Algebra

D. Zack Garza

August 27, 2019

Contents

---

1 Summary

Groups and rings, including Sylow theorems, classifying small groups, finitely generated abelian groups, Jordan-Holder theorem, solvable groups, simplicity of the alternating group, euclidean domains, principal ideal domains, unique factorization domains, noetherian rings, Hilbert basis theorem, Zorn's lemma, and existence of maximal ideals and vector space bases.

Previous course web pages:

- Fall 2017, Asilata Bapat

2 Major Theorems

Theorem 1 (Cauchy)**.** For any prime p dividing the order of G, there is an element x of order p (and thus a subgroup $H = \langle x \rangle$).

Theorem 2 (Lagrange)**.** If $H \leq G$ is a subgroup, then $|H| \,\Big|\, |G|$.

Theorem 3 (Sylow 1)**.** If $|G| = n = \prod p_i^{a_i}$ as a prime factorization, then G has subgroups of order $p_i^{a_i}$ for every i. Moreover, this holds for any $1 \leq r \leq a_i$.

Theorem 4 (Classification of finitely generated abelian groups)**.** If G is a finitely generated abelian group, then $G \cong F \oplus T$, where F is free abelian and T is a torsion group. If $|T| = n$, then $T \cong \bigoplus \mathbb{Z}_{p_i^{\alpha_i}}$ where $n = \prod p_i^{\alpha_i}$ is some factorization of n with the p_i **not necessarily distinct**.

Theorem 5. Conjugacy classes partition G

$$|G| = |Z(G)| + \sum_{\text{One representative in each orbit}} |C_G(g_i)| = \sum_{asdsa} [G : C(g_i)].$$

Some nice lemmas:

- Every subgroup of a cyclic group is itself cyclic.

3 Lecture 1 (Thu 15 Aug 2019)

> We'll be using Hungerford's Algebra text.Show that a finite abelian group that is not cyclic contains a subgroup which is isomorphic

3.1 Definitions

The following definitions will be useful to know by heart:

- The order of a group

- Cartesian product
- Relations
- Equivalence relation
- Partition
- Binary operation
- Group
- Isomorphism
- Abelian group
- Cyclic group
- Subgroup
- Greatest common divisor
- Least common multiple
- Permutation
- Transposition
- Orbit
- Cycle
- The symmetric group S^n
- The alternating group A_n
- Even and odd permutations
- Cosets
- Index
- The direct product of groups
- Homomorphism
- Image of a function
- Inverse image of a function
- Kernel
- Normal subgroup
- Factor group
- Simple group

Here is a rough outline of the course:

- Group Theory
  - Groups acting on sets
  - Sylow theorems and applications
  - Classification
  - Free and free abelian groups
  - Solvable and simple groups
  - Normal series
- Galois Theory
  - Field extensions
  - Splitting fields
  - Separability
  - Finite fields
  - Cyclotomic extensions
  - Galois groups
  - Solvability by radicals
- Module theory
  - Free modules

    - Homomorphisms
    - Projective and injective modules
    - Finitely generated modules over a PID
- Linear Algebra
    - Matrices and linear transformations
    - Rank and determinants
    - Canonical forms
    - Characteristic polynomials
    - Eigenvalues and eigenvectors

3.2 Preliminaries

Definition 1. A **group** is an ordered pair $(G, \cdot : G \times G \to G)$ where G is a set and $\cdot$ is a binary operation, which satisfies the following axioms:

- Associativity: $(g_1 g_2)g_3 = g_1(g_2 g_3)$,
- Identity: $\exists e \in G \ni ge = eg = g$,
- Inverses: $g \in G \implies \exists h \in G \ni gh = gh = e$.

Example 1.

- $(\mathbb{Z}, +)$
- $(\mathbb{Q}, +)$
- $(\mathbb{Q}^{\times}, \times)$
- $(\mathbb{R}^{\times}, \times)$
- $(\mathrm{GL}(n, \mathbb{R}), \times) = \{A \in \mathrm{Mat}_n \ni \det(A) \neq 0\}$
- $(S_n, \circ)$

Definition 2. A subset $S \subseteq G$ is a **subgroup** of G iff

1. $s_1, s_2 \in S \implies s_1 s_2 \in S$
2. $e \in S$
3. $s \in S \implies s^{-1} \in S$

We denote such a subgroup $S \leq G$.

