Algebra I and II Notes

Eric Walker*

Contents

*Drs. Day, Dummit, Foote

1 Algebra 1

1.1 Introduction to Groups

Definition 1.1.1 (group)**.** A **group** is a set G with a binary operation $\bullet$ satisfying:
1. $\bullet$ is associative,
2. G has an identity, and
3. every element $g \in G$ has an inverse under $\bullet$.

Definition 1.1.2 (binary product)**.** A **binary product** is a function $\bullet : G \times G \to G$ written $g \bullet h$ or gh instead of $\bullet(g, h)$.

Remark 1.1.3. Note that a function needs to be well-defined; i.e., there must be an unambiguous rule defined for all inputs, and it must be closed.

Definition 1.1.4 (associative)**.** An operation is **associative** if for all $x, y, z \in G$, $(xy)z = x(yz)$.

Definition 1.1.5 (identity)**.** An **identity** is an element $1 \in G$ such that for all $x \in G$, $1x = x$ and $x1 = x$.

Definition 1.1.6 (inverse)**.** We define the inverse of $x \in G$ to be an element $y \in G$ such that $xy = 1$ and $yx = 1$.

Example 1.1.7. The following are groups:
- $\mathbf{Z}$ under addition.
- $\mathbf{C}$, $\mathbf{R}$, and $\mathbf{Q}$ under addition.
- Any vector space V under vector addition.
- Permutations on a set S; i.e., $\{f : S \to S \mid f \text{ is a bijection}\}$ under function composition.
- The trivial group; i.e., $\{1\}$ under multiplication or $\{0\}$ under addition or $\{a\}$ under an operation.
- $GL_n(\mathbf{R})$, the general linear group; i.e., the set of invertible $n \times n$ matrices with real entries under matrix multiplication (**Definition 1.5.3**).

Definition 1.1.8 (abelian)**.** A group G is **abelian** if for all $g, h \in G$, $gh = hg$.

Example 1.1.9. $GL_2(\mathbf{R})$ is nonabelian, because

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \neq \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}.$$

Remark 1.1.10. In terms of notation, groups can be written additively or multiplicatively. Multiplicative notation uses $\bullet$, $\times$, juxtaposition, $\circ$, $*$, and so on. 1 is the identity, g^{-1} is the inverse of g, $g^0 = 1$, and for $n \geq 1$, $g^n = g \cdots g$ and $g^{-n} = g^{-1} \cdots g^{-1}$ n times. Additive notation uses $+$. The convention is that additive notation is only used for abelian groups. 0 is the identity, $-g$ is the inverse of g, $0 \cdot g = 0$, and for $n \geq 1$, $ng = g + \cdots + g$ and $-ng = -g + \cdots + -g$ n times.

Proposition 1.1.11. *Let G be a group. The following facts are easily proven.*
- *The identity is unique.*
- *For all $g \in G$, g has a unique inverse; i.e., there is a well-defined function $G \to G$ that sends g to g^{-1}.*
- *For all $g \in G$, $(g^{-1})^{-1} = g$.*
- *For all $g, h \in G$, $(gh)^{-1} = h^{-1}g^{-1}$.*
- *n-fold products are independent of association.*
- *Power laws hold; i.e., $g^{n+m} = g^n g^m$ and $g^{nm} = (g^n)^m$.*
- *Cancellation holds; i.e., if $gx = gy$ for some g then $x = y$ and if $xg = yg$ then $x = y$. This implies three-term equations have unique solutions in G; i.e., $gx = h$ and $xg = h$ both have unique solutions $x \in G$.*

Definition 1.1.12 (order of a group)**.** If G is a group, then the **order** of G is its cardinality as a set. We usually write $|G|$ or sometimes $\#G$.

Definition 1.1.13 (order of an element)**.** If G is a group, for any $g \in G$, the **order** of g is the smallest nonnegative $n \in \mathbf{Z}$ such that $g^n = 1$, or ∞ if no such n exists. We write $|g|$.

Example 1.1.14. Since

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},$$

the matrix

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

has order 2. One can see that the matrix

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

has order ∞.

Remark 1.1.15. When it can be written, the multiplicative table of a group is a good way to communicate that group. For instance, the group $\mathbf{Z}/3\mathbf{Z} = \{0, 1, 2\}$ under addition mod 3 has table

		x		
	$x+y$	0	1	2
	0	0	1	2
y	1	1	2	0
	2	2	0	1

Definition 1.1.16 (dihedral group)**.** The **dihedral group** D_{2n} is the set of isometries of the regular n-gon with operation composition. The isometries can be thought of as inducing permutations of $\{1, \dots, n\}$ that respect adjacent vertices.

Remark 1.1.17. The order of D_{2n} is $2n$.

Example 1.1.18. The group D_6 is the set of isometries of a regular triangle. Label the vertices 1, 2, and 3. There are two distinguished isometries: the first, s, is a reflection about the vertex 1. As a permutation, s is the function $1 \mapsto 1$, $2 \mapsto 3$, and $3 \mapsto 2$. The second, r, is a rotation counterclockwise. As a permutation, r is the function $1 \mapsto 2$, $2 \mapsto 3$, and $3 \mapsto 1$. The isometries r and s easily generalize to D_{2n} for all n.

We claim D_{2n} is not abelian, as $rs \neq sr$. In D_6, this computation is quickly evident; rs is the function $1 \mapsto 2$, $2 \mapsto 1$, and $3 \mapsto 3$, while sr is the function $1 \mapsto 3$, $2 \mapsto 2$, and $3 \mapsto 1$.

In fact, in D_{2n}, $rs = sr^{-1}$. To see this, we compute:

i	1	2	3	$\cdots$	$n-1$	n
$s(i)$	1	n	$n-1$	$\cdots$	3	2

and

i	1	2	3	$\cdots$	$n-1$	n
$r(i)$	2	3	4	$\cdots$	n	1

Therefore a quick computation verifies that

i	1	2	3	$\cdots$	$n-1$	n
$rs(i)$	2	1	n	$\cdots$	4	3
$sr^{-1}(i)$	2	1	n	$\cdots$	4	3

as claimed.

We can verify a few other relations among r and s. It is evident that $s^2 = 1$ and that $r^n = 1$. Furthermore, $r^k \neq 1$ for $k \in \{1, \dots, n-1\}$. Therefore, $|r| = n$ and $|s| = 2$.

As a set, $D_{2n} = \{1, r, r^2, \dots, r^{n-1}, s, rs, r^2 s, \dots, r^{n-1} s\}$. In fact, D_{2n} is generated by r and s, meaning every element $x \in D_{2n}$ can be attained as a finite composition of r and s. Furthermore, the relations above completely characterize D_{2n}; i.e., every equation in D_{2n} in r and s is a consequence of the relations $s^2 = 1$, $r^n = 1$, and $rs = sr^{-1}$. We thus say that D_{2n} has the *presentation* $\langle s, r \mid s^2 = r^n = 1, rs = sr^{-1} \rangle$.

Definition 1.1.19 (group homomorphism)**.** $\varphi : G \to H$ is a **(group) homomorphism** if for all $a, b \in G$, $\varphi(ab) = \varphi(a)\varphi(b)$.

Definition 1.1.20 (group isomorphism)**.** $\varphi : G \to H$ is a **(group) isomorphism** if φ is a bijective homomorphism.

Remark 1.1.21. Being isomorphic is the right notion of sameness for groups. Also note that being isomorphic is an equivalence relation on the class of groups.

Definition 1.1.22 (kernel of a group homomorphism)**.** If $\varphi : G \to H$ is a group homomorphism, then the **kernel** of the map φ is $\ker \varphi = \{g \in G \mid \varphi(g) = 1\}$.

Proposition 1.1.23. *φ is injective if and only if* $\ker \varphi = \{1\}$*.*

Remark 1.1.24. One may show that $G \cong H$ by defining a function $\varphi : G \to H$ that you suspect is an isomorphism. Show that φ is a well-defined group homomorphism. One may use presentations, if available. Then show φ is injective, often by showing $\ker \varphi = \{1\}$ (see **Lemma 1.7.47** to come), and show φ is surjective, often by showing $\varphi(G)$ contains a generating set for H. Also, one can simply produce a φ^{-1}.

Remark 1.1.25. On the other hand, to show $G \not\cong H$, find a property or invariant that is preserved by isomorphisms which G and H do not share.

1.2 Presentations

Example 1.2.1. The presentation $\langle s, t \mid st^2s^{-1} = t^3, ts^2t^{-1} = t^3, st = ts\rangle$ is trivial, but not obviously so. To see this, observe that

$$\begin{aligned} st^2s^{-1} &= t^3 \\ tsts^{-1} &= t^3 \text{ via the relation } st = ts \\ t^2ss^{-1} &= t^3 \text{ via the relation } st = ts \\ t^2 &= t^3 \\ 1 &= t. \end{aligned}$$

Similarly, $s = 1$. Thus this is the trivial group.

Example 1.2.2. The following are presentations for known groups:
- $\langle a \mid \emptyset\rangle \cong \mathbf{Z}$.
- $\langle a, b \mid ab = ba\rangle \cong \mathbf{Z}^2$.
- $\langle a \mid a^n = 1\rangle \cong \mathbf{Z}/n\mathbf{Z}$.
- $\langle a, b \mid \emptyset\rangle$ is the free group on two generators.

Remark 1.2.3. We are reasoning about group presentations without having defined them, but this is okay. We will define group presentations based on free groups, then later define free groups. This is the general idea.

Let S be a set of letters. Let R be a set of equations in S under a group operation. Given any equation $u = v$, it can be written as $uv^{-1} = 1$. Starting with $F = \langle S \mid \emptyset\rangle$, the free group on S, we then consider $R = \{r_1, r_2, \ldots, \} \subseteq F$, which are terms that we want to equal 1. Recall that G/N has elements xN where $x \in N$ if and only if $xN = 1N$. N is the set of elements forced to be 1 in the quotient. Thus build the smallest possible normal subgroup of F containing R. Define a normal subgroup $N = \langle\{xrx^{-1} \mid r \in R, x \in F\}\rangle \trianglelefteq F$. Then define $\langle S \mid R\rangle = F/N$.

Definition 1.2.4 (string)**.** Let S be a set (of letters). A **string** on S is a finite sequence of elements of S, written $s_1s_2 \cdots s_n$ for $s_i \in S$.

Definition 1.2.5 (Kleene star)**.** The set of all strings in S, written S^*, is the **Kleene star** of S.

Example 1.2.6. If $S = \{a, b, c\}$, then some elements of S^* are a, aaa, $abcabc$, and ε, the empty/null string.

Remark 1.2.7. Note that S^* has a binary product, given by concatenation. So $a \cdot abcabc = aabcabc$, and $a \cdot \varepsilon = a$.

Definition 1.2.8 (monoid)**.** A **monoid** is a "group that doesn't necessarily have inverses." That is, it is a set with a binary product such that the binary product is associative and there exists an identity element.

Proposition 1.2.9. *S^* is a monoid under concatenation with identity element ε.*

Remark 1.2.10. Of course, there is the problem that no nonidentity element of S^* has a inverse. We introduce the following definition to remedy this.

Definition 1.2.11 (free group)**.** Let S be a set. Let S^{-1} be the set of formal inverses of S; i.e., elements written s^{-1} for each $s \in S$. Consider the free monoid $(S \cup S^{-1})^*$. Quotient by the relation $\sim$, where $\sim$ is the finest/smallest equivalence relation that satisfies $waa^{-1}v \sim wv$. We define the **free group** on S to be $F(S) = (S \cup S^{-1})^*/\sim$. When $S = \{a_1, \ldots, a_n\}$, $F(S) = F_n$. The operation on $F(S)$ is induced concatenation.

Proposition 1.2.12. *$F(S)$ is a well-defined group.*

Remark 1.2.13. Inverses in $F(S)$ are constructed by reversing the order of a word and replacing each letter with its inverse, like general inverses. For instance,

$$(abca^{-1}b^{-1}c)^{-1} = c^{-1}bac^{-1}b^{-1}a^{-1}.$$

Definition 1.2.14 (freely reduced)**.** A word in $(S \cup S^{-1})^*$ is **freely reduced** if it has no subwords of the form aa^{-1} or $a^{-1}a$ for $a \in S$.

Proposition 1.2.15. *Each equivalence class in $F(S)$ is represented by a unique freely reduced word.*

Corollary 1.2.16. *If $S \neq \emptyset$, then $F(S)$ is not trivial. Moreover, $F(S)$ is of infinite order.*

Lemma 1.2.17. *If $|S| = 1$, then $F(S) \cong \mathbf{Z}$.*

Proof. Since $F(S) = \{\ldots, a^{-2}, a^{-1}, \varepsilon = a^0, a^1, a^2, \ldots\}$, the result is obvious. $\square$

Lemma 1.2.18. *If $|S| \geq 2$, then $F(S)$ is nonabelian.*

Proof. Let $a, b \in S$ be distinct. Then ab and ba are different freely reduced words, so $a \cdot b \neq b \cdot a$ in $F(S)$. $\square$

Proposition 1.2.19. *Let G be a group and let $f : S \to G$ be a function of sets. There is a unique homomorphism $\varphi : F(S) \to G$ such that $\varphi(s) = f(s)$ for all $s \in S$.*

Remark 1.2.20. Proposition 1.2.19 is the defining property of free groups up to isomorphism. It says that free groups have a basis, S. The proof idea simply exploits the construction $\varphi({s_1}^{\eta_1} \cdots {s_n}^{\eta_n}) \coloneqq f(s_1)^{\eta_1} \cdots f(s_n)^{\eta_n}$.

Example 1.2.21. Let's now show that our presentation $\langle s, r \mid s^2 = r^n = 1, rs = sr^{-1} \rangle$ for D_{2n} is correct. Note first that $\langle s, r \mid s^2 = r^n = 1, rs = sr^{-1} \rangle$ has at most $2n$ elements: $\{1, r, r^2, \ldots, r^{n-1}, s, rs, r^2s, \ldots, r^{n-1}s\}$. It could have less, if there is some nontrivial way to relate two elements.

Let $S = \{s, r\}$ and let $F = F(S)$. Define $\varphi : F \to D_{2n}$ by $\varphi(s) = s$ and $\varphi(r) = r$. By **Proposition 1.2.19**, φ is a homomorphism. φ is surjective, since s and r in D_{2n} generate D_{2n} by **Example 1.1.18**. Furthermore, φ descends to a homomorphism $\overline{\varphi} : F/\overline{\langle R \rangle} \to D_{2n}$, where $R = \{s^2, r^n, rs^{-1}rs\}$. Note that $F/\overline{\langle R \rangle} = \langle S \mid R \rangle$. Now, $\overline{\varphi}$ is a surjective homomorphism from a group with at most $2n$ elements to a group with exactly $2n$ elements. Therefore, $\overline{\varphi}$ is a bijective homomorphism - an isomorphism.

Remark 1.2.22. The above example generalizes. We see that $G = \langle S \mid R \rangle$ if there is an isomorphism $F(S)/\overline{\langle R \rangle} \to G$, or equivalently, there is a surjective homomorphism $F(S) \to G$ with kernel $\overline{\langle R \rangle}$. Identify S with its image under these maps; i.e., S is the set of generators of G, rather than letters.

Proposition 1.2.23. *Let $G = \langle S \mid R \rangle$ and let H be a group. Suppose $f : S \to H$ is a function, and for all $r \in R$, if we substitute $f(s)$ for s in r for all $s \in S$, we get $1 \in H$. Then there is a unique homomorphism $\varphi : G \to H$ with $\varphi(s) = f(s)$ for all $s \in S$.*

Remark 1.2.24. This gives great utility to group presentations. The proof sketch is as follows: by **Proposition 1.2.19**, f extends to $\widetilde{\varphi} : F(S) \to H$. Define $\varphi(g) = \widetilde{\varphi}(w)$ where w represents g; i.e., $w \in F(S)$ and under the homomorphism coming from the presentation, $w \mapsto g$. This construction is well-defined, as $\widetilde{\varphi}(r) = 1 \in H$ for all $r \in R$. If $G = \langle S \mid \emptyset \rangle$, then for all $g \in G$, there exists $a_1, \ldots, a_k \in S \cup S^{-1}$ such that $g = a_1 \cdots a_k$. Then, $\varphi(g) = \varphi(a_1 \cdots a_k) = \varphi(a_1) \cdots \varphi(a_k)$.

