

# Title

D. Zack Garza

Sunday 26<sup>th</sup> July, 2020

## Contents

0.1	Sylow Theorems . . . . .	1
0.1.1	Sylow 1 (Cauchy for Prime Powers) . . . . .	1
0.1.2	Sylow 2 (Sylows are Conjugate) . . . . .	2
0.1.3	Sylow 3 (Numerical Constraints) . . . . .	2
0.2	Products . . . . .	2
0.3	Isomorphism Theorems . . . . .	3
0.4	Special Classes of Groups . . . . .	5
0.5	Classification of Groups . . . . .	5
0.6	Finitely Generated Abelian Groups . . . . .	6

## 0.1 Sylow Theorems

### Definition 0.0.1.

A  $p$ -group is a group  $G$  such that every element is order  $p^k$  for some  $k$ . If  $G$  is a finite  $p$ -group, then  $|G| = p^j$  for some  $j$ .

Write

- $|G| = p^k m$  where  $(p, m) = 1$ ,
- $S_p$  a Sylow- $p$  subgroup, and
- $n_p$  the number of Sylow- $p$  subgroups.

Some useful facts:

- Coprime order subgroups are disjoint, or more generally  $\mathbb{Z}_p, \mathbb{Z}_q \subset G \implies \mathbb{Z}_p \cap \mathbb{Z}_q = \mathbb{Z}_{(p,q)}$ .
- The Chinese Remainder theorem:  $(p, q) = 1 \implies \mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}$

### 0.1.1 Sylow 1 (Cauchy for Prime Powers)

$\forall p^n$  dividing  $|G|$  there exists a subgroup of size  $p^n$

Idea: Sylow  $p$ -subgroups exist for any  $p$  dividing  $|G|$ , and are maximal in the sense that every  $p$ -subgroup of  $G$  is contained in a Sylow  $p$ -subgroup.

If  $|G| = \prod p_i^{\alpha_i}$ , then there exist subgroups of order  $p_i^{\beta_i}$  for every  $i$  and every  $0 \leq \beta_i \leq \alpha_i$ . In particular, Sylow  $p$ -subgroups always exist.

### 0.1.2 Sylow 2 (Sylows are Conjugate)

All sylow- $p$  subgroups  $S_p$  are conjugate, i.e.

$$S_p^i, S_p^j \in \text{Syl}_p(G) \implies \exists g \text{ such that } gS_p^i g^{-1} = S_p^j$$

#### Corollary 0.1.

$$n_p = 1 \iff S_p \trianglelefteq G$$

### 0.1.3 Sylow 3 (Numerical Constraints)

1.  $n_p \mid m$  (in particular,  $n_p \leq m$ ),
2.  $n_p \equiv 1 \pmod{p}$ ,
3.  $n_p = [G : N_G(S_p)]$  where  $N_G$  is the normalizer.

#### Corollary 0.2.

$p$  does not divide  $n_p$ .

#### Proposition 0.3.

Every  $p$ -subgroup of  $G$  is contained in a Sylow  $p$ -subgroup.

Something proof title="Something"

*Proof .*

Let  $H \leq G$  be a  $p$ -subgroup. If  $H$  is not *properly* contained in any other  $p$ -subgroup, it is a Sylow  $p$ -subgroup by definition.

Otherwise, it is contained in some  $p$ -subgroup  $H^1$ . Inductively this yields a chain  $H \subsetneq H^1 \subsetneq \dots$ , and by Zorn's lemma  $H := \bigcup_i H^i$  is maximal and thus a Sylow  $p$ -subgroup. ■

#### Theorem 0.4(Fratini's Argument).

If  $H \trianglelefteq G$  and  $P \in \text{Syl}_p(G)$ , then  $HN_G(P) = G$  and  $[G : H]$  divides  $|N_G(P)|$ .

## 0.2 Products

#### Theorem 0.5(Recognizing Direct Products).

We have  $G \cong H \times K$  when

- $H, K \trianglelefteq G$
- $G = HK$ .
- $H \cap K = \{e\} \subset G$

Note: can relax to  $[h, k] = 1$  for all  $h, k$ .