Examples of subgroups:

- $(\mathbb{Z}, +) \leq (\mathbb{Q}, +)$
- $\mathrm{SL}(n, \mathbb{R}) \leq \mathrm{GL}(n, \mathbb{R})$, where $\mathrm{SL}(n, \mathbb{R}) = \{A \in \mathrm{GL}(n, \mathbb{R}) \ni \det(A) = 1\}$

3.3 Cyclic Groups

Definition 3. A group G is **cyclic** iff G is generated by a single element.

Exercise 1. Show $\langle g \rangle = \{g^n \ni n \in \mathbb{Z}\} \cong \bigcap \{H \leq G \ni g \in H\}$.

Theorem 6. Let G be a cyclic group, so $G\langle g \rangle$.

- If $|G| = \infty$, then $G \cong \mathbb{Z}$.
- If $|G| = n < \infty$, then $G \cong \mathbb{Z}_n$.

Definition 4. Let $H \leq G$, and define a **right coset of** G by $aH = \{ah \ni H \in H\}$. A similar definition can be made for **left cosets**.

Then $aH = bH \iff b^{-1}a \in G$ and $Ha = Hb \iff ab^{-1} \in H$.

Some facts:

- Cosets partition H, i.e. $b \notin H \implies aH \bigcap bH = \{e\}$.
- $|H| = |aH| = |Ha|$ for all $a \in G$.

Theorem 7 (Lagrange)**.** If G is a finite group and $H \leq G$, then $|H| \, \Big| \, |G|$.

Definition 5. A subgroup $N \leq G$ is **normal** iff $gN = Ng$ for all $g \in G$, or equivalently $gNg^{-1} \subseteq N$. I denote this $N \trianglelefteq G$.

When $N \trianglelefteq G$, the set of left/right cosets of N themselves have a group structure. So we define

$$G/N = \{gN \ni g \in G\} \text{ where } (g_1N)(g_2N) = (g_1g_2)N.$$

Given $H, K \leq G$, define $HK = \{hk \ni h \in H, k \in K\}$. We have a general formula,

$$|HK| = \frac{|H||K|}{|H \bigcap K|}.$$

3.4 Homomorphisms

Definition 6. Let G, G' be groups, then $\varphi : G \to G'$ is a **homomorphism** if $\varphi(ab) = \varphi(a)\varphi(b)$.

Example 2.
- $\exp : (\mathbb{R}, +) \to (\mathbb{R}^{>0}, \cdot)$ where $\exp(a+b) = e^{a+b} = e^a e^b = \exp(a)\exp(b)$.
- $\det : (\mathrm{GL}(n, \mathbb{R}), \times) \to (\mathbb{R}^\times, \times)$ where $\det(AB) = \det(A)\det(B)$.
- Let $N \trianglelefteq G$ and $\varphi G \to G/N$ given by $\varphi(g) = gN$.
- Let $\varphi : \mathbb{Z} \to \mathbb{Z}_n$ where $\phi(g) = [g] = g \mod n$ where $\mathbb{Z}_n \cong \mathbb{Z}/n\mathbb{Z}$

Definition 7. Let $\varphi : G \to G'$. Then φ is a **monomorphism** iff it is injective, an **epimorphism** iff it is surjective, and an **isomorphism** iff it is bijective.

3.5 Direct Products

Let G_1, G_2 be groups, then define

$$G_1 \times G_2 = \{(g_1, g_2) \ni g_1 \in G, g_2 \in G_2\} \text{ where } (g_1, g_2)(h_1, h_2) = (g_1h_1, g_2, h_2).$$

We have the formula $|G_1 \times G_2| = |G_1||G_2|$.

3.6 Finitely Generated Abelian Groups

Definition 8. We say a group is **abelian** if G is commutative, i.e. $g_1, g_2 \in G \implies g_1g_2 = g_2g_1$.

