Group Theory.

Alec Zabel-Mena

August 20, 2023

Contents

1 Groups. **5**
- 1.1 Definitions and Examples. 5
- 1.2 Dihedral Groups and Group Generators. 10
- 1.3 Permutation Groups and the Symmetric Group. 12
- 1.4 The General and Special Linear Groups of $n \times n$ Matrices. 15
- 1.5 Homomorphism. 18

2 Subgroups. **23**
- 2.1 Definitions and Examples. 23
- 2.2 Special Subgroups. 24
- 2.3 Cyclic Groups. 26
- 2.4 Subgroups of Generating Sets. 29
- 2.5 Lattices of Groups. 31

3 Quotient Groups, and Homomorphisms. **35**
- 3.1 Quotient Groups. 35
- 3.2 Alternative Definitions. 37
- 3.3 Lagrange's Theorem. 40
- 3.4 The Isomorphism Theorems. 43
- 3.5 Composition Series, Simple Groups, and Solvable Groups. 45
- 3.6 The Alternating Group. 47

4 Group Actions. **51**
- 4.1 Group Actions and Permutation Representations. 51
- 4.2 Cayley's Theorem. 55
- 4.3 The Class Equation. 56
- 4.4 Automorphisms. 59
- 4.5 Sylow's Theorems 62
- 4.6 Applications of Sylow's Theorems 65

Chapter 1

Groups.

1.1 Definitions and Examples.

Definition. Let G be set, we define a **binary operation**, $*$, on G to be a map $* : G \times G \to G$ that takes $(a, b) \to a*b$. We say that a binary operation $*$ is **associative** if for any $a, b, c \in G$, $(a*b)*c = a*(b*c)$. We say that a binary operation, $*$ is **commutative** if for any $a, b \in G$, $a*b = b*a$

We also write ab instead of $a*b$ for convinience, and when context is clear.

Example 1.1. (1) The usual addition, $+$ is an associative and commutative binary operation on the sets $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$ of integers, rationals, and real numbers. The addition of complex numbers, $+$ is an associative and commutative binary operation on the complex numbers $\mathbb{C}$

(2) The usual multiplication $\cdot$ is an associative and commutative binary operation on $\mathbb{Z}^*$, $\mathbb{Q}^*$ and $\mathbb{R}^*$. Complex multiplication on $\mathbb{C}^*$ is also an associative, commutative binary operation. Note we define $F^* = F \backslash \{0\}$, where $F = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.

(3) The usual subtration, is a noncomutative binary operation on $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$, complex subtraction is noncommutative on $\mathbb{C}$. The map $a \to -a$ is not binary.

(4) The usual subtraction is not a binary operation on $\mathbb{Z}^+$, Q^+, and $\mathbb{R}^+$, notice that if $a < b$, $a - b \notin F$ where $F = \mathbb{Z}, \mathbb{Q}, \mathbb{R}$.

(5) The cross prodcuct, $\times$ on two vectors in real 3-space is a nonassociative binary operation on $\mathbb{R}^3$.

(6) The operation $+_n$ of addition $\mod n$ is a binary operation on the set of integers mod n, $\mathbb{Z}/n\mathbb{Z}$. Notice that for $k, l, m \in \mathbb{Z}$, that $a \mod n$ is of the form $a + kn$, thus b mod n and $c \mod n$, have the forms $b+ln$ and $c+mn$. Thus $((a+kn)+(b+ln))+(c+mn) = (a+b)+(l+k)n+(c+mn) = a+b+c+(l+k+m)n = (a+kn)+(b+c)+(l+m)n = (a+kn)+((b+ln)+(c+mn))$. This implies that $(a+b)+c \mod n = a(b+c) \mod n$; additionally, $(a+kn)+(b+ln) = (a+b)+(k+l)n = (b+a)+(l+k)n = (b+ln)+(a+kn)$, so $a+b \mod n = b+a \mod n$. That is $+_n$ is associative and commutative. We abbreviate addition $\mod n$ and write $+$ instead of $+_n$.

(7) Multiplictation $\mod n$ is a binary operation on $\mathbb{Z}/_{n\mathbb{Z}}$ which is associative and commutative.

(8) The operation of function composition $\circ$ is a binary operation on any set of mappings. We have that for mappings f, g, and h that $(f \circ g) \circ h = f \circ (g \circ h)$, making $\circ$ associative; but $f \circ g \neq g \circ f$, making $\circ$ noncommutative.

Definition. Let G be a set, and $H \subseteq G$, and let $*$ be a binary operation on G. We say that H is **closed** under $*$ if $*|_H$ is a binary operation on H.

Definition. Let G be a nonempty set, and let $*$ be a binary operation on G. We call the pair $(G, *)$ a **group** if:

(0) For every $a, b \in G$, $ab \in G$. That is G is closed under $*$.

(1) $(ab)c = a(bc)$ for all $a, b, c \in G$, i.e. $*$ is associative.

(2) There exists an element $e \in G$ called the **identity** element such that $ae = ea = a$ for all $a \in G$

(3) For each $a \in G$, there is an element $b \in G$, called the **inverse** of a such that $ab = ba = e$, where e is the identity element.

Remark. We make note that property (0) of this definition is impled by stating $*$ as a binary operation on G, we however list it, becuase when verifying a given set is a group, we usually want to check for closure.

Remark. Instead of stating $(G, *)$ as a group, we will often just say that G is a group under $*$, or simply, G is a group.

Example 1.2. (1) The set $G = \{e\}$ of one element forms a group under any operation, and is called the **trivial** group. We write $G = \langle e \rangle$.

(2) The sets $\mathbb{Z}$, $\mathbb{R}$, and $\mathbb{Q}$ are all groups under the usual addition. Here 0 is the identity, and $-a$ is the inverse of a. $\mathbb{C}$ is a group under complex addition with $0 = 0 + i0$ the identity and $-a - ib$ the inverse of $a + ib$.

(3) $\mathbb{Q}$ and $\mathbb{R}$ are groups under the usual multiplication, with identity 1 and inverse $a^{-1} = \frac{1}{a}$. $\mathbb{Z}$ is not a group under this operation, as $\frac{1}{a} \notin \mathbb{Z}$ whenever $a \in \mathbb{Z}$. $\mathbb{C}$ is a group under complex multiplication with identity $1 = 1 + i0$ and inverse $\frac{a}{a^2+b^2} - i\frac{b}{a^2+b^2}$ for $a + ib$.

(4) Consider the set of integers $\mod n$, $\mathbb{Z}/_{n\mathbb{Z}}$ under addition $\mod n$, $+$. Since $+$ is a binary operation on $Z/_{n\mathbb{Z}}$, closure is guaranteed. We also see that associativity hold. Now, notcie that $n \equiv 0 \mod n$, by definition, so $a + n = n + a \equiv 0 + a \mod n \equiv a + 0 \mod n \equiv a$. Moreover, $n - a \equiv 0 - a \equiv -a \mod n$, and $(n-a)+a = n(-a+a) = n \equiv 0 \mod n$ and $a + (n - a) = n + (a - a) = n \equiv 0 \mod n$. So $(\mathbb{Z}/_{n\mathbb{Z}}, +_n)$ is a group, with identity element $0 \mod n$ and inverse element $-a \mod n$ for each $a \in \mathbb{Z}/_{n\mathbb{Z}}$.

Example 1.3. Suppose we removed the restriction to be nonempty in the definition of a group. We see that if $G = \emptyset$, then G cannot be a group, since it is not closed, trivially; furthurmore, there is no identity, nor inverse to each element. Therefore the minimum number of elements a group can have is 1. This makes the trivial group minimal.

Definition. We call a group G under a binary operation $*$ **Abelian**, or **commutative** if for every $a, b \in G$, $ab = ba$.

Example 1.4. The above examples of groups are also examples of abelian groups.

Example 1.5. Consider $(\mathbb{Z}/n\mathbb{Z})\backslash\{0\}$ under multiplication $\mod n$, $\cdot_n$ (abbreviated as $\cdot$). This is not a group as not every element has an inverse. Specifically, take $n = 6$, then in $\mathbb{Z}/6\mathbb{Z}$, $2 \cdot 3 = 6 \equiv 0 \mod 6 \notin (\mathbb{Z}/n\mathbb{Z})\backslash\{0\}$. However, one can still impose a group structure with modular multiplication.

Define the set $U(\mathbb{Z}/n\mathbb{Z}) = \{a \in \mathbb{Z}/n\mathbb{Z} : (a, n) = 1\}$, that is it is the set of all integers mod n coprime with n. We have that $U(\mathbb{Z}/n\mathbb{Z})$ is closed under $\cdot$. Notice that if $(a, n) = 1$, and $(b, n) = 1$, then $(ab, n) = 1$. Also notice that $U(\mathbb{Z}/n\mathbb{Z}) \subseteq \mathbb{Z}/n\mathbb{Z}$, and so inherits associativity. Moreover, notice that $(1, n) = 1$, and $a1 = 1a = a \in U(\mathbb{Z}/n\mathbb{Z})$, so $1 \mod n$ is the identity of the set. Now for any $a \in U(\mathbb{Z}/n\mathbb{Z})$, since $(a, n) = 1$, there exist $b, m \in \mathbb{Z}$ such that $ab + mn = 1$, that is $ab \equiv 1 \mod n$, and moreover notice that if $(ab, n) = 1$ and $(a, n) = 1$, then $(b, n) = 1$, thus $b \in U(\mathbb{Z}/n\mathbb{Z})$, and is an inverse of a. Thus we have shown that $U(\mathbb{Z}/n\mathbb{Z})$ is a group under $\cdot$. We call the group the **group of units,** $\mod n$, or simply the **unit group** $\mod n$. Moreover, we see that this group is commutative.

Example 1.6.
(1) The vector space axioms for some vector space V specify that under vector addition $+$, $(V, +)$ forms a group.

(2) Let $(A, *)$, $(B, \cdot)$ be groups under binary operations $*$ and $\cdot$. Consider the product $A \times B$ and take the map $\circ : (a_1, b_1)(a_2, b_2) \to (a_1 * a_2, b_1 \cdot b_2)$. Then $\circ$ is a binary operation on $A \times B$. Then $(A \times B, \circ)$ forms a group. We have that since A and B is closed, then so is $A \times B$. Furthermore, by associativity of $*$ and $\cdot$, $((a_1, b_1) \circ (a_2, b_2)) \circ (a_3, b_3) = (a_1, b_1) \circ ((a_2, b_2) \circ (a_3, b_3))$; making $\circ$ associative. Now if e_1 and e_2 are the identities of A and B respevively, then (e_1, e_2) is the identiy for $A \times B$; finding the inverse of an element (a, b) follow similarly.

Theorem 1.1.1. *Let G be a group under a binary operation $*$ then the identy of G is unique, and the inverse of $a \in G$ is unique.*

Proof. Suppose there exists $e, f \in G$ such that for any $a \in G$ $ae = ea = a$ and $af = fa = a$. Then we have that $fe = e$ and $ef = fe = f$; thus $e = f$.

Now let $a \in G$, and suppose a has inverses $b, c \in G$, then $ab = ba = e$ and $ac = ca = e$, where e is the identity of G. Then we have $b = be = b(ac) = (ba)c = ec = c$, thus $b = c$. ■

Remark. Since the inverse of an element a is unique, we will now denote it a^{-1}.

Corollary. $(a^{-1})^{-1} = a$ *and* $(ab)^{-1} = b^{-1}a^{-1}$

Proof. Since inverses are unique, the $a^{-1} \in G$ has the unique inverse a^{-1-1}. Then taking $aa^{-1} = e$, applying inverses, we get $a(a^{-1}(a^{-1})^{-1}) = e(a^{-1})^{-1}$, $a = (a^{-1})^{-1}$.

Now Let $a, b \in G$, then $ab(ab)^{-1} = e$. Applying the inverse of a on the right to both sides, we get $b(ab)^{-1} = a^{-1}$; agian with the inverse of b yields $(ab)^{-1} = b^{-1}a^{-1}$. ■

Theorem 1.1.2 (Generalized Associativity)**.** *Let G be a group under a binary operation $*$, then for any $a_1, a_2, \dots, a_n \in G$, the product $a_1 * a_1 * \cdots * a_n$ is independent of the ordering of any brackets.*

Proof. By induction on n, for $n = 1$, we just have the element a_1, for $n = 2$ we have a_1a_2 has only one possible bracketing (a_1b_1); and for $n = 3$, the associativty group law guarantees $a_1(a_2a_3) = (a_1a_2)a_3$.

Now for any $k < n$, the the braketing of k elements $a_1, \dots, a_k$ is can be reduced to the expression

$$a_1 * (a_2 * (a_3 * (\cdots * a_k))).$$

Now we see that $a_1 * \cdots * a_n$ can be bracketed into the products:

$$(a_1 * \cdots * a_k) * (a_{k+1} * \cdots * a_n)$$

which can be bracketed, by hypothesis as:

$$(a_1 * (a_2 * (a_3 * (\cdots * a_k)))) * (a_{k+1} * (a_{k+2} * (a_{k+3} * (\cdots * a_n))))$$

Therefore, applying the assocaitive group law to this product, we get that

$$a_1 * \cdots * a_n = a_1 * (a_2 * (a_3 * (\cdots * a_n)))$$

This completes the proof. ■

Theorem 1.1.3 (The Cancellation Laws)**.** *Let G be a group under a binary operation $*$. Then for $a, b, c \in G$, we have:*

(1) $ab = ac$ implies $b = c$ (Left Cancellation Law).

(2) $ba = ca$ implies $b = c$ (Right Cancellation Law).

Proof. Suppose that $ab = ac$, then applying the inverse of a on the left, we get $(a^{-1}a)b = (a^{-1}a)c$, hence $eb = ec$, thus $b = c$. Similarly, we get $b = c$ if we apply a^{-1} to the right in the equation $ba = ca$. ■

Corollary. *For $x, y \in G$, the equations $ax = b$ and $ya = b$ have unique solutions.*

Proof. We have $x = ba^{-1}$ and $y = a^{-1}b$. Since inverses are unique, so are the solutions x and y. ■

Definition. Let G be a group under a binary opeartion $*$. For any $a \in G$, and $n \in \mathbb{Z}^+$, we define the **n-th power** of a to be:

$$a^n = \underbrace{a * \cdots * a}_{n \text{ times.}}$$

We define $a^0 = e$ and $a^{-n} = (a^{-1})^n$.

Lemma 1.1.4. *Let G be a group under a binary operation $*$, and let $a \in G$ and $m, n \in \mathbb{Z}^+$. Then:*

(1) $a^m a^n = a^{m+n}$.

(2) $(a^m)^n = a^{mn}$.

Proof. We have by definition that $a^m a^n = \underbrace{a * \cdots * a}_{m \text{ times.}} \underbrace{a * \cdots * a}_{n \text{ times.}} = \underbrace{a * \cdots * a}_{m+n \text{ times.}} = a^{m+n}$.

Likewise, $(a^m)^n = \underbrace{a^m * \cdots * a^m}_{n \text{ times.}} = \underbrace{a * \cdots * a}_{nm \text{ times.}} = a^{mn}$. ■

We can now, unless context isn't clear enough, drop all mention to the binary operation of a group.

Definition. We define the **order** of a group G to be the number of elements of G and denote it $\operatorname{ord} G$. That is, $\operatorname{ord} G = |G|$. If G is infinite, then we say that G has **infinite order**; otherwise, we say G is of **finite order**.

Definition. Let G be a group and let $a \in G$. We define the **order** of a to be the smallest positive integer $n \in \mathbb{Z}^+$ for which $a^n = e$. If there is no such integer n, then we say a has **infinite order**, otherwise, we say a has **finite order**, and write $\operatorname{ord} a = n$.

We conclude the section with more examples and one last definition.

Lemma 1.1.5. *Let G be a group, suppose $a, b \in G$ are elements with* $\operatorname{ord} a = m$, $\operatorname{ord} b = n$, *for $m, n \in \mathbb{Z}^+$, and that $ab = ba$. Then* $\operatorname{ord} ab = [m, n]$.

Proof. Let $\operatorname{ord} ab = k$ for $k \in \mathbb{Z}^+$. Since a and b commute, we get $a^k = e$ and $b^k = e$. Now, by the division theorem, there are integers $q_1, q_2, r_1, r_2 \in \mathbb{Z}^+$ such that $k = q_1 m + r_1$ and $k = q_2 n + r_2$. Then we get that $a^k = a^{q_1 m + r_1} = a^{q_1 m} a^{r_1} = a^{r_1} = e$. Since $\operatorname{ord} a = m$, this makes $r_1 = 0$. Similarly, we get that $b^k = b^{r_2} = e$ implies $r_2 = 0$. Therefore, $k = q_1 m = q_2 n$; moreover, $\operatorname{ord} ab = k$ is minimal by definition, thus we get $\operatorname{ord} ab = k = [m, n]$. ■

Corollary. *For $a_1, \dots, a_k \in G$, with* $\operatorname{ord} a_i = n_i$ *and $a_i a_j = a_j a_i$ for all $1 \leq i, j \leq n$, then* $\operatorname{ord} a_1 a_2 \dots a_k = [n_1, \dots, n_k]$.

Proof. By induction, when $k = 1$, the case is trivial. Now, for $k = 2$, the result follows by the above theorem. Now suppose that $\operatorname{ord} a_1 \dots a_k = [n_1, \dots, n_k]$. Take $a_{k+1} \in G$ with $\operatorname{ord} a_{k+1} = n_{k+1}$ and $(a_1 \dots a_k)a_{k+1} = a_{k+1}(a_1 \dots a_k) = a_1 \dots a_k a_{k+1}$. Then, by the above theorem, we get $\operatorname{ord} a_1 \dots a_k a_{k+1} = [[n_1, \dots, n_k], n_{k+1}] = [n_1, \dots, n_k, n_{k+1}]$. ■

Example 1.7. (1) $\operatorname{ord} \langle e \rangle = 1$.

(1) In any group G, $\operatorname{ord} e = 1$, and if $a \in G$ has $\operatorname{ord} a = 1$, then necessarily, $a = e$. That is in any group, the only element of order 1 is the identity.

(2) The additive groups $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ have infinite order, and their nonzero elements also have infinite order.

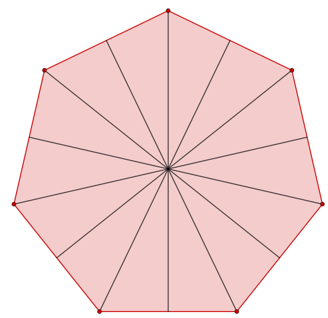

Figure 1.1: The group, D_{14} of symmetries on a heptagon.

(3) The multiplicative group $\mathbb{C}^*$ has infinite order, morover, since $i^4 = 1$ and $i^3 = -i$, $\operatorname{ord} i = 4$.

(4) $\operatorname{ord} \mathbb{Z}/n\mathbb{Z} = n$, and every element is of finite order. $\operatorname{ord} U(\mathbb{Z}/n\mathbb{Z}) = \phi(n)$, where *phi* is the Euler totient function. Every element of $U(\mathbb{Z}/n\mathbb{Z})$ also has finite order.

Definition. Let $G = \{g_1, \ldots, g_n\}$ be a finite group of order n with $g_1 = e$. We define the **Cayley table**, or **multiplication table** of G to be the $n \times n$ matrix defined by the entries (g_{ij}) where

$$g_{ij} = g_i g_j$$

for $1 \leq i, j \leq n$.

1.2 Dihedral Groups and Group Generators.

Let $\mathbb{Z}^+$ and define D_{2n} to be the set of symetries of a regular n-gon, where a symmetry is just a permutation of the vertices. That is, if S is the set of vertices, then a symmetry on S is just a map taking $S \to S$. We would like to characterize the symmetries of D_{2n} (See figure 1.2).

Since the set of vertices of the n-gon is arbitrary, but finite, we can label S how we see fit. Let us label $S = \mathbb{Z}/n\mathbb{Z}$ and define the symmetries $t : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ and $r : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ by $t : i \to i$ and $r : i \to i + 1$. That is t is a transposition (or reflection) of the veritices, and r is a rotation if the vertices by an angle of $\frac{2\pi}{n}$. Now, define the "identity" symmetry $e : i \to i$. Then notice that $t^2 : i \to -i \to -(-i) = i$, and $r^n : i \to i + 1 \to \ldots, \to i + n \equiv i$. So $t^2 = r^n = e$ (more over, if we treat e as a rotation of the veritces by an angle of 2π, then note that r^n applies a rotation of the vertices by an angle of $\frac{2n\pi}{n} = 2\pi$, which makes it the identity symmetry). It is easy to see that t and r are $1-1$ and onto, so $t^{-1} = t$ and $r^{-1} = r^{n-1}$.

Now that we have characterized the symmetries r and t, what about $r \circ t$? Abbreviating $r \circ t$ as rt, we see that $rt : i \to -i \to -i + 1 = -(i + 1)$. Now, notice that $r^{-1} = r^{n-1} : i \to i + (n - 1) \equiv i - 1$. Then, $tr^{-1} : i \to i - 1 \to -(i - 1) = -i + 1$. Thus $rt = tr^{-1}$. This gives us the following lemma.

Lemma 1.2.1. *For the symmetries r and t, and for $i \in \mathbb{Z}/n\mathbb{Z}$, $r^i t = tr^{-i}$.*

Proof. By induction on i, we have for $i = 1$ that $rt = tr^{-1}$. Now suppose for i that $r^i t = tr^{-i}$. Then $r^{i+1}t = r(r^i t) = (rt)r^{-i} = tr^{-1}r^{-i} = tr^{-i-1} = tr^{-(i+1)}$. ∎

We can now characterize the set D_{2n}.

Definition. Let S be a set of n elements, we define the **dihedral group** to be the set of all permutations on S with the form $D_{2n} = \langle r, t : r^n = t^2 = e, rt = tr^{-1} \rangle$

Theorem 1.2.2. *D_{2n} forms a group under function composition $\circ$, and the elements of D_{2n} are of the forn $r^i t^j$ with $i \in \mathbb{Z}/n\mathbb{Z}$ and $j \in \mathbb{Z}/2\mathbb{Z}$.*

Proof. Since $r, t \in D_{2n}$, we have that $rt \in D_{2n}$ since rt is also a permutation. Now by the above relations, we have that any element in D_{2n} has the form $r^i t^j$ where $i \in \mathbb{Z}/n\mathbb{Z}$ and $j \in \mathbb{Z}/2\mathbb{Z}$. Now let $r^i t^j, r^l t^k \in D_{2n}$ with $i, l \in \mathbb{Z}/n\mathbb{Z}$ and $j, k \in \mathbb{Z}/2\mathbb{Z}$. Then $(r^i t^j)(r^l t^k) = r^i (t^j t^k) r^{-l} = r^i t^{j+k} r^{-l} = (r^i r^l) t^{j+k} = r^{i+l} t^{j+k}$. Now, by the closure of both $\mathbb{Z}/n\mathbb{Z}$, and $\mathbb{Z}/2\mathbb{Z}$, we get that $r^{i+l} t^{j+k} \in D_{2n}$ which establishes closure of D_{2n} under $\circ$. We also see that since D_{2n} is a set of permutations, it inherits the associativity of $\circ$.

Now consider the identity symmetry $e : i \to i$. We have $e = r^n t^2$, so for any $r^i t^j$, $(r^i t^j)(r^n t^2) = r^{i+n} t^{j+2} = r^i r^n t^j t^2 = r^i e t^j e = r^i t^j$. Likewise $(r^n t^2)(r^i t^j) = (r^i t^j)$. We also get that since $t^{-1} = t$ and $r^{-1} = r^{n-1}$ then if $s \in D_{2n}$, then $(r^i t^j)s = e$ implies, by cancellation laws, that $s = t^j r^{-i}$, which serves as an inverse to $r^i t^j$. Therefore D_{2n} is a group. ∎

Corollary. $\operatorname{ord} D_{2n} = 2n$.

Proof. We have that each element of D_{2n} is of the form $r^i t^j$ where $i \in \mathbb{Z}/n\mathbb{Z}$ and $j = 0$ or $j = 1$. Thus there are two possible choices for j and n possible choices for i, therefore there are $2n$ possible choices for $r^i t^j$, since this element is arbitrary, we have that this enumerates all the elements of D_{2n}. ∎

Corollary. $D_{2n} = \{e, t, r, r^2, \ldots r^{n-1}, rt, r^2 t, \ldots, r^{n-1} t\}$.

Proof. Compute each element $r^i t^j$, iterating over i and j. ∎

Thus we have entirely described the set of symmetries of a regular n-gon in group theoretic terms; and have found that they follow a certain (special case, of a more general) group structure. In fact, we have found elementd r, t that "generate" the symmetries, and found relations which we can use to describe the group. This leads us to the following definition.

Definition. Let G be a grou p. We say that a subset, $S \subseteq G$ **generates** the group G if for every $g \in G$, g is the finite product of elements of S. We write $G = \langle S \rangle$ and call S the **generator** of G. If the elements of S satisfy a set of relations $R_1, \ldots R_n$, then we say G is **represented** by S by $R_1, \ldots R_n$ and write $G = \langle S : R_1, \ldots, R_n \rangle$, and call this form the **representation** of G.

Example 1.8. (1) $\mathbb{Z} = \langle 1 \rangle$.

(2) $\mathbb{Z}/n\mathbb{Z} = \langle 1 \rangle$.

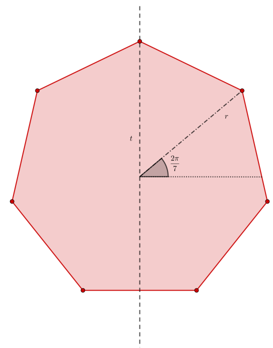

Figure 1.2: The transposition $t \in D_{14}$ of vertices of a heptagon and the rotation $r \in D_{14}$ about an angle of $\frac{2\pi}{7}$ of the vertices.

(3) $D_{2n} = \langle r, t \rangle$

(4) Define $X_{2n} = \langle x, y : x^n = y^2 = e, xy = yx^2 \rangle$. Since $y^2 = e$, we have $x = xy^2 = (xy)y = y(x^2y) = y^2x^4 = x^4$; thus $x^4 = x$, hence $x^3 = e$. Therefore for any n, $\operatorname{ord} X_{2n} = 6$, by the same argument we made for D_{2n}.