Example 1.2.25. Let $G = D_{2n} = \langle r, s \mid s^2 = r^n = 1, rs = sr^{-1} \rangle$. We wish to construct a homomorphism $\varphi : D_{2n} \to \mathbf{Z}/n\mathbf{Z}$ satisfying $\varphi(r) = 1$ and $\varphi(s) = 0$. Notice that

$$\begin{aligned} \varphi(r^n) &= \varphi(r) + \cdots + \varphi(r) = n\varphi(r) = n \cdot 1 = 0, \\ \varphi(s^2) &= \varphi(s) + \varphi(s) = 0 + 0 = 0, \text{ and} \\ \varphi(1) &= 0. \end{aligned}$$

However,

$$\begin{aligned} \varphi(rs) &= \varphi(r) + \varphi(s) = 1 + 0 = 1 \text{ and} \\ \varphi(sr^{-1}) &= \varphi(s) - \varphi(r) = 0 - 1 = -1. \end{aligned}$$

If $n \geq 3$, then $1 \neq -1$, and we have a contradiction. In this case, no such homomorphism exists.

Example 1.2.26. Consider instead a homomorphism $\varphi : D_{2n} \to \mathbf{Z}/2\mathbf{Z}$ with $\varphi(r) = 0$ and $\varphi(s) = 1$. This does work, as

$$\begin{aligned} \varphi(r^n) &= 0, \\ \varphi(s^2) &= 0, \\ \varphi(rs) &= 1, \text{ and} \\ \varphi(sr^{-1}) &= 1. \end{aligned}$$

Remark 1.2.27. How do we find presentations? We have the following techniques.

- If G is finite, find a generating set S and relations R such that $\langle S \mid R \rangle$ has at most $|G|$ elements. Then $G = \langle S \mid R \rangle$, as $F(S)/\overline{\langle R \rangle} \to G$ is a surjective homomorphism. Note that you must be able to count $\langle S \mid R \rangle$ in this approach.
- If we know $G = \langle S \mid R \rangle$ and $M \trianglelefteq G$, then we can find a presentation for G/M.

  Example 1.2.27.1. We know $\mathbf{Z} = \langle t \mid \emptyset \rangle$. Since $n\mathbf{Z} = \{kn \mid k \in \mathbf{Z}\} = \langle n \rangle$, t^n represents $n \in \mathbf{Z}$, so $\mathbf{Z}/n\mathbf{Z} = \langle t \mid t^n = 1 \rangle$.

  In general, start with your generating set, and set relations to 1. Suppose $R' \subseteq F(S)$ such that R' represents a set of generators for M in G (or normal generators). Then $G/M = \langle S \mid R \cup R' \rangle$; i.e., we have a surjective homormorphism $F(S) \to G/M$ with kernel $\overline{\langle R \cup R' \rangle}$.
- Suppose G has normal subgroup $M \trianglelefteq G$ and $H \leq G$ such that $M \cap H = \{1\}$ and $MH = G$ (i.e., $G = \langle M \cup H \rangle$). Suppose $M = \langle S_1 \mid R_1 \rangle$ and $H = \langle S_2 \mid R_2 \rangle$ which are finite presentations. For every $s \in S_2 \cup {S_2}^{-1}$ and $t \in S_1$, find a word $w_{s,t} \in F(S_1)$ such that $sts^{-1} = w_{s,t}$ in G. Then let $R_3 = \{sts^{-1}{w_{s,t}}^{-1} \mid s \in S_2 \cup {S_2}^{-1}, t \in S_1\}$. Then $G = \langle S_1 \cup S_2 \mid R_1 \cup R_2 \cup R_3 \rangle$.

  Example 1.2.27.2. Let $G = D_{2n}$. Let $M = \langle r \rangle \cong \mathbf{Z}/n\mathbf{Z} = \langle r \mid r^n = 1 \rangle$ and $H = \langle s \rangle \cong \mathbf{Z}/2\mathbf{Z} = \langle s \mid s^2 = 1 \rangle$. Now declare $s^{-1}rs = r^{-1}$ and $srs^{-1} = r^{-1}$. (Note that the second is redundant from the other relations.) It follows that $D_{2n} = \langle s, r \mid s^2 = r^n = 1, s^{-1}rs = r^{-1} \rangle$.
- Suppose $G = \langle S_1 \mid R_1 \rangle$ and $H = \langle S_2 \mid R_2 \rangle$. Let $R_3 = \{sts^{-1}t^{-1} \mid s \in S_1, t \in S_2\} \subseteq F(S_1 \cup S_2)$. Note that the elements in $\overline{\langle R_3 \rangle}$ are $sts^{-1}t^{-1} = 1$, so $st = ts$. Then $G \times H = \langle S_1 \cup S_2 \mid R_1 \cup R_2 \cup R_3 \rangle$.

  Example 1.2.27.3. Let $\mathbf{Z} = \langle s \mid \emptyset \rangle$ and $\mathbf{Z} = \langle t \mid \emptyset \rangle$. Then $\mathbf{Z} \times \mathbf{Z} = \langle s, t \mid sts^{-1}t^{-1} \rangle$.
- We can also attempt to brute force a presentation. Let $S = G \setminus \{1\}$. Let $R = \{s_1 s_2 \mid s_1, s_2 \in S, s_1 s_2 = 1\} \cup \{s_1 s_2 s_3 \mid s_1, s_2, s_3 \in S, s_1 s_2 s_3 = 1\} \cup \cdots$. That is, write the entire multiplication table. Then $G = \langle S \mid R \rangle$. Therefore, every group has a presentation.

Definition 1.2.28 (Tietze transformations)**. Tietze transformations** are permissible computations that can be applied to a group presentation without changing its isomorphism class. Let $G = \langle S \mid R \rangle$. The Tietze transformations are

1. Adding a generator: let t be a letter such that $t \notin S$. Pick $w \in F(S)$. Then $G = \langle S \cup \{t\} \mid R \cup \{tw^{-1}\} \rangle$.
2. Removing an unnecessary generator: pick $s \in S$. Suppose $r \in R$ such that there is exactly one $s^{\pm 1}$ in r, and further, s appears nowhere else in R. Then $G = \langle S \setminus \{s\} \mid R \setminus \{r\} \rangle$.
3. Adding a true relation: Suppose $w \in \overline{\langle R \rangle}$. Then $G = \langle S \mid R \cup \{w\} \rangle$.
4. Removing a redundant relation: suppose $r \in R$ and $r \in \overline{\langle R \setminus \{r\} \rangle}$. Then $G = \langle S \mid R \setminus \{r\} \rangle$.

Example 1.2.29. One can derive $D_{2n} = \langle a, b \mid a^2, b^2, (ab)^n \rangle$ from $D_{2n} = \langle r, s \mid r^n, s^2, s^{-1}rsr \rangle$.

1.3 The Symmetric Group

Definition 1.3.1 (symmetric group)**.** Let X be a set. The **symmetric group** on X is the set of bijections $X \to X$ with binary product composition. We write $\mathrm{Sym}(X)$, but if $X \cong \{1, 2, \ldots, n\}$, we write S_n.

Remark 1.3.2. The following are easily verified.

- For any X, $\mathrm{Sym}(X)$ is a group.
- $|S_n| = n!$, and if $|X| = \infty$, then $|\mathrm{Sym}(X)| = \infty$.
- One may record elements of S_n as tables, written as follows:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 4 & 7 & 2 & 6 & 3 & 1 \end{pmatrix} \in S_7.$$

  To compose, simply stack tables:

$$\sigma^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 2 & 1 & 4 & 3 & 7 & 5 \end{pmatrix}.$$

  To invert, turn the table upside down and reorder:

$$\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 4 & 6 & 2 & 1 & 5 & 3 \end{pmatrix}.$$

- There is a better notation though; cycle notation. If $a_1, \ldots, a_k \in \{1, \ldots, n\}$ are distinct, then we write $\tau = (a_1, \ldots, a_k) \in S_n$, where $\tau(a_i) = a_{i+1}$ for $i \in \{1, \ldots, k-1\}$ and $\tau(a_k) = a_1$. For completeness, $\tau(x) = x$ if $x \notin \{a_1, \ldots, a_k\}$. We say τ is a cycle. The standard notation for the identity is (1).

Proposition 1.3.3. *Every permutation in S_n can be expressed as a product of disjoint cycles. This expression is unique up to ordering cycles, cyclically permuting cycle notation, and including trivial cycles.*

Remark 1.3.4. There is an algorithm for expressing a permutation as a product of disjoint cycles. If

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 4 & 7 & 2 & 6 & 3 & 1 \end{pmatrix},$$

then $\sigma = (1, 5, 6, 3, 7)(2, 4)$. Furthermore, $\sigma^2 = (1, 5, 6, 3, 7)(2, 4)(1, 5, 6, 3, 7)(2, 4) = (1, 6, 7, 5, 3)(2)(4) = (1, 6, 7, 5, 3)$. Also, $\sigma^{-1} = (7, 3, 6, 5, 1)(4, 2)$.

Example 1.3.5. Here is a few more computations. If $\sigma = (1, 6, 7, 5, 3)(2, 4)$ and $\tau = (1, 2, 3, 4, 5, 6, 7)$, then $\sigma \circ \tau = (1, 6, 7, 5, 3)(2, 4)(1, 2, 3, 4, 5, 6, 7) = (1, 4, 3, 2)(5, 7, 6)$ and $\tau \circ \sigma = (1, 7, 6)(2, 5, 4, 3)$.

Remark 1.3.6. Note that $(1, 2)(2, 3) \neq (2, 3)(1, 2)$, so S_n is nonabelian for $n \geq 3$.

1.4 The Quaternion Group

Definition 1.4.1 (quaternion group)**.** The **quaternion group**, Q_8, is the set $\{1, i, j, k, -1, -i, -j, -k\}$ with multiplication table derived from $i^2 = j^2 = k^2 = -1$, $ij = k$, $ji = -k$, and $-1x = -x$.

Remark 1.4.2. There are much nicer ways to communicate Q_8. For example,

$$Q_8 \cong \left\langle \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} \right\rangle \leq GL_2\mathbf{C}.$$

We traditionally refer to

$$\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \text{ and } \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}$$

as i and j, respectively. In addition, $Q_8 = \langle a, b \mid a^4 = 1, b^2 = a^2, bab^{-1} = a^{-1}\rangle$. This presentation shows that Q_8 has at most the following elements: $\{1, a, a^2, a^3, b, ab, a^2b, a^3b\}$. Then, there is a homomorphism $\varphi(a) = i$ and $\varphi(b) = j$ which is surjective from $\langle a, b \mid a^4 = 1, b^2 = a^2, bab^{-1} = a^{-1}\rangle \to \langle i, j\rangle$. Thus, these definitions are equivalent.

Remark 1.4.3. The following properties of Q_8 are easily verified.

- $|Q_8| = 8$.
- Q_8 is nonabelian.
- Observe the following table:

order of an element	number of elements with that order
1	1
2	1
4	6

Contrast that with the same information for the group D_8:

order of an element	number of elements with that order
1	1
2	5
4	2

Thus $Q_8 \ncong D_8$.

1.5 Fields

Definition 1.5.1 (field)**.** A **field** is a set F with two binary operations, $+$ and $\bullet$, such that:

1. $(F, +)$ is an abelian group,
2. $(F \setminus \{0\}, \bullet)$ is an abelian group (note 0 is the identity for $+$), and
3. distributivity holds; i.e., for all $a, b, c \in F$, $a(b + c) = ab + ac$.

Example 1.5.2. The following are fields.

- $\mathbf{Q}$, $\mathbf{R}$, and $\mathbf{C}$.
- If p is a prime, $\mathbf{Z}/p\mathbf{Z}$.
- $\mathbf{Q}[\sqrt{2}] = \{a + b\sqrt{2} \in \mathbf{R} \mid a, b \in \mathbf{Q}\}$.
- For each prime p and positive $n \in \mathbf{N}$, there is a unique field of order p^n. Write $\mathbf{F}_{p^n}$.

Definition 1.5.3 (general linear group)**.** For any field F and n a positive integer, define the **general linear group** GL_nF, which is the set of $n \times n$ invertible matrices with entries in F. GL_nF is a group with matrix multiplication as the operation.

Definition 1.5.4 (special linear group)**.** For any field F and n a positive integer, define the **special linear group** SL_nF, which is the set of $n \times n$ matrices with determinant 1 and entries in F. SL_nF is a group with matrix multiplication as the operation.

Remark 1.5.5. Recall that a matrix is invertible if and only if it has nonzero determinant.

Remark 1.5.6. Note that linear algebra works the same way over an arbitrary field F as it does over $\mathbf{R}$ or $\mathbf{C}$, except for orthogonality.

Proposition 1.5.7. *If F is a finite field with $|F| = q$, then $|GL_nF| = (q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{n-1})$.*

Example 1.5.8. By **Proposition 1.5.7**, $|GL_3(\mathbf{Z}/2\mathbf{Z})| = (2^3 - 1)(2^3 - 2)(2^3 - 2^2) = 7 \cdot 6 \cdot 4 = 168$.

1.6 Homomorphisms and Isomorphisms

Remark 1.6.1. Recall **Definitions 1.1.19** and **1.1.20**. Recall also the approach for showing $G \cong H$ or $G \not\cong H$ outlined in **Remarks 1.1.24** and **1.1.25**.

Example 1.6.2. Recall that $D_6 = \langle r, s \mid r^3 = s^2 = 1, srs = r^{-1} \rangle$ and S_3 is the group of permutations on $\{1,2,3\}$, which we write in cycle notation (**Remark 1.3.2**). Define $\varphi : D_6 \to S_3$ by $\varphi(r) = (1,2,3)$ and $\varphi(s) = (1,2)$. To check the relations:

$$\begin{aligned}(1,2,3)^3 &= (1) \text{ as } (1,2,3) \text{ is a 3-cycle,}\\ (1,2)^2 &= (1) \text{ as } (1,2) \text{ is a 2-cycle,}\\ (1,2)(1,2,3)(1,2) &= (1,3,2) = (1,2,3)^{-1}.\end{aligned}$$

Thus φ is a well-defined homomorphism.

Furthermore, φ is surjective, since $\langle (1,2,3)(1,2) \rangle = S_3$. To see this, observe that

$$\begin{aligned}&(1,2,3)(1,2)(1,2,3)^{-1} = (2,3), \text{ and}\\ &(1,2,3)(2,3)(1,2,3)^{-1} = (1,3),\end{aligned}$$

giving us 6 distinct elements from $(1,2,3)$ and $(1,2)$. This is a specific result of the more general fact that an n-cycle and a 2-cycle generate S_n.

Since φ is a surjective homomorphism between two groups of order 6, φ is an isomorphism.

Example 1.6.3. Recall from **Remark 1.4.2** that $Q_8 = \langle a, b \mid a^4 = 1, a^2 = b^2, aba^{-1} = b^{-1} \rangle$. Define $\varphi : Q_8 \to (\mathbf{Z}/2\mathbf{Z})^2$ by $\varphi(a) = (1,0)$ and $\varphi(b) = (0,1)$. To check the relations:

$$\begin{aligned}4(1,0) &= (4,0) = (0,0),\\ 2(1,0) &= (2,0) = (0,0) = (0,2) = 2(0,1),\\ (1,0) + (0,1) - (1,0) &= (0,1) = -(0,1).\end{aligned}$$

Thus φ is a well-defined homomorphism. Surjectivity is obvious, since $\langle (1,0), (0,1) \rangle = (\mathbf{Z}/2\mathbf{Z})^2$, but φ is not injective, because $\ker \varphi = \langle a^2 \rangle$.

Example 1.6.4. One may show that there is a nontrivial homomorphism $D_8 \to (\mathbf{Z}/2\mathbf{Z})^2$. Further, there is an isomorphism $D_8 \to H(\mathbf{Z}/2\mathbf{Z})$, the Heisenberg group. The Heisenberg group of a field F is

$$H(F) = \left\{ \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \mid a, b, c \in F \right\}.$$

Example 1.6.5. Define $\varphi : H(F) \to F \times F$ by

$$\varphi\left(\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \right) = (a, c).$$

φ is indeed a homomorphism, as

$$\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a+d & e+af+b \\ 0 & 1 & c+f \\ 0 & 0 & 1 \end{bmatrix}.$$

φ is clearly surjective and not injective.