Definition 9. A group is **finitely generated** if there exist $\{g_1, g_2, \cdots g_n\} \subseteq G$ such that $G = \langle g_1, g_2, \cdots g_n \rangle$.

This generalizes the notion of a cyclic group, where we can simply intersect all of the subgroups that contain the g_i to define it.

We know what cyclic groups look like – they are all isomorphic to $\mathbb{Z}$ or $\mathbb{Z}_n$. So now we'd like a structure theorem for abelian finitely generated groups.

Theorem 8. Let G be a finitely generated abelian group. Then

$$G \cong \mathbb{Z}^r \times \prod_{i=1}^{s} \mathbb{Z}_{p_i^{\alpha_i}}$$

for some finite $r, s \in \mathbb{N}$ and p_i are (not necessarily distinct) primes.

Example 3. Let G be a finite abelian group of order 4. Then $G \cong \mathbb{Z}_4$ or $\mathbb{Z}_2^2$, which are not isomorphic because every element in $\mathbb{Z}_2^2$ has order 2 where $\mathbb{Z}_4$ contains an element of order 4.

3.7 Fundamental Homomorphism Theorem

Let $\varphi : G \to G'$ be a group homomorphism and define $\ker\varphi = \{g \in G \ni \varphi(g) = e'\}$.

3.7.1 The First Homomorphism Theorem

Theorem 9. There exists a map $\varphi' : G/\ker\varphi \to G'$ such that the following diagram commutes:

$$\begin{tikzcd}
G \arrow[r, dotted, "\varphi"] \arrow[d, "\eta"'] & G' \\
G/\ker\varphi \arrow[ur, "\varphi'"] &
\end{tikzcd}$$

That is, $\varphi = \varphi' \circ \eta$, and φ' is an isomorphism onto its image, so $G/\ker\varphi = \text{im } \varphi$. This map is given by $\varphi'(g(\ker\varphi)) = \varphi(g)$.

Exercise 2. Check that φ is well-defined.

3.7.2 The Second Theorem

Theorem 10. Let $K, N \leq G$ where $N \trianglelefteq G$. Then

$$\frac{K}{N \bigcap K} \cong \frac{NK}{N}$$

Proof. Define a map $K \xrightarrow{\varphi} NK/N$ by $\varphi(k) = kN$. You can show that φ is onto by looking at $\ker\varphi$; note that $kN = \varphi(k) = N \iff k \in N$, and so $\ker\varphi = N \bigcap K$. $\square$

4 Lecture 2

Last time: the fundamental homomorphism theorems.

Theorem 1: Let $\varphi : G \to G'$ be a homomorphism. Then there is a canonical homomorphism $\eta : G \to G/\ker\varphi$ such that the usual diagram commutes. Moreover, this map induces an isomorphism $G/\ker\varphi \cong \text{im }\varphi$.

Theorem 2: Let $K, N \leq G$ and suppose $N \trianglelefteq G$. Then there is an isomorphism

$$\frac{K}{K \bigcap N} \cong \frac{NK}{N}$$

(Show that $K \bigcap N \trianglelefteq G$, and NK is a subgroup exactly because N is normal).

Theorem 3: Let $H, K \trianglelefteq G$ such that $H \leq K$.

1. H/K is normal in G/K.
2. The quotient $(G/K)/(H/K) \cong G/H$.

Proof: We'll use the first theorem. First make a map

$$\begin{aligned} G/K &\to G/H \\ \phi(gk) &= gH \end{aligned}$$

Exercise: Show that this map is onto, and that $\ker\phi \cong H/K$.

4.1 Permutation Groups

Let A be a set, then a *permutation* on A is a bijective map $A\circlearrowleft$. This can be made into a group with a binary operation given by composition of functions. Denote S_A the set of permutations on A.

Theorem: S_A is in fact a group. Check associativity, inverses, identity, etc.

In the special case that $A = \{1, 2, \cdots n\}$, then $S_n \coloneqq S_A$.