(5) Let $Y = \langle u, v : u^4 = v^3 = e, uv = v^2u^2 \rangle$. We have $u = uv^3 = v^6u^2 = (v^3)^2u^2 = e^2u^2 = u^2$, hence $u^2 = u$, hence $u = e$; thus we also get that $v^2 = v$, hence $v = e$. Therefore $Y = \langle e \rangle$, the trivial group.

The previous two examples show that not every relation may be listed in the representation of a given group. It turns out in the case of D_{2n}, that all the relations are listed, but as in the above example with X_{2n} and Y, we had the relations $x^4 = x$ and $u^2 = u, v^{=}v$. Thus one may be careful when dealing with group representations and take care that no relations are left unattended. One consequence might be an erroneous arguing of group order; one can be led to believe that $\operatorname{ord} X_{2n} = 2n$, where in reality $\operatorname{ord} X_{2n} = 6$ and that $\operatorname{ord} Y = 6$, where in reality, $\operatorname{ord} Y = 1$.

1.3 Permutation Groups and the Symmetric Group.

Definition. Let S be any set, we define $S(A)$ to be the **symmetric group** on A of all permutations from A onto itself. If $A = \mathbb{Z}/n\mathbb{Z}$ for $n \in \mathbb{Z}^+$, we write $S(A) = S_n$.

Theorem 1.3.1. *For any set S, $A(S)$ is a nonabelian group under function composition.*

Proof. For any $f, g \in A(S)$, we get that $f \circ g$ is also a permutation, so $f \circ g \in A(S)$; moreover, $A(S)$ is associative on account of $\circ$.

Now, the identity map $e : i \to i$, for any $i \in S$ is the identity of $A(S)$, and since $f \in A(S)$ is $1 - 1$ and onto, $f^{-1} \in A(S)$. This makes $A(S)$ a group. That $A(S)$ is nonabelian follows from the noncommutativity of $\circ$. ■

Corollary. $\operatorname{ord} S_n = n!$.

Proof. The proof of this follows by a combinatorial argument counting the number of $1-1$ maps, and the number of onto maps. ■

Definition. We define the **cycle** of a permutation $s \in S_n$ to be a string of integers of ${}^{\mathbb{Z}}\!/\!_{n\mathbb{Z}}$, $(a_0\ \ldots\ a_{n-1})$ where $s : a_i \to a_{i+1}$, where $i \in {}^{\mathbb{Z}}\!/\!_{n\mathbb{Z}}$. We call two cycles **disjoint** if they share no entries.

Lemma 1.3.2. *The cycle decomposition of a given permutation $s \in S_n$ is finite.*

Proof. Let $s = (a_0\ \ldots\ a_{n-1})$ be the cycle decomposition of s. Then by definition, we get $s : a_{n-1} \to a_{(n-1)+1} = a_n = a_0$. ■

Example 1.9. The cycle $(2\ 0\ 1)$ represents the permutation $s : 2 \to 0 \to 1$ in S_3.

Now, since cycles of permutations of S_n are finite, we can define the "lenght" of a cycle.

Definition. The **length** of a cycle of a permutation $s \in S_n$ is the number of entries in the cycle. We call a cycle of length $k \in \mathbb{Z}^+$ a ***k*-cycle**.

Lemma 1.3.3. *For any permutation $s \in S_n$, the elements of ${}^{\mathbb{Z}}\!/\!_{n\mathbb{Z}}$ can be grouped into k cycles of the form:*

$$(a_0\ a_2\ \ldots\ a_{m_1})(a_{m_1+1}\ \ldots\ a_{m_2})\ldots(a_{m_{k-1}}\ \ldots\ a_{mk}) \tag{1.1}$$

Proof. Since s is $1-1$ and onto, s will permute through the entirety of ${}^{\mathbb{Z}}\!/\!_{n\mathbb{Z}}$; so every integer mod n will be represented in the cycle for s.

Now, find $x \in {}^{\mathbb{Z}}\!/\!_{n\mathbb{Z}}$ in a cycle for s. If x is not at the end of the cycle, i.e. if $s(x)$ is not some previous element of cycle of x, then $s(x)$ is next integer in the cycle of x. Otherwise, $s(x)$ is the first integer of another cycle of s, i.e. if $x = a_{m_i}$, then $s(x) = a_{m_i+1}$. There are k such possible cycles for s, where $k \in \mathbb{Z}^+$. ■

Definition. For any permutation $s \in S_n$, we call the concatenation of all cycles of s the **cycle decomposition** of s.

We introduce a neat algorithm for finding the cycle decomposition of a permutation.

Algorithm (The Cycle Decomposition Algorithm)**.** *Let $s \in S_n$ be a permutation of the elements of ${}^{\mathbb{Z}}\!/\!_{n\mathbb{Z}}$.*

step 1: *Choose the smallest $i \in {}^{\mathbb{Z}}\!/\!_{n\mathbb{Z}}$ which has not appeared in a previous cycle; if there is no previous cycle, $i = 0$. Start the cycle at i.*

step 2: *Compute $s(i)$. If $s(i) = i$, close the cycle, and return to **step 1**. Else, concatenate $s(i)$ to i in the cycle.*

step 3: *Repeat **step 2** with $s(i)$.*

step 4: *If ${}^{\mathbb{Z}}\!/\!_{n\mathbb{Z}}$ has been exhausted, go to **step 5**; else return to **step 3**.*

step 5: *Remove all* 1*-cycles and stop.*

Remark. A neat excersise immediately introduces itself as the problem of how to program this cycle decomposition algorithm so that one can simply feed a permutation into a computer and get its cycle decomposition as an output.

Example 1.10. Define the permutation $s \in S_{13}$ by:

$$\begin{array}{rrr} s:1\to 12 & s:2\to 0 & s:3\to 3 \\ s:4\to 1 & s:5\to 11 & s:6\to 9 \\ s:7\to 5 & s:8\to 10 & s:9\to 6 \\ s:10\to 4 & s:11\to 7 & s:12\to 8 \\ s:0\to 2 & & \end{array}$$

Using the cycle decomposition algortithm we get:

$$s = (0\ 2)(1\ 12\ 8\ 10\ 4)(5\ 11\ 7)(6\ 9)$$

The cycle decomposition algorthm provides a neat way of finding the cycle decomposition s; what about s^{-1}, when we are given s?

Lemma 1.3.4. *Let $s \in S_n$ be a permutation with the cycle decomposition $s = (a_0\ a_2\ \ldots\ a_{m_1})(a_{m_1+1}\ \ldots\ a_{m_2})\ldots(a_{m_{k-1}}\ \ldots\ a_{mk})$. Then s^{-1} has the cycle decomposition:*

$$s^{-1} = (a_{m_1} \ldots\ a_2\ \ a_0)(a_{m_2}\ \ldots\ a_{m_1+1})\ldots(a_{mk}\ \ldots\ a_{m_{k-1}}) \tag{1.2}$$

Proof. If $s : a_{m_i} \to a_{m_i+1}$, then $s^{-1} : a_{m_i+1} \to a_{m_i}$. Then by the cycle decomposition algorithm we can derive equation (1.3). ■

We finally come wish to introduce the "product" of cycles.

Definition. Let $s, t \in S_n$ be a permutation with a cycle decompositions defined by the rules $s : a_{m_i} \to a_{m_i+1}$ and $t : b_{m_i} \to b_{m_i+1}$. Then we define the **product** of cycle decompositions, $\circ$, to be: $s \circ t$ whose cycle decomposition is defined by the rule $s \circ t : b_{m_i} \to b_{m_i+1} \to a_{m_j}$, where $a_{m_j} = s(b_{m_i+1})$ and $b_{m_i+1} = t(b_{m_i})$. We define the concatenation of cycles to be the product of cycle decompositions.

Example 1.11. Consider the cycles $(1\ 3)$ and $(1\ 2)(3\ 0)$ in S_4. Then $(1\ 3) \circ (1\ 2)(3\ 0) = (1\ 3\ 0)$.

We can now refphrase theorem 1.3.1 as:

Theorem 1.3.5. *Define S_n to be the set of all cycle decompositions of permutations of the elements of ${}^{\mathbb{Z}}\!/_{n\mathbb{Z}}$. Then S_n is a group under cycle products.*

Corollary. *S_n is nonabelian for $n \geq 3$.*

Corollary. *Disjoint cycles commute.*

Lemma 1.3.6. *Let $s \in S_n$ be a k-cycle. Then* $\operatorname{ord} s = k$.

Proof. We have that $s = (a_1\ a_2\ \dots\ a_k)$, thus s maps $a_i \to a_{i+1}$, for $i \in \mathbb{Z}/k\mathbb{Z}$; also notice that $s : a_{k-1} \to a_0$. Then $s^k : a_i \to a_{i+k \mod k} = a_i$, for all i, thus $s^k = (1)$. Moreover, if $m \in \mathbb{Z}^+$ such that $s^m : a_i \to a_{i+m \mod k}$, then $a_i = a_j$ for some other $j \in \mathbb{Z}/n\mathbb{Z}$, which implies that s is a $k-1$-cycle, which cannot happen. Thus $\operatorname{ord} s = k$. ■

Corollary. *If $s, t \in S_n$ are k and m-cycles, respectively, then* $\operatorname{ord} st = [k, m]$.

Corollary. *Let $s \in S_n$, then the cycle composition of s is a product of disjoint m_k cycls where $k \in \mathbb{Z}/n\mathbb{Z}$.*

1.4 The General and Special Linear Groups of $n \times n$ Matrices.

One special class of groups are those that can be defined on matrices. We first need to define, in an elementary sense what a "field" is; though we will not go into their study here. We assume familiarity with matrix algebra such as matrix multiplication and determinants. This makes this section, in a sense, optional.

Definition. Let F be a set together with binary operations $+$, called **addition** and $\cdot$, called **multiplication**. We call $(F, +, \cdot)$ a **field** if:

(1) $(F, +)$ forms an abelian group.

(2) $(F^*, \cdot)$ forms an abelian group; where $F^* = F \backslash \{e\}$, e is the identity of F under $+$.

(3) $\cdot$ **distributes** over $+$; that is, for $a, b, c \in F$, $a(b + c) = ab + ac$.

Example 1.12. (1) The sets $\mathbb{Q}$ and $\mathbb{R}$ are fields under the usual addition and multiplication.

(2) $\mathbb{C}$ is a field under complex addition and complex multiplication. So is $\mathbb{R}$ if we take all $a \in \mathbb{R}$ to have the form $a + i0$.

(3) $\mathbb{Z}/p\mathbb{Z}$, with $p \in \mathbb{Z}^+$ prime forms a field under addition and multiplication $\mod p$.

Definition. Let F be a field. We define $F^{n \times n}$ to be the field of all $n \times n$ matrices with entries in F. We define the **general linear group** to be $GL(n, F) = \{A \in F^{n \times n} : \det A \neq 0\}$. We define the **special linear group** to be $SL(n, F) = \{A \in F^{n \times n} : \det A = 1\}$. If $F = \mathbb{Z}/p\mathbb{Z}$, we write $GL(n, \mathbb{Z}/p\mathbb{Z}) = GL(n, p)$ and $SL(n, \mathbb{Z}/p\mathbb{Z}) = SL(n, p)$.

Theorem 1.4.1. *For any field F, and $n \in \mathbb{Z}^+$, $GL(F, n)$ forms a group under matrix multiplication.*

Proof. Let $A, B \in GL(F, n)$ be $n \times n$ matrices. Then $\det A \neq 0$ and $\det B \neq 0$, so $detAB = \det A \det B \neq 0$, by a well known property of determinants. So $GL(F, n)$ is closed. Now since matric multiplication is associative, then $GL(F, n)$ satisfies the associative law.

Now consider the $n \times n$ identity matrix I, we have for any $A \in GL(F, n)$, $AI = IA = A$, moreover, $\det I = 1 \neq 0$ making $I \in GL(F, n)$. Likewise, since for $A \in GL(F, n)$, $\det A \neq 0$, A is invertible, by well known properties of matrices, so A^{-1} exists, and $\det A^{-1} = \det A \neq 0$. Thus $A^{-1} \in GL(F, n)$ and since $AA^{-1} = A^{-1}A = I$, this makes A^{-1} the inverse of A. ■

Corollary. *$SL(F, n)$ forms a group under matrix multiplication.*

Proof. Notice that $SL(F, n) \subseteq GL(F, n)$, so $SL(F, n)$ inherits closure (and associativity). Now, for $A \in SL(F, n)$, $A \in GL(F, n)$, so A^{-1} exists. Moreover, $\det A^{-1} = \det A = 1$, making $A^{-1} \in SL(F, n)$. This also implies that $I \in SL(F, n)$. ■

Example 1.13.

$$GL(2,2) = \{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\}$$

Labeling these elements as I, A, B, C, D, and E, consecutively we find the orders to be: $\operatorname{ord} I = 1$, $\operatorname{ord} A = 2$, $\operatorname{ord} B = 2$, $\operatorname{ord} C = 3$, $\operatorname{ord} D = 3$, and $\operatorname{ord} E = 2$.

Example 1.14. Consider $GL(2, 2)$, and considering the labeling of the above example, we compute the Cayeley table to be:

$$\begin{pmatrix} I & A & B & C & D & E \\ A & I & D & E & B & C \\ B & C & I & A & E & D \\ C & B & E & D & I & A \\ D & E & I & I & C & I \\ E & D & C & B & A & I \end{pmatrix}$$

which is not symmetirc, hence $GL(2, 2)$ is not Abelian. In general, for $n, p \in \mathbb{Z}^+$ and p prime, for $A, B \in GL(n, p)$ we have

$$\begin{pmatrix} A & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} B & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} AB & 0 \\ 0 & 1 \end{pmatrix}$$

while

$$\begin{pmatrix} B & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} A & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} BA & 0 \\ 0 & 1 \end{pmatrix}$$

then

$$\begin{pmatrix} AB & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} BA & 0 \\ 0 & 1 \end{pmatrix}$$

if, and only if $AB = BA$, which is in general, not true for matrices. So $GL(n, p)$ is not necesarrily Abelian.

Now, we would like to observe the order of the group $GL(n, p)$, the order of $SL(n, p)$ will be derived later.

Example 1.15. (1) We have that if F is a field with $\operatorname{ord} F = p$, then $\operatorname{ord} GL(n, F) < p^{n^2}$, for, notice for any $A \in F^{n\times n}$, there are n^2 entries, and p choices for each entry, thus $\operatorname{ord} F^{n\times n} = n^2$, now, by definition, $GL(n, F)$ excludes those with $\det = 0$, thus we get the result.

(2) Let $A \in GL(2, 2)$ where:

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

where $a, b, c, d \in {}^{\mathbb{Z}}\!/_{2\mathbb{Z}}$. Then we have that if $ad - bc \neq 0$, then $ad \neq bc$, thus a is a multiple of c and d is a multiple of b, let us consider the columns. We have that if $a = c = 0$, then $\det A = 0$, thus a and c cannot be both 0, also notice that there are 2^2 possible choices for a and c, so the fist column, $\begin{pmatrix} a \\ c \end{pmatrix}$, hase $2^2 - 1$ possible choices. Now, obvserving column $\begin{pmatrix} b \\ d \end{pmatrix}$, we have the 2^2 choices for both entries, however, since b and d are multiples of eachother, we must exclude the 2 choices for the multiples ad and bc. Thus the column $\begin{pmatrix} b \\ d \end{pmatrix}$ has $2^2 - 2$ choices. That is, $\operatorname{ord} GL(2, 2) = (2^2 - 1)(2^2 - 2) = 2 \cdot 3 = 6$.

Observing further, we can see that $\operatorname{ord} GL(n, 3) = (3^n - 1) \dots (3^n - 3)$, and so on. Thus we have:

Theorem 1.4.2. *For $n, p \in \mathbb{Z}^+$ and p prime :*

$$\operatorname{ord} GL(n, p) = \prod_{j=1}^{n-1} (p^n - p^{n-j}) \tag{1.3}$$

Proof. Consider the $n \times n$ matrix $A = (a_{ij}) \in GL(n, p)$, observe that there are $p^n - 1$ choices for the first column, $\begin{pmatrix} a_{11} \\ \vdots \\ a_{n1} \end{pmatrix}$ since $a_{11}, \dots, a_{n1}$ cannot all be 0. Now, we have $\det A = \sum_{j=1}^{n} (-1)^{i+j} a_{ij} \det A_{ij}$, with A_{ij} the cofactor of A about the entry a_ij. So, for the $j^{th} column \begin{pmatrix} a_{1j} \\ \vdots \\ a_{nj} \end{pmatrix}, then a_{ij} \det A_{ij} = \sum_{l=1}^{j-1} (-1)^{i+j} a_{il} \det A_{il} + \sum_{l=1}^{j+1} (-1)^{i+j} a_{il} \det A_{il}$, for which there are $p^n - p^j$ choices, given that each of the a_{ij} entries are multiples of the previous entries, for $1 \leq i \leq n$. Taking $2 \leq j \leq n$ (since we already evaluated the first column), we get there are:

$$\prod_{j=1}^{n-1} (p^n - p^{n-j})$$

choices for the matrix A. Since A is abritrary, we get the order of $GL(n, p)$. ■

We also need to comment on the order of $GL(n, F)$ when the field F is infinite.

Theorem 1.4.3. *For any field F, $GL(n,F)$ is of infinite order if, and only if F is of infinite order.*

Proof. We show by contrapositives. Suppose that F is finite with $\operatorname{ord} F = k$. Then by the same argument of theorem 1.4.2, we find there are $\prod (k^n - k^j)$ matrices $A \in GL(n,F)$. Any additional elements contradict this result, and so $GL(n,F) = \prod (k^n - k^j)$.

On the otherhand, if $\operatorname{ord} GL(n,F) = k$ then there are k $n \times n$ matrices over F with $\det \neq 0$. Now, if F were not finite, then there exists a distrinct matrix $A \in GL(n,F)$, making $\operatorname{ord} GL(n,F) = k+1$ a contradiciton. Thus, F must be finite. ■

We now introduce a seperate group from the general and special linear groups.

Definition. Let F be a field. We define the **Heisenberg** group over F to be the set:

$$H(F) = \{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} : a,b,c \in F\} \tag{1.4}$$

That is, $H(F)$ is the set of all upper triangular matrices over F with diagonal entries equal to 1 (the identity element of F).

Lemma 1.4.4. *For any field F, $H(F)$ is a group under matrix multiplication.*

Proof. Let $X = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$, and $Y = \begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix}$. Then $XY = \begin{pmatrix} 1 & a+d & e+af+b \\ 0 & 1 & f+c \\ 0 & 0 & 1 \end{pmatrix}$. So $H(F)$ is closed. Additionally, $H(F)$ inherits the associativity of matrix multiplication.

Now, we get that $I = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ serves as the identity, and the matrix $Y = \begin{pmatrix} 1 & -a & ac-b \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{pmatrix}$ serves as an inverse to X. This makes $H(F)$ into a group. ■

Corollary. *$H(F)$ is non-Abelian.*

Corollary. $\operatorname{ord} H(F) = (\operatorname{ord} F)^3$.

Proof. Let $\operatorname{ord} F = k$, then we have n choices for a, b, and c, hence n^3 choices for an arbitrary matrix in $H(F)$. ■

Corollary. *$H(F)$ is finite if, and only if F is finite.*

1.5 Homomorphism.

In this section, we relate the structures of groups to each other. The main reason to do this is to determine which groups are "equal", i.e. when two distinct groups share the same group structure. Doing this will often allow us to infer properties of one group from the other.

Definition. Let $(G, *)$ and $(H, \cdot)$ be groups. We call a map $\phi : G \to H$ a group **homomorphism** if for any $a, b \in G$, $\phi(a * b) = \phi(a) \cdot \phi(b)$. We call the homomorphism ϕ a group **isomorphism** if ϕ is both $1-1$ and onto. If such an isomorphism exists between G and H, we call G and H **isomorphic** and write $G \simeq H$.

Remark. Frequently, we will imply the operations on G and H and write $\phi(ab) = \phi(a)\phi(b)$.

Lemma 1.5.1. *Isomorphism of groups is an equivalence relation.*

Proof. Let G and H be groups. First, take $\phi : G \to G$ by $phi : g \to g$, then ϕ is an isomorphism, so $G \simeq G$.

Now suppose that $G \simeq H$, then there is an isomorphism $\phi : G \to H$. Then consider $\phi^{-1} : H \to G$, we have ϕ^{-1} is also $1-1$ and onto; moreover $\phi^{-1}(\phi(ab)) = ab = \phi^{-1}(\phi(a))\phi^{-1}(\phi(b))$. This makes phi^{-1} an isomorphism and so $H \simeq G$.

Lastly, let K be a group and suppose $G \simeq H$ and $H \simeq K$. Then there are isomorphisms $\phi : G \to H$ and $\psi : H \to K$. Then take $\psi \circ \phi : G \to K$ which is $1-1$ and onto by definition. Then $\psi \circ \phi(ab) = \psi(\phi(a)\phi(b)) = \psi(\phi(a))\psi(\phi(b))$. Thus $G \simeq K$. ∎

Example 1.16. (1) The maps $\exp : (\mathbb{R}, +) \to (\mathbb{R}^+, \cdot)$ and $\log : (\mathbb{R}^+, \cdot) \to (\mathbb{R}, +)$ defined by $\exp : x \to e^x$ and $\log : y \to \log y$. Then exp and log are homomorphisms. We have $\exp x + y = \exp x \exp y$ and $\log xy = \log x + \log y$. Moreover, exp and log are group isomorphisms, infact, $\log = \exp^{-1}$.

(2) Let S and T be nonempty finite sets. Then $A(S) \simeq A(T)$ if and only if $|S| = |T|$, i.e. the symmetric groups of S and T are isomorphic if, and only if S and T share the same cardinality.

Suppose S and T are finite, and that $|S| = |T| = n$. Define the map $\phi : A(S) \to A(T)$ by $\phi : s \to tst^{-1}$, there $t : S \to T$ is a bijection. Then ϕ is $1-1$, for $tst^{-1} = ts't^{-1}$ implies $s = s'$. Moreover, we have $\phi(A(S)) = A(T)$, since for any $s \in A(S)$, $tst^{-1} : T \to T$ defines a bijection from T onto itself; hence $tst^{-1} \in A(T)$. Therefore, we get ϕ is an isomorphism form $A(S)$ to $A(T)$. This makes $A(S) \simeq A(T)$.

On the other hand, if $A(S) \simeq A(T)$, then $\operatorname{ord} A(S) = \operatorname{ord} A(T) = n!$, for some $n \in \mathbb{Z}^+$, this implies that $|S| = |T| = n!$.

Lemma 1.5.2. *Let G and H be groups, and let $\phi : G \to H$ be a homomorphism. Then the following are true:*

(1) $\phi(e) = e'$ where e and e' are the identites of G and H, respectively.

(2) $\phi(a^{-1}) = \phi(a)^{-1}$.

Proof. We have that $\phi(e) = \phi(aa^{-1}) = \phi(a)\phi(a^{-1})$. Thus by cancellation, we get $\phi(a)^{-1} = \phi(a^{-1})$. By consequence, we also get that $\phi(e) = \phi(a)\phi(a)^{-1} = e'$; for any $a \in G$. ∎

Corollary. *The following are also true for any $n \in \mathbb{Z}^+$:*

(1) $\phi(a^n) = \phi(a)^n$.

(2) $\phi(a^{-n}) = \phi(a)^{-n}$.

Proof. Firstly, $\phi(a^n) = \underbrace{\phi(a)\dots\phi(a)}_{n \text{ times}} = \phi(a)^n$. Then we get $\phi(a^{-n}) = \phi((a^{-1})^n) = \phi(a^{-1})^n = \phi(a)^{-n}$. ■

Lemma 1.5.3. *Let G and H be groups and suppose $G \simeq H$. Then the following are true:*

(1) $\operatorname{ord} G = \operatorname{ord} H$*.*

(2) G is Abelian if, and only if H is abelian.

(3) For all $x \in G$, $\operatorname{ord} x = \operatorname{ord} \phi(x)$*, where $\phi : G \to H$ is the underlying isomorphism.*

Proof. Let $G \simeq H$, via the isomorphism ϕ. Then since ϕ is $1-1$ and onto, every element of G must get mapped to every element of H. This makes $\operatorname{ord} G = \operatorname{ord} H$.

Now, suppose G is Abelian, then for every $a, b \in G$, $ab = ba$. Thus $\phi(ab) = \phi(ba)$. This makes $\phi(a)\phi(b) = \phi(b)\phi(a)$, since a, b are arbitrary, this makes H Abelian. The converse is an equivalent argument with ϕ^{-1}.

Now suppose that $x \in G$ has order $\operatorname{ord} x = n$. Then $x^n = e$. Thus $\phi(x^n) = \phi(e)$, thus $\phi(x)^n = e'$. Now since n is minimal, any $m < n$ for which $\phi(x)^m = e'$ would imply that $x^m = e$, which cannot happen. Thus $\operatorname{ord} \phi(x) = n$. ■

Corollary. *Let $\phi : G \to H$ be a homomorphism. If H is Abelian, and ϕ is $1-1$, then G is Abelian. On the otherhand, if G is Abelian, and ϕ is onto, then H is Abelian.*

Proof. For $a, b \in G$, $\phi(a)\phi(b) = \phi(b)\phi(a)$, hence $\phi(ab) = \phi(ba)$. Since ϕ is $1-1$, this implies $ab = ba$.

On the otherhand, if $ab = ba$ for any $a, b \in G$ and ϕ is onto, then we get $\phi(ab) = \phi(ba)$ hence $\phi(a)\phi(b) = \phi(b)\phi(a)$. Since $\phi(G) = H$, this completes the proof. ■

Example 1.17. (1) We have $S_3 \not\simeq \mathbb{Z}/6\mathbb{Z}$, despite having the same order. We have S_3 is nonabelian while $\mathbb{Z}/6\mathbb{Z}$ is Abelian.

(2) $(\mathbb{R}, +) \not\simeq (\mathbb{R}^*, \cdot)$ since in $\mathbb{R}^*$, $\operatorname{ord} -1 = 2$, while there are no elements of order 2 in $\mathbb{R}^+$.

