Math 407
Spring 2010
Dr. Seelinger
March 15, 2010

Brief Review of Introductory Group Theory

1 Binary Operations

Let S be a set. We define a **binary operation** on S to be a function $b : S \times S \to S$ on the Cartesian Product of S with itself to S. So, given $s_1, s_2 \in S$, we have $b(s_1, s_2) \in S$ is the binary operation b applied to s_1 and s_2. If we use a symbol like $*$ to represent the binary operation b, we usually denote $b(s_1, s_2)$ by $s_1 * s_2$. (This borrows from the way we usually write additiona and multiplication.)

We say a binary operation $* : S \times S \to S$ is **associative** if for all $s_1, s_2, s_3 \in S$ we have $(s_1 * s_2) * s_3 = s_1 * (s_2 * s_3)$. We say that $e \in S$ is **an identity of** $*$ if $e * s = s = s * e$ for all $s \in S$. We say that $*$ is **commutative** if $s_1 * s_2 = s_2 * s_1$ for all $s_1, s_2 \in S$.

Exercise 1. Prove that if $*$ is an associative binary operation on a nonempty set S, then there can be at most one identity element for $*$.

Examples:

1. Let $\mathbb{Z}$ denote the set of integers. Then the standard addition $+$ is a binary operation on $\mathbb{Z}$. Is it associative? Does it have an identity? Is it commutative?

   A different binary operation on $\mathbb{Z}$ is the standard multiplication. Is it associative? Does it have an identity? Is it commutative?

2. Let R be the set of rotations of the Cartesian Plane about the origin and let $\circ$ denote the composition of rotations. Why is $\circ$ a binary operation on R? Is it associative? Does it have an identity? Is it commutative?

3. Let $M_3(\mathbb{C})$ be the set of 3×3 matrices with entries in the complex numbers $\mathbb{C}$. Then $M_3(\mathbb{C})$ has two binary operations, matrix addition and matrix multiplication. Are they associative? Do they have identities? If so, what are these identities? Are they commutative?

4. Let F be a field and let V be a vector space with scalars in F. Then vector addition is a binary operation on V. Is it associative? Does it have an identity? Is it commutative?

Exercise 2: Let $\times$ be the usual cross-product on $\mathbb{R}^3$. Show that $\times$ is a binary operation that is not associative. Does it have an identity?

Exercise 3: Let S be a nonempty set and let F be the set of functions from S to S. Prove that the composition $\circ$ of functions in F is a binary operation on S. Is it associative? Does it have an identity? Is it commutative?

One example that we want to look at a little more in depth at the integers modulo n, denoted $\mathbb{Z}_n$, when $n > 1$ is an integer. There are a number of ways to look at $\mathbb{Z}_n$. On a more computational level, we can define $\mathbb{Z}_n$ to be the set $\{0, 1, \ldots, n-1\}$ and define a binary operation $*$ on $\mathbb{Z}_n$ as follows. For any $a, b \in \mathbb{Z}_n$, define $a * b$ to be the remainder of $a + b$ when divided by n. More explicitly, we have

$$a * b = \begin{cases} a + b & \text{if } a + b < n \\ a + b - n & \text{if } a + b \geq n. \end{cases}$$

We can think of the time of day as an example of this type of addition when $n = 12$. For example, if a 12 hour clock reads 4:00 now, what time will it read 10 hours from now? To do this, we subtract off 12 from the sum to get 2:00.

Note that the reglar addition in $\mathbb{Z}$ is not a binary operation on $\mathbb{Z}_n$. (Why not?)

While it has the potential to be confusing, we usually denote the above operation $*$ on $\mathbb{Z}_n$ by the usual $+$. It is understood that if $+$ is a binary operation on $\mathbb{Z}_n$, then it must be the one we defined above.

We can also define a modified multiplication on $\mathbb{Z}_n$ as well. In particular, if for any $a, b \in \mathbb{Z}_n$ we define $a \star b$ to be the remainder of ab when divided by n, we also get a binary operation on $\mathbb{Z}_n$. As we did with addition, we usually denote this binary operation on $\mathbb{Z}_n$ by the usual multiplication with the understanding that if this is to be a binary operation on $\mathbb{Z}_n$, it must be this modified one.