Example 1.6.6. Let $U = \{z \in \mathbf{C} \mid |z| = 1\}$ be the unit circle. There is a homomorphism $\varphi : \mathbf{R} \to U$ defined by $\varphi(x) = e^{ix} = \cos x + i \sin x$, with $\ker \varphi = 2\pi\mathbf{Z}$.

1.7 Subgroups

Definition 1.7.1 (induced operation)**.** Let G be a group and let H be a subset of G. If the product on G, $G \times G \to G$, restricts to $H \times H \to H$, then we say $H \times H \to H$ is the **induced operation** on H.

Definition 1.7.2 (subgroup)**.** H is a **subgroup** of G, written $H \leq G$, if H is a group under the induced operation.

Example 1.7.3. $\mathbf{Z} \leq \mathbf{Q} \leq \mathbf{R} \leq \mathbf{C}$ under $+$. Similarly, $\mathbf{Z}^* \leq \mathbf{Q}^* \leq \mathbf{R}^* \leq \mathbf{C}^*$ under $\cdot$.

Remark 1.7.4. For every group G, $\{1\} \leq G$ and $G \leq G$. We call $\{1\}$ the trivial subgroup and G the improper subgroup (if we even want to refer to it at all). We say proper subgroups to exclude the case $G \leq G$.

Example 1.7.5. $\langle r \rangle = \{1, r, \ldots, r^{n-1}\rangle = \mathbf{Z}/n\mathbf{Z} \leq D_{2n}$ is a proper subgroup.

Example 1.7.6. For nonexamples, consider $\mathbf{N} \not\leq \mathbf{Z}$. There is an induced operation; $+$ on $\mathbf{Z}$ induces $+$ on $\mathbf{N}$, but $\mathbf{N}$ is not a group. Usually however, the more common problem is that an induced operation does not exist. For example, $\{r\} \not\leq D_{2n}$. Finally, $\emptyset \not\leq G$, as $\emptyset$ is not a group as well; it has no identity. Though note that $\emptyset$ does vacuously have an induced operation.

Lemma 1.7.7 (First subgroup criterion)**.** *Let G be a group and $H \subseteq G$. $H \leq G$ if and only if*

1. *$H \neq \emptyset$,*
2. *H is closed under taking products in G, and*
3. *H is closed under taking inverses in G.*

Proof. One direction is easy. For the other, assume 1, 2, and 3 hold. Since H is closed under products, H has a well-defined induced product from G. The product on H is associative because this is inherited from G. Since $H \neq \emptyset$, there exists $h \in H$. Since H is closed under inverses, $h^{-1} \in H$ where h^{-1} is the inverse in G. Since H is closed under products, $1_G = hh^{-1} \in H$. 1_G is also the identity for H. Finally, let $h \in H$. By closure, $h^{-1} \in H$ considering h^{-1} as the inverse of h in G, but h^{-1} is also the inverse in H. $\square$

Remark 1.7.8. If $H \leq G$, then $1_H = 1_G$, and for all $h \in H$, h^{-1} in G is h^{-1} in H.

Proposition 1.7.9 (Second subgroup criterion)**.** *Let G be a group and let $H \subseteq G$. $H \leq G$ if and only if*

1. *$H \neq \emptyset$, and*
2. *for all $a, b \in H$, $ab^{-1} \in H$.*

Proposition 1.7.10 (Third subgroup criterion)**.** *Let G be a group. Let H be a nonempty finite subset of G. If H is closed under taking products in G, then H is a subgroup.*

Definition 1.7.11 (subgroup generated by a subset)**.** Let G be a group and let S be a subset of G. Define $\langle S \rangle$ to be the set of all finite length products of $S \cup S^{-1}$. We call $\langle S \rangle$ the **subgroup generated by** S.

Remark 1.7.12. $\langle S \rangle$ is the smallest subgroup of G containing S. Furthermore, for all $H \leq G$, $S \subseteq H$ implies $\langle S \rangle \leq H$, and

$$\langle S \rangle = \bigcap_{\substack{H \leq G \\ S \subseteq H}} H.$$

Definition 1.7.13 (centralizer)**.** Let G be a group. Let $A \subseteq G$. Define $C_G(A) = \{g \in G \mid gag^{-1} = a \text{ for all } a \in A\}$ to be the **centralizer** of A in G.

Remark 1.7.14. The equation $gag^{-1} = a$ is equivalent to the commutativity condition $ga = ag$.

Definition 1.7.15 (center)**.** Define $Z(G) = C_G(G) = \{g \in G \mid gag^{-1} = a \text{ for all } a \in G\}$ to be the **center** of G.

Definition 1.7.16 (normalizer)**.** Define $N_G(A) = \{g \in G \mid gAg^{-1} = A\}$ to be the **normalizer** of A in G.

Definition 1.7.17 (stabilizer)**.** Let G act on S. Let $s \in S$. Define $G_s = \{g \in G \mid g \cdot s = s\}$ to be the **stabilizer** of s.

Lemma 1.7.18. *For any group G, any action on S, and any $s \in S$, the stabilizer G_s is a subgroup of G.*

Proof. By **Lemma 1.7.7 [First subgroup criterion]**. G_s is not empty since $1 \in G_s$. G_s is closed under products since if $g \cdot s = s$ and $h \cdot s = s$, then $(gh) \cdot s = g(h \cdot s) = g \cdot s = s$. Finally, G_s is closed under taking inverses since if $g \cdot s = s$, then $g^{-1} \cdot s = g^{-1}(g \cdot s) = (g^1 g) \cdot s = 1 \cdot s = s$. □

Lemma 1.7.19. *For any group G and any subset $A \subseteq G$, $C_G(A)$ is a subgroup of G.*

Proof. Define $c : G \times G \to G$ by $c(g, h) = ghg^{-1}$. This is the conjugation action of G on G, sometimes written h^g. To see this is an action, observe that $c(1, h) = 1h1^{-1} = h$, and if $a, b \in G$ and $h \in G$, then $c(a, c(b, h)) = c(a, bhb^{-1}) = abhb^{-1}a^{-1}$, and $c(ab, h) = abh(ab)^{-1} = abhb^{-1}a^{-1}$. Thus c is a group action.

Now observe that $C_G(\{a\}) = G_a$, so by **Lemma 1.7.18**, $C_G(\{a\})$ is a subgroup of G.

Next, for any set A,

$$C_G(A) = \bigcap_{a \in A} C_G(\{a\}).$$

Using the fact that arbitrary intersections of subgroups are subgroups, $C_G(A)$ is a subgroup of G. □

Corollary 1.7.20. *The center $Z(G) = C_G(G)$ is a subgroup of G.*

Lemma 1.7.21. *For any group G and $A \subseteq G$, $N_G(A)$ is a subgroup of G.*

Proof. For $g \in G$, let $gAg^{-1} = \{gag^{-1} \mid a \in A\}$. This defines a group action $\alpha : G \times \mathcal{P}(G) \to \mathcal{P}(G)$ defined by $\alpha(g, A) = gAg^{-1}$. Recall that $N_G(A) = \{g \in G \mid gAg^{-1} = A\}$, so $N_G(A) = G_A$ under the conjugation action on subsets. By **Lemma 1.7.18**, $N_G(A)$ is a subgroup of G. □

Example 1.7.22. In D_{2n}, D_{2n} acts on $\{1, \ldots, n\}$. By **Example 1.11.16** to come or by direct computation, the stabilizer of 1, $(D_{2n})_1 = \{1, s\}$ as these are the only actions that fix 1.

Example 1.7.23. To determine the centralizers of a group, often one simply makes a list. In D_{2n}, $C_{D_{2n}}(r) = \langle r \rangle$. If $n = 2m$, then $C_{D_{2n}}(s) = \langle s, r^m \rangle$, as $sr^m s = r^{-m} = r^m$, while if $n = 2m+1$, $C_{D_{2n}}(s) = \langle s \rangle$.

Example 1.7.24. If $n = 2m$, then $Z(D_{2n}) = \langle r^m \rangle$, as it is the intersection of $C_{D_{2n}}(r)$ and $C_{D_{2n}}(s)$. If $n = 2m + 1$, then $Z(D_{2n}) = \{1\}$.

Example 1.7.25. If G is abelian and $A \subseteq G$, then $Z(G) = G$, $C_G(A)$, and $N_G(A) = G$.

Example 1.7.26.

$$N_{D_{2n}}(\langle s \rangle) = \begin{cases} \langle s \rangle & \text{if } n \text{ is odd;} \\ \langle s, r^m \rangle & \text{if } n \text{ is even.} \end{cases}$$

$N_{D_{2n}}(\langle r \rangle) = D_{2n}$.

Example 1.7.27. $C_{S_n}(\sigma)$ is complicated. If $|A| < \infty$, σ has a finite disjoint cycle decomposition. It is easier to see that if $|A| \geq 3$, then $Z(\mathrm{Sym}(A)) = \{1\}$.

Definition 1.7.28 (cyclic subgroup)**.** Let G be a group. Let $x \in G$. Then $\langle x \rangle = \{x^n \mid n \in \mathbf{N}\}$ is the **cyclic subgroup** generated by x.

Definition 1.7.29 (cyclic group)**.** If there is $x \in G$ such that $G = \langle x \rangle$, then we say that G is **cyclic**.

Remark 1.7.30. Cyclic groups are abelian.

Lemma 1.7.31. *If $x \in G$ and $H = \langle x \rangle$, then $|H| = |x|$.*

Proof. Observe that $H = \{1, x, \ldots, x^{n-1}\}$ if $|x| = n$, and $H = \{\ldots, x^{-1}, 1, x, \ldots\}$ if $|x| = \infty$. Notice that H is at most countable by definition. □

Lemma 1.7.32. *If $x^n = 1$ and $x^m = 1$, then $x^d = 1$ where $d = \gcd(m, n)$.*

Proof. If $d = \gcd(m, n)$, then there exist $a, b \in \mathbf{Z}$ such that $d = am + bn$. Simply compute:

$$x^d = x^{am+bn} = (x^m)^a (x^n)^b = 1.$$

□

Theorem 1.7.33 (The classification of cyclic groups)**.** *Let G be cyclic; $G = \langle x \rangle$ for some x.*

1. *$|G|$ is a positive integer or countable infinity.*
2. *Cyclic groups are isomorphic if and only if they have the same order.*

Proof. Note that 1. is obvious. For 2., there are two cases:

- **Case One:** If $|G| = \infty$, then define $\varphi : \mathbf{Z} \to G$ by $\varphi(k) = x^k$. See that φ is a homomorphism by power rules: $x^k x^\ell = x^{k+\ell}$. Furthermore, φ is surjective, by definition of $\langle x \rangle$. Also, φ is injective. If $\varphi(k) = 1$, then $x^k = 1$. If $k \neq 0$, then $|x| \leq |k| < \infty$, a contradiction. Thus $k = 0$, so $\ker \varphi = \{0\}$. Hence, $G \cong \mathbf{Z}$, and any two cyclic subgroups of order ∞ are isomorphic via an isomorphism factored through $\mathbf{Z}$.
- **Case Two:** If $|G| = n < \infty$, then defined $\varphi : \mathbf{Z}/n\mathbf{Z} \to G$ by $\varphi([k]) = x^k$. To see φ is well-defined, assume k and ℓ are two representatives of $[k]$. Then n divides $k - \ell$, so there exists $m \in \mathbf{Z}$ such that $k - \ell = mn$. Then $x^k = x^{mn+\ell} = (x^n)^m x^\ell = x^\ell$. So φ is well-defined. Now, φ is a homomorphism as $\varphi([k] + [\ell]) = \varphi([k + \ell]) = x^{k+\ell} = x^k x^\ell = \varphi([k])\varphi([\ell])$. Also φ is surjective by definitions of $\langle x \rangle$, and φ is injective, since if $\varphi([k]) = 1$, then $x^k = 1$. As $x^k = 1$ and $x^n = 1$, $x^d = 1$ where $d = \gcd(k, n)$ by **Lemma 1.7.32**. Since $n = |x|$, $n = d$. Thus, n divides k, so $[k] = [0]$ and $\ker \varphi = \{[0]\}$. Therefore $G \cong \mathbf{Z}/n\mathbf{Z}$, and any two cyclic subgroups of order n are isomorphic via an isomorphism factored through $\mathbf{Z}/n\mathbf{Z}$.

□

Lemma 1.7.34. *Suppose G is a group and $x \in G$.*

1. *If $|x| = \infty$, then for all $a \in \mathbf{Z} \setminus \{0\}$, $|x^a| = \infty$.*
2. *If $|x| = n < \infty$, then for all $a \in \mathbf{Z}$, $|x^a| = n/\gcd(n, a)$. If a divides n and $a > 0$, then $\gcd(n, a) = a$, so $|x^a| = n/a$.*

Proof. This follows straight from the definitions. □

Example 1.7.35. In $\mathbf{Z}/6\mathbf{Z}$, $|1| = 6$, $|2| = 3$, $|3| = 2$, $|4| = 3$, and $|5| = 6$.

Lemma 1.7.36. *Suppose $H = \langle x \rangle$.*

1. *If $|x| = \infty$, then $H = \langle x^a \rangle$ if and only if $a = \pm 1$.*
2. *If $|x| = n < \infty$, then $H = \langle x^a \rangle$ if and only if $\gcd(a, n) = 1$. In particular, the number of choices of x^a where $H = \langle x^a \rangle$ is $\varphi(n) = |\{k \mid 1 \leq k \leq n \text{ and } \gcd(k, n) = 1\}|$, the Euler φ-function.*

Proof. Follows from **Lemma 1.7.34**. □

Example 1.7.37. Let $G = \mathbf{Z}/24\mathbf{Z}$. We see that $\varphi(24) = \varphi(8)\varphi(3)$, as $\gcd(8, 3) = 1$, and $\varphi(8)\varphi(3) = 4 \cdot 2 = 8$. The explicit elements that work to generate $G = \mathbf{Z}/24\mathbf{Z}$ are 1, 5, 7, 11, 13, 17, 19, and 23, of which there are eight.

Theorem 1.7.38. *Suppose $H = \langle x \rangle$. Then*

1. *Every subgroup of H is cyclic.*
2. *If $K \leq H$, then $K = \langle x^d \rangle$ where d is the smallest positive integer with $x^d \in K$, unless $K = \{0\}$.*
3. *If $|H| = \infty$, then there is a bijective correspondence between subgroups of H and the nonnegative integers, given by $n \mapsto \langle x^n \rangle$.*
4. *If $|H| = n < \infty$, then there is a bijective correspondence between subgroups of H and the positive divisors of n, given by $a \mapsto \langle x^a \rangle$, where a divides n and $n > 0$.*

Proof. Here, we only prove 1. Let $H = \langle x \rangle$ and $K \leq H$ with $K \neq \{0\}$. Let $d \in \mathbf{Z}$ be the smallest positive integer such that $x^d \in K$. Clearly $\langle x^d \rangle \subseteq K$. We would like to show $K \subseteq \langle x^d \rangle$. Let $g \in K$. Then $g \in H$, and so there is $n \in \mathbf{Z}$ such that $g = x^n$. Divide n by d. By the division algorithm, there exist $p, q \in \mathbf{Z}$ such that $n = dp + r$ and $0 \leq r < d$. As $x^n \in K$ and $x^d \in K$, and $r = n - pd$, we have $x^r = x^n (x^d)^{-p} \in K$. If $r \neq 0$, then $r < d$ contradicts the fact that d is minimal. Thus $r = 0$, so $n = dp$, and $x^n = (x^d)^p$. Thus $x^n \in \langle x^d \rangle$. Therefore $K = \langle x^d \rangle$, and every subgroup of H is cyclic. □

Remark 1.7.39. Given a finite group, one can

- enumerate all the cyclic subgroups,
- enumerate the subgroups generated by small subsets, and
- prove that larger subsets generate the entire group.