Recall two line notation

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$$

Moreover, $|S_n| = n!$ by a combinatorial counting argument.

Example: S_3 is the symmetries of a triangle (see notes).

Example: The symmetries of a square are *not* given by S_4, it is instead D_4 (see notes).

4.2 Orbits

Permutations S_A "acts" on A, and if $\sigma \in S_A$, then $\langle\sigma\rangle$ also acts on A.

Define $a \sim b$ iff there is some n such that $\sigma^n(a) = b$. This is an equivalence relation, and thus induces a partition of A. See notes for diagram. The equivalence classes under this relation are called the *orbits* under σ.

Example:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 2 & 6 & 3 & 7 & 4 & 5 & 1 \end{pmatrix} = (18)(2)(364)(57).$$

Definition: A permutation $\sigma \in S_n$ is a *cycle* iff it contains at most one orbit with more than one element. The *length* of a cycle is the number of elements in the largest orbit.

Recall cycle notation: $\sigma = (\sigma(1)\sigma(2)\cdots\sigma(n))$. Note that this is read right-to-left by convention!

Theorem: Every permutation $\sigma \in S_n$ can be written as a product of disjoint cycles.

Definition: A *transposition* is a cycle of length 2. Moreover, we have

and so every permutation is a product of transpositions. This is not a unique decomposition, however, as e.g. $\mathrm{id} = (12)^2 = (34)^2$.

Theorem: Any $\sigma \in S_n$ can be written as **either** an even number of transpositions or an odd number of transpositions.

Define $A_n = \{\sigma \in S_n \ni \sigma \text{ is even}\}$. We claim that $A_n \trianglelefteq S_n$.

1. Closure: If τ_1, τ_2 are both even, then $\tau_1\tau_2$ also has an even number of transpositions.
2. The identity has an even number of transpositions, since zero is even.
3. Inverses: If $\sigma = \prod_{i=1}^s \tau_i$ where s is even, then $\sigma^{-1} = \prod_{i=1}^s \tau_{s-i}$. But each τ is order 2, so $\tau^{-1} = \tau$, so there are still an even number of transpositions.

So A_n is a subgroup. It is normal because it is index 2, or the kernel of a homomorphism, or by a direct computation.

4.3 Groups Acting on Sets

Think of this as a generalization of a G-module.

Definition: A group G is said to *act* on a set X if there exists a map $G \times X \to X$ such that

1. $e \curvearrowright x = x$

Examples:

1. $G = S_A \curvearrowright A$
2. $H \leq G$, then $G \curvearrowright X = G/H$ where $g \curvearrowright xH = (gx)H$.
3. $G \curvearrowright G$ by conjugation, i.e. $g \curvearrowright x = gxg^{-1}$.

Definition: Let $x \in X$, then define the *stabilizer subgroup*

$$G_x = \{g \in G \ni g \curvearrowright x = x\} \leq G$$

We can also look at the dual thing,

$$X_g = \{x \in X \ni g \curvearrowright x = x\}.$$

We then define the *orbit* of an element x as

$$Gx = \{g \curvearrowright x \ni g \in G\}$$

and we have a similar result where $x \sim y \iff x \in Gy$, and the orbits partition X.

Theorem: Let G act on X. We want to know the number of elements in an orbit, and it turns out that

Proof: Construct a map $Gx \xrightarrow{\psi} G/Gx$ where $\psi(g \curvearrowright x) = gGx$. Exercise: Show that this is well-defined, so if 2 elements are equal then they go to the same coset. Exercise: Show that this is surjective.

Injectivity: $\psi(g_1 x) = \psi(g_2 x)$, so $g_1 Gx = g_2 Gx$ and $(g_2^{-1} g_1)Gx = Gx$ so $g_2^{-1} g_1 \in Gx \iff g_2^{-1} g_1 \curvearrowright x = x \iff g_1 x = g_2 x$.

Next time: Burnside's theorem, proving the Sylow theorems.