Lemma 1.5.4. *Let G and H be groups with representations; let $G = \langle S : R_1, \dots R_n \rangle$ and $H = \langle T : R_1', \dots, R_n' \rangle$. Then if the relations R_i is satisfied by the elements of H, for each $1 \leq i \leq n$, then there exits a unique homomorphism ϕ definied by $\phi : R_i \to R_i'$.*

Remark. We defer the proof of this lemma.

Example 1.18. (1) Take $D_{2n} = \langle r, t : r^n = t^2 = e, rt = tr^{-1} \rangle$, and take $X_{2k} = \langle a, b : a^k = b^2 = e, ab = ba^{-1} \rangle$. If $n = km$ for $m \in \mathbb{Z}^+$, then $a^n = (a^k)^m = e$, so the relations of D_{2n} are satisfied by the generators of X_{2n}. Thus take homomorhism $\phi : D_{2n} \to X_{2k}$ by $\phi : r, t \to a, b$. Since $X_{2k} = \langle a, b \rangle$, ϕ is onto. ϕ is $1-1$ if, and only if $n = k$. So, in general, $D_{2n} \not\simeq X_{2k}$.

(2) Consider D_6 and S_3. Let $a = (1\ 2\ 3)$ and $b = (1\ 2)$. Then $a^3 = (1)(2)(3) = (1)$ and $b^2 = (1)$; moreover, $ab = (1\ 2\ 3)(1\ 2) = (1\ 2)(3\ 2\ 1) = ba^{-1}$. Thus take $\phi : D_6 \to S_3$ by $\phi : r, t \to (1\ 2\ 3), (1\ 2)$. By the above reasoning, ϕ is onto. Now since $\operatorname{ord} D_6 = \operatorname{ord} S_3 = 6$, ϕ is $1-1$ and so ϕ is an isomorphism and $D_6 \simeq S_3$.

Example 1.19. (1) $\mathbb{C}^* \not\simeq \mathbb{R}^*$, since $i \in \mathbb{C}^*$ has $\operatorname{ord} i = 4$, while $\mathbb{R}^*$ has no elements of order 4.

(2) $\mathbb{R} \not\simeq \mathbb{Q}$, for $\mathbb{Q}$ is countable, and $\mathbb{R}$ is not. That is if we take $\operatorname{ord} \mathbb{Q}$ and $\operatorname{ord} \mathbb{R}$ to be defined and assume results from set theory and topology, then $\operatorname{ord} \mathbb{Q} < \operatorname{ord} \mathbb{R}$.

(3) $\mathbb{Z} \not\simeq \mathbb{Q}$, for suppose otherwise. If $\phi : \mathbb{Z} \to \mathbb{Q}$ is an isomorphims, then $\phi(1) = a$, then $\phi(\frac{1}{2} + \frac{1}{2}) = a$, then $2\phi(\frac{1}{2}) = a$, likewise $3\phi(\frac{1}{3}) = a$, then $2\phi(\frac{1}{2}) = 3\phi(\frac{1}{3})$, implying $\phi(\frac{1}{2}) = \phi(\frac{1}{3})$, but $\frac{1}{2} \neq \frac{1}{3}$, contradicting the $1-1$ness of ϕ.

(4) Notice that if $n < m$, then $\operatorname{ord} S_n = n! < \operatorname{ord} S_m = m!$, so $S_m \simeq S_n$ if, and only if $n = m$, for $n, m \in \mathbb{Z}^+$.

(5) $D_{24} \not\simeq S_4$. Notice $r \in D_{24} = D_{2\cdot 12}$ has $\operatorname{ord} r = 12$. Now, any permutation in S_4 is either a 4-cycle, a 3-cycle, or a product of two 2-cycles, thus every $s \in S_4$ has $\operatorname{ord} s \leq 4$, and so there are no elements of order 12 in S_4.

We finish with some results.

Lemma 1.5.5. *Let A and B be groups. Then $A \times B \simeq B \times A$.*

Proof. Take the map $A \times B \to B \times A$ by taking $(a, b) \to (b, a)$. This map is $1-1$ and onto, for $(b, a) = (b', a')$ implies $a = a'$ and $b = b'$, and $\operatorname{ord} A \times B = \operatorname{ord} B \times A$. Lastly, notice that $(bb', aa') = (b, a)(b'a')$, which makes it a homomorphism. Thus there is an isomorphism from $A \times B$ onto $B \times A$. ■

Lemma 1.5.6. *Let A, B, C be groups. Then $(A \times B) \times C \simeq A \times (B \times C)$.*

Proof. Consider the map $(A \times B) \times C \to A \times (B \times C)$ by taking $(a, (b, c)) \to ((a, b), c)$. This map is $1-1$ and onto by the same reasoning used in the above lemma, moreover, this map is a homomorphsm by closure. This completes the proof. ■

Chapter 2

Subgroups.

2.1 Definitions and Examples.

Definition. Let G be a group. We call a nonempty subset $H \subseteq G$ a **subgroup** if H is also a group under the binary operation of G. We write $H \leq G$; if $H \neq G$, then we write $H < G$.

There are two immediate results that we can develop.

Theorem 2.1.1 (The Subgroup Critetrion.)**.** *Let G be a group. Then a subset $H \subseteq G$ is a subgroup if, and only if:*

(1) For every $a, b \in H$, $ab \in H$.

(2) $a^{-1} \in H$ whenever $a \in H$.

Proof. Suppose first that $H \leq G$, then by definition, (1) and (2) are satisfied.

Now suppose that H is closed under the operation on G, (1), and that H has inverses (2). Immediately, the closure and inverse laws are satisfied, moreover, since $H \subseteq G$, H inherits the associativity of G under the relavent operation. Now, by (1) and (2) we have $aa^{-1} = e \in H$, and so the identity law is satisfied. This makes $H \leq G$. ■

Corollary. *If H is a finite subset of G, then H is a subgroup if H is closed under the operation of G.*

Proof. Let $a \in H$, by closure, we have $a^n \in H$ for $n \in \mathbb{Z}^+$. So, consider the infinite collection $\{a^i\}_{i=1} \subseteq H$; since H is finite, there are repetitions in the collection $\{a^i\}$, that is, $a^i = a^j$ for some $i \neq j$ and $i, j > 0$. Then $a^{i-j} = e$, so $a^{i-j-1} = a^{-1}$. Now, since $i - j > 0$, we get $i - j - 1 \geq 0$, which makes $a^{-1} \in H$. By the above theorem, we get $H \leq G$. ■

Example 2.1. (1) $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R}$ under the usual addition. $\mathbb{Q}^* \leq \mathbb{R}^*$ under the usual multiplication. $\mathbb{R} \leq \mathbb{C}$ under complex addition, and $\mathbb{R}^* \leq \mathbb{C}^*$ under complex multiplication (here, we take $a \in \mathbb{R}$ to have the form $a + i0$).

(2) For any group G, $G \leq G$ and $\langle e \rangle \leq G$. So the minimum number of subgroups that any group has is 2.

(3) Let $H = \{e, r, \dots r^{n-1}\} \subseteq D_{2n}$. Then $H \leq D_{2n}$.

(4) Let $n\mathbb{Z} = \{na : a \in \mathbb{Z}\}$, for any $n \in \mathbb{Z}$. Then $n\mathbb{Z} \leq \mathbb{Z}$ under the usual addition. Let $na, nb \in n\mathbb{Z}$, then $na + nb = n(a + b) \in n\mathbb{Z}$, and $n(-a) = -na \in n\mathbb{Z}$. We will be interested in the subgroup $n\mathbb{Z}$ of $\mathbb{Z}$, in particular, for $n \in \mathbb{Z}^+$.

(5) Let $Z = \{z \in \mathbb{C} : z^n = 1\}$. Then $Z \leq \mathbb{C}^*$ under complex multiplication. Notice that $z, w \in Z$ implies $z^n w^n = (zw)^n = 1$, and $(z^{-1})^n = \frac{1}{z^n} = 1$, so $z^{-n} = 1$. We call this group the **roots of unity** in $\mathbb{C}$. If we take $n = 4$, then we get that $Z = \{1, i, -1, -i\}$.

(6) Let $\mathbb{Z} + i\mathbb{Z} = \{a + ib \in \mathbb{C} : a, b \in \mathbb{Z}\}$. Then $\mathbb{Z} + i\mathbb{Z} \leq \mathbb{C}$ under complex addition. We call this group the **Gaussian integers.**

(7) Leet $\mathbb{Q} + \sqrt{2}\mathbb{Q} = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$. Then $\mathbb{Q} + \sqrt{2}\mathbb{Q} \leq \mathbb{R}$ under the usual addition.

We now give some nonexamples of subgroups.

Example 2.2. (1) $\mathbb{Q}^* \not\leq \mathbb{R}$ under the usual addition (why?).

(2) $\mathbb{Z}^+ \not\leq \mathbb{Z}$ under the usual addition. Notice the identity of $\mathbb{Z}$, $0 \notin \mathbb{Z}^+$.

(3) $D_6 \not\leq D_8$. Notice $D_6 = \{e, t, r, r^2, rt, r^2t\}$, and $D_8 = \{e, t, r, r^2, r^3, rt, r^2t, r^3t\}$. One might be tempted to think $D_6 \subseteq D_8$, but notice that in D_6, $r^3 = e$ while in D^8, $r^4 = e$. Thus $D_6 \not\subseteq D_8$.

2.2 Special Subgroups.

We introduce now, some very important examples of subgroups.

Definition. Let G be a group. We define the **centralizer** of an element $a \in G$ to be the set $C(a) = \{g \in G : gag^{-1} = a\}$. We define the **centralizer** of a nonemppty subset A of G to be the set $C(A) = \{g \in G : gag^{-1} = a, \text{ for all } a \in A\}$.

Lemma 2.2.1. *Let G be a group. Then for $a \in G$, $C(a) \leq G$. Likewise, for $A \subseteq G$ nonempty, $C(A) \leq G$.*

Proof. Notice that given $a \in A$, $C(a) \subseteq C(A)$. Then we have that $C(a)$, for $eae^{-1} = eae = a$, so $e \in C(a)$, this also implies that $e \in C(A)$.

Now let $x, y \in C(a)$ then $xax^{-1} = a$, and $yay^{-1} = a$. Notice then that $a = y^{-1}ay = y^{-1}a(y^{-1})^{-1}$, so we have $y^{-1} \in C(a)$. Then $(xy)a(xy)^{-1} = xyay^{-1}x^{-1} = x(yay^{-1})x^{-1} = x(yy^{-1}ay^{-1}y)x^{-1} = xax^{-1} = a$, so $xy \in C(a)$, thus $C(a) \leq G$, if we take $a \in A$ arbitrary, this makes $C(A) \leq G$ as well. ■

Corollary. *$C(a) \leq C(A)$ for any $a \in A$.*

Corollary. *$C(A) = \bigcap_{a \in A} C(a)$.*

Remark. In the abve corollary, notice that $\bigcup C(a)$ is not necessarily a disjoint union.

Example 2.3. Let G be abelian, then $C(G) = G$.

Definition. Let G be a group. We define the **center** of G to be the set $Z(G) = \{g \in G : gx = xg \text{ for all } x \in G\}$.

Lemma 2.2.2. *Let G be a group. Then $Z(G) \leq G$.*

Proof. Notice that if $g \in Z(G)$, then for any $x \in G$, $gx = xg$ implies that $gxg^{-1} = g$, making $g \in C(G)$; likewise, $g \in C(G)$ implies $gxg^{-1} = x$ which implies that $xg = gx$, for any $x \in G$; so $g \in Z(G)$. That is, $Z(G) = C(G)$ which makes $Z(G)$ a subgroup. ■

Definition. Let G be a group and let $A \subseteq A$. Define $gAg^{-1} = \{gag^{-1} : a \in A\}$, where $g \in G$. We define the **normalizer** of A to be the set $N(A) = \{g \in G : gAg^{-1} = A\}$.

Lemma 2.2.3. *Let G be a group, and let $A \subseteq G$. Then $N(A) \leq G$.*

Proof. Let $x, y \in N(A)$, then $xAx^{-1} = A$ and $yAy^{-1} = A$, then for any $a \in A$, then for some $a, b \in A$, $xaa^{-1} = b$ and $yaa^{-1} = b$. Then $(xy)a(xy)^{-1} = x(yay^{-1})x^{-1} = xbx^{-1} = b$, thus $xy \in N(A)$. Similarly, $xax^{-1} = b$ implies $a = x^{-1}bx$, thus $x^{-1} \in N(A)$. This makes $N(A) \leq G$. ■

Corollary. $C(A) \leq N(A)$.

Example 2.4.

(1) If G is abelian, then $ab = ba$ for all $a, b \in G$, thus $G = Z(G)$. Similarly, we get $gag^{-1} = gg^{-1}a = a$ for all $a \in A \subseteq G$ and $g \in G$, thus $C(A) = N(A) = G$.

(2) Consider the dihedral group D_{2n}. Let $A = \{e, r, \dots, r^{n-1}\} \leq D_{2n}$. Then $C(A) = A$, We have that $A \subseteq C(A)$, since $r^j r^i r^{-j} = r^{j+i-j} = r^i$. On the other hand we have $(r^j t)r^i(r^j t)^{-1} = r^{j+i-j}t^2 = r^i$, which makes $C(A) \subseteq A$. Moreover, $N(A) = D_{2n}$, since by the above computations we also get $D_{2n} \subseteq N(A)$.

(3) In D_{2n}, $Z(D_{2n}) = \{r^i : r^- = r^{-i}\}$, where $i \in \mathbb{Z}/n\mathbb{Z}$. So in D_8, $Z(D_8) = \{e, r^2\}$. Essentially, to find the center of D_{2n}, find all those powers i of r for which $i \equiv -i \mod n$.

(4) Let $A = \{(1), (1\ 2)\} \leq S_3$. Then $C(A) = N(A) = A$. Moreover, $Z(S_3) = \langle (1) \rangle$. Notice that since $S_3 \simeq D_6$, then to preserve the group structure, $Z(S_3) \simeq Z(D_6)$. Notice then that $Z(D_6) = \langle e \rangle$.

We can treat the fact that, for a subset A of a group G, the normalizer and centralizer of G, and the center of G are all special cases of group actions.

Definition. If G is a group acting on a set A, then we define the **stabalizer** of $a \in A$ in G to be the set $\operatorname{stab} a = \{g \in G : ga = a\}$. We define the **stabalizer** of A to be $\operatorname{stab} A = \{g \in G : ga = a \text{ for all } a \in a\}$.

Lemma 2.2.4. *Let G be group acting on a set S. Then for any $s \in S$, $\operatorname{stab} s \leq G$.*

Proof. For $a, b \in \operatorname{stab} s$, we have $(ab)s = a(bs) = as = s$, so $ab \in \operatorname{stab} a$. Likewise, $a^{-1} \in \operatorname{stab} s$. ■

Corollary. $\ker S \leq G$.

Proof. The proof is identical to that of the above lemma. ■

Corollary. $\operatorname{stab} s \leq \ker s$.

Proof. We have that both $\operatorname{stab} s$ and $\ker s$ are both groups. Then notice that since $s \in S$, then $\operatorname{stab} s \subseteq \ker s$. ■

Corollary. $\ker s = \bigcap_{s \in S} \operatorname{stab} s$.

Example 2.5. (1) Consider the dihedral group D_8 of symmetries of a square acting on the labeling $\mathbb{Z}/_{4\mathbb{Z}}$ of vertices. Then $\operatorname{stab} i = \{e, r^2t\}$, where r^2t is the reflection of the square about the line crossing the vertex i and the center of the square.

(2) In general, consider the dihedral group D_{2n} of symmetries of an n-gon acting on the labeling $\mathbb{Z}/_{n\mathbb{Z}}$ of vertices. Notice that if $r^jt \in \operatorname{stab} i$, for any $i \in \mathbb{Z}/_{n\mathbb{Z}}$, then $(r^jt)i = i$. Then $n + j - i = i$, i.e. $j \equiv 2i \mod n$, and so $\operatorname{stab} i = \{r^jt : j \equiv 2i \mod n\} = \{e, r^2t, r^4t, \ldots, r^{2n-2}t\}$.

(3)

Definition. Let G be a group acting on a set A We define the **conjugation** action of G on A to be the map $G \times A \to A$ defined by $(g, a) \to gag^{-1}$. We define the **conjugation** of A, gAg^{-1} to be the image of this action.

Lemma 2.2.5. *Conjugation is a group action.*

Proof. Let G be and A a nonempty set. Take the map $G \times A \to A$ via $(g, a) \to gag^{-1}$. Then for $e \in G$ the identity, $(e, a) \to eaa^{-1} = a$, now for $x, y \in G$, $(xy, a) \to (xy)a(xy)^{-1} = x(yaa^{-1})x^{-1} = (x, (y, a))$. Thus this map is a group action, and G acts on A via conjugation. ■

Lemma 2.2.6. *Let G be a group acting on a set $A \subseteq G$ via conjugation. Then* $\operatorname{stab} A = N(A)$.

2.3 Cyclic Groups.

Definition. Let G be a group, and let $H \leq G$ be a subgroup. We say that H is **cyclic** if it can be generated by a single element. That is, there is some $x \in H$ for which $H = \{x^n : n \in \mathbb{Z}\}$. We write $H = \langle x \rangle$.

Remark. Notice that if H is cyclic, there is a singleton set that generates H, i.e. $H = \langle \{x\} \rangle$.

Lemma 2.3.1. *If $G = \langle g \rangle$, then $G = \langle g^{-1} \rangle$.*

Proof. For any $h \in G$, if $h = g^n$, then $h^{-1} = x^{-n} = (x^{-1})^n$. ■

Lemma 2.3.2. *If G is a cyclic group, then G is Abelian.*

Proof. Let $G = \langle g \rangle$ and for any $m, n \in \mathbb{Z}^+$. Then $g^m g^n = g^{m+n} = g^{n+m} = g^m g^n$. ■

Example 2.6. (1) In D_{2n}, the set $\{e, r, \ldots, r^n\}$ is cyclic, and $\langle r \rangle \leq D_{2n}$.

(2) $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$.

(3) Consider the subgroup $\mathbb{C}_n = \{z \in \mathbb{C} : z^n = 1\} \leq \mathbb{C}$ of complex primitive n-th roots of unity in $\mathbb{C}$, where $n \in \mathbb{Z}^+$. Then $\mathbb{C} = \langle z \rangle = \langle \frac{1}{z} \rangle$.

(4) $\mathbb{C}_4 = \langle i \rangle = \langle -i \rangle$.

Lemma 2.3.3. *Let $G = \langle g \rangle$ be a finite cyclic group, Then* $\operatorname{ord} G = \operatorname{ord} g$.

Proof. Let $\operatorname{ord} g = n$, by the division theorem, there exists $t, q, r \in \mathbb{Z}$ such that $t = nq + r$, with $0 \leq r < n$; i.e. $t \equiv r \mod n$, so $g^t = g^r$. Thus there are at most n such elements in G. Now, suppose $g^i = g^j$ for $0 \leq i < j < n$, then $g^{j-i} = e$, since $j - i < n$, this contradicts the order of g. Therefore, there are eaxctly $\operatorname{ord} g = n$ such element in G, since $G = \langle g \rangle$, these are the only elements, which proves the result. ■

Corollary. *If $G = \langle g \rangle$ is a finite cyclic group, then g is of finite order.*

Proof. If g is of infinite order, then there are infinitely many powers of g, since g generates G, this contradicts the finiteness of G. ■

Lemma 2.3.4. *Let G be a group and let $g \in G$ and let $m, n \in \mathbb{Z}^+$ distinct, such that $g^n = e$ and $g^m = e$. Then $g^{(m,n)} = e$. Moreover,* $\operatorname{ord} g | m$.

Proof. There exist $p, q \in \mathbb{Z}$ such that $mp + nq = (m, n)$. Then by hypothesis, $g^{(m,n)} = (g^m)^p (g^n)^q = e$. Morevoer, assuming, without loss of generality, that $m < n$, we have by definition of the order of g that either $\operatorname{ord} g = m$, or $(\operatorname{ord} g)|m$. ■

Theorem 2.3.5. *If G and H are finite cyclic groups with* $\operatorname{ord} G = \operatorname{ord} H$*, then $G \simeq H$.*

Proof. Let $G = \langle g \rangle$ and $H = \langle h \rangle$. Take the map $phi : \langle g \rangle \to \langle h \rangle$ via the rule $g^k \to h^k$, for some $k \in \mathbb{N}$. We have that $\phi(g^m g^n)\phi(g^{m+n}) = h^{m+n} = h^m h^n = \phi(g^m)\phi(g^n)$. So ϕ defines a homomorphism. Moreover, if $\operatorname{ord} G = \operatorname{ord} H = n$, and $g^s = g^t$ for $s, t \in \mathbb{Z}^+$, $g^{s-t} = e$, so $n | s - t$, that is $s \equiv t \mod n$. Thus $\phi(g^s) = \phi(g^t)$. This makes ϕ well defined.

Now, by definition, every element of $\langle h \rangle$ is of the form $h^k = \phi(g^k)$ for some $k \in \mathbb{N}$, this makes ϕ onto. Since ϕ is onto, and $\operatorname{ord} G = \operatorname{ord} H$ we get that ϕ is $1 - 1$, and so an isomorphism. ■

Corollary. *If $\langle g \rangle$ is an infinite cyclic group, then $\mathbb{Z} \simeq \langle g \rangle$.*

Proof. Define $\phi : \mathbb{Z} \to \langle g \rangle$ by $m \to g^m$. Then $\phi(m + n) = g^{m+n} = g^m g^n = \phi(m)\phi(n)$, moreover, if $m = n$, then $\phi(m) = g^m = g^n = \phi(n)$; so ϕ is a well defined homomorphism.

Now if $\phi(m) = \phi(n)$, then $g^m = g^n$, that is $g^{m-n} = e$, so $m - n = 0$, hence $m = n$. ϕ is $1 - 1$. ϕ is also onto by definitionm therefore ϕ is an isomorphism of $\mathbb{Z}$ onto $\langle g \rangle$. ■

Example 2.7. (1) In D_{2n}, $\langle r \rangle \simeq \mathbb{Z}/n\mathbb{Z}$, and $\langle t \rangle = \{e, t\} \simeq \mathbb{Z}/2\mathbb{Z}$.

(2) If G is any finite cyclic group of $\operatorname{ord} G = n$, then $G \simeq \mathbb{Z}/n\mathbb{Z}$.

Lemma 2.3.6. *If G is a group, and $g \in G$, and $k \in \mathbb{Z}^*$, then the following are true:*

(1) If g is of infinite order, then so is g^k.

(2) If $\operatorname{ord} g = n$, then $\operatorname{ord} g^k = \frac{n}{(n,k)}$.

Proof. Suppose that g is of infinite order, but that $\operatorname{ord} g^k = m$ for some $m \in \mathbb{Z}^+$. Then $(g^k)^m = g^{km} = e$. Now, either $km > 0$, or $-km > 0$, thus, we get $\operatorname{ord} g \leq km$ or $\operatorname{ord} g \leq -km$. Both contradict the infinite order of g.

Now let $\operatorname{ord} g = n$, and let $h = g^k$ and define $d = (n, k)$. Then $n = dm$ and $k = dl$ for $m, l \in \mathbb{Z}$, $m > 0$. Then we have $na + kb = d$, for $a, b \in \mathbb{Z}$; this implies that $ma + lb = 1$, so $(m, l) = 1$. Now, let $\operatorname{ord} h = p$, then $h^m = g^{km} = g^{dlm} = (g^{dm})^l = (g^n)^l = e$, so $p|m$. On the other hand, since $(m, l) = 1$, we get $m|p$, thus $p = \operatorname{ord} h = m$. Since $m = \frac{n}{d}$, we get the result. ∎

Corollary. *Of $k|n$, then $\operatorname{ord} g^k = \frac{n}{k}$.*

Proof. If $k|n$, then $(n, k) = k$. ∎

Lemma 2.3.7. *Let $\langle g \rangle$ be a cyclic group, then:*

(1) If g is of infinite order, then $\langle g \rangle = \langle g^k \rangle$ if, and only if $k = \pm 1$.

(2) If $\operatorname{ord} g = n$, then $\langle g \rangle = \langle g^k \rangle$ if, and only if $(n, k) = 1$.

Proof. First, if $k = \pm 1$, tjem $g^k = g$ or $g^k = g^{-1}$. By lemma 2.3.1, we get the result. Now suppose $\langle g \rangle = \langle g^k \rangle$ for $k > 1$. Then $g = g^k$ for some $k > 1$. If k is odd, then $k = 2l + 1$ and if k is even, $k = 2l$ for $l \in \mathbb{Z}^+$. Then $g = g^{2l+1} = g^{2l}g$, making $g^{2l} = e$. On the otherhand, if $g = g^k = g^{2l}$, then $g^{2l}g^{-1} = g^{2l-1} = e$. Both these cases contradict the infinite order of g. So $k \leq 1$. Now, since $\langle g \rangle = \langle e \rangle$ cannot happen, $k \neq 0$. Now if $k < -1$, then we get the same result using $-k$. Thus either $k = 1$ or $k = -1$.

Now suppose that $\operatorname{ord} g = n$. Then g^k generates a subgroup of $\operatorname{ord} g^k = \frac{n}{(n,k)}$. Now $\langle g \rangle = \langle g^k \rangle$ if, and only if $\operatorname{ord} g = \operatorname{ord} g^k$. That is, if and only if $n(n, k) = n$, i.e. if, and only if $(n, k) = 1$. ∎

Corollary. *The number of generators of $\langle g \rangle$ is $\phi(n)$, the Euler-ϕ function.*

Example 2.8. (1) Any $k \in \mathbb{Z}/n\mathbb{Z}$, coprime with n generates $\mathbb{Z}/n\mathbb{Z}$. So the generators of $\mathbb{Z}/n\mathbb{Z}$ are the elements of $U(\mathbb{Z}/n\mathbb{Z})$.

(2) $\mathbb{Z}/6\mathbb{Z} = \langle 1 \rangle = \langle 5 \rangle$.