Example 1.7.40. Consider the group $\mathbf{Z}/6\mathbf{Z}$. We know that the divisors of 6 are 1, 2, 3, and 6, so we may draw a lattice of subgroups like so:

$$\begin{tikzcd}
 & \langle 1 \rangle \arrow[dl, dash] \arrow[dr, dash] \arrow[dd, dash, dashed] & \\
\langle 2 \rangle \arrow[dr, dash] & & \langle 3 \rangle \arrow[dl, dash] \\
 & \langle 6 \rangle &
\end{tikzcd}$$

The lines are inclusions, and the number of elements decreases as you go down. Note that this is exactly the lattice of divisibility by **Theorem 1.7.38** part 4.

$$\begin{tikzcd}
 & 6 \arrow[dl, dash] \arrow[dr, dash] \arrow[dd, dash, dashed] & \\
3 \arrow[dr, dash] & & 2 \arrow[dl, dash] \\
 & 1 &
\end{tikzcd}$$

Note that the dotted line is optional, as it can be deduced from the other lines.

Example 1.7.41. Consider $\mathbf{Z}/8\mathbf{Z}$. The divisors of 8 are 1, 2, 4, and 8. Since 8 is a power of a prime, the lattice is uninteresting:

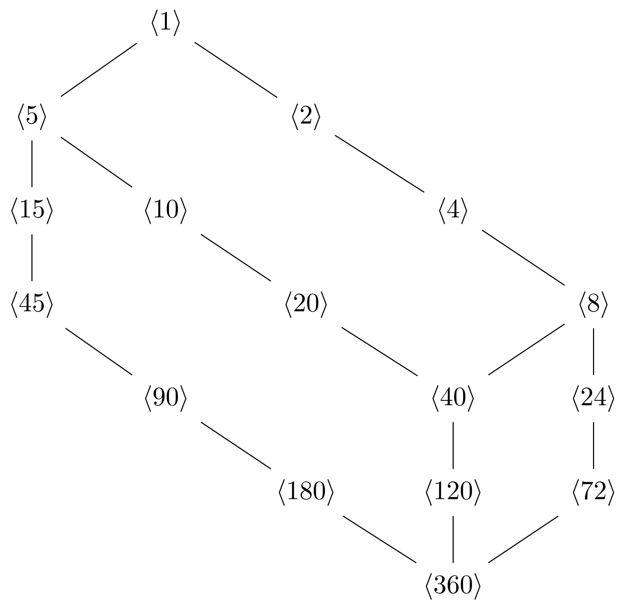
$$\begin{tikzcd}
\langle 1 \rangle \arrow[d, dash] & 8 \arrow[d, dash] \\
\langle 2 \rangle \arrow[d, dash] & 4 \arrow[d, dash] \\
\langle 4 \rangle \arrow[d, dash] & 2 \arrow[d, dash] \\
\langle 8 \rangle & 1
\end{tikzcd}$$

Indeed, in the case that $G = \mathbf{Z}/p^k\mathbf{Z}$ where p is prime, the lattice of subgroups of G is just a tower.

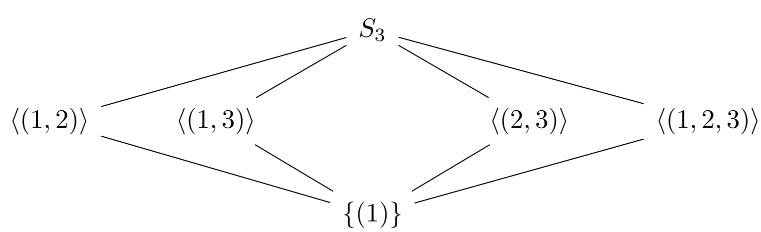
Example 1.7.42. In general, the lattice can be seen to be cubes of high dimensions. If our group is $\mathbf{Z}/30\mathbf{Z}$, then as $30 = 2 \cdot 3 \cdot 5$, we have

$$\begin{tikzcd}
 & \langle 1 \rangle \arrow[dl, dash] \arrow[dr, dash] \arrow[drrr, dash] & & & & \\
\langle 2 \rangle \arrow[dr, dash] \arrow[drrr, dash] & & \langle 3 \rangle \arrow[dl, dash] \arrow[drrr, dash] & & \langle 5 \rangle \arrow[dl, dash] \arrow[dr, dash] & \\
 & \langle 6 \rangle \arrow[drrr, dash] & & \langle 10 \rangle \arrow[dr, dash] & & \langle 15 \rangle \arrow[dl, dash] \\
 & & & & \langle 30 \rangle &
\end{tikzcd}$$

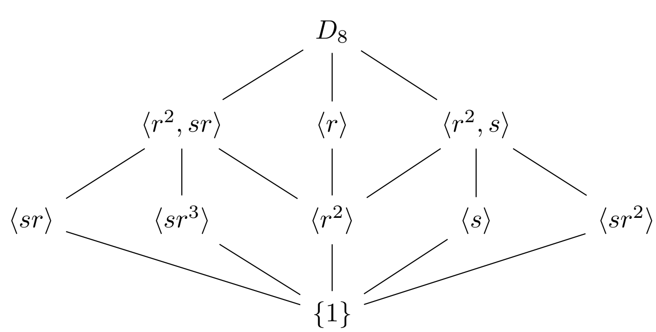
which is a cube. The lattice for $\mathbf{Z}/360\mathbf{Z}$ is also a cube, since $360 = 8 \cdot 9 \cdot 5$. The difference is that the edges of the cube will be subdivided into nodes since $8 = 2^3$ and $9 = 3^2$; that is, "viewing from only one angle" and not "subdividing faces" so as to keep the picture tidier,



Example 1.7.43. What about the lattice of subgroups of a general group; i.e., what if G is not cyclic? Let $G = S_3$. The cyclic subgroups of S_3 are $\langle(1,2,3)\rangle$, $\langle(1,2)\rangle$, $\langle(1,3)\rangle$, $\langle(2,3)\rangle$, and $\langle\emptyset\rangle$. Observe that all set of two elements where neither is trivial and not inverses of each other will generate S_3. All subgroups of S_3 are cyclic, even though S_3 is nonabelian.



Example 1.7.44. Consider $D_8 = \langle r, s\rangle$. The cyclic subgroups are $\langle r\rangle$, $\langle s\rangle$, $\langle sr\rangle$, $\langle sr^2\rangle$, $\langle sr^3\rangle$, $\langle r^2\rangle$, and $\{1\}$. The noncyclic subgroups are $\langle r^2, s\rangle \cong (\mathbf{Z}/2\mathbf{Z})^2$ and $\langle r^2, sr\rangle$. This turns out to be exhaustive.



Example 1.7.45. The lattice of subgroups of Q_8 is

$$\begin{tikzcd}
 & Q_8 \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\langle i \rangle \arrow[dr, dash] & \langle j \rangle \arrow[d, dash] & \langle k \rangle \arrow[dl, dash] \\
 & \langle -1 \rangle \arrow[d, dash] & \\
 & \{1\} &
\end{tikzcd}$$

Proposition 1.7.46. *Let $\varphi : G \to H$ be a homomorphism of groups. Then*

1. *φ respects identities, inverses, and exponents,*
2. *$\operatorname{im} \varphi$ is a subgroup of H, and*
3. *$\ker \varphi$ is a subgroup of G.*

Lemma 1.7.47. *Let $\varphi : G \to H$. $\ker \varphi = \{1\}$ if and only if φ is injective.*

Proof. First, if φ is injective, then at most one element is in $\ker \varphi$. Since $1 \in \ker \varphi$ by **Proposition 1.7.46**, $\ker \varphi = \{1\}$.

Now, let $g, h \in G$ and assume $\varphi(g) = \varphi(h)$. Then $\varphi(g)\varphi(h)^{-1} = 1$, so $\varphi(gh^{-1}) = 1$, and $gh^{-1} \in \ker \varphi = \{1\}$, so $gh^{-1} = 1$, and thus $g = h$. $\square$

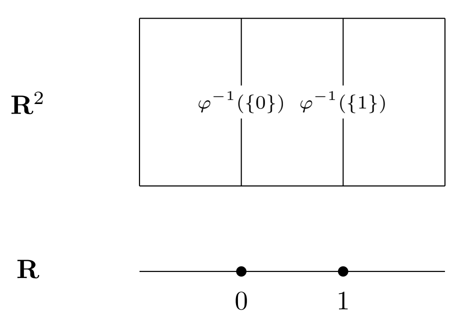
1.8 Quotients

Definition 1.8.1 (group quotient by kernel)**.** Suppose $\varphi : G \to H$ is a homomorphism with kernel K. Then the set of fibers of φ (point preimages) forms a group, denoted G/K.

Definition 1.8.2 (fiber)**.** Let $\varphi : G \to H$. We define a **fiber** $x \in G/K$ to be a subset of G such that $x = \varphi^{-1}(\{h\})$ for some $h \in H$.

Remark 1.8.3. The product on G/K is defined by $\varphi^{-1}(\{g\})\varphi^{-1}(\{h\}) = \varphi^{-1}(\{gh\})$. Note that $\varphi^{-1}(\{g\})$ determines a fiber uniquely. Thus the product is well-defined.

Example 1.8.4. Define $\varphi : \mathbf{R}^2 \to \mathbf{R}$ by $\varphi(x, y) = x$. This is a homomorphism, as it is linear. Let $K = \ker \varphi = \{(0, y) \mid y \in \mathbf{R}\}$. Then $\mathbf{R}/K$ is illustrated by the following picture:



One can observe that $\varphi^{-1}(\{n\}) = \{(n, y) \mid y \in \mathbf{R}\} \in \mathbf{R}^2/K$, and $\mathbf{R}^2/K \cong \mathbf{R}$.

Lemma 1.8.5. *Let G be a group. Suppose $\sim$ is an equivalence relation on G such that for all $a, b, c, d \in G$, if $a \sim b$ and $c \sim d$, then $ac \sim bd$. Set $N = \{a \in G \mid a \sim 1\}$.*

1. *N is a normal subgroup of G, and*
2. *$a \sim b$ if and only if $aN = bN$.*

Remark 1.8.6. We want to define a product on $G/\sim$ by $[a][c] = [ac]$. The hypotheses in **Lemma 1.8.5** ensure this.

Definition 1.8.7 (normal subgroup)**.** N is a **normal subgroup** of G, written $N \trianglelefteq G$, if for all $g \in G$, $gNg^1 = N$.

Definition 1.8.8 (coset)**.** Let $H \leq G$. The **left coset** of H by $g \in G$ is the set $gH = \{gx \mid x \in H\}$. The **right coset** Hg is defined similarly, but not often used.

Remark 1.8.9. If $\varphi : G \to H$ is a homomorphism, then $\sim$ on G defined by $a \sim b$ if and only if $\varphi(a) = \varphi(b)$ is an equivalence relation that satisfies the hypotheses in **Lemma 1.8.5**.

Proof of ***Lemma 1.8.5****, part 1.* We need to show N as defined is a normal subgroup. For $N \leq G$, $1 \in N$ since $1 \sim 1$. Next, let $a \in N$. We show that $a^{-1}N$. Since $a \sim 1$ and $a^{-1} \sim a^{-1}$, we have $a^{-1}a \sim a^{-1}1$, so $a^{-1} \sim 1$, and thus $a^{-1} \in N$. Finally, let $a, b \in N$. We show $ab \in N$. Since $a \sim 1$ and $b \sim 1$, we get $ab \sim 1 \cdot 1 = 1$. Thus $ab \in N$, and $N \leq G$ as claimed.

To see that N is normal, let $g \in G$ and let $a \in N$. Then $a \sim 1$, $g \sim g$, and $g^{-1} \sim g^{-1}$, so we see that $gag^{-1} \sim g1g^{-1} = 1$. Thus, $gag^{-1} \in N$, and hence $gNg^{-1} \subseteq N$. For the other inclusion, switch g with g^{-1} to see that $g^{-1}Ng \subseteq N$, and therefore $N = g(g^{-1}Ng)g^{-1} \subseteq gNg^{-1}$. Thus, $gNg^{-1} = N$, so $N \trianglelefteq G$, as desired. $\square$

Lemma 1.8.10. *If $\varphi : G \to H$ is a homomorphism, then $\ker \varphi \trianglelefteq G$.*

Proof. We know $\ker \varphi \leq G$ by **Proposition 1.7.46**. Let $g \in G$ and let $a \in \ker \varphi$. Since $\varphi(a) = 1$, we see that

$$\varphi(gag^{-1}) = \varphi(g)\varphi(a)\varphi(g)^{-1} = 1.$$

Thus for all $g \in G$, $g \ker \varphi g^{-1} \subseteq \ker \varphi$. It the follows that $g \ker \varphi g^{-1} = \ker \varphi$ by the argument in the proof of **Lemma 1.8.5**; switch g and g^{-1}. $\square$

Proposition 1.8.11. *Let $H \leq G$. Let $x, y \in G$. The following are equivalent.*

1. *x and y are in the same coset of H,*
2. *$x \in yH$,*
3. *$y \in xH$,*
4. *$xH = yH$,*
5. *$y^{-1}x \in H$, and*
6. *$x^{-1}y \in H$.*

Remark 1.8.12. Cosets are orbits (**Definition 1.11.6**), which are equivalence classes that partition a group. They are hence either completely disjoint or completely equal.

Proposition 1.8.13. *Let $N \leq G$. The following are equivalent.*

1. *$N \trianglelefteq G$; i.e., for all $g \in G$, $gNg^{-1} = N$,*
2. *$N_G(N) = G$,*
3. *for all $g \in G$, $gN = Ng$, and*
4. *for all $g \in G$, $gNg^{-1} \subseteq N$.*

Lemma 1.8.14. *Suppose $G = \langle S \rangle$ and $N \leq G$ where $N = \langle T \rangle$. Suppose for all $s \in S$ and $t \in T$, $sts^{-1} \in N$ and $s^{-1}ts \in N$. Then $N \trianglelefteq G$.*

Proof. Use condition 4 in **Proposition 1.8.13**. Let $g \in G$ and let $a \in N$. We wish to show $gag^{-1} \in N$. Since $g = {s_1}^{p_1} \cdots {s_n}^{p_n}$ and $a = {t_1}^{q_1} \cdots {t_m}^{q_m}$,

$$\begin{aligned} gag^{-1} &= {s_1}^{p_1} \cdots {s_n}^{p_n} {t_1}^{q_1} \cdots {t_m}^{q_m} {s_n}^{-p_n} \cdots {s_1}^{-p_1} \\ &= {s_1}^{p_1} \cdots {s_n}^{p_n} {t_1}^{q_1} {s_n}^{-p_n} \cdots {s_n}^{p_n} {t_m}^{q_m} {s_n}^{-p_n} \cdots {s_1}^{-p_1} \\ &= \cdots \end{aligned}$$

Proceed via induction. $\square$

Proof of ***Lemma 1.8.5****, part 2.* Suppose $a, b \in G$ and $a \sim b$. We need to show $aN = bN$, so we proceed via a double inclusion argument. Let $g \in aN$. Let $x \in N$ such that $g = ax$. Notice that $g = bb^{-1}ax = b(b^{-1}ax)$. Since $a \sim b$, $b^{-1}a \sim 1$, so $b^{-1}a \in N$. Hence $b(b^{-1}ax) \in bN$. Thus $aN \subseteq bN$. But by symmetry, $aN \supseteq bN$, so $aN = bN$.

In the other direction, suppose $aN = bN$. Then $ba^{-1} \in N$, so $b^{-1}a \sim 1$, and thus $a \sim b$, as desired. □

Remark 1.8.15. Lemma 1.8.5 is handy for motivating normal subgroups; it says we should consider normal subgroups and quotients rather than equivalence relations, though equivalence relations may at first seem more natural.

Definition 1.8.16 (quotient group)**.** Let G be a group and $N \trianglelefteq G$ a normal subgroup. Define the **quotient group** $G/N = \{gN \mid g \in G\}$. Define a product $G/N \times G/N \to G/N$ by $(gN)(hN) = (gh)N$.

Definition 1.8.17 (canonical projection)**.** Let $N \trianglelefteq G$. Define the **canonical projection** $\pi : G \to G/N$ by $\pi(g) = gN$.

