Group Theory Notes:
Sylow Theorems, Small Groups, and Presentations

Ryan Hausner

October 21st, 2026

Contents

1 Normalizers **2**
- 1.1 The Conjugation Action on Subgroups . . . 2
- 1.2 Definition and the Counting Formula . . . 2
- 1.3 Basic Properties . . . 2
- 1.4 Example: A Normalizer in S_5 . . . 2

2 The Sylow Theorems **2**
- 2.1 Sylow p-Subgroups . . . 2
- 2.2 First Sylow Theorem (Existence) . . . 3
- 2.3 Second Sylow Theorem (Conjugacy) . . . 3
- 2.4 Third Sylow Theorem (Counting) . . . 4

3 Classifying Groups of Small Order **4**
- 3.1 Groups of Order 15 . . . 5
- 3.2 Groups of Order 6 . . . 5
- 3.3 Groups of Order 21 . . . 6
- 3.4 Groups of Order 12 . . . 6

4 Free Groups **8**
- 4.1 Words and Cancellation . . . 8
- 4.2 Reduced Words . . . 8
- 4.3 Equivalence of Words . . . 8
- 4.4 The Free Group on a Set . . . 8
- 4.5 Mapping Property of the Free Group . . . 9

5 Generators and Relations **9**
- 5.1 Relations and Defining Relations . . . 9
- 5.2 The Normal Subgroup Generated by a Set . . . 9
- 5.3 Presentations . . . 9
- 5.4 Mapping Property of Quotient Groups . . . 10
- 5.5 The Canonical Homomorphism from a Presentation . . . 10

1 Normalizers

1.1 The Conjugation Action on Subgroups

Let G act on the set $\{\text{subgroups of } G\}$ by conjugation. The orbit of a subgroup H is

$$O_H = \{g \cdot H \mid g \in G\} = \{gHg^{-1} \mid g \in G\},$$

the set of all subgroups conjugate to H. The stabilizer of H is

$$\text{Stab}(H) = \{g \in G \mid g \cdot H = H\} = \{g \in G \mid gHg^{-1} = H\}.$$

1.2 Definition and the Counting Formula

Definition 1.1 (Normalizer)**.** Given $H \leq G$, the *normalizer* of H is

$$N(H) := \{g \in G \mid gHg^{-1} = H\}.$$

Note that $N(H) = \text{Stab}(H)$ for the conjugation action. The counting formula says

$$|G| = |O_H|\,|N(H)|,$$

so the number of subgroups conjugate to H is $|G|/|N(H)| = [G : N(H)]$.

1.3 Basic Properties

Proposition 1.2 (Properties of the Normalizer)**.** *Let $H \leq G$.*

1. *$H \trianglelefteq N(H)$.*
2. *$H \trianglelefteq G \iff N(H) = G$.*
3. *$|H| \mid |N(H)|$ and $|N(H)| \mid |G|$.*

Proof left as an exercise.

1.4 Example: A Normalizer in S_5

Example 1.3. In S_5, let $H = \langle (12)(34) \rangle$. Then

$$O_H = \{\langle (ab)(cd) \rangle \mid a, b, c, d \text{ are all distinct}\},$$

so $|O_H| = 15$. Then $|S_5| = 15 \cdot |N(H)|$, so $|N(H)| = 120/15 = 8$.

2 The Sylow Theorems

2.1 Sylow p-Subgroups

For a group G, the Sylow subgroups are the subgroups of G of maximal prime power order.

Definition 2.1 (Sylow p-Subgroup)**.** Let G be a group, and let p be a prime that divides $|G|$. Write $|G| = p^l m$, where $\gcd(p, m) = 1$ and $l \geq 1$. Subgroups of G that have order p^l are called *Sylow p-subgroups*.