5 Lecture 3 (Aug 22)

Last time: let G be a group and X be a set; we say G *acts* on X (or that X is a G- set) when there is a map $G \times X \to X$ such that $ex = x$ and $(gh) \curvearrowright x = g \curvearrowright (h \curvearrowright x)$. We then define the *stabilizer of* x as

$$G_x = \{g \in G \ni g \curvearrowright x = x\} \leq G,$$

and the *orbit*

$$G.x = \mathcal{O}_x = \{g \curvearrowright x \ni x \in X\} \subseteq X.$$

When G is finite, we have

$$\#G.x = \frac{\#G}{\#G_x}.$$

We can also consider the fixed points of X,

$$X_g = \{x \in X \ni g \curvearrowright x = x \forall g \in G\} \subseteq X$$

5.1 Burnside's Theorem

Theorem (Burnside): Let X be a G-set and v be the number of orbits. Then

$$v\#G = \sum_{g \in G} \#X_g.$$

Proof:

Define $N = \{(g, x) \ni g \curvearrowright x = x\} \subseteq G \times X$, we then have

$$
\begin{aligned}
|N| &= \sum_{g \in G} |X_g| \\
&= \sum_{x \in X} |G_x| \\
&= \sum_{x \in X} \frac{|G|}{|G.x|} \\
&= |G| \left(\sum_{x \in X} \frac{1}{|Gx|} \right) \\
&= |G|v.
\end{aligned}
$$

Since the orbits partition X, say into $X = \bigcup_{i=1}^{v} \sigma_i$, let $\sigma = \{\sigma_i \ni 1 \leq i \leq v\}$ and abuse notation slightly by replacing each orbit in σ with a representative element $x_i \in \sigma_i \subset X$. We then have

$$
\sum_{x \in \sigma} \frac{1}{|G.x|} = \frac{1}{|Gx|} |\sigma| = 1.
$$

Application: Consider seating 10 people aroung a circular table. How many distinct seating arrangements are there?

Let X be the set of configurations, $G = S_{10}$, and let $G \curvearrowright X$ by permuting configurations. Then v, the number of orbits under this action, yields the number of distinct seating arrangements. By Burnside, we have

$$
v = \frac{1}{|G|} \sum_{g \in G} |Xg| = \frac{1}{10}(10!) = 9!,
$$

since $Xg = \{x \in X \ni gx = x\} = \emptyset$ unless $g = e$, and $X_e = X$.

5.2 Sylow Theory

Recall Lagrange's theorem: If $H \leq G$ and G is finite, then $\#H \mid \#G$.

Consider the converse: if $n \mid \#G$, does there exist a subgroup of size n? The answer is no in general, and a counterexample is A_4 which has $4!/2 = 12$ elements but no subgroup of order 6.

5.2.1 Class Functions

Let X be a G-set, and choose orbit representatives $x_1 \cdots x_v$. Then

$$
|X| = \sum_{i=1}^{v} |Gx_i|.
$$

We can then separately count all orbits with exactly one element, which is exactly $X_G = \{x \in G \ni g \curvearrowright x = x \ \forall g$

We then have

$$|X| = |X_G| + \sum_{i=j}^{v}$$

for some j where $|Gx_i| > 1$ for all $i \geq j$.

Theorem: Let G be a group of order p^n for p a prime, then

$$|X| = |X_G| \mod p$$

Proof: We know that $|Gx_i| = [G : G_{x_i}]$ for $j \leq i \leq v$, and $|Gx_i| > 1$ implies that $Gx_i \neq G$ and thus $p \mid [G : Gx_i]$. The result follows.

Application: If $|G| = p^n$, then the center $Z(G)$ is nontrivial. Let $X = G$ act on itself by conjugaction, so $g \curvearrowright x = gxg^{-1}$. Then

$$X_G = \left\{x \in G \ni gxg^{-1} = x\right\} = \{x \in G \ni gx = xg\} = Z(G)$$

But then, by the previous theorem, hwe have $|Z(G)| \equiv |X| \equiv |G| \mod p$, but since $Z(G) \leq G$ we have $|Z(G)| \cong 0 \mod p$, and so in particular, $Z(G) \neq \{e\}$.