Lemma 1.8.18. *The product on G/N is well-defined.*

Proof. Let $a, b, c, d \in G$ and assume $aN = bN$ and $cN = dN$. We need to show $(ac)N = (bd)N$.

Since $aN = bN$ and $cN = dN$, we know that $a^{-1}b, c^{-1}d \in N$. We can therefore show $(ac)^{-1}(bd) \in N$. To see thism we have $c^{-1}a^{-1}bd = c^{-1}a^{-1}bcc^{-1}d$. Since $a^{-1}b \in N$ and $c^{-1}a^{-1}bc$ is a conjugation of $a^{-1}b$, $c^{-1}a^{-1}bc \in N$ because N is normal. Since $c^{-1}d \in N$, the product $(c^{-1}a^{-1}bc)(c^{-1}d) \in N$, as desired. □

Theorem 1.8.19. *G/N is a group under the product that descended from G, and $\pi : G \to G/N$ is a surjective homomorphism with* $\ker \pi = N$.

Proof. G/N is associative because π is a homomorphism and G is a group:

$$\begin{aligned}(gNhN)kN &= (\pi(g)\pi(h))\pi(k) \\ &= \pi(gh)\pi(k) \\ &= \pi(ghk) \\ &= \pi(g)\pi(hk) \\ &= \pi(g)(\pi(h)\pi(k)) \\ &= gN(hNkN).\end{aligned}$$

The identity in G/N is $1N$, which follows from the definition. Finally, for inverses, for all $gN \in G/N$, if $hN = g^{-1}N$, then hN is the inverse for gN.

π is trivially surjective, and by the fact that if $g, h \in G$, then

$$\pi(gh) = (gh)N = (gN)(hN) = \pi(g)\pi(h),$$

π is a homomorphism. To show the claim that $\ker \pi = N$, use a double inclusion argument. First, if $g \in N$, then $\pi(g) = gN = 1N$, since $1^{-1}g \in N$. Thus $g \in \ker \pi$. On the other hand, if $g \in \ker \pi$, then $\pi(g) = 1N$, so $gN = 1N$ and thus $1^{-1}g \in N$, so $g \in N$. □

Corollary 1.8.20. *Every normal subgroup of a group is the kernel of some homomorphism.*

Remark 1.8.21. A priori, the computation $\pi(gh) = \pi(g)\pi(h)$ above shows that $\pi : G \to G/N$ is a homomorphism of *magmas*.

Definition 1.8.22 (magma)**.** A **magma** is a set with a binary product.

☡ **Warning! 1.8.23.** If $N \trianglelefteq H$ and $H \trianglelefteq G$, that it is not necessarily the case that $N \trianglelefteq G$.

Example 1.8.24. Consider the case that $G = D_8$ and $H = \langle r^2, s \rangle$. Here $H \trianglelefteq G$. If $N = \langle s \rangle$, then $N \trianglelefteq H$, as H is abelian. But $N \ntrianglelefteq G$, and $rsr^{-1} = r^2s \notin N$.

Example 1.8.25. Let $G = D_8$ and $N = \langle r^2 \rangle$. Then $N \trianglelefteq G$. Hence

$$\begin{aligned} G/N &= \{gN \mid g \in G\} \\ &= \{\{1, r^2\}, \{r, r^3\}, \{s, sr^2\}, \{sr, sr^3\}\} \\ &= \{[1], [r], [s], [sr]\} \\ &= \{1N, rN, sN, srN\}. \end{aligned}$$

We can write the multiplication table of G/N.

G/N	1	r	s	sr
1	1	r	s	sr
r	r	1	sr	s
s	s	sr	1	r
sr	sr	s	r	1

By observation, $D_8/\langle r^2 \rangle \cong (\mathbf{Z}/2\mathbf{Z})^2$.

1.9 The Index of a Group and Lagrange's Theorem

Theorem 1.9.1 (Lagrange's Theorem)**.** *Let G be a group and H a subgroup of G. Then $|H|$ divides $|G|$, and the number of left cosets of H in G is $|G|/|H|$.*

Remark 1.9.2. $gH = \{gh \mid h \in H\}$ is the orbit of g under the action of H on G on the *right* by multiplication (**Definition 1.11.6**). Cosets/orbits partition the group/set, and cosets are in bijection with each other.

Definition 1.9.3 (index)**.** Let G be a group and $H \leq G$. The **index** of H in G is the number of left cosets of H in G, written $|G : H|$ or $[G : H]$.

Remark 1.9.4. Thus **Theorem 1.9.1 [Lagrange's Theorem]** states that $[G : H] = |G|/|H|$.

☡ **Warning! 1.9.5. Theorem 1.9.1 [Lagrange's Theorem]** is not true for monoids (recall **Definition 1.2.8**)! The fact that cosets are in bijection relies on the existence of inverses.

Corollary 1.9.6. *Let G be a group and let $x \in G$. Then $|x|$ divides $|G|$. If $|G| < \infty$, then $x^{|G|} = 1$.*

Proof. Observe that $|x| = |\langle x \rangle|$. By **Theorem 1.9.1 [Lagrange's Theorem]**, $|\langle x \rangle|$ divides $|G|$. ☐

Corollary 1.9.7. *If p is prime and G is a group with order p, then G is cyclic and therefore $G \cong \mathbf{Z}/p\mathbf{Z}$.*

Proof. Since p is prime, $p \geq 2$, so $G \setminus \{1\} \neq \emptyset$. Let $x \in G \setminus \{1\}$. Consider $\langle x \rangle \leq G$. Since $x \neq 1$, $|\langle x \rangle| > 1$. By **Theorem 1.9.1 [Lagrange's Theorem]**, $|\langle x \rangle|$ divides $|G| = p$, a prime. Therefore $|\langle x \rangle| = p$, so $\langle x \rangle = G$, and hence G is cyclic. By **Theorem 1.7.33 [The classification of cyclic groups]**, $G \cong \mathbf{Z}/p\mathbf{Z}$. ☐

Remark 1.9.8. The strongest possible converse to **Theorem 1.9.1 [Lagrange's Theorem]** fails; there is a group of order 12 with no subgroup of order 6. Let

$$A_4 = \{\sigma \in S_4 \mid \text{ the cycle decomposition of } \sigma \text{ is } (\bullet, \bullet, \bullet),\ (\bullet, \bullet)(\bullet, \bullet), \text{ or } (1)\}.$$

A_4 is a group, and $|A_4| = 12$ via counting arguments. To see that A_4 is a group, you can look at even/odd permutations (**Definitions 1.12.35** and **1.12.36**), or we can look at permutation matrices; e.g., $(1, 2, 3)$ corresponds to

$$\begin{bmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

We have homomorphisms $\varphi : S_n \to GL_nF$ and $\det : GL_nF \to \{-1, 1\}$. Then A_4 is the kernel of the composition of these homomorphisms, and thus a group. One can check that any two 3-cycles that are not inverses of each other, or any 3-cycle and any cycle of the form $(\bullet,\bullet)(\bullet,\bullet)$ generate A_4. Show that each form can generate 7 elements, and therefore by **Theorem 1.9.1 [Lagrange's Theorem]**, all of A_4.

We can therefore enumerate all subgroups by generating sets. If our generating set includes two 3-cycles or a 3-cycle and $(\bullet,\bullet)(\bullet,\bullet)$, then it will be A_4. If not, they will be too small; i.e., A_4 only has subgroups of order 1, 2, 3, 4, and 12. No subgroup of order 6 exists.

There are, however, special case converses: **Theorem 1.9.11 [Cauchy's Theorem]** and **Theorem 1.9.12 [Sylow's Theorem]** are two such, to come.

Theorem 1.9.9. *If $H \leq G$ and $[G:H]=2$, then $H \trianglelefteq G$.*

Proof. Cosets of H in G are $H = 1H$ and $G \setminus H = xH$ for any $x \notin H$. Thus we can classify the cosets by membership of H alone and need not reference left multiplication at all. Therefore, for all $x \in G$, $xH = Hx$, and by **Proposition 1.8.13**, condition 3, H is normal in G. □

Remark 1.9.10. We can use **Theorem 1.9.9** to prove the claims in **Remark 1.9.8** as well. Suppose $H \leq A_4$ and that $|H| = 6$. Then by **Theorem 1.9.9**, $H \trianglelefteq A_4$. There exists at least one $(a,b,c) \in H$. Since H is normal, for all $\sigma \in A_4$, $\sigma(a,b,c)\sigma^{-1} \in H$, but $\sigma(a,b,c)\sigma^{-1} = (\sigma(a),\sigma(b),\sigma(c))$. Therefore we can conclude that in a normal subgroup of A_4, if we have one 3-cycle, then we have many, and thus we can deduce that $|H| \geq 7$, a contradiction.

Theorem 1.9.11 (Cauchy's Theorem)**.** *If $|G| < \infty$ and p is a prime such that p divides $|G|$, then there exists $x \in G$ such that $|x| = p$ (and thus $p = |\langle x\rangle|$ for $\langle x\rangle \leq G$).*

Theorem 1.9.12 (Sylow's Theorem)**.** *If p is prime, $a \in \mathbf{Z}$, $|G| < \infty$, p^a divides $|G|$, and p^{a+1} does not divide $|G|$, then there exists $H \leq G$ such that $|H| = p^a$.*

Furthermore, if G is abelian, then if n divides $|G|$, then G does have a subgroup of order n.

Additionally, if $|G| = p^n$ for a prime p, then there is a subgroup of any order that divides p^n.

Definition 1.9.13 (concatenation set)**.** If $H, K \leq G$, then define $HK = \{hk \mid h \in H, k \in K\}$.

☡ **Warning! 1.9.14.** In general, $HK \not\leq G$ and $HK \neq \langle H \cup K\rangle$.

Example 1.9.15. Let $G = S_3$, $H = \langle(1,2)\rangle$, and $K = \langle(2,3)\rangle$. Then $HK = \{(1),(1,2),(2,3),(1,2,3)\}$. Note that $|HK| = 4$, and 4 does not divide $|S_3| = 6$, so by **Theorem 1.9.1 [Lagrange's Theorem]**, $HK \not\leq S_3$.

Remark 1.9.16. Notice that

$$HK = \bigcup_{h\in H} hK.$$

Lemma 1.9.17. *Let $H, K \leq G$. Then*

$$|HK| = \frac{|H|\cdot|K|}{|H\cap K|}.$$

Proof. By **Remark 1.9.16**,

$$|HK| = \left|\bigcup_{h\in H} hK\right| = x|K|,$$

where x is the number of distinct cosets hK for $h \in H$. There are $|H|$ formal expressions hK, but given $h_1 \in H$, how many $h_2 \in H$ exist such that $h_1K = h_2K$?

Suppose $h_1K = h_2K$. This is the case if and only if ${h_2}^{-1}h_1 \in K$, if and only if ${h_2}^{-1}h_1 \in H \cap K$, if and only if $h_1(H\cap K) = h_2(H \cap K)$, if and only if $h_2 \in h_1(H\cap K)$.

Thus, the number of choices of h_2 satisfying above is $|h_1(H\cap K)| = |H\cap K|$. Therefore, $x = |H|/|H\cap K|$. This is an integer by **Theorem 1.9.1 [Lagrange's Theorem]**. Therefore, the result is shown. □

Lemma 1.9.18. *Let $H, K \leq G$ and suppose $H \leq N_G(K)$. We say that H* normalizes *K. (By right-left symmetry, K can normalize H too.) If H normalizes K, then $HK \leq G$.*

Proof. By **Lemma 1.7.7 [First subgroup criterion]**.

$1 = 1 \cdot 1 \in HK$, so $HK \neq \emptyset$.

Next, suppose $h_1, h_2 \in H$ and $k_1, k_2 \in K$. We wish to show $h_1k_1h_2k_2 \in HK$. Observe

$$\begin{aligned} h_1k_1h_2k_2 &= h_1h_2{h_2}^{-1}k_1h_2k_2 \\ &= (h_1h_2)(({h_2}^{-1}k_1h_2)k_2). \end{aligned}$$

Since $H \leq N_G(K)$, ${h_2}^{-1}k_1h_2 \in K$. Since H and K are groups, $h_1h_2 \in H$ and $({h_2}^{-1}k_1h_2)k_2 \in K$. Thus, $h_1k_1h_2k_2 \in HK$.

Finally, suppose $h \in H$ and $k \in K$. Then

$$(hk)^{-1} = k^{-1}h^{-1} = h^{-1}hk^{-1}h^{-1} = h^{-1}(hk^{-1}h^{-1}) \in HK,$$

since $h^{-1} \in H$, $k^{-1} \in K$ as H and K are groups, and $hk^{-1}h^{-1} \in K$ as $H \leq N_G(K)$.

Thus, $HK \leq G$, as claimed. □

1.10 The Isomorphism Theorems

Theorem 1.10.1 (The First Isomorphism Theorem)**.** *Suppose $\varphi : G \to H$ is a homomorphism. Then*

$$G/\ker\varphi \cong \varphi(G).$$

Proof. The proof will follow from the following stronger result in **Lemma 1.10.2**. □

Lemma 1.10.2. *Suppose $\varphi : G \to H$ is a homomorphism. Then let $K = \ker\varphi$, and we have a commutative diagram*

$$\begin{tikzcd} G \arrow[r, "\varphi"] \arrow[d, "\pi"'] & H \\ G/K \arrow[r, "\overline{\varphi}", "\sim"'] & \varphi(G) \arrow[u, hook, "i"'] \end{tikzcd}$$

There is an isomorphism $\overline{\varphi} : G/K \to \varphi(G)$ such that the diagram commutes; i.e., $\varphi = i \circ \overline{\varphi} \circ \pi$.

Proof. Define $\overline{\varphi} : G/K \to \varphi(G)$ by $\overline{\varphi}(aK) = \varphi(a)$. This is well-defined, as if $aK = bK$, then $\overline{\varphi}(aK) = \varphi(a)$ and as $a^{-1}b \in K$, $\varphi(a) = \varphi(a)\varphi(a^{-1}b) = \varphi(aa^{-1}b) = \varphi(b) = \overline{\varphi}(bK)$.

Furthermore, $\overline{\varphi}$ is a homomorphism, since $\overline{\varphi}(aKbK) = \overline{varphi}(abK) = \varphi(a)\varphi(b) = \overline{\varphi}(aK)\overline{\varphi}(bK)$. Also, $\overline{\varphi}$ is surjective by construction, and injective because $\ker\overline{\varphi} = \{e\}$.

All that remains follow from the fact that indeed

$$(i \circ \overline{\varphi} \circ \pi)(a) = (i \circ \overline{\varphi})(aK) = i(\varphi(a)) = \varphi(a).$$

□

Remark 1.10.3. If you know all normal subgroups of G, all subgroups of H, and all isomorphisms between quotients of G and subgroups of H, then you know all homomorphisms $G \to H$. For instance, one could find all homomorphisms from Q_8 to D_8, of which there are many.

Example 1.10.4. Suppose p and q are prime numbers. Suppose that $\varphi : \mathbf{Z}/p\mathbf{Z} \to \mathbf{Z}/q\mathbf{Z}$ is a homomorphism. Then either φ is trivial, i.e., constantly 0, or $p = q$ and φ is an isomorphism. To see this, note that the only subgroups of $\mathbf{Z}/p\mathbf{Z}$ are $\{0\}$ and $\mathbf{Z}/p\mathbf{Z}$, by **Theorem 1.9.1 [Lagrange's Theorem]**. Similarly for q. There are two cases for $\ker\varphi$. If $\ker\varphi = \mathbf{Z}/p\mathbf{Z}$, then φ is trivial. If $\ker\varphi = \{0\}$, then φ is an embedding; i.e., it is injective. Thus $\mathbf{Z}/q\mathbf{Z}$ has a subgroup isomorphic to $\mathbf{Z}/p\mathbf{Z}$. Since $p > 1$, $\varphi(\mathbf{Z}/p\mathbf{Z}) \neq \{0\}$, so $p = q$ and therefore $\varphi(\mathbf{Z}/p\mathbf{Z}) = \mathbf{Z}/q\mathbf{Z}$, so φ is surjective too.