2.2 First Sylow Theorem (Existence)

Theorem 2.2 (First Sylow Theorem)**.** *Let $|G| = p^l m$, with $\gcd(p, m) = 1$ and $l \geq 1$. Then G has a subgroup of order p^j for all $1 \leq j \leq l$. In particular, G has a Sylow p-subgroup.*

Proof. By induction on j.

Base case ($j = 1$): since $p \mid |G|$, by Cauchy's Theorem there exists an element $g \in G$ of order p, and so $\langle g \rangle$ has order p.

Inductive step: suppose there exists $H \leq G$ such that $|H| = p^j$ for some $1 \leq j < l$. Consider the action of H on G/H by left multiplication. By the Fixed Point Theorem,

$$|G/H| \equiv |\{\text{fixed points}\}| \pmod{p}.$$

The fixed points are

$$\{xH \mid gxH = xH,\ \forall g \in H\} = \{xH \mid x^{-1}gxH = H,\ \forall g \in H\}.$$

Note that

$$x^{-1}gxH = H\ \forall g \in H \iff x^{-1}gx \in H\ \forall g \in H \iff x^{-1}Hx \subseteq H \iff x^{-1}Hx = H \iff x \in N(H).$$

Hence $\{\text{fixed points}\} = \{xH \mid x \in N(H)\} = N(H)/H$, so $[G : H] \equiv [N(H) : H] \pmod{p}$. Since $|H| = p^j$ with $j < l$, we have $p \mid [G : H]$.

Hence $0 \equiv [N(H) : H] \pmod{p}$; in other words, $p \mid [N(H) : H]$. Then, by Cauchy's Theorem, there exists a subgroup $K/H \leq N(H)/H$ of order p, for some $K \leq N(H)$. Hence $|K| = |H|\,[K : H] = p^j \cdot p = p^{j+1}$, and $K \leq N(H) \leq G$. □

2.3 Second Sylow Theorem (Conjugacy)

Theorem 2.3 (Second Sylow Theorem)**.** *1. The Sylow p-subgroups of G are conjugate. That is, given two Sylow p-subgroups P and Q, there exists $x \in G$ such that $xPx^{-1} = Q$.*

2. Every subgroup of G that is a p-group is contained in a Sylow p-subgroup.

Proof. Let $|G| = p^l m$ with $\gcd(p, m) = 1$, and let P be a Sylow p-subgroup of G, so $|P| = p^l$.

Proof of (2). Let $H \leq G$ be a p-group. Consider the action of H on G/P by left multiplication. Since $|G/P| = [G : P] = m$ and H is a p-group, the Fixed Point Theorem gives

$$m = |G/P| \equiv |\{\text{fixed points}\}| \pmod{p}.$$

Since $\gcd(p, m) = 1$, we have $p \nmid m$, so $|\{\text{fixed points}\}| \not\equiv 0 \pmod{p}$. In particular, there is at least one fixed point $xP \in G/P$.

Since xP is fixed, $hxP = xP$ for all $h \in H$. Then

$$hxP = xP\ \ \forall h \in H \iff x^{-1}hx \in P\ \ \forall h \in H \iff x^{-1}Hx \subseteq P \iff H \subseteq xPx^{-1}.$$

Now xPx^{-1} is a subgroup of G with $|xPx^{-1}| = |P| = p^l$, so it is a Sylow p-subgroup. Hence H is contained in a Sylow p-subgroup.

Proof of (1). Let P and Q be Sylow p-subgroups. Since Q is a p-group, the argument above (with $H = Q$) gives $x \in G$ with $Q \subseteq xPx^{-1}$. But $|Q| = p^l = |xPx^{-1}|$, so $Q = xPx^{-1}$. □

Remark 2.4. A conjugate of a Sylow p-subgroup is also a Sylow p-subgroup.