(3) $\mathbb{Z}/12\mathbb{Z} = \langle 1 \rangle = \langle 5 \rangle = \langle 7 \rangle = \langle 11 \rangle$.

Theorem 2.3.8. *Let $G = \langle g \rangle$ be a cyclic group. The following are true:*

(1) Every subgroup of $\langle g \rangle$ is cyclic, and has the form $\langle g^d \rangle$, with $0 \leq d < \operatorname{ord} g$.

(2) *If $\langle g \rangle$ is infinite, then for any $m, n \in \mathbb{Z}^+$ distinct, $\langle g^m \rangle \neq \langle g^n \rangle$. Moreover, $\langle g^m \rangle = \langle g^{|m|} \rangle$, and there is a $1-1$ map of subgroups of $\langle g \rangle$ onto $\mathbb{N}$.*

(3) *If $\operatorname{ord} \langle g \rangle = n$, then for each divisor k of n, there is a unique subgroup of order k, which is $\langle g^d \rangle$ where $d = \frac{n}{k}$.*

Proof. First, let $H \leq \langle g \rangle$, if $K = \langle e \rangle$, we are done. Otherwise, there is some $k \neq 0$ with $g^k \in K$. If $k < 0$, then $g^{-k} \in K$. Npw, define $P = \{l \in \mathbb{Z}^+ : g^l \in K\}$. We have by above that P is nonempty, thus by the Well Ordering Principle, P has a least element, d. Now, $g^d \in K$ and $K \leq \langle g \rangle$, so $\langle g^d \rangle \leq K$. Now, for any $g^k \in K$, by the division theorem, we have $k = qd + r$, $0 \leq r < d$, with $q, r \in \mathbb{Z}$. Then $g^r = g^{k-qd} = g^k (g^d)^{-q}$. Since $g^k, g^d \in K$, by the minimality of d, we must have $r = 0$. So $k = qd$, this make $g^k = (g^d)^q \in \langle g^d \rangle$ and hence $K \leq \langle g^d \rangle$. Thus K is cyclic. Moreover, if $\operatorname{ord} g = n$, and if $d > n$, then by the division theorem $d \equiv r \mod n$, hence there are n subgroups of $\langle g \rangle$.

Now, if $\langle g \rangle$ is infinite, and if $\langle g^m \rangle = \langle g^n \rangle$, then $g^m = g^n$, so $g^{m-n} = e$, implying that g has finite order; hence $\langle g \rangle$ has finite order. This cannot happen, so $\langle g^m \rangle \neq \langle g^n \rangle$. Morevoer, we get $\langle g^m \rangle = \langle g^{-m} \rangle$, so $\langle g^m \rangle = \langle g^{|m|} \rangle$.

Now, define $\phi : m \to \langle g^m \rangle$. By above, we get ϕ is $1-1$ and onto, so we have established a $1-1$ correspondance between the subgroups of $\langle g \rangle$ onto $\mathbb{N}$.

Finally, let $\operatorname{ord} \langle g \rangle = n$ and let $k|n$. Then letting $d = \frac{n}{(n,k)} = \frac{n}{k}$ we have $\langle g^d \rangle$ is a subgroup of order $\operatorname{ord} \langle g^d \rangle = k$. Now, suppose K is any other subgroup of $\operatorname{ord} K = k$. Then $K = \langle g^l \rangle$, where $l \in \mathbb{Z}^+$ is the smallest integer of the set P in the above arguments. Then $\operatorname{ord} K = \frac{n}{(n,l)} = \frac{n}{d}$, so $\frac{n}{d} = \frac{n}{(n,l)}$ so $d = (n, l)$. In particular, $d|l$, so $g^l \in \langle g^d \rangle$ and since $\operatorname{ord} K = k$, this makes $K = \langle g^d \rangle$. ■

Example 2.9. (1) The subgroups of $\mathbb{Z}/12\mathbb{Z}$ are:

$$\begin{aligned} \mathbb{Z}/12\mathbb{Z} &= \langle 1 \rangle = \langle 5 \rangle = \langle 7 \rangle = \langle 11 \rangle \\ \langle 2 \rangle &= \langle 10 \rangle \\ \langle 3 \rangle &= \langle 9 \rangle \\ \langle 4 \rangle &= \langle 8 \rangle \\ \langle 6 \rangle & \\ \langle 0 \rangle & \end{aligned}$$

(2) Let G be any group, and let $g \in G$. We have that $C(g) = C(\langle g \rangle)$ and $\langle g \rangle \leq N(\langle g \rangle)$.

2.4 Subgroups of Generating Sets.

We now make precise the notion of when a subgroup of a group G is generated by a subset $A \subseteq G$. Namely, A will be a set of "generators".

Lemma 2.4.1. *If $\mathcal{H}$ is a nonempty collection of subgroups of G, then the intersection of all elements of $\mathcal{H}$ forms a subgroup of G.*

Proof. Let $\mathcal{H} = \{H_i\}$ where $H_i \leq G$ for all $i \in \mathbb{Z}^+$, and let $K = \bigcap H_i$. We have $e \in H_i$, for all i, so $e \in K$. Moreover, if $a, b \in K$, then $a, b \in H_i$ for all i, amking $ab^{-1} \in H_i$ for all i. Thus $ab^{-1} \in K$, and so by the subgroup criterion, $K \leq G$. ■

Definition. Let G be a group, and $\{H_i\}$ the collection of all subgroups of G. For any subset $A \subseteq G$, we define the subgroup $\langle A \rangle$ **generated** by A to be the intersection of all subgroups H_i containing A; i.e.

$$\langle A \rangle = \bigcap_{A \subseteq H_i, H_{\leq} G} H_i \tag{2.1}$$

Lemma 2.4.2. *Let A be a nonempty subset of a group G. Then $\langle A \rangle \leq G$.*

Proof. Let $\mathcal{H} = \{H \leq G : A \subseteq H\}$. Then the result follows from lemma 2.4.1. ■

Having $\langle A \rangle$ defined as the intersection of all subgroups containing A, while a useful definition, will not help us much in enumerating the elements of $\langle A \rangle$. For this, we turn to another subgroup, which can allow us to enumerate its elements effectively, and prove that it is equal to $\langle A \rangle$.

Definition. Let G be a group and let $A \subseteq G$. We define the **closure** of A to be the set $\operatorname{cl} A$ of all finite products of elements of A. That is:

$$\operatorname{cl} A = \{a_1^{e_1} \dots a_n^{e_n} : n \in \mathbb{Z}^+, a_i \in A, e_i = \pm 1 \text{ for all } i\} \tag{2.2}$$

We call the elements of $\operatorname{cl} A$ **words**, and we define $\operatorname{cl} A = \langle e \rangle$, if $A = \emptyset$.

Lemma 2.4.3. *Let G be a group and $A \subseteq G$. Then $\operatorname{cl} A = \langle A \rangle$.*

Proof. Notice, that by definition that atleast $e \in \operatorname{cl} A$, for if A is empty, $\operatorname{cl} A = \langle e \rangle$, and if A is not, then $a_i a_i^{-1} = e \in \operatorname{cl} A$. Now, if $a, b \in \operatorname{cl} A$ are words with $a = a_1^{e_1} \dots a_n^{e_n}$, and $b = b_1^{f_1} \dots b_m^{f_m}$, then notice that $b^{-1} = b_m^{-f_m} \dots b_1^{-f_1}$. So $b^{-1} \in \operatorname{cl} A$, so $ab^{-1} \in \operatorname{cl} A$. This makes $\operatorname{cl} A \leq G$.

Furthermore, notice that $A \subseteq \operatorname{cl} A$, hence $\langle A \rangle \subseteq \operatorname{cl} A$. However, also notice that $A \subseteq \langle A \rangle$, and $\langle A \rangle$ is closed under the operation of G, so $\langle A \rangle$ contains all finite products of elements of A; i.e. $\operatorname{cl} A \subseteq \langle A \rangle$. This establishes equivalence. ■

Corollary. $\langle A \rangle = \{a_1^{\alpha_1} \dots a_n^{\alpha_n} : a_i \neq a_{i+1}, n \in \mathbb{Z}^+,$ *and* $\alpha_i \in \mathbb{Z}\}$.

Corollary. *If G is Abelian, then $\langle A \rangle = \{a_1^{\alpha_1} \dots a_n^{\alpha_n} : \alpha_i \in \mathbb{Z}\}$*

Corollary. *If G is Abelian, and if each a_i has order $\operatorname{ord} a_i = d_i$, then $\operatorname{ord} \langle A \rangle \leq d_1 \dots d_n$.*

The above corollary is not always true, and only holds for Abelian groups. For example:

Example 2.10. (1) Consdier $D_8 = \langle r, t \rangle$. let $a = t$, and $b = rt$ and let $A = \{a, b\}$. Then $D_8 = \langle a, b \rangle$. Notice however, that $\operatorname{ord} a = \operatorname{ord} b = 2$, but that $\operatorname{ord} D_8 = 8 \geq 4 = 2 \cdot 2$. Moreover notice that no element of D_8 can be represented in the form $a^\alpha b^\beta$. For example, $aba = trtt = tr$ which cannot be written in the form $a^\alpha b^\beta$.

(2) Consider $S_n = \langle (1\ 2), (1\ 2\ \ldots\ n)\rangle$. We have $\operatorname{ord}(1\ 2) = 2$ and $\operatorname{ord}(1\ 2 \ldots\ n) = n$, but $\operatorname{ord} S_n = n!$.

(3) In $GL(2, \mathbb{R})$, let $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and $B = \begin{pmatrix} 0 & 2 \\ \frac{1}{2} & 0 \end{pmatrix}$. Then $A^2 = B^2 = I$, but $AB = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & 2 \end{pmatrix}$, which has infite order. So $\langle A, B\rangle$ is a subgroup of infinite order, generated by elements of finite order.

2.5 Lattices of Groups.

Definition. Let G be a group. We define the **lattice** of subgroups of G to be a directed graph whose set of vertices are subgroups of G, and whose edges are given by the relation (H, K) if $H \leq K$, for H, K subgroups of G.

We detail an algorithm for generating the lattice of subgroups of a given group G.

Algorithm. *For any group G:*

step 1: *Plot G and $\langle e\rangle$ opposite each other.*

step 2: *Plot a gubgroup H of G. If there are no subgroups A such that $H \leq A \leq G$, connect H to G. If there are no subgroups A such that $\langle e\rangle \leq A \leq H$, connect H to $\langle e\rangle$. If there are no subgroups left to plot, go to **step 5**.*

step 3: *For any other subgroup K plotted on the graph, if there is no subgroup A such that $H \leq A \leq K$, or $K \leq A \leq H$, then connect K to H.*

step 4: *return to **step 2**.*

step 5 *return.*

The lattice of subgroups of a group, can also be viewed as a lattice of partially ordered sets, instead of a graph. We focus however on the graph theoretic apprach. We now ist numerous examples.

Example 2.11. 2.11

(1) For $\mathbb{Z}/m\mathbb{Z} = \langle 1\rangle$, we plot the lattice of subgroups for $m = 2, 4, 12, p^n$ where p prime and $n \in \mathbb{Z}^+$: Notice that only the lattice of $\mathbb{Z}/12\mathbb{Z}$ conatains any cycles.

(2) The lattice of subgroups of $D_8 = \langle r, t\rangle$ is that of figure 2.2 This lattice can be drawn as a planar graph, however it is not true that all lattices of D_8 are planar. The lattice of D_{16} for example, cannot be drawn as a planar graph.

3 The lattice of S_3 is the attice in figure 2.3

(4) The lattice of $U(\mathbb{Z}/12\mathbb{Z})$ is that of figure 2.4

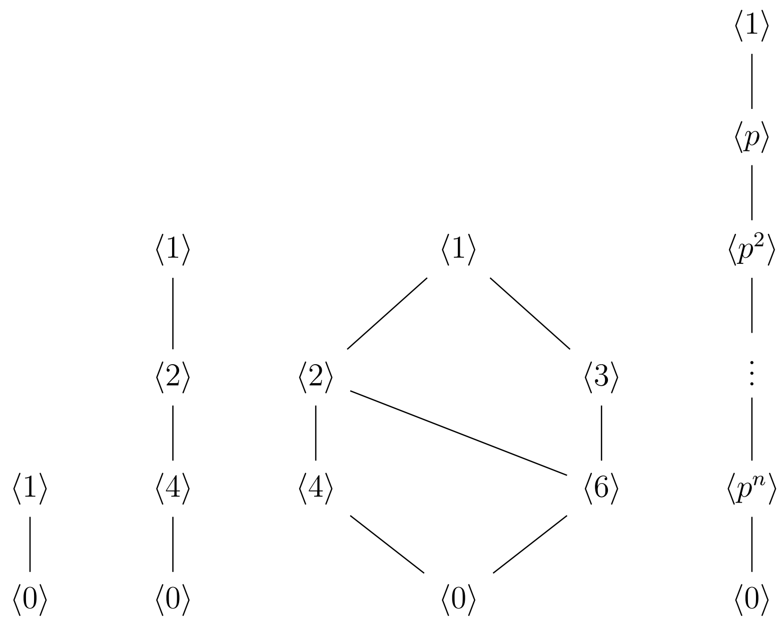

Figure 2.1: The lattices of $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/12\mathbb{Z}$, and $\mathbb{Z}/p^n\mathbb{Z}$ respectively.

(5) The **Klein-4 group** is the Abelian group V_4 defined by the following Cayley table:

1	a	b	c
a	1	c	b
b	c	1	a
c	b	a	1

and has the lattice of figure 2.5. Notice that as a graph, the lattice of subgroups of V_4 is isomorphic to the lattice of subgorups of $U(\mathbb{Z}/12\mathbb{Z})$.

These examples provide intereseting notions. The first is the notion of the "join" of two subgroups.

Definition. For any two distinct subgroups H and K of a group, the **join** of H and K is the smallest subgroup, $vbrack H, K$ containing both H and K.

Lemma 2.5.1. *Let H and K be distinct subgroups of a group. Then the join $\langle H, K\rangle$ is unique.*

Proof. Supose there exists another smallest subgroup containing H and K, and call it A. Then $A \subseteq \langle H, K\rangle$. But by definition, $\langle H, K\rangle$ is minimal, thus it must be contained in A as well, so $\langle H, K\rangle \subseteq A$. This establishes equality, and hence uniqueness. ■

Lemma 2.5.2. *If G and H are isomorphic groups, then they have the same lattice of subgroups.*

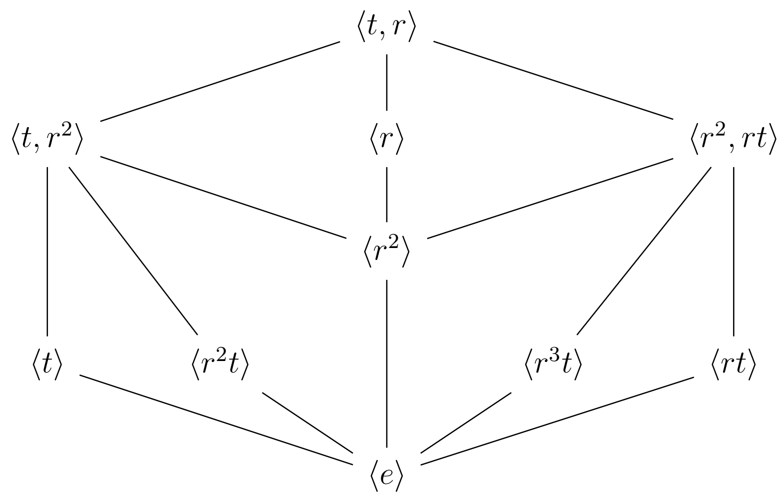

Figure 2.2: The lattices of D_8.

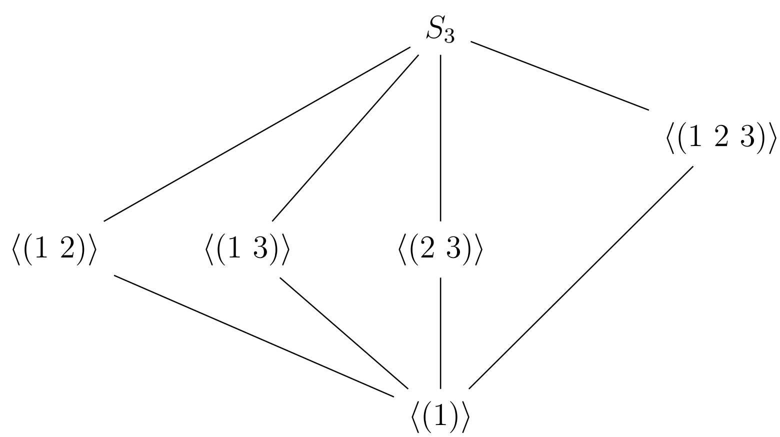

Figure 2.3: The lattices of S_3.

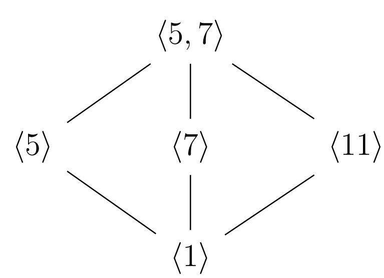

Figure 2.4: The lattices of $U(\mathbb{Z}/12\mathbb{Z})$.

$$
\begin{tikzcd}
 & V_4 \arrow[dl, no head] \arrow[d, no head] \arrow[dr, no head] & \\
\langle a \rangle \arrow[dr, no head] & \langle b \rangle \arrow[d, no head] & \langle c \rangle \arrow[dl, no head] \\
 & \langle e \rangle &
\end{tikzcd}
$$

Figure 2.5: The lattices of V_4.

Chapter 3

Quotient Groups, and Homomorphisms.

3.1 Quotient Groups.

Definition. Let G and H be groups and let $\phi : G \to H$ be a homomorphism of G into H. We define the **fiber** of ϕ over an element $h \in H$ to be the preimage of h under ϕ, i.e. $\phi^{-1}(h) = \{g \in G : \phi(g) = h\}$.

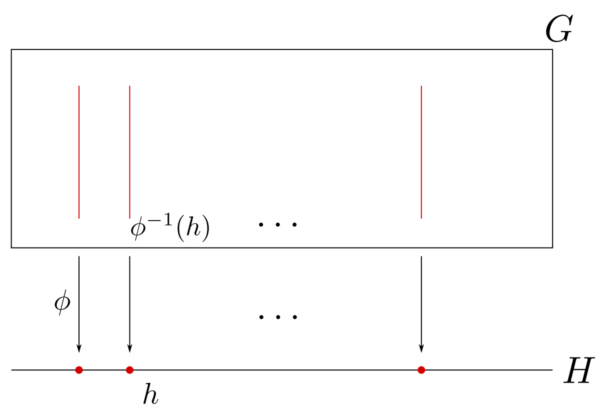

Figure 3.1: The fibers of the elements of H represented as vertical lines.

We can immediately define a special fiber for any homomorphisms.

Definition. Let G and H be groups and let $\phi : G \to H$ be a homomorphism of G into H. We define the **kernel** of ϕ to be the fiber $\phi^{-1}(e')$ where e' is the identity of H. That is:

$$\ker \phi = \{g \in G : \phi(g) = e'\} \tag{3.1}$$

Lemma 3.1.1. *$\phi : G \to H$ is a $1-1$ homomorphism if and only if $\ker \phi = \langle e \rangle$.*

Proof. We have that $\phi(e) = e'$, thus since ϕ is $1-1$, we have $\phi(a) = e'$ implies $a = e$.

On the other hand, suppose $\ker \phi = \langle e \rangle$, and that $\phi(a) = \phi(b)$. Then $\phi(a)\phi(b)^{-1} = \phi(ab^{-1}) = e'$, so that $ab^{-1} = e$. That is, $a = b$. ■

Lemma 3.1.2. *Let G and H be groups and let $\phi : G \to H$ be a homomorphism of G into H. Then $\ker\phi \leq G$, and $\phi(G) \leq H$.*

Proof. We have that $\phi(e) = e'$ and for any $a, b \in \ker\phi$, that $\phi(ab) = \phi(a)\phi(b) = e'$, and that $\phi(a^{-1}) = \phi(a)^{-1} = e'$. This makes $e', ab, a^{-1} \in \ker\phi$. ■

Example 3.1. Let $Z_n = \langle x \rangle$ be the cyclic group of order n and define the homomorphism $\phi : \mathbb{Z} \to Z_n$ by $a \to x^a$. Then $\phi(a+b) = x^{a+b} = a^a x^b = \phi(a)\phi(b)$, so ϕ is a homomrphsim. Moreover, $\phi^{-1}(x^a) = \{m \in \mathbb{Z} : m \equiv a \mod n\} = n\mathbb{Z}$. So the set of fibers is $\mathbb{Z}/n\mathbb{Z}$, moreover, we get the kernel of ϕ to be $\ker\phi = \{m \in \mathbb{Z} : m \equiv 0 \mod n\} = n\mathbb{Z}$ the set of all multiples of n.

This motivates the following results.

Theorem 3.1.3. *Let $\phi^{-1}(H)$ be the set of all fibers of ϕ under elements of H, and define the operation $\phi^{-1}(a)\phi^{-1}(b) = \phi^{-1}(ab)$. Then $\phi^{-1}(H)$ forms a group under this operation.*

Proof. Let $\phi^{-1}(a)$ and $\phi^{-1}(b)$ be fibers of ϕ under a and b re spectively. Then for $g \in \phi^{-1}(a)$ and $g' \in \phi^{-1}(b)$, we have $\phi(gg') = \phi(g)\phi(g') = ab$, so that $gg' \in \phi^{-1}(ab)$, so this ensures that the operation is well defined. Moreover, we have that $\phi^{-1}(H)$ satisfies associativity because of the associativity of H.

Notice, then that $\phi^{-1}(e)$ is the identity, as, for $g_e \in \phi^{-1}(e)$, $\phi(gg_e) = \phi(g)\phi(g_e) = ae = a = ea = \phi(g_e)\phi(g) = \phi(g_e g)$, where $g \in \phi^{-1}(a)$ and $g_e \in \phi^{-1}(e)$. Similarly, we find that $\phi^{-1}(a^{-1})$ is the inverse of $\phi^{-1}(a)$ of $\phi^{-1}(H)$. ■

Definition. Let G and H be groups, and let $\phi : G \to H$ be a homomorphsm with $\ker\phi = K$. We deine the **quotient group** of G **mod** K to be the group G/K of all fibers of ϕ under elements of K.

Lemma 3.1.4. *Let ϕ be a homomorphism defined on a group G with $\ker\phi = K$. Then for any fiber $\phi(a)^{-1} \in G/K$, $a \in K$. we have for any $u \in \phi^{-1}(a)$, that $\phi^{-1}(a) = \{uk : k \in K\}$ and $\phi^{-1}(a) = \{ku : k \in K\}$.*

Proof. Let $uK = \{uk : k \in K\}$. Then since $\phi(u) = a$, for any $k \in K$, we have $\phi(uk) = \phi(u)\phi(k) = ae = a$, making $uk \in \phi^{-1}(a)$. On the other hand, for some other $x \in \phi^{-1}(a)$, let $k = u^{-1}x$. Then $\phi(k) = \phi(u^{-1})\phi(x) = \phi(u)^{-1}\phi(x) = a^{-1}a = e'$, so $k \in K$. Then $x = uk$, this $x \in uK$. This makes $\phi^{-1}(a) = uK$. The second assertion follows similarly. ■

Definition. Let G be a group, and let $H \leq G$. For any gG, we define the **left** and **right cosets** of H in G to be the sets $gH = \{gh : h \in h\}$ and $Hg = \{hg : h \in h\}$, respectively.

Lemma 3.1.5. *Let G and H be groups and $\phi : G \to H$ a homomorphism with kernel K. Then for any $g \in G$, $gK = Kg$.*

Proof. By the previous lemma 3.1.4, if $a \in gK$ then $a \in \phi^{-1}(g)$, which makes $a = kg$ for some $k \in K$, thus $a \in Kg$. Similarly, if $b \in Kg$, then $b \in gK$. ■

It is much easier to think in terms of cosets, rather than fibers, so we develop the theory of cosets furthur. In particucular, if G is a group, and K is the kernel of some homomorphism ϕ defined on G, then define the operation of **coset multiplication** by the rule $aKbK = abK$. Then we get the following result.

Theorem 3.1.6. *Let G be a group and ϕ a homomorphism on G with kernel K. Then the set of all cosets of K in G forms a group under coset multiplication.*

Proof. Let $a' \in aK$ and $b' \in bK$. Then $a' = ak_1$ and $b' = bk_2$, thus $a'b' = (ak_1)(bk_2) = a(k_1b)k_2 = a(bk')k_2 = ab(k'k_2) = abk''$. This makes $a'b' \in abK$, and by definition $aKbK = abK$, we get $a'b'K = abK$. Therefore coset multiplication is well defined.

Now, notice that for the identity element $e \in G$, that $eK = K$ satisfies $aKK = KaK = aeK = aK$. Moreover, for the inverse $a^{-1} \in G$ of a, we have $a^{-1}KaK = aKa^{-1}K = aa^{-1}K = eK = K$. So K is the identity element and $a^{-1}K$ is the inverse of aK. Lastly, associativity is inherited from the associativity of G; i.e. $(aKbK)cK = abKcK = (ab)cK = a(bc)K = aKbcK = aK(bKcK)$ ■

Corollary. *The group of cosets of K in G is precisely the quotient group G/K.*

Proof. This follows directly from lemma 3.1.4. Since G/K is the set of all fiber $\phi^{-1}(a)$ Then notice that $\phi^{-1}(a) = aK = Ka$. ■

Example 3.2. (1) For $\mathbb{Z}$ and $Z_n = \langle x \rangle$ in example 3.2, the homomorphism $\phi : a \to x^a$ has kernel $n\mathbb{Z}$, so the cosets of $n\mathbb{Z}$ in $\mathbb{Z}$ are of the form $a + n\mathbb{Z}$ which are the elements mod n. Thus the quotient group is $\mathbb{Z}/n\mathbb{Z}$.

(2) Let G and H be isomorphic to each other via the isomorpism $\phi : G \to H$. Then $\ker \phi = \langle e \rangle$, and so the cosets are all $a\langle e \rangle = a$ so we get $G/\langle e \rangle = G$.