Theorem 1.10.5 (The Second Isomorphism Theorem)**.** *Suppose $A, B \leq G$ and $A \subseteq N_G(B)$. Then $AB \leq G$, $B \trianglelefteq AB$, $A \cap B \trianglelefteq A$, and*

$$AB/B \cong A/A \cap B.$$

Proof. First, note that $AB \leq G$ follows from **Lemma 1.9.18**, and the normal subgroup claims are easy. Next, define $\varphi : A \to AB/B$ by $\varphi(a) = aB$. Then φ is well-defined, and φ is a homomorphism since

$$\varphi(a_1a_2) = a_1a_2B = a_1Ba_2B = \varphi(a_1)\varphi(a_2).$$

Notice that φ is surjective. To see this, let $(ab)B \in AB/B$; then $a \in A$, $b \in B$, and $\varphi(a) = aB = (ab)B$, since $(ab)^{-1}a = b^{-1} \in B$.

Finally, we show that $\ker\varphi = A \cap B$. To see this, let $x \in A \cap B$. Then $\varphi(x) = xB = 1B$, since $1^{-1}x = x \in B$. On the other hand, let $x \in \ker\varphi \subseteq A$. Also $\varphi(x) = xB = 1B$, so $1^{-1}x \in B$, and thus $x \in A \cap B$.

Therefore, by **Theorem 1.10.1 [The First Isomorphism Theorem]**, $A/(A \cap B) \cong AB/B$. $\square$

Example 1.10.6. Let $G = \mathbf{R}^3$ with addition. Let $A = \operatorname{span}_{\mathbf{R}}(e_1, e_3)$ and $B = \operatorname{span}_{\mathbf{R}}(e_2, e_3)$. See that $A + B = \{a + b \mid a \in A, b \in B\} = \operatorname{span}_{\mathbf{R}}(e_1, e_2, e_3) = \mathbf{R}^3$. (Note that $A + B$ is the additive notation version of AB.) Also see that $A \cap B = \operatorname{span}_{\mathbf{R}}(e_3)$. Thus

$$A + B\big/B = \mathbf{R}^3\big/\operatorname{span}_{\mathbf{R}}(e_2, e_3) = \mathbf{R}, \text{ and}$$
$$A\big/A \cap B = \operatorname{span}_{\mathbf{R}}(e_1, e_3)\big/\operatorname{span}_{\mathbf{R}}(e_3) = \mathbf{R}.$$

For an explicit isomorphism, map A to $(A+B)/B$ by $xe_1 + ye_2 \mapsto (xe_1 + ye_2) + B$. This is a homomorphism, and the kernel is $A \cap B$. Thus, by **Theorem 1.10.1 [The First Isomorphism Theorem]**, we see that $A/(A \cap B) \cong (A + B)/B$.

Theorem 1.10.7 (The Third Isomorphism Theorem)**.** *Suppose $H, K \trianglelefteq G$ with $K \leq H$. Then $K \trianglelefteq H$ and $H/K \trianglelefteq G/K$. Furthermore,*

$$\frac{\left(G\big/K\right)}{\left(H\big/K\right)} \cong G\big/H.$$

Proof. The fact that $K \trianglelefteq H$ is obvious. Next, suppose $hK \in H/K$ and $gK \in G/K$. To see $H/K \trianglelefteq G/K$, see that

$$(gK)(hK)(gK)^{-1} = (ghg^{-1})K \in H\big/K,$$

because $ghg^{-1} \in H$ since $H \trianglelefteq G$.

Finally, to show $(G/K)/(H/K) \cong G/H$, define $\varphi : G/K \to G/H$ be $\varphi(gK) = gH$. φ is well-defined, but not necessarily obviously so. To see that it is, suppose $g_1K = g_2K$. Then ${g_2}^{-1}g_1 \in K$. Since $K \subseteq H$, ${g_2}^{-1}g_1 \in H$, so $g_1H = g_2H$. Now, φ is obviously surjective, and one can show that $\ker\varphi = H/K$. Via an application of **Theorem 1.10.5 [The Second Isomorphism Theorem]**, $(G/K)/(H/K) \cong G/H$, as desired. $\square$

Example 1.10.8. Let $G = \mathbf{Z}/8\mathbf{Z}$, $N = \langle 4\rangle$, and $H = \langle 2\rangle$. Then $H/N \trianglelefteq G/N$, and $(G/N)/(H/N) \cong G/H$. We know that

$$G\big/N = \{N, 1 + N, 2 + N, 3 + N\} \text{ and}$$
$$H\big/N = \{N, 2 + N\}.$$

Thus

$$\frac{\left(G\big/N\right)}{\left(H\big/N\right)} = \left\{H\big/N, (1 + N) + H\big/N\right\},$$

where $(1 + N) + H/N = \{1 + N, 3 + N\} = \{\{1, 5\}, \{3, 7\}\}$. Also, see that $G/H = \{H, 1 + H\}$.

We are done as there is a unique group of order 2, but suppose we want to build an explicit isomorphism. We wish to define $\varphi : G/N \to G/H$ by $\varphi(gN) = gH$. Why should this be well-defined? See that if $gN = hN$, then we claim $gH = hH$. Indeed, we know $h^{-1}g \in N$ and $N \leq H$, so $h^{-1}g \in H$, and therefore $gH = hH$, as desired.

Note that $\varphi(gN) = gH = \pi_H(g)$, where π_H is the quotient projection $\pi_H : G \to G/H$. This leads to the following result:

Lemma 1.10.9. *Let $\Phi : G \to H$ be a homomorphism. Let $N \trianglelefteq G$. Define $\varphi : G/N \to H$ by $\varphi(gN) = \Phi(g)$. φ is well-defined if and only if $N \leq \ker \Phi$. This is the universal property of a quotient.*

$$\begin{tikzcd} G \arrow[r, "\Phi"] \arrow[dr, "\pi"'] & H \\ & G/N \arrow[u, dashed, "\varphi"'] \end{tikzcd}$$

Proof. Assume $N \leq \ker \Phi$. Let $g, h \in G$ such that $gN = hN$. We need to show that $\varphi(gN) = \varphi(hN)$. Since $h^{-1}g \in N \leq \ker \Phi$, $\Phi(h^{-1}g) = 1_H$, so $\Phi(h)^{-1}\Phi(g) = 1_H$, and therefore $\Phi(g) = \Phi(h)$, as desired.

The other direction follows via proof by contrapositive. $\square$

Theorem 1.10.10 (The Fourth Isomorphism Theorem)**.** *Let G be a group and $N \trianglelefteq G$. There is a bijection between*

$$\{H \mid H \leq G, N \leq H\} \leftrightarrow \left\{K \mid K \leq G/N\right\},$$

where $H \mapsto H/N$. Moreover, this bijection respects all *the structure of the subgroup lattice; i.e.,*

- *$H_1 \leq H_2$ if and only if $H_1/N \leq H_2/N$,*
- *if so, $[H_2 : H_1] = [H_2/N : H_1/N]$,*
- *$H_1 \trianglelefteq H_2$ if and only if $H_1/N \trianglelefteq H_2/N$,*
- *if so, $H_2/H_1 \cong (H_2/N)/(H_1/N)$,*
- *$(H_1 \cap H_2)/N = (H_1/N) \cap (H_2/N)$,*
- *$\langle H_1 \cup H_2\rangle/N = \langle (H_1/N) \cup (H_2/N)\rangle$.*

Example 1.10.11. Let $G = \langle a, b \mid a^4 = 1, b^4 = 1, bab^{-1} = a^{-1}\rangle$. One can check that as a set, we have $G = \{a^i b^j \mid i, j \in \{0, 1, 2, 3\}\}$, and $|G| = 16$. This is a twisted semidirect product (**Definition ??**) of $\mathbf{Z}/2\mathbf{Z}$ and $\mathbf{Z}/4\mathbf{Z}$. Let $N = \langle a^2b^2\rangle$. To see that $N \trianglelefteq G$, observe that

$$\begin{aligned} &aa^2b^2a^{-1} = a^2bb^2b^{-1} = a^2b^2, \\ &a^{-1}a^2b^2a = a^2b^2, \\ &ba^2b^2b^{-1} = a^2b^{-2} = a^2b^2, \text{ and} \\ &b^{-1}a^2b^2b = a^2b^2, \end{aligned}$$

so a^2b^2 is central. Next, $G/N = \langle \overline{a}, \overline{b} \mid \overline{a}^4 = 1, \overline{b}^4 = 1, \overline{b}\overline{a}\overline{b}^{-1} = \overline{a}^{-1}, \overline{a}^2\overline{b}^2 = 1\rangle$. Realizing the relation $\overline{a}^2\overline{b}^2 = 1$ as $\overline{a}^2 = \overline{b}^{-2}$ and then as $\overline{a}^2 = \overline{b}^2$, we can see that $G/N \cong Q_8$ (**Remark 1.4.2**).

The lattice is

$$\begin{tikzcd} & G/N \arrow[dl, dash, "2"'] \arrow[d, dash, "2"] \arrow[dr, dash, "2"] & \\ \langle \overline{a} \rangle \arrow[dr, dash, "2"'] & \langle \overline{b} \rangle \arrow[d, dash, "2"] & \langle \overline{a}\overline{b} \rangle \arrow[dl, dash, "2"] \\ & \langle \overline{a}^2 \rangle \arrow[d, dash, "2"] & \\ & \langle \overline{1} \rangle & \end{tikzcd}$$

where the numbers on each edge indicate the index (**Definition 1.9.3**) of the subgroup.

By **Theorem 1.10.10 [The Fourth Isomorphism Theorem]**, we have an incomplete lattice

$$\begin{tikzcd}
 & G \arrow[dl, dash, "2"'] \arrow[d, dash, "2"] \arrow[dr, dash, "2"] & \\
\langle a, a^2b^2\rangle \arrow[dr, dash, "2"'] & \langle b, a^2b^2\rangle \arrow[d, dash, "2"] & \langle ab, a^2b^2\rangle \arrow[dl, dash, "2"] \\
 & \langle a^2, a^2b^2\rangle \arrow[d, dash, "2"] & \\
 & \langle a^2b^2\rangle \arrow[d, dash, "2"] & \\
 & \langle 1\rangle &
\end{tikzcd}$$

The lattice is incomplete because we only see subgroups that contain a^2b^2. For instance, $\langle a\rangle$ does not appear.

Also, for instance, $(G/N)/\langle \overline{a}^2\rangle \cong (\mathbf{Z}/2\mathbf{Z})^2 \cong G/\langle a^2, a^2b^2\rangle$.

1.11 Group Actions

Definition 1.11.1 (group action)**.** Let G be a group and let A be a set. An **action** of G on A is a function $G \times A \to A$, $(g, a) \mapsto ga$, such that

1. for all $g, h \in G$ and $a \in A$, $g(ha) = (gh)a$, and
2. for all $a \in A$, $1a = a$.

Remark 1.11.2. Group actions are like scalar multiplication in vector spaces, but for groups.

Example 1.11.3. D_{2n} acts on the vertices $\{1, \dots, n\}$ by labeling vertices of the regular n-gon and applying isometries. $rk = k + 1$ if $k < n$ while $rn = 1$, and $sk = n + 2 - k \pmod{n}$.

Example 1.11.4. Let G act on A. Let $g \in G$. Define $\sigma_g : A \to A$ by $\sigma_g(a) = ga$. Note that σ_g is a permutation. Indeed, since $\sigma_g \circ \sigma_h = \sigma_{gh}$, one has ${\sigma_g}^{-1} = \sigma_{g^{-1}}$. Thus, σ_g is a bijection.

In fact, $\varphi : G \to \operatorname{Sym}(A)$ defined by $\varphi(g) = \sigma_g$ is a homomorphism. This is called the permutation representation of the action. We can conclude from **Example 1.11.3** that there is a homomorphism $\varphi : D_{2n} \to S_n$ defined by $\varphi(r) = (1, 2, 3, \dots, n)$ and $\varphi(s) = (1)(2, n)(3, n-1) \cdots (a, b)$, where

$$(a, b) = \begin{cases} \left(\frac{n}{2}, \frac{n}{2} + 1\right) & \text{if } n \text{ is even;} \\ \left(\frac{n+1}{2}, \frac{n+1}{2} + 1\right) & \text{if } n \text{ is odd.} \end{cases}$$

Lemma 1.11.5. *Actions of G on A are in bijection with homomorphisms $G \to \operatorname{Sym}(A)$. Moreover, sending the action to the permutation representation (**Example 1.11.4**) is the bijection.*

Proof. Let $\varphi : G \to \operatorname{Sym}(A)$ be any homomorphism. Define a function $G \times A \to A$ by $g \cdot a = (\varphi(g))(a)$. This is an action. □

Definition 1.11.6 (orbit)**.** Let G act on A and let $a \in A$. The **orbit** of a is $Ga = \{ga \mid g \in G\}$.

Definition 1.11.7 (transitive action)**.** Let G act on A. The action is **transitive** if there is only one orbit; i.e., for all $a \in A$, $Ga = A$.

Definition 1.11.8 (kernel of a group action)**.** Let G act on A. The **kernel** of the action is the subset $\{g \in G \mid \text{ for all } a \in A, g \cdot a = a\}$.

Definition 1.11.9 (faithful action)**.** Let G act on A. The action is **faithful** if its kernel is $\{1\}$.

Remark 1.11.10. The kernel of the group action is the same as the kernel of the associated homomorphism. That is, if $\alpha : G \times A \to A$ is a group action, then the kernel of α is the kernel of the permutation representation $\varphi : G \to \mathrm{Sym}(A)$ corresponding to α.

Example 1.11.11. Let G be any group. Let A be any set. Let $ga = a$ for all $g \in G$ and $a \in A$. This is a group action, since $g(ha) = a = (gh)a$ and $1 \cdot a = a$. It is called the *trivial* action. It is not transitive nor faithful.

Example 1.11.12. S_n acts on $\{1, \dots, n\}$ by $\sigma \cdot n = \sigma(n)$. To see this, $(1) \cdot n = n$, and $\sigma(\tau \cdot n) = (\sigma\tau) \cdot n$. Since $(1, k) \cdot 1 = k$ for all k, it follows that the action is transitive. It is also faithful, since the only way to send $\{1, \dots, n\}$ to $\{1, \dots, n\}$ without shuffling is the identity function.

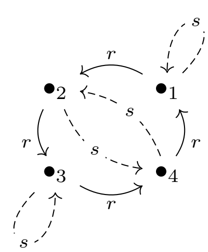
Example 1.11.13. Let F be a field and let V be an F-vector space. If F^* is the group $F \setminus \{0\}$ under multiplication, then F^* acts on V by scalar multiplication. This action is faithful. If $\mathbf{v} \neq 0$, then $s \cdot \mathbf{v} = \mathbf{v}$ implies $s = 1$. The action is transitive if and only if $\dim V = 1$.

Example 1.11.14. $GL_n F$ acts on F^n be matrix-vector multiplication on the left. This action is not transitive. The orbits are $\{0\}$ and $F^n \setminus \{0\}$. This action is faithful.

Example 1.11.15. Let $A = G$. Define $g \cdot h = gh$; i.e., the action is the group operation. We call this the *left regular* action. It is both faithful and transitive.

We get a homomorphism $\varphi : G \to \mathrm{Sym}(G)$ which is an embedding (i.e., it is an injective homomorphism onto its image). Cancellation makes the action faithful, and thus an embedding. This is **Corollary 1.11.19 [Cayley's Theorem]**, to come.

Example 1.11.16. Group actions can be visualized with graphs. For instance, consider D_8 acting on $\{1, 2, 3, 4\}$ as the following graph.



If there is an action where everything loops back, the action is not faithful. If your graph is connected, the action is transitive. Hence D_8 acting on $\{1, 2, 3, 4\}$ is faithful and transitive.

Theorem 1.11.17. *Let G be a group and let H be a subgroup of G. Let $A = \{xH \mid x \in G\}$. Let G act on A by left multiplication; i.e., $g \cdot (xH) = (gx)H$.*

1. *This action is transitive.*
2. *The stabilizer of $1H$ is $G_{1H} = H$.*
3. *The kernel of this action is*

$$\bigcap_{a \in G} aHa^{-1}.$$

Proof. For the first claim, let $aH, bH \in A$. We need to produce a $g \in G$ such that $gaH = bH$. This occurs if and only if $b^{-1}ga \in H$. Let $g = ba^{-1}$; then $b^{-1}ga = b^{-1}ba^{-1}a = 1 \in H$.

