \mathbb{C}^\times$.

(b) $D_n \to \mathrm{GL}_2(\mathbb{C})$. The representation sends $x \mapsto \rho_{2\pi/n}$ rotation by $2\pi/n$ and $y \mapsto r$ reflection about the $x$-axis. As a special case we have $D_3 \cong S_3$ which gives a standard representation of $S_3$.

(c) For two representations $\rho \in \mathrm{Hom}(G, \mathrm{GL}(V)), \tau \in \mathrm{Hom}(G, \mathrm{GL}(W))$ we can produce a new representation $\rho \oplus \tau$ the direct sum which acts on $V \oplus W$.

(d) For $S_3$ we have the $\mathrm{sgn} : S_3 \to \{\pm\} \subseteq \mathbb{C}^\times$ representation.

Can you have a representation of $S_3$ on the cube roots of unity? No since in this case $yxy^{-1} = x \neq x^{-1}$. So the subgroup of rotations in $S_3$ have a representations on the cube roots of unity

**Theorem**. (Representations of $S_3$)
Any representation of $S_3$ is a direct sum of some number of copies of (1) trivial, (2), sgn, and (3) standard representations.

Exercise: Figure out how to get the permutation representation from these.

**Definition**. (Invariance & Complements)
Let $G$ be a group and $(\rho, V)$ a representation of $G$. Then a subrepresentation of $(\rho, V)$ is a subspace $W \subseteq V$ that is $G$-invariant, meaning $\rho_g W \subseteq W$ for all $g \in G$. $G$ is said to be irreducible if its only $G$-invariant subspaces are $0, V$.
It is natural to ask whether $W$ has a $G$-invariant complement (a $U$ such that $V \cong U \oplus W$).

**Theorem**. (Direct sums of representations)
If $G$ has a representation $(\rho, V)$ and $W \subseteq V$ is $G$-invariant, then $W$ admits a $G$-invariant complement. Meaning, $\exists W \subseteq V$ which is $G$-stable such that

$$V = W \oplus W'$$

Example: Fix $G = C_2 = \{e, g\}$ and $V = \mathbb{C}^2$. Then

$$g \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} y \\ x \end{bmatrix}$$

Note that the lines $\langle (1,1) \rangle, \langle (1,-1) \rangle$ are $G$-invariant. This gives us two subrepresentations on sub vector spaces $W, W' \subseteq V$ whose direct sum is $\mathbb{C}^2$.

**Definition**. (Isomorphism of Representations)
Two representations are isomorphic

The number of irreducible representations on a group $G$ is equal to the number of conjugacy classes of $G$.

# LINEAR ALGEBRA

## Bilinear Forms