(3) Let G be a group and define $\phi : G \to \langle e \rangle$ by $g \to e$. Then ϕ is a homomorphism with kernel $\ker \phi = G$. The cosets are precisely all $gG = G$.Thus the quotient group is $G/G \simeq \langle e \rangle$

(4) Define the map $\phi : \mathbb{R}^2 \to \mathbb{R}$ to be the pojection onto the x-axis $(x, y) \to x$. Then $\phi((x_1, y_1) + (x_2, y_2)) = x_1 + x_2 = \phi((x_1, y) + (x_2, y'))$. So ϕ is a homomorphism. Then $\ker \phi = \{x \in \mathbb{R} : \phi(x, y) = 0\} = (0, \mathbb{R})$; i.e. the y-axis. Then the cosets are all the vertical lines $(x, \mathbb{R})$, of the quotient group $\mathbb{R}^2/(0, \mathbb{R})$. Taking $(x, \mathbb{R}) \to x$, we get $\mathbb{R}^2/(0, \mathbb{R}) \simeq \mathbb{R}$.

(5) Consider the quaternions $\mathbb{H}$ and the Kelin-4 group V_4. Take $\phi : \mathbb{H} \to V_4$ defined by the rule $\pm 1 \to 1$, $\pm i \to a$, $\pm j \to b$, and $\pm k \to c$. Then ϕ is a homomorphism with kernel $\ker \phi = \langle -1, 1 \rangle$. Then the cosets of the quotient group $\mathbb{H}/\langle -1, 1 \rangle$ are all $\langle -1, 1 \rangle$, $\langle -i, i \rangle$, $\langle -j, j \rangle$, and $\langle -k, k \rangle$, all collaped to $1, a, b, c \in V_4$.

3.2 Alternative Definitions.

There is another way for driving the theory for quotient groups that does not involve the use of homomorphisms at all. Instead, it relies on the notion of equivalence classes.

Definition. Let G be a group and $H \leq G$ a subgroup. For $a, b \in G$, we say that a is **congruent** to $b \mod H$ if $b^{-1}a \in H$. We write $a \equiv b \mod H$.

Lemma 3.2.1. *For any subgroup H of any group, the relation $\equiv$ of congruence $\mod H$ is an equivalence relation.*

Proof. Let G be group and and $H \leq G$. We have that $a^{-1}a = e' \in H$ so that $a \equiv a \mod H$.

Now, suppose that $a \equiv b \mod H$. Then $b^{-1}a \in H$, so $b^{-1}a = h$. Then $h^{-1} = a^{-1}b \in H$; so $b \equiv a \mod H$. Lastly, suppose that $a \equiv b \mod H$ and that $b \equiv c \mod H$. Then $b^{-1}a \in H$ and $c^{-1}b \in H$. By closure then, $(c^{-1}b)(b^{-1}a) = c^{-1}(bb^{-1})a = c^{-1}a \in H$. So $c^{-1}a \in H$ making $a \equiv c \mod H$. ∎

Corollary. *The equivalence classes of $G/_{\equiv}$ are precisely the left cosets aH, of H in G.*

Proof. We have that the equivalence classes of $\equiv$ in G are of the from $[a] = \{b \in G : b \equiv a \mod H\}$. Then for $b \in [a]$, we have $a^{-1}b = h$ for some $h \in H$, so $b = ah$. Likewise, for $b \in aH$, $b = ah'$ for some $h' \in H$; hence $a^{-1}b = h' \in H$. This makes $[a] = aH$. ∎

Example 3.3. Consider the subgroup $n\mathbb{Z} \leq Z$ and define $\sim$ to be $a \sim b \mod n\mathbb{Z}$ if $a - b \in n\mathbb{Z}$. Then if $a \sim b \mod n\mathbb{Z}$ we have $a - b = nm$, so that $n|(a - b)$, making $a \equiv b \mod n$. Conversely, if $a \equiv b \mod n$, then $n|(a - b)$, making $a - b = nk$, hence $a \sim b \mod n\mathbb{Z}$. Therefore, the equivalence relation $\sim$ defined is exaclty that of $\equiv_n$ of congruence mod n. Thus $Z/_{\sim} = Z/_{\equiv_n} = Z/_{n\mathbb{Z}}$.

Since aH describes the equivalence classes of the relation $a \equiv b \mod H$, they partion the group G into disjoint subsets. That is:

Theorem 3.2.2. *Let G be a group, and $H \leq G$. Then the left cosets of H in G partition G into disjoint subsets. That is:*

$$G = \bigcup_{g \in G} gH \tag{3.2}$$

Where $aH \cap bH = \emptyset$ for $a, b \in G$ distinct.

Proof. We have that $g \in gH$ for all $g \in G$, so that G is the union of left cosets of H in G. Now suppose that $\in aH \cap bH$. Then $g = ah$ and $g = bh'$. So $ah = bh'$, so $b^{-1}a = h'h^{-1} = h''$. So $b \in aH$. This makes $aH = bH$. Therefore if aH and bH are distinct, they are disjoint. ∎

Now to define the quotient group, it is not enough to define left cosets as equivalence classes. In general, coset multiplcation is not well defined for arbitrary cosets. So we wish to make an assertion.

Theorem 3.2.3. *Let G be a group and $H \leq G$, and define the operation of coset multiplication by $aHbH = abH$. Then this opertion is well defined if, and only if for any $h \in H$, $ghg^{-1} \in H$ for all $g \in G$.*

Proof. Suppose that $aHbH = abH$ is well defined. That is, if $a' \in aH$ and $b' \in bH$ then $a'Hb'H = a'b'H = abH$. Now, let $g \in G$ and $h \in H$. Then take $g^{-1}H = hg^{-1}H$. Then, since coset multiplication is well defined, we get $gh^{-1}g^{-1}H = H$, so that $gh^{-1}g^{-1} \in H$ for $h^{-1} \in H$ arbitrary.

Conversly, suppose that $ghg^{-1} \in H$ then $ghg^{-1} = h'$, hence $gh = h'g$. That is $gh \in Hg$ and $h'g \in gH$ making $gH = Hg$. Thus if $a' \in aH$ and $b' \in bH$ then $a' = ah_1$, $b' = bh_2$ so that $a'b' = (ah_1)(bh_2) = a(h_1b)h_2 = ab(bh')h_2 = ab(h'h_2)$, making $a'b' \in abH$. Therefore, $a'Hb'H = a'b'H = abH$ making coset multiplication well defined. ∎

Proof. If H is such that $ghg^{-1} \in H$ for all $g \in G$, then $gH = Hg$. That is, every left coset is also a right coset. ∎

Corollary. *If $ghg^{-1} \in H$ for all $g \in G$, then the set of all cosets of H in G form a group under coset mutliplication.*

Proof. This proof is idential to that of theorem 3.1.6. ∎

Definition. Let G be a group and N a subgroup of H. For $n \in N$ we gng^{-1} the **conjugate** of n by g. We call the set $gNg^{-1} = \{gng^{-1} : n \in N\}$ the **conjugate** of N by g. We say that the subgroup N is **normal** in G if $gNg^{-1} = N$. That is, every every element of G normalizes N. If N is a normal subgroup of G, we write $N \trianglelefteq G$.

Definition. Leet G be a group, and let $N \trianglelefteq G$ be a normal subgroup of G. Then the **quotient group** ${}^{G}\!/_{N}$ is the group of all cosets of N in G.

Lemma 3.2.4. *Let G be a group, and $N \leq G$. Then the following are equivalent:*

(1) $N \trianglelefteq G$.

(2) The normalizer of N is precisely G.

(3) $gN = Ng$ *for all* $g \in G$.

(4) $gNg^{-1} \subseteq N$.

Theorem 3.2.5. *Let G be a group and $N \leq G$. Then N is normal if, and only if it is the kernel of some homomorphism defined on G.*

Proof. We have shown that if ϕ is a homomorphism on G, then $\ker\phi \trianglelefteq G$; see lemmas 3.1.4 and 3.2.4.

Now, suppose that $N \trianglelefteq G$. Now, let $\phi : G \to {}^{G}\!/_{N}$ be defined by $\phi : g \to gN$. Since N is normal, coset multiplicaton is well defined and, we have that $abN = aNbN$, so that ϕ is a homomorphism. Now, notice then that $\ker\phi = \{g \in G : \phi(g) = N\}$. So if $g \in \ker\phi$, then $gN = N$, so that $g \in N$. Moreover, if $g \in N$, then $\phi(g) = gN = N$, so that $g \in \ker\phi$. This makes $\phi = N$. ∎

Corollary. *ϕ is onto.*

Proof. Notice that the cosets of N in G partition G, so that each distinct g gets mapped to a distinct gN. ∎

Remark. With this theorem, we have tied together the equivalence of the quotient group as defined with fibers, to the quotient group as defined with equivalence classes of cosets of normal subgroups.

The homomorphism in theorem 3.2.5 warrants its own definition.

Definition. Let G be a group and $N \trianglelefteq G$. The homomorphism from G onto ${}^{G}\!/_{N}$ defined by $g \to gN$ is called the **natrual projection** of G onto ${}^{G}\!/_{N}$. If $H \leq {}^{G}\!/_{N}$, then the **complete fiber** of H in G is the preimage of H under the natrual projection.

We conclude with some examples.

Example 3.4. (1) let G be any group. Then G and $\langle e \rangle$ are normal in G, with quotient groups ${}^{G}\!/\!_{\langle e \rangle} \simeq G$ and ${}^{G}\!/\!_{G} \simeq \langle e \rangle$.

(2) If G is Abelian, then any subgroup $H \leq G$ is normal. We have $gh = hg$ for all $g \in G$, $h \in h$, so that $gH = Hg$ for all $g \in G$. Thus quotient groups can be described for every subgroup.

(3) Every subgroup of $\mathbb{Z}$ is normal, and cyclic, so $N = \langle n \rangle = N = \langle -n \rangle = n\mathbb{Z}$. The quotient group ${}^{\mathbb{Z}}\!/\!_{n\mathbb{Z}} = \langle 1 \rangle$ is also cyclic.

(4) If $N \leq Z(G)$ for a group G, then $N \trianglelefteq G$.

3.3 Lagrange's Theorem.

Theorem 3.3.1 (Lagrange's Theorem.)**.** *Let G and H be groups, then the order of H divides the order of G, i.e.* $\operatorname{ord} H | \operatorname{ord} G$.

Proof. Let $H \leq G$ and consider the coset gH. We claim that $\operatorname{ord} H = |gH|$. If $g' \in gH$, then $g' = gh$, for some $h \in H$. Now, define the map $\phi : H \to gH$ by $h \to gh$. First, we have that if $gh = gh'$ for $h, h' \in G$, then by cancellation, $h = h'$. Moreover, since gH is defined for all $h \in H$, ϕ is onto. Therefore ϕ is a 1-1 mapping of H onto gH, thus $|gH| = \operatorname{ord} H$.

Now, the group G is partitioned into disjoint subsets by the cosets of H in g. Assume that there are k such cosets. Then:

$$\operatorname{ord} G = \sum_{g \in G} |gH| = \sum_{i=1}^{k} \operatorname{ord} H = k \operatorname{ord} H.$$

Therefore, $\operatorname{ord} H | \operatorname{ord} G$. ■

Corollary. *There are*

$$\frac{\operatorname{ord} G}{\operatorname{ord} H}$$

cosets of H in G.

Proof. We have that $\operatorname{ord} G = k \operatorname{ord} H$, where k is the number of cosets of H in G. ■

Corollary. *If $N \trianglelefteq G$, then*

$$\operatorname{ord} {}^{G}\!/\!_{N} = \frac{\operatorname{ord} G}{\operatorname{ord} N} \tag{3.3}$$

Definition. Let G be a (not necessarily finite) group, and $H \leq H$. We define the **index** of H in G to be the number of left (or right) cosets of H in G, and write $[G : H]$.

Remark. By the above corollaries, we have that if G is finite, then $[G : H] = \frac{\operatorname{ord} G}{\operatorname{ord} H}$.

Lemma 3.3.2. *If G is a finite group, and $g \in G$, then* $\operatorname{ord} g | \operatorname{ord} G$.

Proof. Consider the cyclic subgroup generated by g, $\langle g\rangle \leq G$. By Lagrange's theorem, we get $\operatorname{ord}\langle g\rangle = \operatorname{ord} g | \operatorname{ord} G$. ∎

Corollary. *For any $g \in G$, $g^{\operatorname{ord} G} = e$.*

Proof. $g^{\operatorname{ord} G} = g^{k \operatorname{ord} g} = (g^{\operatorname{ord} g})^k = e^k = e$, for some $k \in \mathbb{Z}^+$. ∎

Lemma 3.3.3. *IF G is a finite group of prime order p, then G is cyclic.*

Proof. Let $\operatorname{ord} G = p$ a prime, and let $g \in G$ be such that $g \neq e$. Then $\operatorname{ord} g > 1$; moreover, we have $\operatorname{ord} g | p$, by lemma 3.3.2. Then either $\operatorname{ord} g = 1$ or $\operatorname{ord} g = p$. By our choice of g, its order cannot be 1, thus $\operatorname{ord} g = p = \operatorname{ord} G$. Then $\operatorname{ord}\langle g\rangle = \operatorname{ord} G$, and since $\langle g\rangle \leq G$, we can conclude that $G = \langle g\rangle$. ∎

Corollary. *If G is of prime order, then $G \simeq \mathbb{Z}/p\mathbb{Z}$.*

Proof. Take the homomorphism $g^i \to i$, for some generator $g \in G$, and $1 \leq i \leq \operatorname{ord} g$ ∎

Example 3.5. (1) Let $H = \langle(1\ 2\ 3)\rangle \leq S_3$. Now, we have that $H \leq N(H) \leq S_3$, so by Lagrange's theorem, $\operatorname{ord} H | \operatorname{ord} N(H) | \operatorname{ord} S_3$. Now, $\operatorname{ord} H = 3$ and $\operatorname{ord} S_3 = 6$. This makes $N(H) = H$ or $N(H) = S_3$. Notice, then that $(1\ 2)(1\ 2\ 3)(1\ 2) = (1\ 2\ 3)$, and $(1\ 2) = (1\ 2)^{-1}$, so $(1\ 2)$ conjugates $(1\ 2\ 3)$, so $(1\ 2) \in N(H)$. This makes $N(H) \neq H$, so $N(H) = S_3$; by lemma 3.2.4, $H \trianglelefteq S_3$.

(2) Let G be any group, and let $H \leq G$, such that $[G : H] = 2$. Thent he total number of left cosets in G is H and gH. Now, suppose that $Hg = H$, since $g \in Hg$, we get $g \in H$, this makes $Hg = H$, but this also makes $gH = H$, implying $[G : H] = 1$, which cannot happen. Thus it must be that $Hg = gH$. By lemma 3.2.4, this makes $H \trianglelefteq G$.

(3) The relation $\trianglelefteq$ defined by HG if H is a normal subgroup of G, is not in general transitive. Take D_8. We have

$$\langle t\rangle \trianglelefteq \langle t, r^2\rangle \trianglelefteq D_8$$

but $\langle t\rangle$ is not normal in D_8, for $(rt)t(rt) = r^2 t \neq t$, so $N(\langle t\rangle) \neq D_8$.

For some nonexamples, we have:

Example 3.6. (1) Let $H = \langle(1\ 2)\rangle \leq S_3$. Notice that $(1\ 3)(1\ 2)(1\ 3) = (2\ 3) \neq (1\ 2)$, since $(1\ 3) = (1\ 3)^{-1}$, we get that $(1\ 3) \notin H$. Thus $N(H) \neq S_3$ meaning that H is not normal in S_3. Moreover, notice that $[S_3 : H] = 3$, then there are 3 left cosets of H in S_3, namely, H, $(1\ 3)H$, and $H(1\ 3)$.

(2) For general S_n, $n \in \mathbb{Z}^+$ let $G_i = \{s \in S_3 : s(i) = i\}$ for $1 \leq i \leq n$. If $t \in S_3$ such that $t(i) = j$ then $ts(i) = j = t(i)$, so that $tst^{-1} = e$. Moreover, if $m(i) = j$, then $t^{-1}m(i) = i$, so that $m \in tG_i$. Thus

$$tG_i = \{m \in S_n : m(i) = j\}$$

Similarly, taking $k = t^{-1}(j)$, we get

$$G_i t = \{l \in S_n : l(k) = i\}$$

Now, if tG_i and mG_i are distinct cosets, we have $tG_i \cap mG_i = \emptyset$ by theorem 3.2.2. Moreover, notice that there are n such cosets, for each distinct image of i. Therefore, $[S_n : G_i] = n$. Notice that, in general $tG_i \neq G_i t$, and that $N(G_i) = G_i$.

(3) $\langle r \rangle$ is the only normal subgroup of order 2 in D_8.

Theorem 3.3.4 (Cauchy). *If G is a finite group, and $p | \operatorname{ord} G$ for some prime p, then G contains an element of order p.*

Theorem 3.3.5 (Sylow). *If G is a finite group of order $p^a m$, p prime and $p \not| m$, then G has an element of order p^a.*

Theorem 3.3.6. *Let H and K be subgroups of a group, and let $HK = \{hk : h \in H, k \in K\}$. If H and K are finite, then*

$$\operatorname{ord} HK = \frac{\operatorname{ord} H \operatorname{ord} K}{\operatorname{ord} H \cap K} \tag{3.4}$$

Proof. Notice that $HK = \bigcup_{h \in H} hK$ is a union of left cosets of K in H. Now, for $h, h' \in H$, $hK = h'K$ if, and only if $h^{-1}h' \in K$, i.e. if, and only if $h^{-1}h' \in H \cap K$. So that $hK = h'K$ if and only if $h(H \cap K) = h'(H \cap K)$. Thus the number of left cosets of $H \cap K$ in H is the same as the number of left cosets of K in H. By Lagrange's thereorem, we then have:

$$[H : K] = [H : H \cap K] = \frac{\operatorname{ord} H}{\operatorname{ord} H \cap K}$$

Then, noticing that there are $\operatorname{ord} K$ elements in each coset hK, gives the result. ■

Lemma 3.3.7. *If H and K are subgroups of a group, then HK is a subgroup if, and only if $HK = KH$.*

Proof. Suppose first, that $HK = KH$. Let $a, b \in HK$, then $a = hk$ and $b = h'k'$ so $ab = (hk)(h'k') = h(kh')k' = h(h''k'')k = (hh'')(k''k) \in HK$. Aditionaly, $a^{-1} = k^{-1}h^{-1} \in KH = HK$. Thus HK is a subgroup.

Conversely, suppose that HK is a subgroup. Then we have $K \leq HK$ and $H \leq HK$, then by closure, we have that $KH \subseteq HK$. On the other hand, since HK is a subgroup, then for every $a \in HK$, $a^{-1} \in HK$. Then if $a = hk$, $a^{-1} = k^{-1}h^{-1}$. That is, $HK \subseteq KH$. Teh equality is established. ■

Corollary. *If $H \leq N(K)$ then HK is a subgroup.*

Proof. If $H \leq N(K)$, then for any $h \in H$, and $k \in K$, $hkh^{-1} \in K$, so $hk = k'h$ for some $k' \in K$. So $hk \in KH$. Conversely, we get $k'h \in HK$ so that $HK = KH$. ■

Corollary. *if K is normal, then HK is a subgroup for any H.*

Definition. Let H be a subgroup of any group. We say that a subset A of the group **normalizes** H if $A \subseteq N(H)$. Similarly, we say A **centralizes** H if $A \subseteq C(H)$.

3.4 The Isomorphism Theorems.

Theorem 3.4.1 (The First Isomorphism Theorem)**.** *Let G and H be groups and $\phi : G \to H$ a homomorphism. Then* $\ker \phi \trianglelefteq G$ *and* ${}^{G}\!/_{\ker \phi} \simeq \phi(G)$.

Proof. Let $K = \ker \phi$ by lemma 3.1.5, we have $gK = Kg$, so K is normal in G.

Now consider $\psi : {}^{G}\!/_{K} \to G$ by $gK \to g$. We have that ψ is a homomorphism, moreover, it is $1-1$. Notice also that the $\phi : G \to \phi(G)$ is onto. Then form the map $\Phi : {}^{G}\!/_{K} \to \phi(G)$ by taking $\Phi = \phi \circ \psi$. That is $\Phi : gK \to \phi(g)$. Then, Φ is a $1-1$ homomorphism of ${}^{G}\!/_{K}$ onto $\phi(G)$; moreover it is well defined, for if $gK = g'K$, then $g = g'k$, then $\phi(g) = \phi(g')\phi(k) = \phi(g')$. This establishes the result. ■

Corollary. $[G : \ker \psi] = \operatorname{ord} \phi(G)$.

$$\begin{tikzcd}
G \arrow[r, "\psi"] \arrow[dr, dashed, "\Phi"'] & {}^{G}\!/_{\ker \phi} \arrow[d, "\phi"] \\
 & \phi(G)
\end{tikzcd}$$

Figure 3.2: The First Isomorphism Theorem

Theorem 3.4.2 (The Second Isomorphism Theorem)**.** *Let G be a group and $A, B \leq G$ such that $A \leq N(B)$. Then $AB \leq B$, $B \trianglelefteq AB$, $A \cap BA$, and* ${}^{AB}\!/_{B} \simeq {}^{A}\!/_{A \cap B}$

Proof. By the corollary to lemma 3.3.7, $A \leq N(B)$ implies that $AB \leq G$. Moreover, since $BN(B)$, $AB \leq N(B)$. Then $(ab)B(ab)^{-1} = abBb^{-1}a^{-1} = aBa^{-1}$, and since $A \leq N(B)$, $aBa^{-1} \subseteq B$, making $B \trianglelefteq AB$.

Now consider the map $\phi : A \to {}^{AB}\!/_{B}$ by $\phi : a \to aB$. Since coset mutliplication is well defined, so is ϕ, moreover, notice that ϕ is a homomorphism, and is onto. Notice then that $\ker \phi = \{a \in A : aB = B\}$, then $a \in B$, necessarily, so $\ker \phi = A \cap B$. Therefor, by the first isomorphism theorem, we get that ${}^{AB}\!/_{B} \simeq {}^{A}\!/_{A \cap B}$. ■

Remark. Notice that $\phi = \Phi|_A : AB \to {}^{AB}\!/_{B}$.

Remark. The second isomorphism theorem states that if A and B are nontrivial subgroups of G (i.e. $A, B \neq \langle e \rangle, G$), then the lattice of G contains the following sublattice described in figure 3.3.

Theorem 3.4.3 (The Third Isomorphism Theorem)**.** *Let G be a group and let $H \trianglelefteq G$ and $K \trianglelefteq G$ such that $H \leq K$. Then* ${}^{K}\!/_{H} \trianglelefteq {}^{G}\!/_{H}$, *and* ${}^{G/H}\!/_{K/H} \simeq {}^{G}\!/_{K}$.

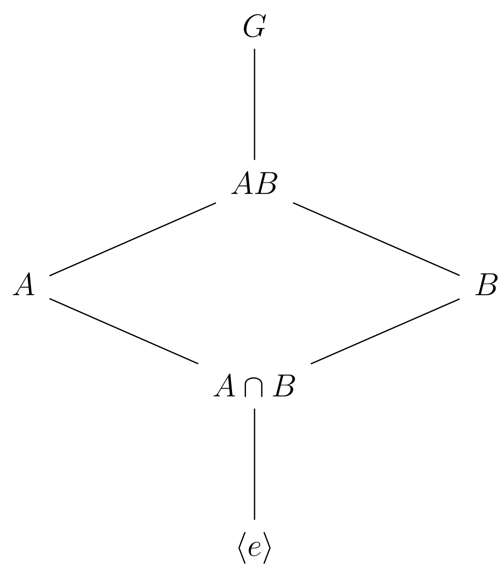

Figure 3.3: The Second Isomorphism Theorem

Proof. Notce that $kH = Hk$ for any $k \in K \leq G$. So that H is normal in K. Now for all $gH \in G/H$, we have $gHkHgH^{-1} = gkg^{-1}H = k'H$, since $K \trianglelefteq G$. Now, we have that $gkg^{-1} = k'$, making $gk \in k'H$, and consequentially $k \in k'H$, so that $kH = k'H$. Thus we have $gkg^{-1}H \subseteq kH$, thus this makes $K/H\, G/H$.

Now consider the map $\phi : G/H \to G/K$, by taking $gH \to gK$. We have that ϕ is a $1-1$ homomorphism of G/H into G/K. Moreover, it is well defined, since if $gH = g'H$, then $g = g'h$, and since $H \leq K$, $g'h \in K$, so that $gK = g'K$.

Notice then that $\ker \phi = \{gH \in G/H : gK = K\} = \{gH \in G/H : g \in K\} = K/H$. By the first isomorphism theorem, we have

$$(G/H)/(K/H) \simeq G/K$$

■

Remark. What this theorem says is that we obtain no new infromation upon taking quotients groups of quotient groups.

Theorem 3.4.4 (The Fourth Isomorphism Theorem)**.** *let G be a group and $N \trianglelefteq G$. Then there is a $1-1$ mapping of the set of all subgroups $A \leq G$ containing N onto the set of subgroups A/N of G/N. In particular, any subgroup of G/N is of the form A/N, and the mapping has the following properties.*

(1) $A \leq B$ if, and only if $A/N \leq B/N$.

(2) If $A \leq B$, then $[B : A] = [B/N : A/N]$.

(3) $\langle A, B\rangle/N = \langle A/N, B/N\rangle$.

(4) $A \cap B/N = A/N \cap B/N$.

(5) $A \trianglelefteq G$ *if, and only if* $A/N \trianglelefteq G/N$.

Remark. What this theorem tells us is how to identify the lattice of subgroups of G/N, which is embedded into the lattice of subgroups of G.

Example 3.7. (1) Let $N = \langle -1 \rangle \trianglelefteq \mathbb{H}$. Since $\mathbb{H}/\langle -1 \rangle \simeq V_4$, the lattice of $\mathbb{H}/\langle -1 \rangle$ is identical to that of V_4.

(2) The lattice of $D_8/\langle r^2 \rangle$ is given by figure 3.4. The lattice of the quotient group is represented by solid lines, while the rest of the lattice of D_8 is represented by dotted lines.