For the second claim, notice that $H \subseteq G_{1H}$, since $h \cdot 1H = hH = 1H$, as $1^{-1}h = h \in H$. It remains to see that $G_{1H} \subseteq H$. Suppose $g \in G_{1H}$, so $g \cdot 1H = 1H$, and therefore $gH = 1H$, so $1^{-1}g = g \in H$, as desired.

For the third claim, we first show that $G_{aH} = aHa^{-1}$. Indeed, $g \in aHa^{-1}$ if and only if there exists an $h \in H$ such that $g = aha^{-1}$. If so, $aha^{-1} \cdot aH = ahH = aH$, so $g \in G_{aH}$. Conversely, $gaH = aH$ if and only if $a^{-1}ga \in H$. Thus there exists $h \in H$ such that $a^{-1}ga = h$, so $g = aha^{-1}$, and therefore $g \in aHa^{-1}$. Thus $G_{aH} = aHa^{-1}$, and therefore the kernel of the action is

$$\bigcap_{a \in G} G_{aH} = \bigcap_{a \in G} aHa^{-1},$$

as claimed. □

Remark 1.11.18. Given any transitive action G acting on A, the action of G on A is the same as the action of G on $\{gG_a \mid g \in G\}$.

Corollary 1.11.19 (Cayley's Theorem)**.** *Let G be a group. There is an injective group homomorphism $G \to \mathrm{Sym}(G)$. Furthermore, if $|G| = n$, then G embeds in S_n.*

Proof. The group G acts on $G/\{1\} \leq G$ by left multiplication. Let $\pi : G \to \mathrm{Sym}(G)$ be the permutation representation of the action (**Example 1.11.4**). This means that for all $g \in G$, $\pi(g) \in \mathrm{Sym}(G)$ such that $(\pi(g))(a) = g \cdot a$. By **Theorem 1.11.17** with $H = \{1\}$ and $A = G/\{1\}$,

$$\ker \pi = \bigcap_{a \in G} a\{1\}a^{-1} = \{1\}.$$

□

Example 1.11.20. Consider D_8. The permutation representation of D_8 acting on itself is

$$\pi(r) = (1, r, r^2, r^3)(s, rs, r^2s, r^3s)$$

and

$$\pi(s) = (1, s)(r, r^3s)(r^2, r^2s)(r^3, rs).$$

Therefore by **Corollary 1.11.19 [Cayley's Theorem]**, $\langle \pi(r), \pi(s) \rangle \cong D_8 \leq \mathrm{Sym}(D_8) \cong S_8$.

Remark 1.11.21. One can check that $D_8 \leq S_n$ for all $n \geq 4$, but $Q_8 \leq S_n$ for all $n \geq 8$, and $Q_8 \not\leq S_7$.

Example 1.11.22. The group $\mathbf{Z}$ acting on itself has permutation representation $\pi : \mathbf{Z} \to \mathrm{Sym}(\mathbf{Z})$ such that $(\pi(1))(n) = n + 1$.

Corollary 1.11.23. *If $|G| = n$, $H \leq G$, and $|G : H| = p$, where p is the smallest prime dividing n, then $H \trianglelefteq G$.*

Proof. Let $\pi : G \to S_p$ be the permutation representation. Let $A = \{gH \mid g \in G\}$. We have $|A| = p$ by **Theorem 1.9.1 [Lagrange's Theorem]**. Furthermore, $\pi : G \to S_p \cong \mathrm{Sym}(A)$. Let $K = \ker \pi$. See that

$$|G : K| = |G : H| \cdot |H : K| = pk$$

for $k \in \mathbf{Z}$. By **Theorem 1.10.1 [The First Isomorphism Theorem]**, G/K is isomorphic to a subgroup of S_p, and $|G/K| = pk$. So $|G/K|$ divides $|S_p|$, so pk divides $p!$, and hence k divides $(p-1)!$. Since

$$|G| = |G : \{1\}| = |G : K| \cdot |K : \{1\}| = pk \cdot |K| = n,$$

k divides n as well. By hypothesis, p is the smallest prime dividing n, so k must be 1. Since $k = |H : K|$, $K = H$, and thus $H = \ker \pi$. Therefore $H \trianglelefteq G$, as desired. □

Corollary 1.11.24 (Alternate proof of **Theorem 1.9.9**)**.** *If G is finite, $H \leq G$, and $|G : H| = 2$, then $H \trianglelefteq G$.*

Example 1.11.25. If $|G| = 21$, $H \leq G$, and $|H| = 7$, then $H \trianglelefteq G$, since $|G : H| = 3$ which is the smallest prime dividing 21.

Theorem 1.11.26 (The Orbit Stabilizer Theorem)**.** *Let G act on A. Let $x \in A$. The orbit Gx has size equal to $|G : Gx|$.*

Proof. Let $H = Gx$, and let $B = \{gH \mid g \in G\}$. Define a function $\varphi : B \to Gx$ where $\varphi(gH) = gx$. To see this function is well-defined, suppose $aH = bH$, so that $b^{-1}a \in H = Gx$. Since H is a group, $a^{-1}b \in H$. Now

$$\varphi(aH) = ax = a(a^{-1}bx) = (aa^{-1}b)x = bx = \varphi(bH),$$

so φ is well-defined.

It is enough to show that φ is a bijection, for then $|B| = |G : Gx|$. We will first show that φ is a surjection. Let $y \in Gx$. There exists g such that $y = gx$, so $y = \varphi(gH)$. Now see that φ is an injection. Suppose aH and bH are in B such that $\varphi(aH) = \varphi(bH)$. So $ax = bx$, and therefore $b^{-1}ax = x$, so $b^{1}a = 1 \in Gx = H$. Thus $aH = bH$, as we needed to show. $\square$

Corollary 1.11.27. *Let $s \in G$, and let $[s]$ be the conjugacy class of s. The size of the conjugacy class $|[s]|$ is equal to $|G : C_G(s)|$. Furthermore, let $S \subseteq G$. The size of the conjugation orbit $|GS|$ is equal to $|G : N_G(S)|$. If G is finite, then $|[s]|$ and $|GS|$ divide $|G|$.*

1.12 Series and Extensions

Definition 1.12.1 (simple)**.** A group G is **simple** if the only normal subgroups of G are G itself and $\{1\}$.

Example 1.12.2. If p is a prime number, then $\mathbf{Z}/p\mathbf{Z}$ is simple. Conversely, if G is abelian, then G is isomorphic to $\mathbf{Z}/p\mathbf{Z}$ for some prime p; i.e., all abelian simple groups are of this form.

Example 1.12.3. Let F be a field. Let $N = \{cI_n \mid c \in F, c \neq 0\} \leq GL_nF$. Define the projective special linear group $PSL_nF \coloneqq SL_nF/(SL_nF \cap N)$ (recall **Definition 1.5.4**). Except in the cases where $n = 2$ and $|F| \in \{2, 3\}$, PSL_nF is a nonabelian simple group. If $|F| = \infty$, then $|PSL_nF|$ may be infinite.

Definition 1.12.4 (alternating group)**.** We define the **alternating group** of order n to be the subgroup of S_n consisting of even permutations.

Example 1.12.5. If $n \geq 5$, then A_n is a nonabelian simple group of order $n!/2$. See **Remark 1.12.39** and **Lemma 1.12.40** to come.

Remark 1.12.6. If $N \trianglelefteq G$, one can study G by studying N and G/N, as we will unpack soon. Thus, simple groups are quickly understood via this approach, due to the lack of normal subgroups.

Definition 1.12.7 (subnormal series)**.** Let G be a group. A **subnormal series** for G is a list of subgroups

$$\{1\} = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_{n-1} \trianglelefteq G_n = G.$$

Definition 1.12.8 (composition series)**.** Given a group G, a subnormal series of G is called a **composition series** if G_{i+1}/G_i is simple for all $i \in \{0, \ldots, n-1\}$.

Definition 1.12.9 (composition factor)**.** Given a composition series of a group G, the quotients G_{i+1}/G_i are called **composition factors**.

Definition 1.12.10 (solvable series)**.** Given a group G, a subnormal series of G is called a **solvable series** if G_{i+1}/G_i is abelian for all $i \in \{0, \ldots, n-1\}$.

Definition 1.12.11 (solvable group)**.** If a group G has a solvable series, then we say that G is **solvable**.

Theorem 1.12.12 (Jordan-Hölder Theorem)**.** *If G is finite, then G has a composition series. If G has a composition series, then any two composition series for G have the same length and composition factors with multiplicity.*

Proof. For the first claim, we induct on the order of G. The base case $|G| = 1$ is trivial, as is $|G| = 2$. For the inductive step, if G is simple, we are done. Otherwise, G has a proper nontrivial normal subgroup, and G/N has order smaller than G, by **Theorem 1.9.1 [Lagrange's Theorem]**.

For the second claim, again proceed via induction on $|G|$, with base case $|G| = 1$ trivial. For the inductive step, take two composition series of G,

$$\{1\} \trianglelefteq H_1 \trianglelefteq H_2 \trianglelefteq \cdots \trianglelefteq H_{k-1} \trianglelefteq H_k = G$$

and

$$\{1\} \trianglelefteq K_1 \trianglelefteq K_2 \trianglelefteq \cdots \trianglelefteq K_{\ell-1} \trianglelefteq K_\ell = G.$$

By the inductive hypothesis, the theorem is true for the groups H_{k-1} and $K_{\ell-1}$. If $H_{k-1} = K_{\ell-1}$, we are done. Otherwise, let $L = H_{k-1} \cap K_{\ell-1}$. The group L has order small enough to invoke the inductive hypothesis and therefore has a composition series

$$\{1\} \trianglelefteq L_1 \trianglelefteq L_2 \trianglelefteq \cdots \trianglelefteq L_{t-1} \trianglelefteq L_t = L.$$

Observe that by **Theorem 1.10.5 [The Second Isomorphism Theorem]**, we realize the isomorphism $H_{k-1}/L = H_{k-1}/(H_{k-1} \cap K_{\ell-1}) \cong G/K_{\ell-1}$, so $L = H_{k-1} \cap K_{\ell-1}$ is a maximal subgroup of H_{k-1}, and therefore

$$\{1\} \trianglelefteq L_1 \trianglelefteq L_2 \trianglelefteq \cdots \trianglelefteq L_{t-1} \trianglelefteq L_t = L \trianglelefteq H_{k-1}$$

is a composition series. By the inductive hypothesis, the composition series

$$\{1\} \trianglelefteq H_1 \trianglelefteq H_2 \trianglelefteq \cdots \trianglelefteq H_{k-1}$$

and

$$\{1\} \trianglelefteq L_1 \trianglelefteq L_2 \trianglelefteq \cdots \trianglelefteq L_{t-1} \trianglelefteq L_t = L \trianglelefteq H_{k-1}$$

have the same length and composition factors with multiplicity, so $t + 1 = k$. Arguing similarly, the composition series

$$\{1\} \trianglelefteq K_1 \trianglelefteq K_2 \trianglelefteq \cdots \trianglelefteq K_{\ell-1}$$

and

$$\{1\} \trianglelefteq L_1 \trianglelefteq L_2 \trianglelefteq \cdots \trianglelefteq L_{t-1} \trianglelefteq L_t = L \trianglelefteq K_{\ell-1}$$

have the same length and composition factors with multiplicity, so $t + 1 = \ell$, and therefore $k = \ell$. Finally, if we consider the composition series obtained by appending G to the aforementioned composition series:

$$\begin{aligned} \{1\} \trianglelefteq H_1 \trianglelefteq H_2 \trianglelefteq \cdots \trianglelefteq H_{k-1} \trianglelefteq G&, \\ \{1\} \trianglelefteq L_1 \trianglelefteq L_2 \trianglelefteq \cdots \trianglelefteq L_t = L \trianglelefteq H_{k-1} \trianglelefteq G&, \\ \{1\} \trianglelefteq K_1 \trianglelefteq K_2 \trianglelefteq \cdots \trianglelefteq K_{\ell-1} \trianglelefteq G&, \text{ and} \\ \{1\} \trianglelefteq L_1 \trianglelefteq L_2 \trianglelefteq \cdots \trianglelefteq L_t = L \trianglelefteq K_{\ell-1} \trianglelefteq G&, \end{aligned}$$

we see that the first two composition series still have the same length and composition factors with multiplicity, as do the last two composition series. Composition series 2 and 4 are the same except for the ending, but by **Theorem 1.10.5 [The Second Isomorphism Theorem]**,

$$H_{k-1}/L = H_{k-1}/H_{k-1} \cap K_{\ell-1} \cong G/K_{\ell-1}$$

and

$$K_{\ell-1}/L = K_{\ell-1}/H_{k-1} \cap K_{\ell-1} \cong G/H_{k-1},$$

so composition series 2 and 4 have the same length and composition factors with multiplicity. Therefore by transitivity, composition factors 1 and 3 have the same length and composition factors with multiplicity, as we wished to show. $\square$

Example 1.12.13. One composition series for D_8 is

$$\{1\} \trianglelefteq \langle r^2 \rangle \trianglelefteq \langle r \rangle \trianglelefteq D_8.$$

The composition factors are $\mathbf{Z}/2\mathbf{Z}$, listed three times. Since $\mathbf{Z}/2\mathbf{Z}$ is abelian, the above series is a solvable series. A different composition series for D_8 is

$$\{1\} \trianglelefteq \langle s \rangle \trianglelefteq \langle s, r^2 \rangle \trianglelefteq D_8,$$

but of course the composition factors are still $\mathbf{Z}/2\mathbf{Z}$, as they should be, by **Theorem 1.12.12 [Jorder-Hölder Theorem]**. A solvable, but not composition, series for D_8 is

$$\{1\} \trianglelefteq \langle r \rangle \trianglelefteq D_8.$$

The quotient $\langle r \rangle/\{1\} \cong \mathbf{Z}/4\mathbf{Z}$ is not a simple group, so the series is not a composition series.

Example 1.12.14. Trivially, if G is simple, then

$$\{1\} \trianglelefteq G$$

is a composition series. The group G, with multiplicity 1, is the only composition factor of G.

Example 1.12.15. The group $\mathbf{Z}$ has no composition series. To see this, we must have at the tail

$$\cdots p\mathbf{Z} \trianglelefteq \mathbf{Z},$$

but $p\mathbf{Z} \cong \mathbf{Z}$, so after finitely many steps we are no closer to finishing the series. Alternatively, one can argue that since $\mathbf{Z}$ is abelian, all its composition factors must be abelian, and since the order of $\mathbf{Z}$ is the product of the order of its composition factors by **Theorem 1.9.1 [Lagrange's Theorem]**, we would have $|\mathbf{Z}| < \infty$.

On the other hand,

$$\{0\} \trianglelefteq \mathbf{Z}$$

is a solvable series, so $\mathbf{Z}$ is solvable.

Lemma 1.12.16. *If G is nonabelian and simple, then G is not solvable.*

Proof. Suppose G were solvable; i.e., there exists a solvable series

$$\{1\} \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_{n-1} \trianglelefteq G.$$

Since G is simple, $G_{n-1} = \{1\}$ or $G_{n-1} = G$. If $G_{n-1} = \{1\}$, then $G/\{1\} = G$ is nonabelian, so the series was not solvable. If $G_{n-1} = G$, then there exists a shorter solvable series; use that instead. Iterate; by finiteness the contradiction is reached. $\square$

Example 1.12.17. Recall the special linear group from **Definition 1.5.4** and the general linear group from **Definition 1.5.3**. We have $SL_2\mathbf{R} \trianglelefteq GL_2\mathbf{R}$. $SL_2\mathbf{R}$ is infinite and has a composition series, but $GL_2\mathbf{R}$ is not solvable, nor does it have a composition series. The composition series of $SL_2\mathbf{R}$ is

$$\{I_2\} \trianglelefteq \left\langle \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \right\rangle \trianglelefteq SL_2\mathbf{R}.$$

Example 1.12.18. The free group of order 2, F_2, is not solvable and has no composition series. Observe that $\mathbf{Z}/p\mathbf{Z} \leq F_2$ since $\langle x, y \mid x^p = 1, y = 1 \rangle \cong \mathbf{Z}/p\mathbf{Z}$, so F_2 would have infinitely many composition factors. One can argue that since F_2 has A_5 as a quotient, and quotients of solvable groups are solvable, since A_5 is not solvable, F_2 cannot be.