**Theorem 0.6 (Recognizing Generalized Direct Products).**

We have  $G = \prod_{i=1}^n H_i$  when

- $H_i \trianglelefteq G$  for all  $i$ .
- $G = H_1 \cdots H_n$
- $H_k \cap H_1 \cdots \widehat{H_k} \cdots H_n = \{1\}$

Note on notation: intersect  $H_k$  with the amalgam *leaving out*  $H_k$ .

**Theorem 0.7 (Recognizing Semidirect Products).**

We have  $G = N \rtimes_{\psi} H$  when

- $G = NH$
- $N \trianglelefteq G$
- $H \curvearrowright N$  by conjugation via a map

$$\begin{aligned} \psi : H &\longrightarrow \text{Aut}(N) \\ h &\mapsto h(\cdot)h^{-1}. \end{aligned}$$

Note relaxed conditions compared to direct product:  $H \trianglelefteq G$  and  $K \leq G$  to get a semidirect product instead

**Useful Facts**

- If  $\sigma \in \text{Aut}(H)$ , then  $N \rtimes_{\psi} H \cong N \rtimes_{\psi \circ \sigma} H$ .
- $\text{Aut}(\mathbb{Z}/(p)^n) \cong \text{GL}(n, \mathbb{F}_p)$ , which has size

$$|\text{Aut}(\mathbb{Z}/(p)^n)| = (p^n - 1)(p^n - p) \cdots (p^n - p^{n-1}).$$

- If this occurs in a semidirect product, it suffices to consider similarity classes of matrices (i.e. just use canonical forms)

$$\text{Aut}(\mathbb{Z}/(n)) \cong \mathbb{Z}/(n)^{\times} \cong \mathbb{Z}/(\varphi(n))$$

where  $\varphi$  is the totient function.

- $\varphi(p^k) = p^{k-1}(p-1)$
- If  $G, H$  have coprime order then  $\text{Aut}(G \oplus H) \cong \text{Aut}(G) \oplus \text{Aut}(H)$ .

**0.3 Isomorphism Theorems**

**Theorem 0.8 (1st Isomorphism Theorem).**

If  $\varphi : G \longrightarrow H$  is a group morphism then

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

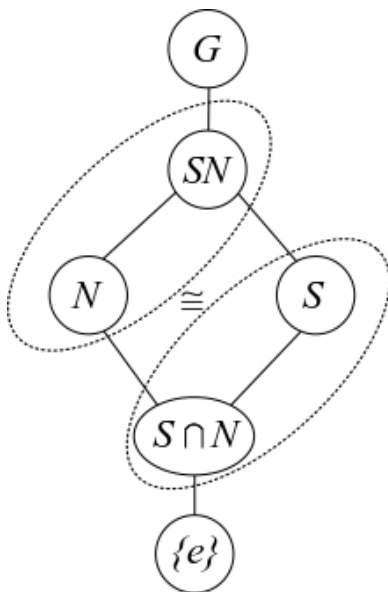


Figure 1: The 2nd “Diamond” Isomorphism Theorem

Note: for this to make sense, we also have

- $\ker \varphi \trianglelefteq G$
- $\text{im } \varphi \leq G$

**Corollary 0.9.**

If  $\varphi : G \rightarrow H$  is surjective then  $H \cong G / \ker \varphi$ .

**Proposition 0.10.**

If  $H, K \leq G$  and  $H \leq N_G(K)$  (or  $K \trianglelefteq G$ ) then  $HK \leq G$  is a subgroup.

**Theorem 0.11 (Diamond Theorem / 2nd Isomorphism Theorem).**

If  $S \leq G$  and  $N \trianglelefteq G$ , then

$$\frac{SN}{N} \cong \frac{S}{S \cap N} \quad \text{and} \quad |SN| = \frac{|S||N|}{|S \cap N|}.$$

Note: for this to make sense, we also have

- $SN \leq G$ ,
- $S \cap N \trianglelefteq S$ ,

**Corollary 0.12.**

If we relax the conditions to  $S, N \leq G$  with  $S \in N_G(N)$ , then  $S \cap N \trianglelefteq S$  (but is not normal in  $G$ ) and the theorem still applies.

**Theorem 0.13 (Cancellation / 3rd Isomorphism Theorem).**

Suppose  $N, K \leq G$  with  $N \trianglelefteq G$  and  $N \subseteq K \subseteq G$ .

