Math 493
Honors Algebra I

University of Michigan
Harrison Centner
Prof. Kartik Prasanna
September 25, 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.

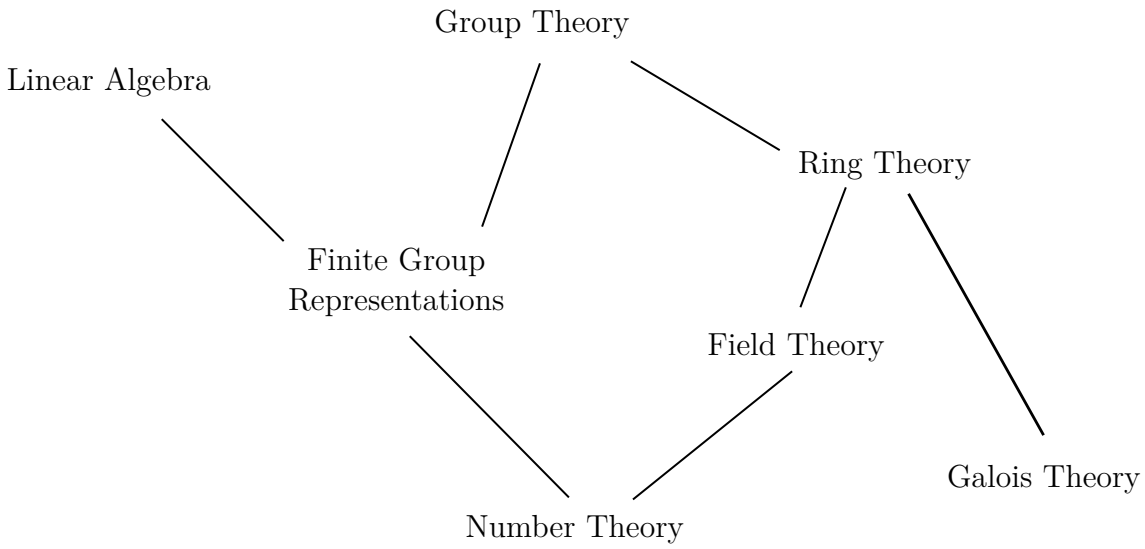


Figure 1: Partial Ordering of Course Topics

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 $(a \star b) \star c = a \star (b \star c)$ (distributivity 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	σ
e	e	σ
σ	σ	e

S_3	e	τ	τ^2	σ	$\sigma\tau$	$\sigma\tau^2$
e	e	τ	τ^2	σ	$\sigma\tau$	$\sigma\tau^2$
τ	τ	τ^2	e	$\sigma\tau^2$	σ	$\sigma\tau$
τ^2	τ^2	e	τ	$\sigma\tau$	$\sigma\tau^2$	σ
σ	σ	$\sigma\tau$	$\sigma\tau^2$	e	τ	τ^2
$\sigma\tau$	$\sigma\tau$	$\sigma\tau^2$	σ	τ^2	e	τ
$\sigma\tau^2$	$\sigma\tau^2$	σ	$\sigma\tau$	τ	τ^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: $S_3, \{e\}, \{e, \sigma\}, \{e, \tau, \tau^2\}, \{e, \sigma\tau\}, \{e, \sigma\tau^2\}$. 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 $\frac{4\pi}{3}$.

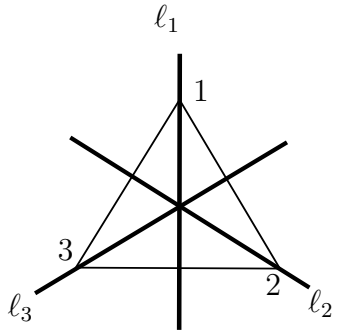


Figure 2: D_3

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 $|D_n| = 2n$.

Lagrange's Theorem & Quotient Groups

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

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

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

(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 $a = ae \in aH \in$ (left cosets).

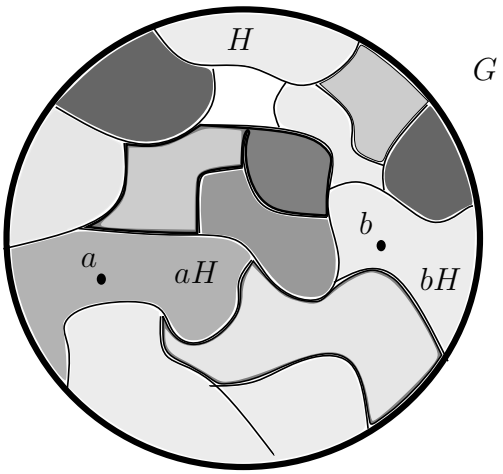


Figure 3: Cosets partition G

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 ϕ an **isomorphism** if ϕ 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 $a = b$. □

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 $H \cong S_2$ 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).

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 ϕ. Meaning,

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

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

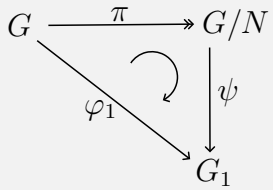
Now to prove the converse, Define a map $\psi : G \to G/N$ where $\psi(a) = aN$.

□

We will show this is a universal property. 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 φ_1 annihilates N.
Then $\exists! \psi$ a homomorphism 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 ψ exists, it must be unique and must be given by the formula $\psi(aN) = \varphi_1(a)$ since φ is surjective.

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

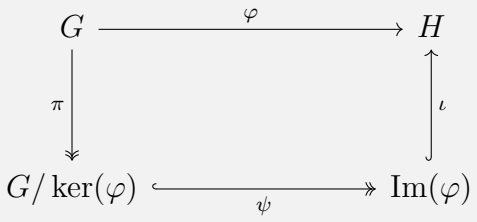
Now we show the second portion. Suppose $N = \ker(\varphi_1)$, then ψ is injective because $\ker(\psi) = \{e\}$. This follows since $\psi(aN) = e \iff \varphi_1(a) = e \iff a \in N$.

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

By prof: ψ 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** φ through $\ker(\varphi)$. Meaning, $\exists! \psi \in \mathrm{Hom}(G/\ker(\varphi), H)$ such that $\varphi = \psi \circ \pi$ where π is projection onto the kernel, ψ is an isomorphism witnessing $G/\ker(\varphi) \cong \mathrm{Im}(\varphi)$, and ι 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. □

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 γ 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. (Nontrivial Centers)
If $|G| = p^n$ for p prime, then $\mathcal{Z}(G) \neq \{e\}$.
Corollary.
Any group of order p^2 is abelian.

Exercise: Hint use the Class Equation.

If $x \notin \mathcal{Z}(G)$, then $|\mathcal{Z}_G(x)| = p^i$ for $i < n$ which gives that $\frac{|G|}{|\mathcal{Z}_G(x)|}$ is divisible by p. It follows from this that $p|\mathcal{Z}_G(x)| \implies |\mathcal{Z}(g)| \geq p \implies \mathcal{Z}(G) > (e)$

Argue that if $|\mathcal{Z}(G)| = p$ then somthing has gone wrong

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

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

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 $g \in \text{Stab}(s)$. 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. □

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

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

What can we say about $p \cdot q$ for primes p and q. If there's only one

Suppose $n = p_1 \cdot p_2$ with $p_1 > p_2$ then p_1, p_2 by the Third Sylow we know that the number of p_2-Sylow subgroups is congruent to 1 mod p_1.

FINISH AT HOMME

LINEAR ALGEBRA

Bilinear Forms