An alternate way to view $\mathbb{Z}_n$ that requires a little more background and is an example of what we will see is a factor group, is to introduce and equivalence relation on $\mathbb{Z}$ and think of $\mathbb{Z}_n$ as the set of equivalence classes relative to this equivalence relation. While this approach makes it easier to show that both $+$ and $\times$ are associative, commutative binary operations on $\mathbb{Z}_n$, we will delay introducing this approach until after a discussion of equivalence relations. (See Section 0.3 of Dummit and Foote – which we denote by DF – for more detail on this approach.)

2 Groups

We are now ready to define a group. We have seen that a given set can have more than one associative binary operation associated to it. When we define a group, we need to specify both a set and a binary operation on this set.

Definition 1 *Let G be a set and let $*$ be a binary operation on G. Hence we have* **closure** *in that*

0. **Closure:** *For all $a, b \in G$, the element $a * b$ is in G.*

Then the ordered pair $(G, *)$ is a **group** *if:*

1. **Associativity:** *For all $a, b, c \in G$, we have $(a * b) * c = a * (b * c)$.*

2. **Identity:** *There exists an* **identity element** *$e \in G$ such that $a * e = a = e * a$ for all $a \in G$.*

3. **Inverses:** *For each $a \in G$ there exists an* **inverse** *element $b \in G$ such that $a * b = e$ and $b * a = e$.*

One of our first goals is to develop a catalog of examples of groups so that we can get a deeper understanding of various group structures. Note that the pair $(\mathbb{Z}, +)$ is a group but $(\mathbb{Z}, \times)$ is NOT a group. (Why is $(\mathbb{Z}, \times)$ not a group?) We also have the following groups: $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(M_3(\mathbb{C}), +)$, $(R, \circ)$ (where R is the set of rotations of the Cartesian Plane about the origin), $(V, +)$, where V is a vector space with scalars in the field F, and $(\mathbb{Z}_n, +)$ where $n > 1$ is an integer. Note almost all of these examples involve a form of addition and in all of these cases the binary operation is commutative. A group whose binary operation is commutative is called an **abelian group**.

One very important example of a non-abelian group is the set of all nonsingular $n \times n$ matrices with entries in a field F using the standard matrix multiplication. We call this group the **general linear group of $n \times n$ matrices with entries in F** and denote it by $GL_n(F)$. For example,

$$GL_2(\mathbb{R}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbb{R} \text{ and } ad - bc \neq 0 \right\}.$$

Question: What is the smallest possible group? Can a group be an empty set with a binary operation?

One of the goals of group theory is to classify all group structures on all sets in a useful way. This is considered an unobtainable task, but this course will introduce a number of structure theorems that will help us understand the basic structures of some of classes these groups. By analyzing these structures, in many cases we will be able to tell when two groups are not equivalent or be able to make substantial progress in determining if two groups are equivalent. (We will consider two groups equivalent if they are isomorphic to each other. The concept of an isomorphism will be covered later in Section 1.6 of DF.)

We start with some basic properties of identities and inverses of groups given in the following proposition.

Proposition 1 *Let $(G, *)$ be a group.*

1. *The identity of $(G, *)$ is unique.*
2. *For each $a \in G$, there exists a unique inverse $b \in G$ of a. (We denote this inverse by a^{-1}.)*
3. *For each $a \in G$, $(a^{-1})^{-1} = a$.*
4. *For each $a, b \in G$, we have $(a * b)^{-1} = b^{-1} * a^{-1}$.*

We leave the proof of this as an exercise. (See Proposition 1.1.1 of DF.)

NOTES ON NOTATION:

1. Above, we've emphasized that to define a group you must specify not only the set, but also the binary operation. Despite that emphasis, it is traditional to denote a group by only denoting the set. We will follow this tradition and specify the binary operation whenever it becomes useful to do so. For an arbitrary group G, we will usually denote the binary operation using multiplicative notation.

2. When working with abelian groups, we sometimes use the addition sign to denote the binary operation. One avoids using the addition sign to denote a (potentially) noncommutative binary operation. When using this additive notation for a group G, we denote the identity using a 0 or 0_G, and if $a \in G$ we denote the inverse of a by $-a$.