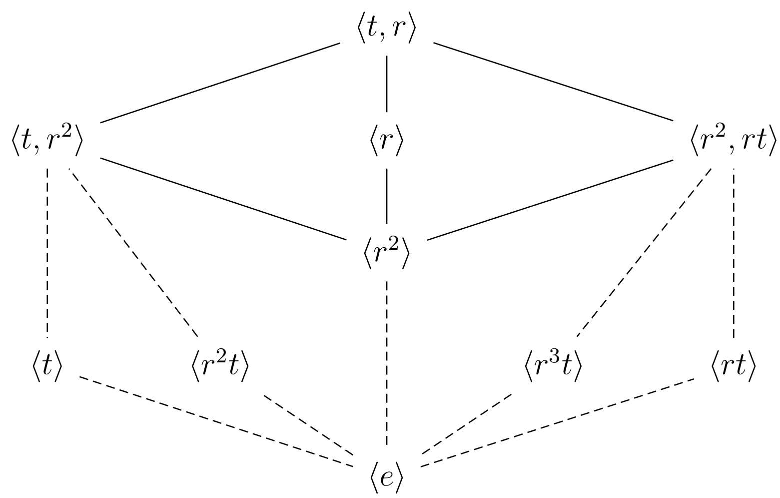

Figure 3.4: The Lattice of subroups of $D_8/\langle r^2 \rangle$ in the lattice of subgroup of D_8.

Notice also that $D_8/\langle r^2 \rangle \simeq V_4$.

3.5 Composition Series, Simple Groups, and Solvable Groups.

The bulk of this section is concerned primarily with results, and not their proofs. As such, the majority of the theorems are preseneted without proof.

Theorem 3.5.1. *Let G be a finite abelian group, and let $p | \operatorname{ord} G$ a prime. Then G contains an element of order p.*

Proof. By induction, let $\operatorname{ord} G > 1$, then there exists an $x \in G$ with $x \neq e$. Now, suppose that $\operatorname{ord} G = p$. By Lagrange's theorem, $\operatorname{ord} x = p$.

Now suppose that $\operatorname{ord} G > p$. If $p | \operatorname{ord} x$, then $\operatorname{ord} x = pn$ for some $n \in \mathbb{Z}^+$. Thus by lemma 2.3.6 $\operatorname{ord} x^p = \frac{p}{(n,p)} = p$, and we are done.

Now assume that $p \not| \operatorname{ord} x$, and consider the cyclic subgroup generated by x, $\langle x\rangle$. Since $\langle x\rangle$ is abelian, we have that $\langle x\rangle \trianglelefteq G$. Thus, by Lagrange's theorem, we have $[G:\langle x\rangle] = \frac{\operatorname{ord} G}{\operatorname{ord} x}$, and since $\langle x\rangle \neq \langle e\rangle$, we have $[G:\langle x\rangle] < \operatorname{ord} G$. Since $p \not| \operatorname{ord} x$, we get $p|[G:\langle x\rangle]$. By hypothesis then, we have that ${}^{G}\!/\!_{\langle x\rangle}$ contains an element of order p, $g\langle x\rangle$. Then $(g\langle x\rangle)^p = g^p\langle x\rangle = \langle e\rangle$ so that $g^p \in \langle x\rangle$. Moreover, $\langle g^p\rangle \neq \langle g\rangle$, so that $\operatorname{ord} g^p | \operatorname{ord} g$. That is, $p|\operatorname{ord} g$. Therefore, by the above argument, G contains an element of order p. ∎

Remark. This theorem and its proof illustrates that one can prove certain results about groups using normal subgroups and quotients. However, they usually hinge on these structures being nontrivial. It is not always the case that a group will have nontrivial normal subgroups.

Definition. We call a group G **simple** if its only normal subgroups are $\langle e\rangle$ and G itself.

Proof. These simple groups consitute something analogous to a prime number. ∎

Example 3.8. If $\operatorname{ord} G = p$, then by Lagrange's theorem, it is simple.

With a prime analog for groups, one would be motivated to try and construct something analogous to "prime" factorization of groups. This motivates the following definition.

Definition. Let G be a group and $\{H_i\}_{i=}^k$ a sequence of subgroups with $H_0 = \langle e\rangle$, $H_k = G$, and $H_i \leq H_{i+1}$, If $H_i \trianglelefteq H_{i+1}$ and ${}^{H_{i+1}}\!/\!_{H_i}$ is simple for all $0 \leq i \leq k$, then we call the sequence $\{H_i\}$ a **composition series**. We call the quotients ${}^{H_{i+1}}\!/\!_{H_i}$ **composition factors** of G.

Example 3.9. D_8 has two composition series: $\langle e\rangle \trianglelefteq \langle t\rangle \trianglelefteq \langle t, r^2\rangle \trianglelefteq D_8$ and $\langle e\rangle \trianglelefteq \langle r^2\rangle \trianglelefteq \langle r\rangle \trianglelefteq D_8$.

Theorem 3.5.2 (Jordan-Hölder)**.** *Let G be a nontrivial finite group. Then:*

(1) G has a composition series.

(2) The composition factors of G are uniquely determined. That is, if $\langle e\rangle = N_0 \leq N_1 \leq \cdots \leq N_k = G$ and $\langle e\rangle = M_0 \leq M_1 \leq \cdots \leq M_s = G$ are composition series of G, then $r = s$ and for some permutation $\pi \in S_r$, the quotients:

$$ {}^{M_{\pi(i)+1}}\!/\!_{M_{\pi(i)}} \simeq {}^{N_{i+1}}\!/\!_{N_i} $$

Remark. This theorem serves as the group theoretic analog for the fundamental theorem of arithmetic. In enssence, every group has a unique "prime" factorizations. The uniqueness of the factorization comes from the fact that the composition factors turn out to be isomorphic.

The study of simple groups, particulalry, finite simple groups motivates the following problem: to classify all finite simple groups. Another problem motivated by the study of simple groups is to construct other groups from simple groups.

Theorem 3.5.3. *There are* 18 *inifinite families of simple groups and* 26 *simple groups not belonging to any one family, such that every finite simple group is isomorphic to one of the groups in the families.*

Remark. We call these 26 groups the **sporadic** simple groups.

Example 3.10. (1) One of the 18 families is the collection $\{\mathbb{Z}/p\mathbb{Z} : p \text{ is prime}\}$.

(2) Another familiy is the collection $\{SL(n, \mathbb{F}_q)/Z(SL(n, \mathbb{F}_q)) : n \in \mathbb{Z}^+, n \geq 2, \mathbb{F}_q \text{ a finite field}\}$

Theorem 3.5.4 (Feit-Thompson)**.** *If G is a simple group of odd order, then $G \simeq \mathbb{Z}/p\mathbb{Z}$ for some prime p.*

Likewise, in addition to simplicity of groups, we also have the notion of solvability. Solvable groups play a role in the theory of polynomials and in certain geometric constructions.

Definition. A group G is **solvable** if there exists a sequence of normal subgroups $\langle e \rangle = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_k = G$ such that G_{i+1}/G_i is abelian for each $0 \leq i \leq k-1$.

Theorem 3.5.5. *A finite group is solvable if and only if for every n dividing* $\operatorname{ord} G$*, with $(n, \frac{\operatorname{ord} G}{n}) = 1$, G has a subgroup of order n.*

We conclude with a lemma.

Lemma 3.5.6. *Let G be a group and $N \trianglelefteq G$. If N and G/N are solvable, then so is G.*

Proof. Let $\overline{G} = G/N$, and let $\langle e \rangle = N_0 \trianglelefteq N_1 \trianglelefteq \cdots \trianglelefteq N_n = N$ a sequence of normal subgroups with N_{i+1}/N_i abelian. Let $\langle e \rangle = \overline{G_0} \trianglelefteq \overline{G_1} \cdots \trianglelefteq \overline{G_m} = \overline{G}$ be another such sequence. By the fourth isomporphism theorem, there are subgroups $G_i \leq G$ with $N \leq G_i$ such that $G_i/N = \overline{G_i}$ and $G_i \trianglelefteq G_{i+1}$. Theb by the third isomorphism theorem, we have

$$\overline{G_{i+1}}/\overline{G_i} = {G_{i+1}/N}/{G_i/N} \simeq G_{i+1}/G_i$$

Thus, $\langle e \rangle = N_0 \trianglelefteq N_1 \trianglelefteq \cdots \trianglelefteq N_n = N = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_m = G$ is a sequence of subgroups whose subsequent quotients are abelian. That is, G is solvable. ∎

3.6 The Alternating Group.

We now go over transpositions and the generation of S_n.

Definition. A 2-cycle in S_n is called a **transposition**.

Lemma 3.6.1. *Every element of S_n can be written as a product of transpositions in S_n. That is, $S_n = \langle T \rangle$, where $T = \{(i\ j) : 1 \leq i \leq j \leq n\}$.*

Proof. Observe that $(a_1\ a_2\ \ldots\ a_m) = (a_1\ a_m)(a_1\ a_{m-1}) \ldots (a_1\ a_2)$ for any m-cycle. ∎

Example 3.11. The permutation $s = (1\ 12\ 8\ 10\ 4)(2\ 13)(5\ 11\ 7)(6\ 9)$ can be written as: $s = (1\ 4)(1\ 10)(1\ 8)(1\ 12)(2\ 13)(5\ 7)(5\ 11)(6\ 9)$.

For the following, let $x_1, \ldots, x_n$ be independent variables and define the polynomial:

$$\Delta = \prod_{1 \leq i \leq j \leq n} (x_i - x_j) \tag{3.5}$$

Example 3.12. For $n = 4$, $\Delta = (x_1 - x_2)(x_1 - x_3)(x_1 - x_4)(x_2 - x_3)(x_2 - x_4)(x_3 - x_4)$.

Now, for $s \in S_n$, let s act on Δ by permuting the indices of the terms. That is:

$$\Delta = \prod (x_{s(i)} - x_{s(j)})$$

It can be verified that $s(\Delta)$ and Δ only differ by a sign. That is $s(\Delta) = \pm\Delta$.

Definition. Let Δ be the polynomial of equation (3.5), and let $s \in S_n$ act on Δ by permuting the indices of the terms. We define the **sign** of s to be:

$$\varepsilon(s) = \begin{cases} 1, \text{ if } s(\Delta) = \Delta \\ -1, \text{ if } s(\Delta) = -\Delta \end{cases} \tag{3.6}$$

We call s **even** if $\varepsilon(s) = 1$, and **odd** if $\varepsilon(s) = -1$.

Lemma 3.6.2. *The sign map of a permutation $\varepsilon : S_n \to \langle -1, 1 \rangle$ is a homomorphism.*

Proof. By definition, for $s, t \in S_n$, we have $ts(\Delta) = \prod (x_{ts(i)} - x_{ts(j)})$. Now suppose that $s(\Delta)$ has k factors, of the form $x_j - x_i$ with $i < j$. Then we have $\varepsilon(s) = (-1)^k$. We also have that ts has k factors of the form $x_{t(j) - x_{t(i)}}$. Then the terms of the k factors are permuted, and so have the form $x_{t(p)} - x_{t(q)}$, where $p < q$. Then

$$ts(\Delta) = \varepsilon(s) \prod (x_{t(p)} - x_{t(q)})$$

So, by definition of ε,

$$\varepsilon(t)\Delta = \prod (x_{t(p)} - x_{t(q)})$$

so that $ts(\Delta) = \varepsilon(t)\varepsilon(s)\Delta$. Therefore, we get that $\varepsilon(ts) = \varepsilon(t)\varepsilon(s)$. ∎

Example 3.13. Let $n = 4$, $s = (1\ 2\ 3\ 4)$ and $t = (4\ 2\ 3)$. Then $ts(\Delta) = (1\ 3\ 2\ 4)\Delta = (x_3 - x_2)(x_3 - x_2)(x_3 - x_1)(x_4 - x_2)(x_4 - x_1)(x_2 - x_1) = (-1)^5$. So that $\varepsilon(ts) = -1$. Now, we also have that $s(\Delta) = (1\,2\,3\,4)\Delta = (x_2 - x_3)(x_2 - x_4)(x_2 - x_1)(x_3 - x_4)(x_3 - x_1)(x_4 - x_1) = (-1)^3\Delta$. Additionally, $t(\Delta) = (x_1 - x_3)(x_1 - x_4)(x_1 - x_2)(x_3 - x_4)(x_3 - x_2)(x_4 - x_2) = (-1)^2\Delta$. So $\varepsilon(t) = 1$, and $\varepsilon(s) = -1$, so $\varepsilon(t)\varepsilon(s) = -1$.

Theorem 3.6.3. *Transpositions are all odd permutations, and the sign of a permutation is onto.*

Proof. Notice for any $s \in S_n$, ε maps s to 1 or -1, so ε is onto.

Now, consider the transposition $(1\ 2)$. Then $(1\ 2)\Delta$ takes $x_1 - x_2$ to $x_2 - x_1$. So $\varepsilon((1\ 2)) = -1$. Now, for any transposition $(i\ j)$, let λ be the permutation taking $1 \to i$, $2 \to j$, and fixes all other entries. Then $(i\ j) = \lambda(1\ 2)\lambda$. And so we get:

$$\begin{aligned}\varepsilon((i\ j)) &= \varepsilon(\lambda(1\ 2)\lambda) \\ &= \varepsilon(\lambda)\varepsilon((1\ 2))\varepsilon(\lambda) \\ &= (-1)(\varepsilon((1\ 2)))^2 \\ &= (-1)\end{aligned}$$

Making $(i\ j)$ an odd permutation. ■

We can now define the following group:

Definition. The **Alternating group** of **degree** n, A_n, is the kernel of ε. That is, it is the group of all even permutations of S_n.

Lemma 3.6.4. ord $A_n = \frac{1}{2}n!$.

Proof. By the first isomorphism theorem, we have that ${}^{S_n}\!/_{A_n} = \varepsilon(S_n) = \langle -1, 1\rangle$. So ord $A_n = \frac{1}{2}$ ord $S_n = \frac{1}{2}n!$.

$$\begin{tikzcd} A_n \arrow[rr] \arrow[drr, dashed] & & \varepsilon(S_n) \arrow[d] \\ & & \langle -1, 1\rangle \end{tikzcd}$$

■

Corollary. *For $s \in S_n$:*

$$\varepsilon(s) = \begin{cases} 1, & \textit{if } s \textit{ is a product of an even number of transpostions.} \\ -1, & \textit{if } s \textit{ is a product of an odd number of transpostions.} \end{cases}$$

Proof. Since ε is a homomorphism, and any $s \in S_n$ can be written as the product of transpositions, $s = t_1 \dots t_k$, so that $\varepsilon(s) = \varepsilon(t_1)\dots\varepsilon(t_k)$. ■

Lemma 3.6.5. *A permutation s is odd if, and only if the number of cycles of even length in the decomposition of s is odd.*

Proof. For any $s \in S_n$, let $a_1, \dots, a_k$ be its cycle decomposition. Then $\varepsilon(s) = \varepsilon(a_1)\dots\varepsilon(a_k)$, where $\varepsilon(a_i) = -1$ for all $1 \le i \le k$, if and only if a_i has even length. So $\varepsilon(s) = (-1)^k$, so k must be odd if $\varepsilon(s) = 1$. ■

Example 3.14. (1) $A_1 = A_2 = \langle (1) \rangle$.

(2) ord $A_3 = 3$, so $A_3 = \langle (1\ 2\ 3) \rangle \simeq {}^{\mathbb{Z}}\!/_{3\mathbb{Z}}$.

(3) $|A_4| = 12$, and A_4 has the following lattice of figure 3.5

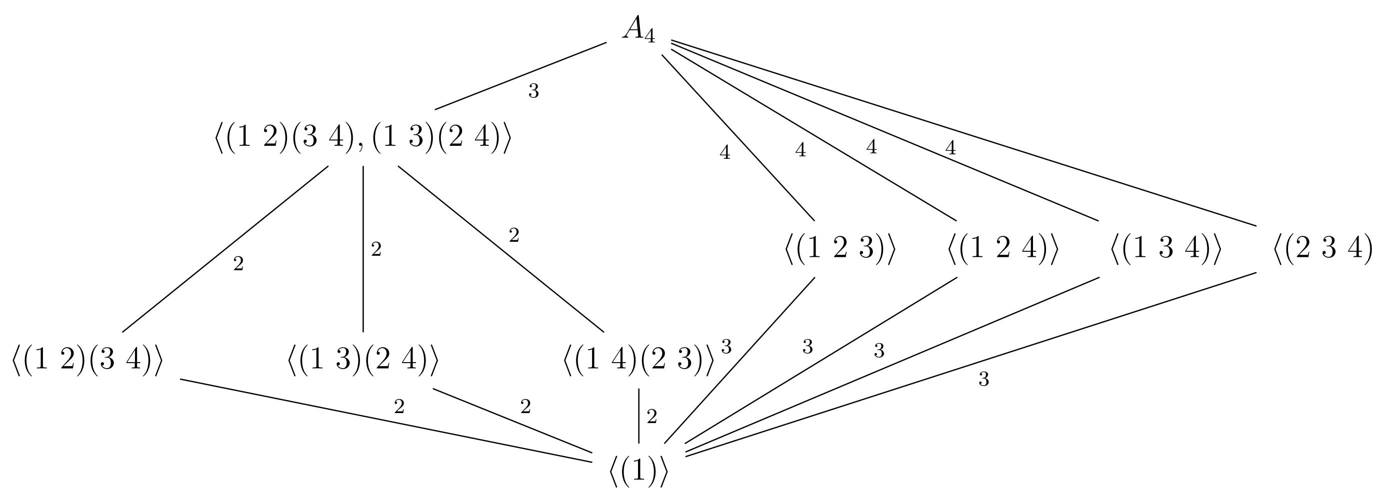

Figure 3.5: The lattice of subgroups for A_4.

Chapter 4

Group Actions.

4.1 Group Actions and Permutation Representations.

We now present the notion of a group "acting" on a given set. The study of these "actions" will allow us to prove results for groups and also for finding underlying structures of specific sets.

Definition. A **left** group **action** of a group G on a set A is a map $\cdot : G \times A \to A$ such that for all $g \in G$ and $a \in A$:

(1) $g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a$.

(2) $e \cdot a = a$, where e is the identity of G.

Remark. As before, we will drop explicit mention of the action $\cdot$ and mearly werite ga. It should be taken into account that the group action $\cdot$ is not a binary operation.

Remark. Similarly, one can define **right** group actions. Our study will consist of left group actions, so we drop the indication.

Lemma 4.1.1. *Let G be a group acting on a set S. For each $g \in G$, define the map $s_g : S \to S$ by $s_g : a \to ga$. Then:*

(1) For each $g \in G$, s_g is a permutation of S.

(2) The map $G \to A(S)$ defined by $g \to s_g$ is a homomorphism.

Proof. Let $a, b \in S$ and suppose that $s_g(a) = s_g(b)$. Then $ga = gb$, and by the cancellation laws, $a = b$. This makes s_g $1-1$. On the otherhand, since $ga \in A$ for all $a \in A$, we get that s_g is onto. This makes s_g a permutation. Now, consider $g^{-1} \in G$, and notice that $s_{g^{-1}} s_g(a) = s_{g^{-1}}(ga) = g^{-1}(ga) = (g^{-1}g)a = ea = a$. Thus we get $s_g^{-1} = s_{g^{-1}}$.

Now consider the map $\phi : g \to s_g$. Then $\phi(gg')(a) = s_{gg'}(a) = (gg')a = g(g'a) = s_g s_{g'}(a) = \phi(g)\phi(g')$. ■

Remark. The main takeaway of this lemma is that group actions on a set S are merely permutations of the elements of S.

Definition. Let G be a group acting on a set S, and define $s_g : a \to ga$, and define $\phi : G \to A(S)$ by $\phi : g \to s_a$. We call ϕ the **permutation representation** of S associated with g.

Example 4.1. Let G be a group, and $A \neq \emptyset$. Then:

(1) Define the action $ga = a$ for all $g \in G$. Then $g_1(g_2)a = g_1a = a$ and $(g_1g_2)a = a$, so $g_1(g_2)a = (g_1g_2)a$, and $ea = a$, so we indeed have an action. We call this the **trivial** action, and we say that G acts **trivially** on A. Define then $s_g : a \to ga = a$, then s_g is the identity map. So the permutation representation associated with g is the identity map.

(2) In the vector space axioms, scalar multiplication $\cdot : F^* \times V \to V$ is an action of F^* on V. We have for any $\alpha, \beta \in F$, and $v \in V$, $\alpha(\beta)v = (\alpha\beta)v$, and $1v = v$. Here F is a field, and so F^* forms a multiplicative group under the relavent multiplication.

(3) For any $S \neq \emptyset$, the symmetric group $A(S)$ acts on S via the action $sa = s(a)$.

(4) Consider again the regular n-gon. Label its veritces to be the set $\mathbb{Z}/n\mathbb{Z}$, then we can see that the symmetries of the n-gon act on vertices of the n-gon.

Consider the map $D_{2n} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ of $D_{2n} \times \mathbb{Z}/n\mathbb{Z}$ onto $\mathbb{Z}/n\mathbb{Z}$ via the map $(r^jt, i) \to r^jt(i)$, where $j \in \mathbb{Z}/n\mathbb{Z}$. This map forms a group action of D_{2n} on $\mathbb{Z}/n\mathbb{Z}$. Also notice that distinct symmetries induce distinct permutations of the vertices.

(5) Let G be any group, and let $A = G$. Then the binary operation on G is a group action of G onto itself. We have $a(bc) = (ab)c$, and so the first prppertiy is satisfied by associativity, and $ea = a$ and the second property is satisfied by the identity law. We call the binary operation a **left regular** action. Also notice that distinct elements of G induce distinct permutations of G.

We end the section, and the chapter with two more definitions.

Definition. Let G be a group acting on a set A. We call the action of G on A **faithful** if distinct elements of G induce distinct permutations on G. That is if ϕ is the permutation representation associated with G, then ϕ is $1-1$.

Definition. Let G be a group acting on a set A. We define the **kernel** of the group action on A to be $\ker A = \{g \in G : ga = a \text{ for all } a \in A\}$

Lemma 4.1.2. *The kernel of a group action is precisely the kernel of the associated permutation representation.*

Proof. Let G be a group acting on a set A. Now, for any $g \in \ker A$, we have $ga = a$ for all $a \in A$. Now let $\sigma : a \to ga$, and consider the permutation representation of A with respect to g, $\phi : g \to s_g$. We can then see that $\phi(g) = s_g$, for which $s_g(a) = a$ for all $a \in A$, so that $\phi(g) = (1)$, hence, $g \in \ker\phi$. Conversely, we also get that if $g \in \ker\phi$, then $\phi(g) = s_g = (1)$, so that for all $a \in A$, $a = ga$, which makes $g \in \ker A$. ∎

Corollary. *Two group elements induce the same permutation on A if, and only if they are in the same coset of the kernel; i.e. if, and only if they are in the same fiber of the permutation representation ϕ.*

Example 4.2. (1) Let $n \in \mathbb{Z}^+$, then the symmetric group S_n, acts on the set $A = \{1, \ldots, n\}$ by the action $s \cdot i = s(i)$. for all $i \in A$. The permutation representation of A is then the map $\phi : S_n \to S_n$ taking $s \to s$; i.e. the identity map. Snce ϕ is 1–1, we get that ϕ is faithful, and that for each $i \in A$, the $\operatorname{stab} i \simeq \mathrm{S}_{n-1}$.

(2) Consider D_8 acting on the set A of 4 vertices of a square with $A = \{1, 2, 3, 4\}$. Letting r be the rotation of the square by $\frac{\pi}{2}$, and t the reflecton of the square about the line cutting vertices 1 and 3. Then the permutations of A via r and t are $s_r = (1\ 2\ 3\ 4)$ and $s_t = (2\ 4)$. Notice then that $s_{rt} = s_r s_t = (1\ 3)(2\ 4) = (1\ 4)(2\ 3)$. The action of D_8 on A is also faithful, since $\ker A = \langle e \rangle$. We can also see that $\operatorname{stab} a \leq D_8$ and that $\operatorname{ord}(\operatorname{stab} a) = 2$.

(3) Consider the square labeled by the vertices in the previous example and let A be the set of unordered pairs of opposite vertices $A = \{\{1, 3\}, \{2, 4\}\}$. Then D_8 acts on A with the permutations s_r and s_t. Letting $1' = \{1, 3\}$ and $2' = \{2, 4\}$, we get that $s_r = (1'\ 2')$ and $s_t = (1')$. This action is not faithful, as $\ker A = \langle t, r^2 \rangle$.

Theorem 4.1.3. *For any group G acting on a nonempty set S, there is a 1–1 correspondence of teh actions of G onto homomorphisms of G into $A(S)$.*

Proof. Let $\phi : G \to A(S)$ be a homomorphism, and define the action $ga = \phi(g)(a)$. Then the kernel of the action is $\ker A = \{g \in G : \phi(g)(a) = a\} = \{g \in G : \phi(g) = e\} = \ker G$. Moreover, the permutation representation of ga is precisely ϕ. ■

Definition. For any group G, a **permutation representation** of G is a homomorphism of G into $A(S)$.

Lemma 4.1.4. *Let G be a group acting on a nonempty set A. The $\sim$ on A defined by ab if, and only if $a = gb$ for some $g \in G$ is an equivalence relation.*

Proof. We have $a = ea$, so $a \sim a$. Now, if $a \sim b$, then $a = gb$ for $g \in G$. Then $b = g^{-1}a$ so that $b \sim a$. Now let $a \sim b$ and $b \sim c$. Then $a = gb$ and $b = hc$ for $g, h \in G$. Then $a = g(hc) = (gh)c$, and by closure of G, this makes $a \sim c$. ■

Corollary. *For each $a \in A$, the number of elements in the equivalence class of a is the index of* $\operatorname{stab} a$ *in G; i.e.* $[G : \operatorname{stab} a]$.