Remark 1.12.19. Let G be a group. The following facts are easily verified.

1. If $N \trianglelefteq G$ and N and G/N are solvable, then G is solvable.
2. If G is solvable, then for all $H \leq G$, H is solvable, and for all $N \trianglelefteq G$, G/N is solvable.

3. Let $|G| < \infty$. G is solvable if and only if all the composition factors of G are abelian.

Definition 1.12.20 (extension)**.** A group G is an **extension** of H by K if G has a normal subgroup N with $N \cong H$ and $G/N \cong K$. Equivalently,

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

is a short exact sequence (**Definition ??**).

Example 1.12.21. $H \times K$ is an extension of H by K; via a short exact sequence this is obvious, as is $H \times \{1\} \cong H$ and $(H \times K)/(H \times \{1\}) \cong K$.

Example 1.12.22. The groups $(\mathbf{Z}/2\mathbf{Z})^3$, $(\mathbf{Z}/2\mathbf{Z}) \times (\mathbf{Z}/4\mathbf{Z})$, D_8, and Q_8 are all extensions of $\mathbf{Z}/2\mathbf{Z}$ by $(\mathbf{Z}/2\mathbf{Z})^2$. For instance, $\langle r^2 \rangle \trianglelefteq D_8$ and $\langle -1 \rangle \trianglelefteq Q_8$.

Remark 1.12.23. The Hölder program asks us to classify all finite simple groups. It is a monster, but it has been done. The fact that all finite groups are constructed as a series of extensions with finite simple groups is reason enough to do this.

Remark 1.12.24. All abelian groups are solvable. If G is abelian, then

$$\{0\} \trianglelefteq G$$

is a solvable series.

Remark 1.12.25. The class of isomorphism types of solvable groups is the smallest one that contains all abelian groups and is closed under group extensions. To see this, given a solvable series

$$\{0\} \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_{n-1} \trianglelefteq G,$$

we have G_2 is an extension of G_1 by G_2/G_1. The group $G_1 \cong G_1/\{0\}$ is abelian, so G_2/G_1 is abelian. Similarly, G_3 is an extension of G_2 by G_3/G_2, which is abelian. Continue in this manner. G is an extension of an interated extension of abelian groups by an abelian group.

Example 1.12.26. Most nonabelian groups we have seen so far are solvable. S_3, Q_8, D_8, D_{10}, and S_4 are all solvable. In fact, all groups of order less than 60 are solvable. Recall from **Definition 1.12.4** the group A_5, the alternating group of order $5!/2 = 60$. This is a nonabelian simple group by **Lemma 1.12.40** to come, so by **Lemma 1.12.16**, A_5 is not solvable. Further, S_5 has A_5 as a composition factor, and therefore S_5 is not solvable. A composition series is

$$\{1\} \trianglelefteq A_5 \trianglelefteq S_5.$$

Definition 1.12.27 (transposition)**.** A 2-cycle (a, b) in S_n is called a **transposition**.

Lemma 1.12.28. *For all n, S_n is generated by the set of all transpositions.*

Proof. Induct on n. If $n = 0$ or $n = 1$, the base case is vacuously true. Let $n = 2$. We know $S_2 \cong \mathbf{Z}/2\mathbf{Z}$, and as a set $S_2 = \{(1), (1, 2)\}$, so the base case is still true. For the inductive step, let $\sigma \in S_n$. As a function $\sigma : \{1, \dots, n\} \to \{1, \dots, n\}$, so $\sigma(n) \in \{1, \dots, n\}$. There are two cases. First suppose $\sigma(n) = n$, in which case σ is in the stabilizer (**Definition 1.7.17**) $(S_n)_n$. The stabilizer is isomorphic to S_{n-1} via sending transpositions to transpositions. Invoking the inductive hypothesis on S_{n-1}, we are done. Second suppose $\sigma(n) = i \neq n$. Then $(i, n)\sigma \in (S_n)_n$. As in the previous case, $(i, n)\sigma$ is a product of transpositions, so σ is. □

Example 1.12.29. We can write $\sigma = (1, 5, 4, 2, 3)$ as a product of transpositions. First, $\sigma(5) = 4$, so $(4, 5)\sigma \in (S_5)_5 \cong S_4$. Next, $((4, 5)\sigma)(4) = 2$, so $(2, 4)(4, 5)\sigma$ stabilizes 4 and 5. Continuing, $(1, 3)(2, 4)(4, 5)\sigma$ fixes 3, 4, and 5, and finally $(1, 2)(1, 3)(2, 4)(4, 5)\sigma$ fixes 2, 3, 4, and 5, and therefore 1 as well. So $(1, 2)(1, 3)(2, 4)(4, 5)\sigma = (1)$, and solving for σ, we see that

$$\sigma = (4, 5)(2, 4)(1, 3)(1, 2).$$

Remark 1.12.30. We can use **Lemma 1.12.28** to write a presentation for S_n. Write s_{ij} for (i, j); we have the following relations.

- $s_{ij} = s_{ji}$.
- ${s_{ij}}^2 = 1$.
- If $\{i, j\} \cap \{k, \ell\} = \emptyset$, then $s_{ij}s_{k\ell} = s_{k\ell}s_{ij}$.
- $s_{ij}s_{jk}{s_{ij}}^{-1} = s_{ij}s_{jk}s_{ij} = s_{ik}$. We call this the braiding relation.

Let R be the set of all four types of relations above, and let $S = \{s_{ij} \mid i, j \in \{1, \ldots, n\}, i \neq j\}$. The group $\langle S \mid R\rangle$ is a presentation for S_n.

Example 1.12.31. One can use this presentation to show that

$$s_{14}s_{12}s_{15}s_{13}s_{45}s_{35}s_{24}s_{13} = 1.$$

Definition 1.12.32 (sign homomorphism)**.** Define the **sign homomorphism** $\varepsilon : S_n \to \{-1, 1\}$ by the unique group homomorphism such that $\varepsilon(\sigma) = -1$ when σ is a transposition.

Lemma 1.12.33. *The sign homomorphism ε is well-defined.*

Proof. Given the presentation of S_n in **Remark 1.12.30**, we can show that ε respects the set of relations R. Observe that

- $\varepsilon(s_{ij}) = -1 = \varepsilon(s_{ji})$,
- $\varepsilon(s_{ij}s_{ij}) = \varepsilon(s_{ij})\varepsilon(s_{ij}) = (-1)(-1) = 1 = \varepsilon(1)$,
- $\varepsilon(s_{ij}s_{k\ell}) = \varepsilon(s_{ij})\varepsilon(s_{k\ell}) = (-1)(-1) = 1 = (-1)(-1) = \varepsilon(s_{k\ell})\varepsilon(s_{ij}) = \varepsilon(s_{k\ell}s_{ij})$, and
- $\varepsilon(s_{ij}s_{jk}s_{ij}) = \varepsilon(s_{ij})\varepsilon(s_{jk})\varepsilon(s_{ij}) = (-1)(-1)(-1) = -1 = \varepsilon(s_{ik})$.

□

Remark 1.12.34. If σ is a k-cycle, then $\varepsilon(\sigma) = (-1)^{k-1}$.

Definition 1.12.35 (odd permutation)**.** Let $\sigma \in S_n$. If $\varepsilon(\sigma) = -1$, then σ is **odd**.

Definition 1.12.36 (even permutation)**.** Let $\sigma \in S_n$. If $\varepsilon(\sigma) = 1$, then σ is **even**.

Remark 1.12.37. If σ is a k-cycle, then σ is even if and only if k is odd (and vice versa).

Definition 1.12.38 (alternating group 2)**.** Another way to define the alternating group on n symbols $A_n \trianglelefteq S_n$ is that $A_n = \ker(\varepsilon : S_n \to \{-1, 1\})$. In other words, $A_n = \{\sigma \in S_n \mid \sigma \text{ is even}\}$, as in **Definition 1.12.4**.

Remark 1.12.39. By **Theorem 1.10.1 [The First Isomorphism Theorem]**, $|A_n| = n!/2$, since $S_n/A_n \cong \{1, -1\}$, so by **Theorem 1.9.1 [Lagrange's Theorem]**, $|S_n : A_n| = |S_n|/|A_n| = 2$. Thus $|A_n| = |S_n|/2 = n!/2$.

Lemma 1.12.40. *If $n \geq 5$, then A_n is a nonabelian simple group.*

Proof. A_n is clearly nonabelian; $(1, 2)(2, 3) = (1, 3, 2) \neq (1, 2, 3) = (2, 3)(1, 2)$. We will only prove that A_5 is simple. In S_5, we will build an exhaustive table of the conjugacy classes of elements (the orbits under the conjugation action), the size of the classes, and the image of the class under ε, since the parity of a permutation is invariant under conjugacy. We have

Representative	Size	Image under ε
(1)	1	1
$(1, 2)$	10	-1
$(1, 2, 3)$	20	1
$(1, 2, 3, 4)$	30	-1
$(1, 2, 3, 4, 5)$	24	1
$(1, 2)(3, 4)$	15	1
$(1, 2)(3, 4, 5)$	20	-1

In A_5, however, we have

Representative	Size
(1)	1
$(1,2,3)$	20
$(1,2)(3,4)$	15
$(1,2,3,4,5)$	12
$(2,1,3,4,5)$	12

By **Proposition 1.8.13**, if $N \trianglelefteq G$, then N is a union of conjugacy classes of G. Suppose A_5 has a normal subgroup N. By **Theorem 1.9.1 [Lagrange's Theorem]**, $|N|$ divides 60. A union of classes in the second table must have cardinality dividing 60, but there is no way to do that nontrivially. Thus, A_5 is simple. ☐

1.13 The Class Equation

Theorem 1.13.1 (The Class Equation)**.** *Let G be a finite group. Let $g_1, \ldots, g_r$ be representatives of the conjugacy classes of G which are not in $Z(G)$, the center of G. One has*

$$|G| = |Z(G)| + \sum_{i=1}^{r} |G : C_G(g_i)|.$$

Proof. As a set, $G = Z(G) \sqcup [g_1] \sqcup \cdots \sqcup [g_r]$. Thus,

$$|G| = |Z(G)| + |[g_1]| + \cdots + |[g_r]|.$$

By **Corollary 1.11.27**, $|[g_i]| = |G : C_G(g_i)|$, and the result is shown. ☐

Corollary 1.13.2. *If P is a group of order p^α where p is prime, then $Z(P) \neq \{1\}$.*

Proof. Let $g_1, \ldots, g_r$ be representatives of noncentral conjugacy classes. Reduce the class equation modulo p. We have

$$\begin{aligned} 0 \equiv p \equiv |P| &\equiv |Z(P)| + \sum_{i=1}^{r} |P : C_P(g_i)| \pmod p \\ &\equiv |Z(P)| + \sum_{i=1}^{r} 0 \pmod p. \end{aligned}$$

So $|Z(P)| \equiv 0 \pmod p$, and therefore $Z(P) \neq \{1\}$. ☐

Corollary 1.13.3. *If $|P| = p^2$, then P is abelian. Furthermore, $P \cong \mathbf{Z}/p^2\mathbf{Z}$ or $P \cong (\mathbf{Z}/p\mathbf{Z})^2$.*

Proof. By **Corollary 1.13.2**, $Z(P) \neq \{1\}$. Consider $|P/Z(P)|$. It must be either 1 or p. If $|P/Z(P)| = p$, then $P/Z(P)$ is cyclic by **Corollary 1.9.7**. By a homework exercise, P is abelian. Otherwise, if we have $|P/Z(P)| = 1$, then $P \cong Z(P)$ is abelian. ☐

Remark 1.13.4. Given **Theorem 1.13.1 [The Class Equation]**, one may ask: how do you find the classes $[g_i]$? First, find $Z(G)$. We know that $Z(G) \subseteq C_G(g_i)$, and we also know that $\langle Z(G), g_i \rangle \leq C_G(g_i)$. This gives a lower bound on $|C_G(g_i)|$, and an upper bound on $|G : C_G(g_i)| = |[g_i]|$. Pick $h \in G$ not in $\langle g \rangle$ or $Z(G)$. We want to know whether or not $h \in C_G(g_i)$, so compute hg_ih^{-1}. If $hgh^{-1} \neq g_i$, then $hg_ih^{-1} \in [g_i]$. If $hg_ih^{-1} = g_i$, then $h \in C_G(g_i)$, so $\langle Z(G), g, h \rangle \leq C_G(g_i)$. We know have a better upper bound on $|[g_i]|$; repeat.

Example 1.13.5. For abelian groups, $|G| = |Z(G)|$, so the class equation is unhelpful.

Example 1.13.6. Consider $D_6 = \{1, r, r^2, s, sr, sr^2\}$. We have

$$\begin{aligned}
[r] &= \{r, r^2\} \\
C_{D_6}(r) &= \langle r \rangle \\
srs^{-1} &= r^{-1} = r^2 \\
[s] &= \{s, sr, sr^2\} \\
C_{D_6}(s) &= \langle s \rangle \\
rsr^{-1} &= sr^2r^{-1} = sr \\
rsrr^{-1} &= rs = sr^2.
\end{aligned}$$

The class equation is therefore

$$\begin{aligned}
|D_6| &= |Z(D_6)| + |D_6 : C_{D_6}(r)| + |D_6 : C_{D_6}(s)| \\
6 &= 1 + 2 + 3.
\end{aligned}$$

Example 1.13.7. Consider $Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$. The center of Q_8 is $Z(Q_8) = \langle -1 \rangle = \{1, -1\}$. Let $g \in Q_8 \setminus Z(Q_8)$. We have $\langle Z(Q_8), g \rangle \leq C_{Q_8}(g)$ and $\langle Z(Q_8), g \rangle$ has at least four elements, so $|[g]| \leq 2$, and therefore must be 2. We can figure out the conjugacy classes with computation:

$$\begin{aligned}
[i] &= \{i, -i\} \\
[j] &= \{j, -j\} \\
[k] &= \{k, -k\}.
\end{aligned}$$

The class equation is

$$\begin{aligned}
|Q_8| &= |Z(Q_8| + |[i]| + |[j]| + |[k]| \\
8 &= 2 + 2 + 2 + 2.
\end{aligned}$$

Lemma 1.13.8. *Two elements of S_n are conjugate if and only if they have the same cycle type; i.e., they have the same partition of $n \in \mathbf{Z}$. The conjugacy classes of S_n correspond to the partitions of n.*

Proof. First, let $\sigma, \tau \in S_n$. We want to show that $\tau\sigma\tau^{-1}$ and σ have the same cycle type. Write

$$\sigma = (a_{11}, \ldots, a_{1\ell_1})(a_{21}, \ldots, a_{2\ell_2}) \cdots (a_{k1}, \ldots, a_{k\ell_k}).$$

The cycle type of σ is the partition $n = \ell_1 + \ell_2 + \cdots + \ell_k$. Now via computation,

$$\tau\sigma\tau^{-1} = (\tau(a_{11}), \ldots, \tau(a_{1\ell_1}))\,(\tau(a_{21}), \ldots, \tau(a_{2\ell_2})) \cdots (\tau(a_{k1}), \ldots, \tau(a_{k\ell_k}))\,.$$

The cycle types of σ and $\tau\sigma\tau^{-1}$ are the same.

In the other direction, suppose $\sigma, \tau \in S_n$ have the same cycle type. That means that

$$\sigma = (a_{11}, \ldots, a_{1\ell_1}) \cdots (a_{k1}, \ldots, a_{k\ell_k})$$

and

$$\tau = (b_{11}, \ldots, b_{1\ell_1}) \cdots (b_{k1}, \ldots, b_{k\ell_k}).$$

Define a permutation $\rho : \{1, \ldots, n\} \to \{1, \ldots, n\}$ via $\rho(a_{ij}) = b_{ij}$ for all ij. By construction, $\rho \in S_n$, and a computation verifies $\rho\sigma\rho^{-1} = \tau$, so σ and τ are conjugate, as desired. $\square$