Corollary 2.5 (Unique Sylow Subgroups Are Normal)**.** *A group has just one Sylow p-subgroup $\iff$ that subgroup is normal.*

2.4 Third Sylow Theorem (Counting)

Theorem 2.6 (Third Sylow Theorem)**.** *Let $|G| = p^l m$ with $\gcd(p, m) = 1$ and $l \geq 1$, and let n_p be the number of Sylow p-subgroups of G. Then*

1. *$n_p = [G : N(P)]$ for any Sylow p-subgroup P,*
2. *$n_p \mid m$ (in particular $n_p \mid |G|$),*
3. *$n_p \equiv 1 \pmod{p}$.*

Proof. Let $\mathrm{Syl}_p(G)$ denote the set of Sylow p-subgroups of G, so $n_p = |\mathrm{Syl}_p(G)|$.

Proof of (1) and (2). Let G act on $\mathrm{Syl}_p(G)$ by conjugation. (This is well defined, since a conjugate of a Sylow p-subgroup is a Sylow p-subgroup.) By the Second Sylow Theorem, any two Sylow p-subgroups are conjugate, so the action is transitive: for any Sylow p-subgroup P, the orbit O_P is all of $\mathrm{Syl}_p(G)$. The stabilizer of P is $N(P)$, so by the counting formula

$$n_p = |O_P| = \frac{|G|}{|N(P)|} = [G : N(P)].$$

Since $P \leq N(P) \leq G$, we have

$$[G : P] = [G : N(P)]\,[N(P) : P],$$

so $n_p = [G : N(P)]$ divides $[G : P] = m$.

Proof of (3). Fix a Sylow p-subgroup P, and let P act on $\mathrm{Syl}_p(G)$ by conjugation. Since P is a p-group, the Fixed Point Theorem gives

$$n_p \equiv |\{\text{fixed points}\}| \pmod{p}.$$

The fixed points are

$$\{Q \in \mathrm{Syl}_p(G) \mid xQx^{-1} = Q,\ \forall x \in P\} = \{Q \in \mathrm{Syl}_p(G) \mid P \leq N(Q)\}.$$

We claim the only fixed point is P itself.

First, P is a fixed point, since $P \leq N(P)$.

Now suppose Q is a fixed point, so $P \leq N(Q)$. Also $Q \leq N(Q)$ and $Q \trianglelefteq N(Q)$. Since $|P| = |Q| = p^l$ is the largest power of p dividing $|G|$, and $|N(Q)|$ divides $|G|$, both P and Q are Sylow p-subgroups of the group $N(Q)$. Since Q is normal in $N(Q)$, by the Second Sylow Theorem applied to $N(Q)$, every Sylow p-subgroup of $N(Q)$ is conjugate to Q in $N(Q)$, hence equal to Q. Therefore $P = Q$.

So there is exactly one fixed point, and

$$n_p \equiv 1 \pmod{p}.$$ □

3 Classifying Groups of Small Order

Throughout this section, "the product proposition" refers to the proposition on product groups from Artin §2.11: if $H, K \trianglelefteq G$, $H \cap K = \{e\}$, and $HK = G$, then $G \cong H \times K$.

3.1 Groups of Order 15

Proposition 3.1 (Groups of Order 15)**.** *Every group of order* 15 *is isomorphic to* C_{15}*.*

Proof. Let $|G| = 15 = 3 \cdot 5$.

By the Third Sylow Theorem, $n_3 \mid 5$ and $n_3 \equiv 1 \pmod 3$. The divisors of 5 are 1 and 5, and $5 \equiv 2 \pmod 3$, so $n_3 = 1$.

Similarly, $n_5 \mid 3$ and $n_5 \equiv 1 \pmod 5$. The divisors of 3 are 1 and 3, and $3 \not\equiv 1 \pmod 5$, so $n_5 = 1$.

Since G has a unique Sylow 3-subgroup P and a unique Sylow 5-subgroup Q, both are normal, with $|P| = 3$ and $|Q| = 5$.

Now $P \cap Q$ is a subgroup of both P and Q, so $|P \cap Q|$ divides $\gcd(3, 5) = 1$, and hence $P \cap Q = \{e\}$.