Definition: A group G is a p-group iff every element in G has order p^k for some k. A subgroup is a p-group exactly when it is a p-group in its own right.

5.2.2 Cauchy's Theorem

Theorem (Cauchy): Let G be a finite group, where $p \,\Big|\, |G|$ is a prime. Then G is an element (and thus a subgroup) of order p.

Proof: Consider $X = \{(g_1, g_2, \cdots, g_p) \in G^{\oplus p} \ni g_1 g_2 \cdots g_p = e\}$. Given any $p-1$ elements, say $g_1 \cdots g_{p-1}$, the remaining element is completely determined by $g_p = (g_1 \cdots g_{p-1})^{-1}$. So $|X| = |G|^{p-1}$.

Since $p \,\Big|\, |G|$, we have $p \,\Big|\, |X|$. Now let $\sigma \in S_p$ the symmetric group act on X by index permutation, i.e. $\sigma \curvearrowright (g_1, g_2 \cdots g_p) = (g_{\sigma(1)}, g_{\sigma(2)}, \cdots, g_{\sigma(p)})$.

Exercise: Check that this gives a well-defined group action.

Let $\sigma = (1\ 2\ \cdots\ p) \in S_p$, and note $\langle\sigma\rangle \leq S_p$ also acts on X where $|\langle\sigma\rangle| = p$. Therefore we have

$$|X| = \left|X_{\langle\sigma\rangle}\right| \mod p.$$

Since $p \,\Big|\, |X|$, it follows that $\left|X_{\langle\sigma\rangle}\right| = 0 \mod p$, and thus $p \,\Big|\, \left|X_{\langle\sigma\rangle}\right|$.

If $\langle\sigma\rangle$ fixes $(g_1, g_2, \cdots g_p)$, then $g_1 = g_2 = \cdots g_p$.

Note that $(e, e, \cdots) \in X_{\langle\sigma\rangle}$, as is $(a, a, \cdots a)$ since $p \,\Big|\, \left|X_{\langle\sigma\rangle}\right|$. So there is some $a \in G$ such that $a^p = 1$. Moreover, $\langle a\rangle \leq G$ is a subgroup of size p.

5.2.3 Normalizers

Let G be a group and $X = S$ be the set of subgroups of G. Let G act on X by $g \curvearrowright H = gHg^{-1}$. What is the stabilizer? $G_x = G_H = \left\{g \in G \ni gHg^{-1} = H\right\}$, making G_H the largest subgroup such that $H \trianglelefteq G_H$. So we define $N_G(H) = G_H$.

Lemma: Let H be a p-subgroup of G of order p^n. Then $[N_G(H) : H] = [G : H] \mod p$.

Proof: Thet $S = G/H$ be the set of left H-cosets in G. Now let H act on S by $H \curvearrowright x + H = (hx) + H$.

By a previous theorem, $|G/H| = |S| = |S_H| \mod p$, where $|G/H| = [G : H]$. What is S_H? Thus is given by $S_H = \left\{x + H \in S \ni xHx^{-1} \in H \forall h \in H\right\}$. Therefore $x \in N_G(H)$.

Corollary: Let $H \leq G$ be a subgroup of order p^n. If $p \,\Big|\, [G : H]$ then $N_G(H) \neq H$. Proof: Exercise.

Theorem: Let G be a finite group, then G is a p-group iff $|G| = p^n$.

Proof: Suppose $|G| = p^n$ and $a \in G$. Then $|\langle a \rangle| = p^\alpha$ for some α. Conversely, suppose G is a p-group. Factor $|G|$ into primes and suppose $\exists q$ such that $q \,\Big|\, |G|$ but $q \neq p$. By Cauchy, we can then get a subgroup $\langle c \rangle$ such that $|\langle c \rangle| \,\Big|\, q$, but then $|G| \neq p^n$.