Proof. Let $\mathcal{O}_a = \{ga : g \in G\}$ be the equivalence class of $a \in A$ under $\sim$. Notice that $g \operatorname{stab} a$ is a left coset of G, and so consider the map $\phi : ga \to g \operatorname{stab} a$ from $\mathcal{O}_a \to {}^{G}\!/_{\operatorname{stab} a}$. We get that ϕ is onto since $ga \in \mathcal{O}_a$ for every $g \in G$. Moreover, ϕ is 1–1 since $ga = hb$ if, and only if $(h^{-1}g)a = b$ so that $(h^{-1}g) \operatorname{stab} a = \operatorname{stab} b$, hence $g \operatorname{stab} a = h \operatorname{stab} b$. This make $\mathcal{O}_a \simeq {}^{G}\!/_{\operatorname{stab} a}$. ■

Definition. Let G be a group acting on a nonempty set A. We call the equivalence class $\operatorname{orb} a = \{ga : g \in G\}$ of a the **orbit** of a. We call the action of G on A **transitive** if there is only one orbit.

Example 4.3. (1) For any group G and set A, if G acts trivially on A, then $\operatorname{stab} a = G$ for all $a \in A$, and $\operatorname{orb} A = A$. Then the trivial action is transitive if, and only if $|A| = 1$.

(2) The symmetric group S_n acts on $A = \{1, \dots n\}$ transitively in its usual action. Notice that for any $i \in A$, $[S_n : \operatorname{stab} i] = |A| = n$.

(3) If G is any group acting on A, and $H \leq G$, then H also acts on A. Now suppose that G acts on A transitively, in particular let $G = S_n$. Let $H = \langle (1\ 2), (3\ 4) \rangle \leq S_n$. Then the orbits of H on $A = \{1, \dots, n\}$ are the sets $\{1, 2\}$ and $\{3, 4\}$, and there is no element taking $2 \to 3$. Thus H does not act transitively on A. For any group G acting on A transitively, H need not act on A transitively.

(4) D_8 acts transitively on the vertices of a square. The stabalizer of any vertex is the subgroup of order 2 generated by the reflection about the line passing through that vertex.

Theorem 4.1.5. *Every element of S_n has a unique cycle decomposition.*

Proof. Let $A = \{1, \dots, n\}$ and let $s \in S_n$, and consider $\langle s \rangle$. Then $\langle s \rangle$ acts on A, and hence partitions it into orbits. Now, consider an orbit $\mathcal{O}$ under s, and let $x \in \mathcal{O}$. Then we have that $\mathcal{O} = A$, and there is a 1–1 correspondence of cosets of $\operatorname{stab} x$ in G onto elements of $\mathcal{O}$, defined by the map $s^i x \to s^i \operatorname{stab} x$. Now, since $\langle s \rangle$ is cyclic, we get $\operatorname{stab} x \trianglelefteq \langle s \rangle$, and $\langle s \rangle / \operatorname{stab} x$ must be cyclic of order d, where d is the least integer for which $s^d \in \operatorname{stab} x$. Then we get that $d = [\langle s \rangle, \operatorname{stab} x] = |\mathcal{O}|$ and the cosets can be listed in order as:

$$\operatorname{stab} x \qquad s \operatorname{stab} x \qquad \dots \qquad s^{d-1} \operatorname{stab} x$$

So $\mathcal{O}$ has elements

$$x \qquad s(x) \qquad \dots \qquad s^{d-1}(x)$$

So s cycles through $\mathcal{O}$; that is s is a d-cycle on $\mathcal{O}$ which gives s a cycle decomposition.

Moreover, teh orbits of $\langle s \rangle$ are uniquely determined by s, so choosing $s^i(x)$ we can reorder the elements of $\mathcal{O}$ as

$$s^i(x) \qquad s^{i+1}(x) \qquad \dots \qquad s^{d-1}(x) \qquad x \qquad s(x) \qquad \dots \qquad s^{i-1}(x)$$

which is a cycle permutation. ∎

Definition. We call the subgroups of the symmetric group **permutation groups**.

4.2 Cayley's Theorem.

Consider a group G acting on itself via left multiplication; i.e. the action $G \times G \to G$ defined by $g \cdot a \to ga$. if $\operatorname{ord} G = n$, then $G = \{g_0, \dots, g_{n-1}\}$, where $g_0 = e$. Conisder then the permutation $s_g : i \to j$ if, and only if $gg_i = j$. Moreover, we can consider G a group, and $H \leq G$, such that G acts on the factor set ${}^{G}\!/_{H}$ via the action $g \cdot aH \to (ga)H$. Then we can take the permutation above as $s_g : i \to j$ if, and only if $g \cdot a_i H = a_j H$.

Example 4.4. (1) Consider the Klein 4-group acting on its self. Let $V_4 = \{1, a, b, c\}$ and label $a = 2, b = 3$, and $c = 4$. Define the permutation $s_a : i \to j$. Then $s_a(1) = 2$, $s_a(2) = 1$, $s_a(3) = 4$ and $s_a(4) = 3$, so we get $s_a = (1\ 2)(3\ 4)$. By similar computation, we get $s_b = (1\ 3)(2\ 4)$ and $s_c = (1\ 4)(2\ 3)$.

(2) Consider D_8 the dihedral group acting on the factor set ${}^{D_8}\!/_{\langle t \rangle} = \{\langle t \rangle, r\langle t \rangle, r^2\langle t \rangle, r^3\langle t \rangle\} \simeq \{1, 2, 3, 4\}$. Taking the permutation $s_t : i \to j$ if, and only if $ti = j\langle t \rangle$, we get $s_t(1) = 1$, $s_t(2) = 4$, $s_t(3) = 3$ and $s_t(4) = 2$. So $s_t = (2\ 4)$. Similarly.

Theorem 4.2.1. *Let G be a group, and H a subgroup on H. Conisder G acting on ${}^{G}\!/_{H}$ via $g \cdot aH \to (ga)H$, and let π_H be the permutation representation of this action. Then the following are true:*

(1) G acts faithfully on ${}^{G}\!/_{H}$.

(2) $\operatorname{stab} H = H$.

(3) $\ker \pi_H = \bigcap_{x \in G} xHx^{-1}$, and $\ker \pi_H$ is the largest normal subgroup of G contained in H.

Proof. Let $aH, bH \in {}^{G}\!/_{H}$, and $g = ba^{-1}$. Then $g \cdot aH = (ga)H = (ba^{-1}a)H = bH$ so that aH and bH are in the same orbit. Since $a, b \in G$ are arbitrary, we get there is only one such orbit. So G acts faithfully on ${}^{G}\!/_{H}$.

Now, notice that $\operatorname{stab} H = \{g \in G : g \cdot 1H = 1H\}$. So, if $g \in \operatorname{stab} H$, then $gH = H$, which makes $g \in H$. On the other hand, if $g \in H$, then $gH = (g1)H = g \cdot 1H = 1H$, which puts $g \in \operatorname{stab} H$. Therefore $\operatorname{stab} H = H$.

Lastly, notice that $\ker \pi_H = \{g \in G : gxH = xH\}$. Now, if $g \in \ker \pi_H$, then $gxH = xH$ so that $x^{-1}gxH = H$, so $x^{-1}gx \in H$ so that $g \in xHx^{-1}$. Likewise, if $g \in xHx^{-1}$, then $x^{-1}gx \in H$ which puts $x^{-1}gx = H$. Therefore $gxH = xH$ which puts $g \in \ker \pi_H$, for all $x \in G$. That is, $\ker \pi_H = \bigcap xHx^{-1}$.

Now, since $\ker \pi_H \trianglelefteq G$, if $N \trianglelefteq G$, then $N = xNx^{-1} \leq xHx^{-1}$ for all $x \in G$. This puts $N \leq \bigcap xHx^{-1} = \pi_H$. This makes $\ker \pi_H$ the largest normal subgroup of G, contained in H. ■

Corollary (Cayley's Theorem)**.** *Every group is isomorphic to a subgroup of the symmetric group.*

Proof. Let $H = \langle e \rangle$, then ${}^{G}\!/_{\langle e \rangle} = G$ acts on intself by the left regular action. Let $\pi_{\langle e \rangle} = \pi : G \to A(G)$ be the permutation representation of this action. By above, we get that $\ker \pi = \langle e \rangle$, which makes π 1–1. Moreover, since $\pi(G) \leq A(G)$, we get that $\pi : G \to \pi(G)$ defines an isomorphism of G onto a subgroup of $A(G)$. ■

Corollary. *if G is as group of order n, then G is isomorphic to a subgroup of S_n.*

Example 4.5. (1) $V_4 \simeq \langle (1\ 2)(3\ 4), (1\ 3)(2\ 4) \rangle \leq S_4$.

(2) $D_8 \simeq \langle (2\ 4), (1\ 2\ 3\ 4) \rangle \leq S_8$.

Lemma 4.2.2. *If G is a finite group of order n, and p is the smallest prime dividing n, then every subgroup of index p, in G is normal.*

Proof. Let $H \leq G$ with $[G : H] = p$. Let π_H the permutation representation of the action $g \cdot aH \to (ga)H$ and let $K = \ker \pi_H$, and $[H : K] = k$. Then $[G : K][G : H][H : K] = pk$. Now, since H has p left cosets in G, by the first isomorphism theorem and Cayley's theorem, we get ${}^{G}\!/_{K}$ is isomorphic to a subgroup of S_p. Now, by Lagrange's theorem, $pk|p!$, i.e. $k|\frac{p!}{p} = (p-1)!$. However, all prime divisors of $(p-1)!$ are less than p, so by minimality, every prime divisor q of k is such that $p \leq q$. Therefore $k = 1$ and $H = K \trianglelefteq G$. ■

4.3 The Class Equation.

Definition. Let G be a group. We call two elements $a, b \in G$ **conjugate** if $b = gag^{-1}$ for some $g \in G$. We call the orbits of G acting on itself via conjugation the **conjugacy classes** of G.

Example 4.6. (1) If we define the relation $\sim$ on G by $a \sim b$ if and only if $b = gag^{-1}$ for some $g \in G$, we can see that $\sim$ is reflexive and transitive; however $\sim$ is not symmetric. If $a \sim b$, then $b = gag^{-1}$, os $b^{-1} = g^{-1}a^{-1}g$, which makes $a^{-1} = gb^{-1}g^{-1}$. So $b^{-1} \sim a^{-1}$. This means that conjugacy of elements is not an equivalence relation.

(2) If G is Abelian then the conjugacy class of any $a \in G$ is the point-set $\{a\}$.

(3) For any group G of order $\operatorname{ord} G > 1$, G does not act on itself transitively via conjugation, as $a = gag^{-1}$ if, and only if $a \in Z(G)$.

Definition. Let G be a group. We call subsets $S, T \subseteq G$ **conjugate** if $T = gSg^{-1}$ for some $g \in G$.

Lemma 4.3.1. *The number of conjugates of a subset S of a group G is the indexs of the normalizer of S in G; i.e. $[G : N(S)]$. In particular, the number of conjugates of an element $s \in G$ is $[G : C(s)]$.*

Proof. By the corollary to lemma 4.1.4, we have that S has $[G : \operatorname{stab} S]$ conjugates. Notice then that $\operatorname{stab} S = \{g \in G : gSg^{-1} = S\} = N(S)$, by definition. Moreover, notice that $N(\{s\}) = C(s)$ for any $s \in G$. ■

Theorem 4.3.2 (The Class Equation)**.** *Let G be a finite group and $g_1, \ldots, g_r$ representatives of distinct conjugacy classes of G not in $Z(G)$. Then*

$$\operatorname{ord} G = \operatorname{ord} Z(G) + \sum_{i=1}^{r} [G : C(g_i)]$$

Proof. Notice that x has conjugacy class $\{x\}$ if, and only if $x \in Z(G)$. then $x = gxg^{-1}$ for all $x \in G$. Let $Z(G) = \{z_1, \dots, z_m\}$, with $z_1 = e$ and let $\mathcal{K}_1, \dots, \mathcal{K}_r$ the conjugacy classes of G not in $Z(G)$ with representatives $g_1, \dots, g_r$. Then the conjugacy classes of G are precisely:

$$\langle e \rangle \qquad \{z_2\} \qquad \dots \qquad \{z_m\} \qquad \mathcal{K}_1 \qquad \dots \qquad \mathcal{K}_r$$

Since these conjugacy classes partition G, we get

$$\operatorname{ord} G = \sum_{i=1}^{m} 1 + \sum_{i=1} r|\mathcal{K}_i| = \operatorname{ord} Z(G)| \sum [G : C(g_i)]$$

■

Example 4.7. (1) For any Abelian group G, $\operatorname{ord} G = \operatorname{ord} Z(G)$ and the class equation gives nothing interesting.

(2) In any group G, notice that $\langle g \rangle \leq C(g)$. Now, consider the quaternion group $\mathbb{H}$, then $\langle i \rangle \leq C(i)$ and since $i \in Z(\mathbb{H})$, we have $[\mathbb{H} : \langle i \rangle] = 2$ so that $\langle i \rangle = C(i)$. So i has two conjugates: itself, and $-i = kik^{-1}$. By similar reasoning, the conjugacy classes of $\mathbb{H}$ are

$$\langle 1 \rangle \qquad \{-i, i\} \qquad \{-j, j\} \qquad \{-k, k\}$$

Then the class equation gives $\operatorname{ord} \mathbb{H} = 2 + 2 + 2 + 2 = 8$.

(3) The conjugacy classes of D_8 are

$$\langle e \rangle \qquad \langle r^2 \rangle \qquad \{r, r^2\} \qquad \{t, tr^2\} \qquad \{tr, tr^3\}$$

and the class equation gives $\operatorname{ord} D_8 = 2 + 2 + 2 + 2 = 8$.

Theorem 4.3.3. *If $p \in \mathbb{Z}^+$ is prime, and P is a group of order p^r, for some $r \in \mathbb{Z}^+$, then P has nontrivial center.*

Proof. By the class equation, we have $\operatorname{ord} P = \operatorname{ord} Z(P) + \sum [P : C(g_i)]$, where each g_i are representatives of distinct non central conjugacy classes. By definition, we cannot have $C(g_i) = P$, so $p|[P : C(g_i)]$. Since we also have that $p| \operatorname{ord} P$, we must have that $p| \operatorname{ord} Z(P)$.

■

Corollary. *If $\operatorname{ord} P = p^2$, then P is Abelian; in particular $P \simeq \mathbb{Z}/_{p^2\mathbb{Z}}$ or $P \simeq \mathbb{Z}/_{p\mathbb{Z}} \times \mathbb{Z}/_{p\mathbb{Z}}$.*

Consider now, the conjugation of symmetric groups. We then have the following.

Lemma 4.3.4. *let $s, t \in S_n$ be permutations where s has cycle decomposition*

$$s = (a_1\ a_2\ \dots\ a_{k_1})(b_1\ b_2\ \dots\ b_{k_2}) \dots$$

Then tst^{-1} has cycle decomposition

$$tst^{-1} = (t(a_1)\ \dots\ t(a_{k_1}))(t(b_1)\ \dots\ t(b_{k_2})) \dots$$

Proof. If $s : i \to j$, then $tst^{-1} : t(i) \to t(j)$. So if the pair (i, j) appears in the cycle decomposition of s, the pair $(t(i), t(j))$ appears in the cycle decomposition of tst^{-1}. ■

Definition. If $s \in S_n$ is the product of cycles (including 1-cycles) of lengths $n_1, \dots, n_r$, with $n_1 \leq \cdots \leq n_r$, then we call the r-tuple $(n_1, \dots, n_r)$ the **cycle type** of s.

Definition. A **partition** of a positive integer $n \in \mathbb{Z}^+$ is any nondecreasing sequence of positive integers whose sum is n.

Lemma 4.3.5. *Two elements of S_n are conjugates if and only if they have the same cycle type.*

Proof. By lemma 4.3.4, two conjugate permutations have the same cycle type. Now suppose that permutations $s_1, s_2 \in S_n$ have the same cycle tipe. Order s_1 and s_2 in cycles of non-decreasing lenght (including 1-cycles). Then s_1 and s_2 is just a list of integers from 1 to n appearing exactly once. Label s_1 and s_2 as:

$$s_1 = s_{11}\ s_{12}\ \dots\ s_{1n}$$
$$s_1 = s_{21}\ s_{22}\ \dots\ s_{2m}$$

Define now, the map $t : s_{1i} \to s_{2i}$ sending the i-th entry of s_1 to the i-th entry of s_2. Then $t \in S_n$ is a permutation and moreover, $ts_1t^{-1} = s_2$. ■

Corollary. *The number of conjugacy classes of S_n is the number of partitions of n.*

Example 4.8.

(1) Letg $s_1 = (1)(3\ 5)(8\ 9)(2\ 4\ 7\ 6)$ and $s_2 = (3)(4\ 7)(8\ 1)(5\ 2\ 6\ 9)$. Define $t : 1 \to 3 \to 4, 5 \to 7, 8 \to 8$. Then
$$t = (1\ 3\ 4\ 2\ 5\ 7\ 6\ 9)(8)$$
and $ts_1t^{-1} = s_2$.

Lemma 4.3.6. *Normal subgroups of a group are unions of conjugacy classes of the group.*

Theorem 4.3.7. *The alternating group A_5 of order 60 is simple.*

Proof. The representatives of the cycle types of even permutations are given by

$$(1) \qquad (1\ 2\ 3) \qquad (1\ 2\ 3\ 4\ 5) \qquad (1\ 2)(3\ 4)$$

We notice that there are 20 3-cycles in S_5, so that all 20 3-cycles in A_5 are conjugate. Now, notice that there are 24 5-cycles in A_5, with only 12 of them conjugates of the cycle $(1\ 2\ 3\ 4\ 5)$. So there is a 5-cycle, s, not conjugate to $(1\ 2\ 3\ 4\ 5)$ in A_5. Now, s also has 12 distinct conjugates so that the 5-cycles of A_5 lie in two conjugacy classes of A_5, each with size 12.

Now the remaining 15 nonidentity elements of A_5 must have order 2, which gives us the cycle type $(2,2)$. Then notice that the cycle decomposition $(1\ 2)(3\ 4)$ has 15 distinct conjugates, all of which are the 15 elements of order 2.

We then get that the conjugacy classes of A_5 are of the following orders:

$$1 \qquad 12 \qquad 12 \qquad 15 \qquad 20$$

Suppose now, that $H \trianglelefteq A_5$, then by lemma 4.3.6, H is the union of conjugacy classes of A_5. Then $\operatorname{ord} H | 60$ and $\operatorname{ord} H$ is the sum of elements of subsets of the multiset $\{1, 12, 12, 15, 20\}$. Therefore the only options are that $\operatorname{ord} H = 60$ or $\operatorname{ord} H = 1$; that is, $H = A_5$ or $H = \langle (1) \rangle$. ■

4.4 Automorphisms.

Definition. Let G be a group. An **automorphism** of G is an isomorphism from G onto itself. We denote the set of all automorphisms of G as $\operatorname{Aut} G$ and call it the **automorphism group** of G.

Lemma 4.4.1. *Let G be a group, then $\operatorname{Aut} G$ is a group.*

Proof. Let $s, t \in \operatorname{Aut} G$. Notice then that $s, t \in A(G)$. ■

Lemma 4.4.2. *Let G be a group and let $H \trianglelefteq G$ be a normal subgroup of G. Then G acts via conjugation on H as automorphisms. More preciesly, the map $H \to H$ given by $h \to ghg^{-1}$ is an automorphsim of H.*

Proof. We have tha the map $H \to H$ given by $h \to ghg^{-1}$, for some $g \in G$ is onto since $H \trianglelefteq G$. Moreover, we have that $ghg^{-1} = gh'g^{-1}$ implies $h = h'$, by cancellation; so that this map is 1–1 as well. Lastly, notice that $ghh'g^{-1} = (ghg^{-1})(gh'g^{-1})$ which makes it an automorphism of H. ■

Corollary. *The permutation representation of this action is a homomorphism of $G \to \operatorname{Aut} H$ with kernel $C(H)$. In particular, we have that ${}^{G}\!/_{C(H)}$ is isomorphic to some subgroup of $\operatorname{Aut} H$.*

Proof. Define the permutation representation $\psi : G \to \operatorname{Aut} H$ given by $g \to \phi_g$, where $\phi_g : H \to H$ is the automorphism given by $\phi_g : h \to ghg^{-1}$. Then ψ is a homomorphism, as $\psi'_g \psi_g = \psi_{g'g}$. Moreover, we have $\ker \psi = \{g \in G : \phi_g(h) = h\} = \{g \in G : ghg^{-1} = h\} = C(H)$. Lastly, by the first isomorphism theorem, we have the following diagram

$$\begin{tikzcd}
G \arrow[r, "\psi"] \arrow[dr] & {}^{G}\!/_{C(H)} \arrow[d, "\phi"] \\
& \phi(H)
\end{tikzcd}$$

which gives us the isomorphism. ■

Corollary. *If K is a subgroup of G, then $K \simeq gKg^{-1}$ for any $g \in G$.*

Corollary. *For any subgroup H of G, we have ${}^{N(H)}\!/\!{}_{C(H)}$ is isomorphic to a subgroup of* $\operatorname{Aut} H$*, in particular, ${}^{G}\!/\!{}_{Z(G)}$ is isomorphic to a subgroup of* $\operatorname{Aut} G$*.*

Proof. Notice that $H \trianglelefteq N(H)$, so that by above ${}^{N(H)}\!/\!{}_{C(H)}$ is isomoprphic to a subgroup of $\operatorname{Aut} H$. Now take $H = G$, then $N(G) = G$ and $C(G) = Z(G)$. ■

Definition. Let G be a group. We call conjugation by some $g \in G$ an **inner autormorphism** of G. We denote the set of all inner automorphisms of G by $\operatorname{Inn} G$.

Lemma 4.4.3. *For any group G,* $\operatorname{Inn} G \leq \operatorname{Aut} G$*.*

Corollary. $\operatorname{Inn} G \simeq {}^{G}\!/\!{}_{Z(G)}$.

Example 4.9. (1) A group G is Abelian if, and only if every inner automorphism of G is trivial. Let $H \trianglelefteq G$ be Abelian, such that $H \not\subseteq Z(G)$. Then there exists a $g \in G$ such that conjugation by g, restricted to h (i.e. taking $\phi|_H$ where $\phi : x \to gxg^{-1}$, $x \in G$) is not an inner automorphsim of H.

(2) Using above, consder the alternating group A_4, and consider the Klein 4-group V_4 as a subgroup of A_4 (writing the elements of V_4 as even permutations). Now, let g be any 3-cycle of A_4, then conjugation by g restricted to V_4 is not an inner automorphism.

(3) $Z(\mathbb{H}) = \langle -1 \rangle$, so $\operatorname{Inn} \mathbb{H} \simeq V_4 \simeq {}^{\mathbb{Z}}\!/\!{}_{2\mathbb{Z}} \times {}^{\mathbb{Z}}\!/\!{}_{2\mathbb{Z}}$.

(4) $Z(D_8) = \langle r^2 \rangle$ so that $\operatorname{Inn} D_8 \simeq V_4 \simeq {}^{\mathbb{Z}}\!/\!{}_{2\mathbb{Z}} \times {}^{\mathbb{Z}}\!/\!{}_{2\mathbb{Z}}$.

(5) For $n \geq 3$, $Z(S_n) = \langle (1) \rangle$, so that $\operatorname{Inn} S_n \simeq S_n$.

(6) If $H \simeq {}^{\mathbb{Z}}\!/\!{}_{2\mathbb{Z}}$, since H has elements of order 1 and 2, we get $\operatorname{Aut} H = \langle e \rangle$. Then by hypothesis, $N(H) = C(H)$. Moreover if $H \trianglelefteq G$, then $H \leq Z(G)$.

Definition. We call a subgroup H of a group G **characteristic** in G if every automorphism of G restricted to H is onto. That is $s(H) = H$ for every $s \in \operatorname{Aut} G$. We write $H \operatorname{char} G$

Lemma 4.4.4. *The following are true for any group G and $H \leq G$.*

(1) If $H \operatorname{char} G$, then $H \trianglelefteq G$.

(2) If H is the unique subgroup of a given order in G, then H is characteristic in G.

(3) If $K \leq H \trianglelefteq G$ such that $K \operatorname{char} H$, then $K \trianglelefteq G$.

Proof. (1) Let $H \operatorname{char} G$. Then for every $s \in \operatorname{Aut} G$, $s(H) = H$. In particular, choose $s : G \to G$ taking $x \to gxg^{-1}$. Then $gHg^{-1} = H$.

(2) Let H be the unique subgroup of order n in G. Since automorphsims of G preserve the order of subgroups, we have $\operatorname{ord} s(H) = \operatorname{ord} H = n$, moreover since s is 1–1 and onto, we get $s(H) = H$, for any $s \in \operatorname{Aut} G$. Therefore $H \operatorname{char} G$.

(3) Lastly, let $K \operatorname{char} H$ where $K \leq H \trianglelefteq G$. By statement (1), we have our result.

■

Theorem 4.4.5. *The automorphism group of a cyclic group of order n is isomorphic to the unit group $U(\mathbb{Z}/n\mathbb{Z})$.*

Proof. Let Z_n be a cyclic group of order n, such that $Z_n = \langle x \rangle$. Let $\psi \in \operatorname{Aut} Z_n$, then $\psi : x \to x^a$ for some $a \in \mathbb{Z}/n\mathbb{Z}$, since $\operatorname{ord} x = n$. Now we have that since ψ is an automorphism, it is uniquely determinde by a. Let ψ_a be such an automorphism. We also get that $\psi_a : x \to x^a$ preserves order so that $\operatorname{ord} x = \operatorname{ord} x^a = n$ and by lemma 2.3.6, $(a, n) = 1$. Therefore we have a map $\Psi : \operatorname{Aut} Z_n \to U(\mathbb{Z}/n\mathbb{Z})$ taking $\psi_a \to a$. We have that this map is 1–1 by above, and moreover it is onto. Lastly, notice that $\psi_a\psi_b(x) = \psi_a(x^b) = x^{ab} = \psi_{ab}(x)$ so Ψ is a homomorphism. Therefore we have an isomorphism of $\operatorname{Aut} Z_n$ onto $U(\mathbb{Z}/n\mathbb{Z})$. ■

Example 4.10. Let G be a group of order pq, where $p, q \in \mathbb{Z}^+$ are primes such that $p \leq q$. Suppose that $p \not| q - 1$. If $Z(G) \neq \langle e \rangle$, then $G/Z(G)$ is cyclic Lagrange's theorem, which makes G cyclic.