1. If  $K \leq G$  then  $K/N \leq G/N$  is a subgroup
2. If  $K \trianglelefteq G$  then  $K/N \trianglelefteq G/N$ .
3. Every subgroup of  $G/N$  is of the form  $K/N$  for some such  $K \leq G$ .
4. Every *normal* subgroup of  $G/N$  is of the form  $K/N$  for some such  $K \trianglelefteq G$ .
5. If  $K \trianglelefteq G$ , then we can cancel normal subgroups:

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

**Theorem 0.14** (*The Correspondence Theorem / 4th Isomorphism Theorem*).

Suppose  $N \trianglelefteq G$ , then there exists a correspondence:

$$\begin{aligned} \left\{ H < G \mid N \subseteq H \right\} &\iff \left\{ H \mid H < \frac{G}{N} \right\} \\ \left\{ \begin{array}{c} \text{Subgroups of } G \\ \text{containing } N \end{array} \right\} &\iff \left\{ \begin{array}{c} \text{Subgroups of the} \\ \text{quotient } G/N \end{array} \right\}. \end{aligned}$$

In words, subgroups of  $G$  containing  $N$  correspond to subgroups of the quotient group  $G/N$ . This is given by the map  $H \mapsto H/N$ .

Note:  $N \trianglelefteq G$  and  $N \subseteq H < G \implies N \trianglelefteq H$ .

## 0.4 Special Classes of Groups

**Definition 0.14.1** (2 out of 3 Property).

The “**2 out of 3 property**” is satisfied by a class of groups  $\mathcal{C}$  iff whenever  $G \in \mathcal{C}$ , then  $N, G/N \in \mathcal{C}$  for any  $N \trianglelefteq G$ .

**Definition 0.14.2** (p-groups).

If  $|G| = p^k$ , then  $G$  is a **p-group**.

**Definition 0.14.3** (Normalizers Grow).

If for every proper  $H < G$ ,  $H \trianglelefteq N_G(H)$  is again proper, then “normalizers grow” in  $G$ .

## 0.5 Classification of Groups

General strategy: find a normal subgroup (usually a Sylow) and use recognition of semidirect products.

- Keith Conrad: Classifying Groups of Order 12
- Order  $p$ : cyclic.
- Order  $p^2q$ : ?

**0.6 Finitely Generated Abelian Groups****Definition 0.14.4** (Invariant Factor Decomposition).

$$G \cong \mathbb{Z}^r \times \prod_{j=1}^m \mathbb{Z}/n_j\mathbb{Z} \quad \text{where } n_1 \mid \cdots \mid n_m.$$

**Invariant factors  $\longrightarrow$  Elementary Divisors:**

- Take prime factorization of each factor
- Split into coprime pieces

**Example 0.1.**

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{2^3 \cdot 5^2 \cdot 7} \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{2^3} \times \mathbb{Z}_{5^2} \times \mathbb{Z}_7$$

**Going from elementary divisors to invariant factors:**

- Bin up by primes occurring (keeping exponents)
- Take highest power from each prime as *last* invariant factor
- Take highest power from all remaining primes as next, etc

**Example 0.2.**

Given the invariant factor decomposition

$$G = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{5^2}$$

$p = 2$	$p = 3$	$p = 5$
$2, 2, 2$	$3, 3$	$5^2$

$$\implies n_m = 5^2 \cdot 3 \cdot 2$$

$p = 2$	$p = 3$	$p = 5$
$2, 2$	$3$	$\emptyset$

$$\implies n_{m-1} = 3 \cdot 2$$

$p = 2$	$p = 3$	$p = 5$
$2$	$\emptyset$	$\emptyset$

$$\implies n_{m-2} = 2$$

and thus

$$G \cong \mathbb{Z}_2 \times \mathbb{Z}_{3 \cdot 2} \times \mathbb{Z}_{5^2 \cdot 3 \cdot 2}$$

**Classifying Abelian Groups of a Given Order:**

Let  $p(x)$  be the integer partition function.

Example:  $p(6) = 11$ , given by  $6, 5 + 1, 4 + 2, \dots$ .

Write  $G = p_1^{k_1} p_2^{k_2} \dots$ ; then there are  $p(k_1)p(k_2)\dots$  choices, each yielding a distinct group.