3. Let G be a group and let $a \in G$. If n is a positive integer, we define

$$a^n = a * a * \cdots * a (n \text{ times}), \quad a^0 = e, \quad \text{and } a^{-n} = a^{-1} * a^{-1} * \cdots * a^{-1} (n \text{ times}).$$

When using additive notation, we have

$$na = a + a + \cdots + a (n \text{ times}), \quad 0a = 0_G, \quad \text{and } (-n)a = -a + (-a) + \cdots + (-a)) (n \text{ times}).$$

Let G be a group with identity element e and let $a \in G$. We say a has **finite order** if there exists a positive integer m such that $a^m = e$. We say a has **infinite order** if $a^m \neq e$ for all positive integers m. If a has finite order, we define the **order of** a to be the smallest positive integer n such that $a^n = e$.

For example, $1 \in \mathbb{Z}$ has infinite order (when $\mathbb{Z}$ is considered a group under addition), but $1 \in \mathbb{Z}_5$ has order 5 (when $\mathbb{Z}_5$ is considered a group under the modified addition).

(**) Let G be a group and let $a \in G$ have order n. Then it is not hard to show that $a^{-1} = a^{n-1}$.

One of the properties of groups is that the cancellation law holds. In particular, if G is a group and $a, b, u, v \in G$, then $au = av \Rightarrow u = v$ since $au = av \Rightarrow a^{-1}au = a^{-1}av \Rightarrow eu = ev \Rightarrow u = v$. Similarly $ub = vb \Rightarrow ubb^{-1} = vbb^{-1} \Rightarrow u = v$. This Cancellation Law gives us some strong properties for groups.

We say a group G is a **finite group** if its underlying set only has a finite number of elements. In this case we say the **order of** G is the number of elements in the underlying set of G. If the underlying

set of G is infinte, we say G is an **infinite group**. In this case we say G has infinite order. So $(\mathbb{Z}_n, +)$ is a finite group, but $(\mathbb{Z}, +)$ is an infinite group.

One immediate observation (which will become obvious later) is that for two groups to be equivalent, they must have the same order.

Exercise 4: Prove that if G is a finite group that every element of G has finite order. Can you find an example of a group in which every element has finite order, but the group is infinite?

As stated above, we now look at a few examples of groups.

3 Cyclic Groups

We start with one of the more basic types of groups, cyclic groups.

Definition 2 *Let G be a group. Then G is* **cyclic** *if there exists an $c \in G$ such that*

$$G = \{c^j : j \in \mathbb{Z}\}.$$

In this case we write $G = \langle c \rangle$ and we say that c is a **generator** *for G.*

We make the following observations about cyclic groups. Let G be a group.

1. If G is a cyclic group, it must be abelian. Not all abelian groups are cyclic.
2. Cyclic groups can be finite or infinite.
3. If G is finite group, then G is cyclic if and only if there exists an element c of G whose order is equal to the order of G.

We consider two examples of cyclic groups. The first is $\mathbb{Z}$, which is an infinite cyclic group (under addition) with generator $1 \in \mathbb{Z}$. Note that -1 is the only other generator for this group.

The second example is $\mathbb{Z}_n$ (under our modified addition) where $n \geq 1$ is a positive integer. In this case, $1 \in \mathbb{Z}_n$ is a generator for $\mathbb{Z}_n$. Note that there are typically more generators for $\mathbb{Z}_n$ than just 1.

Exercise 5: What are all the generators of the cyclic group $\mathbb{Z}_8$? Of $\mathbb{Z}_{15}$? Of $\mathbb{Z}_{23}$? What can you say in general about the generators of $\mathbb{Z}_n$ when $n > 1$ is a positive integer?

Exercise 6: Prove that $\mathbb{R}$ as a group under addition is NOT cyclic.

It turns out that all cyclic groups can be shown to be equivalent to either $\mathbb{Z}$ or $\mathbb{Z}_n$. This is not hard to see once we define the concept of an isomorphism.

4 Dihedral Groups

Dihedral groups are motivated by symmetries of plane figures and are some of the simplest nonabelian groups. Hence, they are a useful class of examples for us.