6 Appendix

6.0.1 Big List of Notation

$$
\begin{aligned}
C(x) &= & \left\{g \in G : gxg^{-1} = x\right\} && \subseteq G && \text{Centralizer} \\
C_G(x) &= & \left\{gxg^{-1} : g \in G\right\} && \subseteq G && \text{Conjugacy Class} \\
G_x &= & \{g.x : x \in X\} && \subseteq X && \text{Orbit} \\
x_0 &= & \{g \in G : g.x = x\} && \subseteq G && \text{Stabilizer} \\
Z(G) &= & \left\{x \in G : \forall g \in G,\ gxg^{-1} = x\right\} && \subseteq G && \text{Center} \\
\mathrm{Inn}(G) &= & \left\{\phi_g(x) = gxg^{-1}\right\} && \subseteq \mathrm{Aut}(G) && \text{Inner Aut.} \\
\mathrm{Out}(G) &= & \mathrm{Aut}(G)/\mathrm{Inn}(G) && \hookrightarrow \mathrm{Aut}(G) && \text{Outer Aut.} \\
N(H) &= & \left\{g \in G : gHg^{-1} = H\right\} && \subseteq G && \text{Normalizer}
\end{aligned}
$$

7 Lecture 4: TODO

8 Lecture 5 (Tuesday 8/27)

Let G be a finite grou and p a prime. TFAE:

- $|H| = p^n$ for some n
- Every element of H has order p^α for some α.

If either of these are true, we say H is a *p-group*.

Let H be a p-group, last time we proved that if $p \bigm| [G : H]$ then $N_G(H) \neq H$.

8.1 Sylow Theorems

Let G be a finite group and suppose $|G| = p^n m$ where $(m, n) = 1$. Then

8.1.1 Sylow 1

Motto: take a prime factorization of $|G|$, then there are subgroups of order p^i for *every* prime power appearing, up to the maximal power.

1. G contains a subgroup of order p^i for every $1 \leq i \leq n$.
2. Every subgroup H of order p^i where $i < n$ is a normal subgroup in a subgroup of order p^{i+1}.

Proof: By induction on i. For $i = 1$, we know this by Cauchy's theorem. If we show (2), that shows (1) as a consequence. So suppose this holds for $i < n$. Let $H \leq G$ where $|H| = p^i$, we now want a subgroup of order p^{i+1}. Since $p \bigm| [G : H]$, by the previous theorem, $H < N_G(H)$ is a proper subgroup (?).

Now consider the canonical projection $N_G(H) \to N_G(H)/H$. Since $p \bigm| [N_G(H) : H] = |N_G(H)/H|$, by Cauchy there is a subgroup of order p in this quotient. Call it K. Then $\pi^{-1}(K) \leq N_G(H)$.

Exercise: $|\phi^{-1}(K)| = p^{i+1}$.

It now follows that $H \trianglelefteq \phi^{-1}(K)$. $\square$

Definition: For G a finite group and $|G| = p^n m$ where $p \not\bigm| m$. Then a subgroup of order p^n is called a Sylow p-subgroup. (By Sylow 1, these exist.)

8.2 Sylow 2

If P_1, P_2 are Sylow p-subgroups of G, then P_1 and P_2 are conjugate.

Proof: Let $\mathcal{L}$ be the left cosets of P_1, i.e. $\mathcal{L} = G/P_1$. Then let P_2 act on $\mathcal{L}$ by $p_2 \curvearrowright (g + P_1) := (p_2 g) + P_1$.

By a previous theorem about orbits and fixed points, we have

$$|\mathcal{L}_{P_2}| = |\mathcal{L}| \mod p.$$

Since $p \not\bigm| |\mathcal{L}|$, we have $p \not\bigm| |\mathcal{L}_{P_2}|$. So $\mathcal{L}_{P_2}$ is nonempty.

So there exists a coset xP_1 such that $xP_1 \in \mathcal{L}_{P_2}$, and so $yxP_1 = xP_1$ for all $y \in P_2$.

