Group Theory.

Alec Zabel-Mena

February 26, 2022

Contents

Chapter 1

Groups.

1.1 Motiviations of Groups.

The notion of a "group" is perhaps the most fundamental notion in all of abstract algebra (without going into more granular structures which tend to be reserved for more advanced settings). It forms the building blocks for the study of the "ring" and "field" structures prevalent in algebra, and it even forms its (rightfully) interesting field of study.

THere are a number of motivations and examples for group theory and its study. Historically, the definition of a group finds itself motivated by the study of algebraic equations; specifically polnyomial equations of the form $ax^2 + bx + c = 0$, $ax^3 + bx^2 + cx + d = 0$, and more generally, $a_n x^n + \cdots + a_1 x + a_0 = 0$. That is the so called quadratic, cubic, and other polynomial equations. Specifically, the solutions of such equations were of interest, and finding a general form for them proved invaluble. It is know that the quadratic, $ax^2 + bx + c = 0$ has the general solution:

$$x = -\frac{b}{2a} \pm \frac{\sqrt{b^2 - 4ac}}{2a} \tag{1.1}$$

dubbed the "quadratic" formula. The general solution for the cubic equation is far more convoluted. What about the solution for polynomial equations of higher degree? It was shown that the quintic equation (of degree 5) and higher has no general form for their solutions.

The study of these polynomial equations and their geenral solutions led mathematicians such as Neils Abel and Evariste Galois to develop the fondations for algebra. In particular, Galois, on the eve of his duel composed a manuscript concerning these equations which would form the foundations for group theory in which others would build upon.

There are other applications and motivations for group theory asides from polynomials. IN number theory, one is concerned with the properites of positive integers, which form a "group" structure. For example, if the integer a^{40} has its last two digits 01 if it is not congruent 0 mod 2, nor 0 mod 5; i.e. it is not divisible by either 2 nor 5. Leonhard Euler proved this using group theoretic techniques developed by Joseph Louis Lagrange.

Group theory also plays an essential role in finding rational solutions (i.e. solutions in $\mathbb{Q}$), to certain algebraic equations called Diophantine equations; $y^2 = x^3 - x$ is an example. Solutuions to these equations can be found by intersecting straight lines with these

curves. The result is that if an arithmetic is defined on the points of thes curves using line intersections, the one can obtain a group sturcture. The most famous example of this is are elliptic curves, which have the form $y^2 = f(x)$ where f is a polynomial. These curves form a group structure and have an intimite connection to number theory. Pierre de Fermat was interested in Diophantine equations, especially the equation $x^n + y^n = z^n$; which was claimed not to have solutions for $n > 2$, and to which Fermat scribbled in a copy of Diophantus' book: "I have a marvelous proof to this theorem, but the margin is to small to contain it ". This problem became known as "Fermat's Last Theorem" and went unproved until Andrew Wiles proved it using Elliptic curves (its much more complicated than that, but the story of Fermat's last theorem rightfully deserves its own book).

The study of the arithmetic of Elliptic curve is an area of active research and has wide applications, specifally in the field of cryptography.

1.2 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 $\mathbb{Z}/n\mathbb{Z}$, 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 1.2.1. *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 1.2.2 (Generalized Associativity)**.** *Let G be a group under a binary operation $*$, then for any $a_1, a_2, \ldots, a_n \in G$, 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 $a_1, \ldots, a_k$ 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 1.2.3 (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 1.2.4. *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 1.2.5. *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 $a_1, \ldots, a_k \in G$, 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 $\operatorname{ord} a_1 a_2 \ldots a_k = [n_1, \ldots, n_k]$.*

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

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.

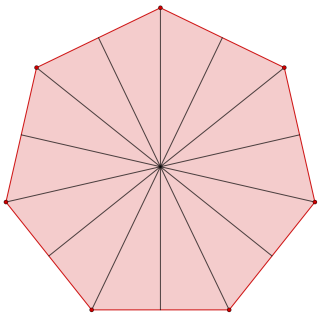

Figure 1.1: The group, D_{14} of symmetries on a heptagon.

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

1.3 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 1.3.1. *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 1.3.2. *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) $\mathbb{Z}/n\mathbb{Z} = \langle 1 \rangle$.

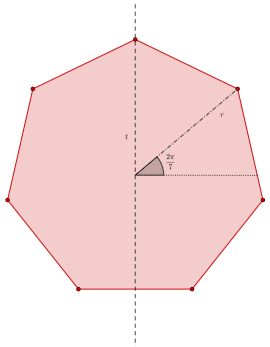

Figure 1.2: The transposition $t \in D_{14}$ of vertices of a heptagon and the rotation $r \in D_{14}$ about an angle of $\frac{2\pi}{7}$ of the vertices.

(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, $\operatorname{ord} Y = 1$.

1.4 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 permutiations from A onto itself. If $A = \mathbb{Z}/n\mathbb{Z}$ for $n \in \mathbb{Z}^+$, we write $S(A) = S_n$.

Theorem 1.4.1. *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 $\mathbb{Z}/n\mathbb{Z}$, $(a_0 \ \dots \ a_{n-1})$ 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 1.4.2. *The cycle decomposition of a given permutation $s \in S_n$ is finite.*

Proof. Let $s = (a_0 \ \dots \ a_{n-1})$ 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 1.4.3. *For any permutation $s \in S_n$, the elements of $\mathbb{Z}/n\mathbb{Z}$ can be grouped into k cycles of the form:*

$$(a_0 \ a_2 \ \dots \ a_{m_1})(a_{m_1+1} \ \dots \ a_{m_2}) \dots (a_{m_{k-1}} \ \dots \ a_{mk}) \tag{1.2}$$

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

$$s^{-1} = (a_{m_1}\dots\ a_2\ \ a_0)(a_{m_2}\ \dots\ a_{m_1+1})\dots(a_{mk}\ \dots\ a_{m_{k-1}}) \tag{1.3}$$

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 1.4.1 as:

Theorem 1.4.5. *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 1.4.6. *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 $k \in \mathbb{Z}/n\mathbb{Z}$.*

1.5 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 1.5.1. *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 1.5.2. *For $n, p \in \mathbb{Z}^+$ and p prime :*

$$\operatorname{ord} GL(n, p) = \prod_{j=1}^{n-1} (p^n - p^{n-j}) \tag{1.4}$$

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 1.5.3. *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 1.5.2, 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:

$$H(F) = \{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} : a, b, c \in F \} \tag{1.5}$$

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 1.5.4. *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.*

1.6 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 1.6.1. *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 bujection. 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 1.6.2. *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 1.6.3. *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 1.6.4. *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 $1 \le i \le n$, 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 1.6.5. *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 1.6.6. *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. ■

1.7 Group Actions.

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

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

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

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

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

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 $\sigma_g : a \to ga$, and define $\phi : G \to A(S)$ by $\phi : g \to \sigma_a$. We call ϕ the **permutation representation** of S associated with g.

Example 1.20. 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 $\sigma_g : a \to ga = a$, then σ_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 $\ker A = \{g \in G : ga = a \text{ for all } a \in A\}$

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 $A = \{e, r, \ldots, r^{n-1}\} \leq D_{2n}$. 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 $\langle g\rangle \leq N(\langle g\rangle)$.

Bibliography

[1] D. S. Dummit and R. M. Foote, *Abstract Algebra*. John Wiley & Sons, Inc., 2004.