Since $P, Q \trianglelefteq G$ and $P \cap Q = \{e\}$, we have $PQ \cong P \times Q$. Moreover, $|PQ| = |P|\,|Q| = 15 = |G|$, so $G = PQ$. Therefore

$$G \cong P \times Q \cong C_3 \times C_5.$$

Since $\gcd(3, 5) = 1$, the Chinese Remainder Theorem gives $C_3 \times C_5 \cong C_{15}$. Hence $G \cong C_{15}$. □

Remark 3.2 (The Cyclic Group C_{15})*.* C_{15} denotes the cyclic group of order 15. It is generated by a single element g with $g^{15} = e$, so

$$C_{15} = \langle g \rangle = \{e, g, g^2, \ldots, g^{14}\} \cong \mathbb{Z}/15\mathbb{Z}.$$

So the proposition says that every group with 15 elements is just the integers mod 15 under addition, up to isomorphism. In particular, every group of order 15 is abelian.

Remark 3.3 (Groups of Order pq)*.* More generally, if $|G| = pq$ with $p < q$ primes and $p \nmid q - 1$, then $G \cong C_{pq}$. If $p \mid q - 1$, there is also a nonabelian group of order pq (for example, S_3 for $p = 2$, $q = 3$). The next two subsections work out the cases $pq = 6$ and $pq = 21$.

3.2 Groups of Order 6

Proposition 3.4 (Groups of Order 6)**.** *Let* $|G| = 6$*. Then* $G \cong C_6$ *or* $G \cong S_3$*.*

Proof. $|G| = 6 = 2 \cdot 3$. By the Third Sylow Theorem, $n_2 \mid 3$ and $n_2 \equiv 1 \pmod 2$, while $n_3 \mid 2$ and $n_3 \equiv 1 \pmod 3$. Hence $n_2 = 1$ or 3, and $n_3 = 1$.

Let P_3 be the unique Sylow 3-subgroup and P_2 a Sylow 2-subgroup. Then $|P_3| = 3$, so $P_3 \cong C_3$ and $P_3 \trianglelefteq G$. Also $|P_2| = 2$, so $P_2 \cong C_2$.

Case 1: $n_2 = 1$**.** Then P_2 is the unique Sylow 2-subgroup, so $P_2 \trianglelefteq G$. Moreover, $P_2 \cap P_3 = \{e\}$ and $|P_2 \times P_3| = 6$. Hence by the product proposition,

$$G \cong P_2 \times P_3 \cong C_2 \times C_3 \cong C_6.$$

Case 2: $n_2 = 3$**.** Let P_2^1, P_2^2, P_2^3 be the three Sylow 2-subgroups of G. Then G acts by conjugation on $\{P_2^1, P_2^2, P_2^3\}$ (Second Sylow Theorem), which gives a group homomorphism $\phi : G \to S_3$.

By the Second Sylow Theorem, the action has only one orbit. Hence $|G| = |O_{P_2^i}|\,|N(P_2^i)|$, i.e. $6 = 3\,|N(P_2^i)|$, so $|N(P_2^i)| = 2$ for all $i = 1, 2, 3$. Since $P_2^i \leq N(P_2^i)$, it follows that $P_2^i = N(P_2^i)$.

Since $P_2^i \cap P_2^j = \{e\}$ for $i \neq j$, the only element that fixes all three Sylow 2-subgroups is e. Hence $\phi : G \to S_3$ is injective, and $|G| = 6 = |S_3|$, so ϕ is also surjective. Hence ϕ gives $G \cong S_3$. □

3.3 Groups of Order 21

Proposition 3.5 (Groups of Order 21)**.** *Let $|G| = 21$. Then $G \cong C_{21}$ or*

$$G \cong \langle x, y \mid x^7 = 1,\ y^3 = 1,\ yx = x^2 y \rangle,$$

the group generated by x and y subject to the relations $x^7 = 1$, $y^3 = 1$, $yx = x^2 y$.