Then $x^{-1}yxP_1 = P_1$ for all $y \in P_2$, and so $x^{-1}P_2 x = P_1$. But then P_1 and P_2 are conjugate. $\square$

8.3 Sylow 3

Let G be a finite group, and $p \bigm| |G|$. Let r_p be the number of Sylow p-subgroups of G. Then

- $r_p \cong 1 \mod p$.
- $r_p \mid |G|$.
- $r_p = [G : N_G(P)]$

Let $X = \mathcal{S}$ be the set of Sylow p-subgroups, and let $P \in X$ be a fixed Sylow p-subgroup. Let $P \curvearrowright \mathcal{S}$ by conjugation, so for $\overline{P} \in \mathcal{S}$ let $x \curvearrowright \overline{P} = x\overline{P}x^{-1}$.

By the same old theorem, we have

$$|\mathcal{S}| = \mathcal{S}_P \mod p$$

What are the fixed points $\mathcal{S}_P$?

$$\mathcal{S}_P = \left\{ T \in \mathcal{S} \ni xTx^{-1} = T \quad \forall x \in P \right\}.$$

Let $\mathcal{T} \in \mathcal{S}_P$, so $xTx^{-1} = T$ for all $x \in P$. Then $P \leq N_G(T)$, so both P and T are Sylow p-subgroups in $N_G(H)$ as well as G.

Then there exists a $f \in N_G(T)$ such that $T = gPg^{-1}$. But the point is that in the normalizer, there is only **one** Sylow p- subgroup. But then T is the unique largest normal subgroup of $N_G(T)$, which forces $T = P$.

But then $\mathcal{S}_P = \{P\}$, and using the formula, we have $r_p \cong 1 \mod p$.

Now modify this slightly by letting G act on $\mathcal{S}$ (instead of just P) by conjugation. Since all Sylows are conjugate, by Sylow (1) there is only one orbit, so $\mathcal{S} = GP$ for $P \in \mathcal{S}$. But then

$$r_p = |\mathcal{S}| = |GP| = [G : G_p] \mid |G|.$$

Note that this gives a precise formula for r_p, although the theorem is just an upper bound of sorts, and $G_p = N_G(P)$.

8.4 Applications

Of interest historically: classifying finite *simple* groups, where a group G is *simple* If $N \trianglelefteq G$ and $N \neq \{e\}$, then $N = G$.

Example: Let $G = \mathbb{Z}_p$, any subgroup would need to have order dividing p, so G must be simple.

Example: $G = A_n$ for $n \geq 5$ (see Galois theory)

One major application is proving that groups of a certain order are *not* simple.

Applications:

1. Let $|G| = p^n q$ with $p > q$. Then G is not simple.

> Strategy: Find a proper normal nontrivial subgroup using Sylow theory.

Consider r_p, then $r_p = p^\alpha q^\beta$ for some α, β. But since $r_p \cong 1 \mod p$, $p \not\mid r_p$, we must have $r_p = 1, q$. But since $q < p$ and $q \neq 1 \mod p$, this forces $r_p = 1$.

So let P be a sylow p-subgroup, then $P < G$. Then gPg^{-1} is also a sylow, but there's only 1 of them, so P is normal.

2. Let $|G| = 45$, then G is not simple. (Exercise)

3. Let $|G| = p^n$, then G is not simple if $n > 1$.

By Sylow (1), there is a normal subgroup of order p^{n-1} in G.

4. Let $|G| = 48$, then G is not simple.

Note $48 = 2^4 3$, so consider r_2, the number of Sylow 2-subgroups. Then $r_2 \cong 1 \mod 2$ and $r_2 \Bigm| 48$. So $r_2 = 1, 3$. If $r_2 = 1$, we're done, otherwise suppose $r_2 = 3$.

Let $H \neq K$ be Sylow 2-subgroups, so $|H| = |K| = 2^4 = 16$. Now consider $H \bigcap K$, which is a subgroup of G. How big is it?

Since $H \neq K, |H \bigcap K| < 16$. The order has to divides 16, so we in fact have $|H \bigcap K| \leq 8$. Suppose it is less than 4, towards a contradiction. Then

$$|HK| = \frac{|H||K|}{|H \bigcap K|} \geq \frac{(16)(16)}{4} = 64 > |G| = 48.$$

So we can only have $|H \bigcap K| = 8$.