Now suppose that $Z(G) = \langle e \rangle$. Then if every nonidentity element of G has order p, by the class equation, we have that $pq = 1 + kq$ for some $k \in \mathbb{Z}^+$. Now, $q|pq$ and $q|kq$, but $q \not| 1$; so there must be an element of G of order q. Let x be such element and let $H = \langle x \rangle$. Then $[G : H] = p$ which is the smallest prime dividing $\operatorname{ord} G$. By lemma 4.2.2, we get that $H \trianglelefteq G$. This makes $C(H) = H$ so that $G/H \simeq N(H)/H$ is a group of order p, isomorphic to a subgroup of $\operatorname{Aut} H$, by the corllary to lemma 4.4.2. Now, by theorem 4.4.5, we get that $\operatorname{ord}(\operatorname{Aut} H) = \phi(q) = q - 1$, where *phi* is Euler's Totient function. This makes $p|q-1$ which cannot happen. Therefore $Z(G)$ is nontrivial and G must be Abelian.

Theorem 4.4.6. *The following are true:*

(1) If $p > 2$ is prime and $n \in \mathbb{Z}^+$, then the automorphism group of a cyclic group is order $\phi(p) = p - 1$ where ϕ is Euler's Totient function.

(2) For all $n \geq 3$, the automorphism group of a cyclic group of order 2^n is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z}$. Moreover, it has a cyclic subgroup of index 2.

(3) If $p \in \mathbb{Z}^+$ is prime and V is an Abelian group such that $v^p = 0$ for all $v \in V$. If $\operatorname{ord} V = p^n$, then V is an n-dimensional vector space over the field $\mathbb{F}_p$. Moreover the automorphisms of V are nonsingular linear transformations from V onto itself and $\operatorname{Aut} V \simeq GL(n, \mathbb{F}_p)$.

(4) For all $n \neq 6$, $\operatorname{Aut} S_n = \operatorname{Inn} S_n \simeq S_n$. If $n = 6$, then $[\operatorname{Aut} S_6 : \operatorname{Inn} S_6] = 2$

(5) Notice that $D_8 \trianglelefteq D_{16}$. Then $\operatorname{Inn} D_{16} \simeq \operatorname{Aut} D_8$ and notice that $Z(D_{16}) = \langle r^4 \rangle$. So $\operatorname{Aut} D_8 \simeq D_{16}/\langle r^4 \rangle \simeq D_8$. Therefore $\operatorname{ord}(\operatorname{Aut} D_8) = 8$.

(6) *Notice that* $V_4 \operatorname{char} D_8$ *and that* $D_8 \operatorname{char} S_4$*, so we get that* $V_4 \operatorname{char} S_4$

(7) *Notice that* $\langle r \rangle$ *is the unique subgroup of order* n *of* D_{2n}*, and so* $\langle r \rangle \operatorname{char} D_{2n}$*.*

Example 4.11. Suppose that G is a group of order $45 = 3^2 5$ with a normal subgroup P of order 3^2. We get that ${}^{G}\!/\!_{C(P)} \simeq P'$, where $P' \leq \operatorname{Aut} P$, and $\operatorname{ord}(\operatorname{Aut} P) = 6$ or $\operatorname{ord}(\operatorname{Aut} P) = 48$. Since P has order the square of a prime, P must be Abelian so taht $P \leq C(P)$. Then $\operatorname{ord} C(P)$ is divisible by 9 so that $\operatorname{ord} {}^{G}\!/\!_{C(P)} = 1$ or $\operatorname{ord} {}^{G}\!/\!_{C(P)} = 5$. We then get that it must be the former, so that $C(P) = G$ and $P \leq Z(G)$. Since ${}^{G}\!/\!_{Z(G)}$ is cyclic, G must be Abelian.

Lemma 4.4.7. *For any group* G*,* $\operatorname{Inn} G \trianglelefteq \operatorname{Aut} G$*.*

Proof. We have that $\operatorname{Inn} G \leq \operatorname{Aut} G$. Now, let $s \in \operatorname{Aut} G$, and consider the map $\phi_g : x \to gxg^{-1}$ of conjugation by some $g \in G$. Then we have $s\phi_g s^{-1}(x) = s(\phi_g(s^{-1}(x))) = s(gs^{-1}(x)g^{-1}) = s(g)xs^{-1}(g)$ So that $s(\operatorname{Inn} G)s^{-1} \subseteq \operatorname{Inn} G$. ∎

Definition. Let G be a group. We call the factor group ${}^{\operatorname{Aut} G}\!/\!_{\operatorname{Inn} G}$ the **outer automorphism group** of G.

Lemma 4.4.8. *Let* G *be Abelian of order* pq*, where* $p, q \in \mathbb{Z}^+$ *are distinct primes. Then* G *is cyclic.*

Proof. By Cauchy's theorem, we have that $p|pq$ and $q|pq$, so there exist elements $x, y \in G$ such that $\operatorname{ord} x = p$ and $\operatorname{ord} y = q$. Then we have that $((xy)^p)^q = (xy)^{pq} = (x^p)^q(y^q)^p = e$ so that $\operatorname{ord} xy = pq$ (since p and q are prime, pq is the smalles such integer for which $(xy)^{pq} = e$). Then we have that $\operatorname{ord} G = \operatorname{ord} xy$. Therefore G ∎

4.5 Sylow's Theorems

Definition. Let G be a group and p a prime. A p**-subgroup** of G is a subgroup of G of order p^r for some $r \in \mathbb{Z}^+$. If $\operatorname{ord} G = p^r$, we call G a p**-group**.

Definition. If G is a group of order $p^r m$, where p is prime, and $p \not| m$ for $m, r \in \mathbb{Z}^+$, then we call a subgroup of G a **Sylow** p**-subgroup** (or p**-Sylow**) of G if it has order p^r. We denote the set of all Sylow p-subgroups of G by $\operatorname{Syl}(p, G)$. We denote $n_p(G) = |\operatorname{Syl}(p, G)|$ to be the number of Sylow p-subgroups of G.

Lemma 4.5.1. *Let* $P \in \operatorname{Syl}(p, G)$ *be a* p*-Sylow of a group* G*. If* Q *is a* p*-group of* G*, then* $Q \cap N(P) = Q \cap P$*.*

Proof. Let $H = Q \cap N(P)$, since $P \leq N(P)$, we have $Q \cap P \leq H$. Now, by definition, $H \leq Q$. Since $H \leq N(P)$, PH is a group, and $PH \leq G$. Then we have

$$\operatorname{ord} PH = \frac{\operatorname{ord} P \operatorname{ord} H}{|P \cap H|} = \frac{p^r p^l}{p^m} = p^\alpha$$

for some $r, l, m, \alpha \in \mathbb{Z}^+$. So PH is a p-subgroup of G. Then $p^r|p^\alpha$ and $p^r|\operatorname{ord} G$ so p^r is the largest prime power dividing $\operatorname{ord} G$. This makes $m = l$ and $r = \alpha$ hence $\operatorname{ord} PH = p^r$. So $P = PH$ making $H \leq P$. Therefore $H = Q \cap P$. ∎

Theorem 4.5.2 (Sylow's Theorems). *Let G be a group of order $p^r m$, where p is a prime and $p \nmid m$ for $m, r \in \mathbb{Z}^+$. Then the following statements are true.*

(1) There exist Sylow p-subgroups of G; i.e. $\mathrm{Syl}\,(p, G) \neq \emptyset$.

(2) If Q is a p-subgroup of G, and P is a Sylow p-subgroup in G, then there exists a $g \in G$ such that $Q \leq gPg^{-1}$. In particular, any two Sylow p-subgroups are conjugate in G.

(3) $n_p(G) \equiv 1 \mod p$.

Proof. By induction on $\mathrm{ord}\, G$, if $\mathrm{ord}\, G = 1 = p^0 \cdot 1$, then we are done. Now, suppose that there exist p-Sylows for any group of order less than $p^r m$. Now, if $p | \mathrm{ord}\, Z(G)$, then by Cauchy's theorem $Z(G)$ has an element of order p which generates a cyclic subgroup N of order p in $Z(G)$. Consider then the factor set G/N. Then $|G/N| p^{r-1} m$ and by hypothesis, G/N has a p-Sylow subgroup of order p^{r-1}. If P is the subgroup of G containing N for which P/N exists, then $\mathrm{ord}\, P = |P/N| \,\mathrm{ord}\, N = p^r$ making P a p-Sylow in G.

Now, suppose that $p \nmid \mathrm{ord}\, Z(G)$, and let $g_1, \ldots, g_l$ be the representatives of distinct noncentral conjugacy classes of G. Then by the class equation:

$$\mathrm{ord}\, G = \mathrm{ord}\, Z(G) + \sum_{i=1}^{l} [G : C(g_i)]$$

Now, if $p | \sum [G : C(g_i)]$, since $p | \mathrm{ord}\, G$ we must also have $p | \mathrm{ord}\, Z(G)$, which cannot happen by assumption; therefore $p \nmid \sum [G : C(g_i)]$. There is then some $1 \leq i \leq l$ for which $p \nmid [G : C(g_i)]$, so that $\mathrm{ord}\, C(g_i) = p^r k$ for some $k \in \mathbb{Z}^+$, where pk. Since $g_i \notin Z(G)$ for all i, and $\mathrm{ord}\, C(g_i) < \mathrm{ord}\, G$, by hypothesis $C(g_i)$ has a p-Sylow, P, making P a p-Sylow of G. Therefore $\mathrm{Syl}\,(p, G) \neq \emptyset$.

Now, let P be a Sylow p-subgroup of G and let $0 = \{P_1, \ldots, P_s\}$ such that $P_i = gPg^{-1}$ for some $g \in G$. That is, S is the set of all conjugates of P. Let Q be any p-subgroup of G, then Q acts on S via conjugation, that

$$S = \bigcup_{i=1}^{s} \mathcal{O}(P_i)$$

Where $\mathcal{O}(P_i)$ is the orbit of P_i under the action of Q. Then we have

$$r = \sum_{i=1}^{s} |\mathcal{O}(P_i)|$$

Then by the corollary to lemma 4.1.4, $|\mathcal{O}(P_i)| = [G : N_Q(P_i)]$ where $N_Q(P_i)$ is the normalizer of P_i in Q. Then $N_Q(P_i) = Q \cap N(P_i) = Q \cap P_i$ by lemma 4.5.1; and we get $|\mathcal{O}(P_i)| = [G : P_i \cap Q]$ for all $1 \leq i \leq s$.

Now take $Q = P_1 = gPg^{-1}$ for some $g \in G$. Then $|\mathcal{O}(P_1)| = 1$, now for all $i > 1$, we have $P_1 \neq P_i$ so $[P_1 : P_1 \cap P_i] = p^l$ for $l \in \mathbb{Z}^+$. That is, $p||\mathcal{O}(P_i)|$ Therefore

$$r = |\mathcal{O}(P_1)| + \sum_{i=2}^{s} |\mathcal{O}(P_i)| = 1 + kp \equiv 1 \mod p$$

Now, let Q be any p-subgroup of G not contained in P_i for all $1 \leq i \leq s$. Then $Q \not\leq gPg^{-1}$ for all $g \in G$. THen $Q \cap P_i \leq Q$ so that $|\mathcal{O}(P_i)| = [Q : Q \cap P_i] = 1$, which makes $p|\mathcal{O}(P_i)|$ for all i which makes $p|r$. But $r \equiv 1 \mod p$, a contradiction. Therefore we must have that $Q \leq gPg^{-1}$ for some $g \in G$. Now if Q is any p-Sylow of G, then Q is a p-subgroup of G. So that $Q \leq gPg^{-1}$ for some other p-Sylow P. Now since $\operatorname{ord} Q = \operatorname{ord} gPg^{-1} = p^r$, we get that $Q = gPg^{-1}$ making p-Sylows conjugates of eachother. Moreover, we get that $S = \operatorname{Syl}(p, G)$ so that $n_p(G) = r \equiv 1 \mod p$. ∎

Corollary. *f P is p-Sylow in G, then $[G : N(P)] = n_p(G)$ and $n_p(G)|m$.*

Proof. By lemma 4.3.1 $n_p = |\operatorname{Syl}(p, G)| = [G : N(P)]$ for all $P \in \operatorname{Syl}(p, G)$. ∎

Corollary. *The following are equivalent for any group G.*

(1) P is the unique Sylow p-subgroup of G and $n_p(G) = 1$.

(2) $P \trianglelefteq G$.

(3) $P \operatorname{char} G$

(4) All subgroups generated by elements of order a power of p are p-subgroups. That is, if $X \subseteq G$ such that $\operatorname{ord} x = p^l$ for all $x, \in X$, $l \in \mathbb{Z}^+$, then $\langle X \rangle$ is a p-subgroup of G.

Proof. Suppose that $\operatorname{Syl}(p, G) = \{P\}$ and $n_p(G) = 1$, then $gPg^{-1} = P$, for all $g \in G$ making $P \trianglelefteq G$. COnversly, if $P \trianglelefteq G$, and $Q \in \operatorname{Syl}(p, G)$ then there exists a $g \in G$ such that $Q = gPg^{-1} = P$, making $Q = P$ the unique p-Sylow of G.

Now, if $P \operatorname{char} G$, then $P \trianglelefteq G$. On the other hand, suppose that $P \trianglelefteq G$. Then P is the unique group of order p^r in G, for some $r \in \mathbb{Z}^+$, so that $P \operatorname{char} G$.

Now, suppose that $\operatorname{Syl}(p, G) = \{P\}$ and $n_p(G) = 1$. Let $X \subseteq G$ such that $\operatorname{ord} x = p^l$ for some $l \in \mathbb{Z}^+$. By conjugation, for all $x \in X$, there exists a $g \in G$ such that $x \in gPg^{-1} = P$, so that $X \subseteq P$. Necessarily we then get $\langle X \rangle \leq P$, making $\langle X \rangle$ a p-subgroup. Conversely if $\langle X \rangle$ is a p-subgroup of G, let $X = \bigcup P$ where $P \in \operatorname{Syl}(p, G)$. Then any P is a subgroup of $\langle X \rangle$, and since P is also a p-subgroup of G, of maximum order p^r, then $P = \langle X \rangle$ making $\operatorname{Syl}(p, G) = \{P\}$ and hence $n_p(G) = 1$. ∎

Remark. We call theorem 4.5.2 **Sylow's theorems** and refer to items (1), (2), and (3) of this theorem as Sylow's **first**, **second**, and **third** theorems, respectively.

Example 4.12. Let G a finite group of order n, and p a prime.

(1) If $p \nmid n$, then the Sylow p-subgroup of G is trivial. Otherwise, if $n = p^r$ for some $r \in \mathbb{Z}^+$, then G is the unique Sylow p-subgroup of itself, by maximality.

(2) If G is Abelian, then it has a unique Sylow p-subgroup for each prime p. We call these Sylow p-subgroups **p-primary components** of G.

(3) S_3 has three 2-Sylows, $\langle(1\ 2)\rangle$, $\langle(2\ 3)\rangle$, and $\langle(1\ 3)\rangle$. There is also a unique 3-Sylow, $\langle(1\ 2\ 3)\rangle \simeq A_3$. Notice that $3 \equiv 1 \mod 2$.

(4) A_4 has a unique 2-Sylow, $\langle(1\ 2)(3\ 4),(1\ 3)(2\ 4)\rangle \simeq V_4$. It has four 3-Sylows, $\langle(1\ 2\ 3)\rangle$, $\langle(1\ 2\ 4)\rangle$, $\langle(1\ 3\ 4)\rangle$, and $\langle(2\ 3\ 4)\rangle$. Notice that $4 \equiv 1 \mod 3$.

(5) S_4 has $n_2 = 3$, and $n_3 = 4$. Since S_4 containes a subgroup isomorphic to D_8, then every 2-Sylow of S_4 is isomorphic to D_8.

4.6 Applications of Sylow's Theorems

We go over some specific examples which utilize Sylow's theorems.

Example 4.13 (Groups of order pq, where $p < q$)**.** Let G be a group of order $\operatorname{ord} G = pq$, where $p < q$, for p, q primes. Let $P \in \operatorname{Syl}(p, G)$ and let $Q \in \operatorname{Syl}(q, G)$. Since $n_q(G) \equiv 1 \mod q$, $n_q(G) = 1 + kq$ for some $K \in \mathbb{Z}^+$. Now, $n_q(G)|p$, and since $p < q$ we get $k = 0$ so that $n_q(G) = 1$. This makes $Q \trianglelefteq G$ by the corollory to Sylow's theorems.

Now, we also have that $n_p(G)|q$, so $n_{p(}G) = 1$ or $n_{p(}G) = q$. Now if $p \not| q-1$, then $n_p(G) = 1$ making PG. Letting $P = \langle x\rangle$ and $Q = \langle y\rangle$. If $P \trianglelefteq G$, then ${}^{G}\!/_{C(P)}$ is isomorphic to a subgroup of $\operatorname{Aut} {}^{\mathbb{Z}}\!/_{p\mathbb{Z}}$ of order $p-1$. By Cayley's theorem. Now, by Lagrange's theorem, and since $p, q \not| p-1$ we must have $G = C(P)$; so that $x \in P \leq Z(G)$. Therefore x and y commute and $\operatorname{ord} xy = pq$, which makes $G \simeq {}^{\mathbb{Z}}\!/_{p\mathbb{Z}}$.

Now, if $p|q-1$, then letting $\operatorname{ord} N(Q) = q(q-1)$ and by Cauchy's theorem, $N(Q)$ has a sbgroup of order p. This makes $PQ \leq G$, and since $C(Q) = Q$, PQ is abelian. Since $\operatorname{Aut} {}^{\mathbb{Z}}\!/_{p\mathbb{Z}}$ is cyclic, this makes PQ unique.

Example 4.14 (Groups of order 30)**.** Let G be a group of order $\operatorname{ord} G = 30 = 5 \cdot 3 \cdot 2$. Let $P \in \operatorname{Syl}(5, G)$ a 5-Sylow, and let $Q \in \operatorname{Syl}(3, Q)$ a 3-Sylow. If $P \trianglelefteq G$ or $Q \trianglelefteq G$, then $\operatorname{ord} PQ = 5 \cdot 3 = 15$; moreover, $P \operatorname{char} PQ$ and $Q \operatorname{char} PQ$, making $P \trianglelefteq G$ and $Q \trianglelefteq G$.

Now suppose that neither P nor Q are normal in G. Since $n_5(G) \equiv 1 \mod 5$, $n_3(G) \equiv 1 \mod 3$ and $n_5(G)|6 = 3\cdot 2$ and $n_3(G)|10 = 5\cdot 2$, we must have that $n_5(G) = 6$ and $n_3(G) = 10$. Now, each element of order 5 lies in a 5-Sylow, so by Lagrange's theorem, distinct 5-Sylows intersect at $\langle e\rangle$. Therefore G has $4 \cdot 6 = 24$ elements of order 5. Similarly G has $2 \cdot 10 = 20$ element of order 3. This makes $\operatorname{ord} G \geq 20 + 24 = 44 > 30$, which is a contradiction. Hence either P, or Q must be normal in G. This also implies that P is the unique Sylow p-subgroup of G.

Example 4.15 (Groups of order 12)**.** Let G be a group of order $\operatorname{ord} G = 12 = 2^2\cdot 3$. Suppose that $n_3 \neq 1$, and let $P \in \operatorname{Syl}(3, G)$. Then $n_3|4 = 2^2$ and since $n \equiv 1 \mod 3$, we get $n_3 = 4$. Now, by Lagrange's theorem, distinct 3-Sylows intersect at $\langle e\rangle$, so that G has $2 \cdot 4 = 8$ elements of order 3. Moreover, $[G : N(P)] = n_3 = 4$ so that $N(P) = P$. Consider then the permutation representation $\phi : G \to S_4$ of conjugation by G on $\operatorname{Syl}(3, p)$. Then $\ker\phi \leq P$, and since $P \not\trianglelefteq G$, $\ker\phi = \langle e\rangle$. So ϕ is 1–1 making G isomorphic to a subgroup of S_4, by Cayley's theorem. So $G \simeq \phi(G) \leq S_4$. Now, since there are precisely 8 elements of order 3 in S_4, $\phi(G) \cap A_4$ is a subgroup of at least order 8. Since $\operatorname{ord} G = \operatorname{ord} A_4 = 12$, we get $G \simeq A_4$.

Example 4.16 (Groups of order p^2q, where p, and q are distinct)**.** Let G be a group of order p^2q, where $p \neq q$, for primes p and q. Let $P \in \operatorname{Syl}(p,G)$ and $Q \in \operatorname{Syl}(q,G)$. Suppose that $p > q$, then $n_p(G)|q$ and $n_p(G) \equiv 1 \mod p$ force $n_p(G) = 1$. This makes $P \trianglelefteq G$ and hence P is the unique Sylow p-subgroup of G.

Now, i $p < q$, if $n_q(G) = 1$, we are done, so suppose that $n_q(G) \neq 1$. Since $n_q(G)|p^2$ $n_q(G) = p$ or $n_q(G) = p^2$. Since $n_q(G) \equiv 1 \mod q$, we must have $n_q(G) = p^2$. Moreover notice that $n_q(G) = 1 + tq$ for some $t \in \mathbb{Z}^+$. So we have

$$tq = p^2 - 1 = (p-1)(p+1)$$

So $q|p-1$ or $q|p+1$. But since $q > p$, we must have $q|p+1$. This forces $p = 2$ and $q = 3$ so that $\operatorname{ord} G = 12$, making $Q \trianglelefteq G$.

We now characterize groups of order 60.

Theorem 4.6.1. *Let G be a group of order $60 = 2^2 \cdot 5 \cdot 3$. If G has more than one Sylow 5-subgroup, then G is a simple group.*

Proof. Suppose that $n_5 = n_5(G) > 1$, but that G is not simple. Then G has at least one nontrivial normal subgroup N. now, since $n_5 \equiv 1 \mod 5$, and $n_5|12 = 2^2 \cdot 3$, then $n_5 = 6$. Choose then a Sylow 5-subgrop $P \in \operatorname{Syl}(5,G)$ for which $\operatorname{ord} N(P) = 10$, so that $[G : N(P)] = n_5 = 6$.

Suppose then that $n_5 | \operatorname{ord} N$, then by Cauchy's theorem, N has a 5-Sylow, Q and since $N \trianglelefteq G$, $gQg^{-1} \leq N$ for all $g \in G$. The number of conjugates of Q is n_5, so we have $\operatorname{ord} N \geq 1 + 6 \cdot 4 = 25$. By Lagrange's theorem, $\operatorname{ord} N = 30$, but every group of order 30 has a unique 5-Sylow, making $n_5 = 1$, a contradiction. Hence $n_5 \nmid \operatorname{ord} N$. Now, if $\operatorname{ord} N = 6$ or $\operatorname{ord} N = 12$, then N has a normal Sylow subgroup H in G. let $\operatorname{ord} H = 2$, or $\operatorname{ord} H = 3$, or $\operatorname{ord} H = 4$ then $\operatorname{ord} G/H = 30$, $\operatorname{ord} G/H = 20$, or $\operatorname{ord} G/H = 15$. In each case G/H has a normal 5-subgroup H'. Let H' be the complete preimage of H' in G, then $H' \trianglelefteq G$ is nontrivial and $5 | \operatorname{ord} H$, which contradicts the above assumption. ■

Corollary. *The alternating group of degree 5, A_5 is simple.*

Proof. Notice that $\operatorname{ord} A_5 = \frac{\operatorname{ord} S_5}{2} = \frac{120}{2} = 60$ and that $\langle (1\ 2\ 3\ 4\ 5) \rangle$ and $\langle (1\ 3\ 2\ 4\ 5) \rangle$ are Sylow 5-subgroups. ■

Theorem 4.6.2. *If G is a simple group of order 60, then $G \simeq A_5$.*

Proof. Let G be a simple group of order $60 = 2^2 \cdot 5 \cdot 3$. Then $n_2 = 3, 5$, or 15. Let $P \in \operatorname{Syl}(2,G)$, so that $[G : N(P)] = n_2$. If H were a subgroup of index 3, 4, or 2, then G has a normal subgroup K in H, with $H/K \simeq S_4, S_3$, or S_2. Since $K \neq G$, and G is simple, we must have $K = \langle e \rangle$. But $60 \nmid 4! = 12$, so $n_2 \neq 3$.

Now suppose that $n_2 = 5$ and consider the permutation representation of left multiplication of G on G/N, from $G \to S_5$. Since $\ker \trianglelefteq G$, and $\ker \neq G$, we must have $\ker = \langle e \rangle$, making the permutation representation from $G \to S_5$ 1–1. By Cayley's theorem, G is isomorphic to a subgroup of S_5. Now, without loss of generality, let G_5. If $G \not\leq A_5$, then $S_5 = GA_5$. By the second isomorphism theorem, we get $[G : G \cap A_5] = 2$, a contradiction since G has no normal subgroup of index 5. SO $G \leq A_5$. Since $\operatorname{ord} G = \operatorname{ord} A_5 = 60$, we then get that $G = A_5$.

Lastly, if $n_2 = 15$, and $P, Q \in \operatorname{Syl}(2, G)$, with $P \cap Q = \langle e \rangle$, then G has $3 \cdot 15 = 45$ elements of order 5 So $\operatorname{ord} G \geq 24 + 45 = 69 > 60$ which is a contradiction. So we must have that $|P \cap Q| = 2$. Let $M = N(P \cap Q)$, since $\operatorname{ord} P = \operatorname{ord} Q = 4$, we have tht P and Q are Abelian, and $P, Q \leq M$. Since G is simple, $M \neq G$. So $4 | \operatorname{ord} M$ so $\operatorname{ord} M = 5$ making $[G : M] = 5$. By above we get that $G \simeq A_5$. But $n_2(A_5) = 5$, a contradiction so $n_2 \neq 15$. ■

Bibliography

[1] D. Dummit, *Abstract algebra.* Hoboken, NJ: John Wiley & Sons, Inc, 2004.

[2] I. N. Herstein, *Topics in algebra.* New York: Wiley, 1975.