Proof. $|G| = 21 = 3 \cdot 7$. By the Third Sylow Theorem, $n_3 \mid 7$ and $n_3 \equiv 1 \pmod 3$, while $n_7 \mid 3$ and $n_7 \equiv 1 \pmod 7$. Hence $n_3 = 1$ or 7, and $n_7 = 1$.

Let P_7 be the unique Sylow 7-subgroup. Then $P_7 \trianglelefteq G$ and $|P_7| = 7$, so $P_7 \cong C_7$. Let P_3 be one of the Sylow 3-subgroups; then $|P_3| = 3$, so $P_3 \cong C_3$. Let x be a generator of P_7 and y a generator of P_3. Then $x^7 = 1$ and $y^3 = 1$.

Every element is $x^i y^j$. Since $P_3 \cap P_7 = \{e\}$, the map

$$P_7 \times P_3 \to G, \qquad (x^i, y^j) \mapsto x^i y^j$$

is injective. Since $|P_7 \times P_3| = 21 = |G|$, it is also surjective, hence bijective. So every element of G can be written as $x^i y^j$ for $0 \le i < 7$, $0 \le j < 3$.

The conjugation relation. Since $P_7 \trianglelefteq G$, we have $yxy^{-1} \in P_7$, so $yxy^{-1} = x^i$ for some $1 \le i < 7$. Moreover,

$$x = y^3 x y^{-3} = y^2 x^i y^{-2} = y x^{i^2} y^{-1} = x^{i^3}.$$

Hence $i^3 \equiv 1 \pmod 7$, that is, $i = 1, 2$, or 4. So x and y satisfy the relations

1. $x^7 = 1$,
2. $y^3 = 1$,
3. $yxy^{-1} = x^i$, where $i \in \{1, 2, 4\}$.

These relations are enough to determine the whole multiplication table of G.

Case 1: $i = 1$. Then $yxy^{-1} = x$, so $yx = xy$ and x and y commute. Hence P_3 is also normal, and $P_3 \cap P_7 = \{e\}$. Since $|P_3 \times P_7| = 21$, the product proposition gives

$$G \cong P_3 \times P_7 \cong C_3 \times C_7 \cong C_{21}.$$

Case 2: $i = 2$. Then $yxy^{-1} = x^2$. We show that a group with this multiplication table exists. Take the matrices

$$x = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \qquad y = \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}$$

with entries in $\mathbb{F}_7$. Then $x^7 = 1$, $y^3 = 1$, and $yxy^{-1} = x^2$. Hence $H = \langle x, y \mid x^7 = 1,\ y^3 = 1,\ yxy^{-1} = x^2 \rangle$ is a group, and one can check that it has 21 elements.

Case 3: $i = 4$. This gives the same group as Case 2: y^2 is also a generator of P_3, and if $yxy^{-1} = x^4$ then $y^2 x y^{-2} = x^{16} = x^2$. So replacing y by y^2 reduces to Case 2. □

3.4 Groups of Order 12

Theorem 3.6 (Groups of Order 12)**.** *Let $|G| = 12$. Then G is isomorphic to exactly one of:*

1. $C_4 \times C_3$,
2. $C_2 \times C_2 \times C_3$,
3. A_4,

4. D_{12},

5. $\langle x, y \mid x^4 = 1,\ y^3 = 1,\ xy = y^2x \rangle$.

Here, D_{12} is the group of symmetries of the regular hexagon.

Proof. $|G| = 12 = 2^2 \cdot 3$. By the Third Sylow Theorem, $n_2 \mid 3$ and $n_2 \equiv 1 \pmod 2$, while $n_3 \mid 4$ and $n_3 \equiv 1 \pmod 3$. Hence $n_2 = 1$ or 3, and $n_3 = 1$ or 4.

Let P_3 be a Sylow 3-subgroup and P_2 a Sylow 2-subgroup. Then $|P_3| = 3$, so $P_3 \cong C_3$, and $|P_2| = 4$, so $P_2 \cong C_4$ or $P_2 \cong C_2 \times C_2$. Also $P_2 \cap P_3 = \{e\}$, so the product map $P_2 \times P_3 \to G$ is injective. Since $|P_2 \times P_3| = 12$, it is bijective (as a map of sets). Hence every element of G has the form $x \cdot y$ for $x \in P_2$, $y \in P_3$.

Case 1: $P_2 \trianglelefteq G$ and $P_3 \trianglelefteq G$. By the product proposition,

$$G \cong P_2 \times P_3 \cong \begin{cases} C_2 \times C_2 \times C_3, \\ C_4 \times C_3. \end{cases}$$

Case 2: P_3 is not normal. Then $n_3 = 4$. Let $P_3^1, P_3^2, P_3^3, P_3^4$ be the Sylow 3-subgroups. Then G acts on $\{P_3^i \mid 1 \le i \le 4\}$ by conjugation (well defined by the Second Sylow Theorem), which determines a group homomorphism $\phi : G \to S_4$.

The action has a unique orbit by the Second Sylow Theorem. Hence $|G| = |O(P_3^i)| \cdot |N(P_3^i)|$ for all $1 \le i \le 4$, i.e. $12 = 4 \cdot |N(P_3^i)|$, so $|N(P_3^i)| = 3$. Since $P_3^i \le N(P_3^i)$, we get $P_3^i = N(P_3^i)$.

Since $N(P_3^i) = P_3^i$ and $P_3^i \cap P_3^j = \{e\}$ for $i \ne j$, only the identity stabilizes all of these subgroups. Hence ϕ is injective and $G \cong \operatorname{Im}(\phi)$.

We show that $\operatorname{Im}(\phi) = A_4$. Since G has 4 Sylow 3-subgroups, it contains 8 elements of order 3. So there are 8 elements of order 3, i.e. 8 3-cycles, in the image of ϕ. Then every 3-cycle in S_4 is in $\operatorname{Im}(\phi)$, so $A_4 \subseteq \operatorname{Im}(\phi)$. But $|A_4| = 12 = |G| = |\operatorname{Im}(\phi)|$. Hence $A_4 = \operatorname{Im}(\phi)$.

Case 3: $P_3 \trianglelefteq G$, but P_2 is not normal. Then $n_3 = 1$ and $n_2 = 3$. Write $P_3 = \{e, y, y^2\}$. Since $P_3 \trianglelefteq G$, P_2 acts on P_3 by conjugation. On the other hand, since P_2 is not normal and every element of G has the form $x \cdot y^i$ with $x \in P_2$, there must exist $z \in P_2$ that does not commute with y. Hence $zyz^{-1} = y^2$.

- **Case 3a: $P_2 \cong C_4$.** We can assume that z generates P_2. Hence G is generated by z and y, which satisfy the relations

  $$z^4 = 1, \qquad y^3 = 1, \qquad zy = y^2 z.$$

  These relations are enough to determine the multiplication table of G, so there is at most one isomorphism class of such a group. We present a group satisfying these relations. Let w be a primitive third root of unity. Then the complex matrices

  $$z = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \qquad y = \begin{bmatrix} w & 0 \\ 0 & w^2 \end{bmatrix}$$

  satisfy the relations and generate a group of order 12.

- **Case 3b: $P_2 \cong C_2 \times C_2$.** P_2 acts on $\{y, y^2\}$ by conjugation. As above, some element of P_2 does not commute with y, so the orbit of y is $\{y, y^2\}$, of size 2. Hence $|P_2| = |\operatorname{Stab}(y)| \cdot |O(y)|$, i.e. $4 = |\operatorname{Stab}(y)| \cdot 2$, so $|\operatorname{Stab}(y)| = 2$. Hence P_2 contains an element $z \ne e$ such that $zyz^{-1} = y$, and an element x such that $xyx^{-1} = y^2$. Since P_2 is abelian, $xz = zx$. Hence G is generated by x, y, z with relations

  $$x^2 = 1, \quad y^3 = 1, \quad z^2 = 1, \quad yz = zy, \quad xz = zx, \quad xy = y^2 x.$$

  These relations determine the multiplication table of the group, so there is at most one isomorphism class. The dihedral group D_{12} is one such group, so $G \cong D_{12}$. □

4 Free Groups

Definition 4.1 (Free Group, Informal)**.** A group is *free* if it is generated by a subset of elements that satisfy no relations between them.

The rest of this section makes this precise by constructing the free group on a set.

4.1 Words and Cancellation

Let $S = \{a, b, c, \dots\}$ be a set, whose elements we call *letters*. A *word* is a finite string of letters, for example $aabccda$. Words are composed by juxtaposition:

$$ab,\ adc \longmapsto abadc.$$

The unit for this operation is the *empty word*, denoted 1.

Now add inverses: for every $x \in S$ we add a new symbol x^{-1}, giving

$$S' = \{a, a^{-1}, b, b^{-1}, \dots\}.$$

Let W' denote the set of words on S'. We set $xx^{-1} = 1$ and $x^{-1}x = 1$ for all $x \in S$; that is, whenever such a pair appears next to each other in a word, we may *cancel* it.

4.2 Reduced Words

Definition 4.2 (Reduced Form)**.** Let w be a word on S'. Applying finitely many cancellations, we arrive at a word w_0 in which no further cancellation is possible. This is the *reduced form* of w.

Proposition 4.3 (Uniqueness of the Reduced Form)**.** *The reduced form of a word is unique: it does not depend on the order in which the cancellations are performed.*

4.3 Equivalence of Words

Definition 4.4 (Equivalent Words)**.** We call $w, w' \in W'$ *equivalent*, written $w \sim w'$, if they have the same reduced form. This is an equivalence relation.

Example 4.5. $a \sim abb^{-1}$, and $abcc^{-1}a \sim aba \sim abb^{-1}ba$.

Proposition 4.6 (Juxtaposition Respects Equivalence)**.** *If $w \sim w'$ and $v \sim v'$, then $wv \sim w'v'$.*

Proof. To obtain the reduced form of wv, we can first reduce w to w_0, then v to v_0, to obtain w_0v_0, and then keep reducing until done. The reduced forms of w' and v' are also w_0 and v_0, respectively. So to reduce $w'v'$, we can also first reduce to w_0v_0 and then continue. Since both can be reduced to w_0v_0 first, the final reduced forms of wv and $w'v'$ are the same. □

4.4 The Free Group on a Set

Definition 4.7 (Free Group on S)**.** Let F be the set of equivalence classes of words in W'. Then F, with the operation of juxtaposition, is called the *free group* on S.

Proposition 4.8 (The Free Group Is a Group)**.** *F is a group.*

Proof. The product is well defined by the previous proposition. Multiplication is associative (this is clear), and the empty word is the unit. It remains to check that every element of F has an inverse. Let $w \in F$ be the class of $x_1x_2\cdots x_l$ with $x_i \in S'$. Then its inverse is the class of

$$\bar{w} = x_l^{-1} \cdots x_2^{-1}x_1^{-1},$$

since $w\bar{w} = 1$, the empty word. □

We can use power notation in F: for example, $aab = a^2b$.

Example 4.9 (Free Group on One Letter)**.** Take $S = \{a\}$. Then the free group on S is $F = \{a^n \mid n \in \mathbb{Z}\} \cong \mathbb{Z}$.

4.5 Mapping Property of the Free Group

Proposition 4.10 (Mapping Property of the Free Group)**.** *Let F be the free group on a set $S = \{a, b, c, \dots\}$, and let G be a group. Any map of sets $f : S \to G$ extends in a unique way to a group homomorphism $\phi : F \to G$.*

Explicitly, if we write $\tilde{x} := f(x)$ for $x \in S$, then ϕ sends a word in $S' = \{a, a^{-1}, b, b^{-1}, \dots\}$ to the corresponding product of the elements $\tilde{a}, \tilde{a}^{-1}, \tilde{b}, \tilde{b}^{-1}, \dots$ in G.

5 Generators and Relations

Now we study groups that are not free: there are non-trivial relations among the generators.

5.1 Relations and Defining Relations

Definition 5.1 (Relation)**.** A *relation* R among elements $x_1, \dots, x_n$ of a group G is a word R in the free group on the set $\{x_1, \dots, x_n\}$ that equals 1 in G. We write this as $R = 1$.

Example 5.2 (Defining Relations of D_8)**.** In D_8, let r be rotation by 90 degrees and s a reflection. Then

$$r^4 = 1, \qquad s^2 = 1, \qquad srsr = 1$$

are relations. One can use these relations to show that any element of D_8 can be written as $r^j s^k$ with $0 \le j \le 3$ and $k = 0, 1$. So the whole multiplication table is determined. Relations with this property are called *defining relations* of the group.

5.2 The Normal Subgroup Generated by a Set

Lemma 5.3 (Normal Subgroup Generated by a Set)**.** *Let $R \subseteq G$. There exists a unique smallest normal subgroup $N \trianglelefteq G$ such that $R \subseteq N$, called the* normal subgroup generated by R*: if $K \trianglelefteq G$ and $R \subseteq K$, then $N \le K$. The elements of N can be described in either of the following ways.*

1. *An element of G is in N if and only if it can be obtained from the elements of R using a finite sequence of multiplications, inversions, and conjugations.*
2. *Let R' be the set of all elements r and r^{-1} for $r \in R$. An element of G is in N if and only if it can be written as a product $y_1 \cdots y_l$ for some $l \ge 0$, where each y_j is conjugate to an element of R'.*

5.3 Presentations

Definition 5.4 (Group Defined by Generators and Relations)**.** Let F be the free group on a set $S = \{x_1, \dots, x_n\} \neq \emptyset$, and let $R = \{w_1, \dots, w_k\}$ be a set of elements of F. The *group generated by S with relations $w_1 = 1, \dots, w_k = 1$* is the quotient

$$\mathcal{G} = F/\mathcal{R},$$

where $\mathcal{R}$ is the normal subgroup of F generated by R. We denote $\mathcal{G}$ by

$$\langle x_1, \dots, x_n \mid w_1 = 1, \dots, w_k = 1 \rangle,$$

and call this a *presentation* of the group.

5.4 Mapping Property of Quotient Groups

Remark 5.5 (Mapping Property of Quotient Groups). Let $f : G \to G'$ be a group homomorphism and let $N \trianglelefteq G$. If $N \subseteq \ker(f)$, then f induces a well-defined homomorphism

$$\bar{f} : G/N \to G', \qquad \bar{f}(gN) = f(g).$$

5.5 The Canonical Homomorphism from a Presentation

Combining the mapping properties of free groups and of quotient groups gives the following.

Corollary 5.6 (Canonical Homomorphism)**.** *Let $S = \{x_1, \ldots, x_n\} \subseteq G$, and let $R = \{R_1, \ldots, R_k\}$ be a set of relations among the elements of S in G. Let F be the free group on S, let $\mathcal{R}$ be the normal subgroup of F generated by R, and let $\mathcal{G} := F/\mathcal{R}$.*

1. *There is a canonical homomorphism $\Psi : \mathcal{G} \to G$ sending x_i to x_i.*
2. *Ψ is surjective $\iff$ S generates G.*
3. *Ψ is injective $\iff$ every relation among the elements of S is in $\mathcal{R}$.*