First, we define an **isometry** of the Cartesian Plane $\mathbb{R}^2$ to be an invertible function $f : \mathbb{R}^2 \to \mathbb{R}^2$ that preserves both lengths and angles (usually as defined by the dot product). In other words, f is an isometry if for any $x, y \in \mathbb{R}^2$ we have $(f(x) - f(0)) \cdot (f(y) - f(0)) = x \cdot y$, where $\cdot$ represents the usual dot product.

If X is a subset of $\mathbb{R}^2$, we define a **symmetry of** X to be an isometry $f : \mathbb{R}^2 \to \mathbb{R}^2$ that takes X to itself. (In other words, $f(X) = X$.)

Exercise 7: Let X be a subset of $\mathbb{R}^2$. Prove that the set of symmetries of X form a group under composition of functions.

Now for each integer $n \geq 3$, let Δ_n be a regular n-gon with center at the origin. Then any symmetry of Δ_n must preserve the origin. We call the group of planar symmetries of Δ_n the **dihedral group of order** $2n$ and denote it by D_{2n}.

This is a nice definition, but it is not always the easiest to work with. Instead, we want to develop a more algebraic way of working with dihedral groups. So we take a closer look at the symmetries of a regular n-gon.

Fix an integer $n \geq 3$. Let $r : \mathbb{R}^2 \to \mathbb{R}^2$ be the counter-clockwise rotation about the origin through an angle of $2\pi/n$ radians. Then r will be a symmetry of Δ_n. You can also show that r^j is also a symmetry of Δ_n for any integer j and that $r^n = \mathrm{id}$, the identity function.

Next, fix a line ℓ through one of the vertices of Δ_n and the origin. Then we can define $s : \mathbb{R}^2 \to \mathbb{R}^2$ as the reflection of $\mathbb{R}^2$ about the line ℓ. One can also show that s is also a symmetry of Δ_n.

Exercise 8: Consider the regular pentagon Δ_5 with a vertex at $(0, 1)$. Let r be the counter-clockwise of $2\pi/5$ radians about the origin and let s be the reflection about the y-axis. Prove the following:

1. $r^2 s$ is a symmetry of Δ_5.
2. $rs = sr^4$.
3. The group of symmetries of Δ_5 has underlying set

$$D_{10} = \{\mathrm{id}, r, r^2, r^3, r^4, s, sr, sr^2, sr^3, sr^4\}.$$

The results in the above exercise can be generalized to D_{2n} in general. (How would you generalize Exercise 8?) So, we can describe D_{2n} in a purely algebraic way as follows. Let r be an element of order n and s be an element of order 2 (so $r^n = \mathrm{id} = \mathrm{s}^2$). Then

$$D_{2n} = \left\{\mathrm{id}, r, r^2, \ldots, r^{n-1}, s, sr, sr^2, \ldots, sr^{n-1}\right\}$$

where $r^n = \mathrm{id} = \mathrm{s}^2$ and $rs = sr^{-1} = sr^{n-1}$. We abbreviate the above by writing

$$D_{2n} = \langle r, s : r^n = s^2 = \mathrm{id}, rs = sr^{-1}\rangle.$$

With this description, it is easy to compute products. For example, in D_{10} we have

$$(r^3)(sr^2) = r^2(rs)r^2 = r^2(sr^4)r^2 = r(rs)r^6 = r(sr^4)r = (rs)r^5 = (sr^4)\mathrm{id} = sr^4.$$

Note that in doing this computation, we did not need to look at Δ_5 at all. These computations were purely algebraic.

Exercise 9: Let $n \geq 3$ be an integer and let $r, s \in D_{2n}$ be as above. Prove that sr^j has order 2 for every $0 \leq j \leq n - 1$.

5 Symmetric Groups

If we are working on classifying all groups, one result that might be helpful is Cayley's Theorem, which describes all groups in terms of symmetric groups. It is a nice result, but it gives us some sense as to how complex symmetric groups can be. We start with a definition.

Definition 3 *Let X be a nonempty set. We define the set* $\mathrm{Symm}(X)$ *to be the set of all invertible functions $f : X \to X$.*

Next, we have the following propisition.

Proposition 2 *Let X be a nonempty set. Then the set* $\mathrm{Symm}(X)$ *with the binary operation $\circ$ being composition of functions is a group.*

Outline of Proof: We first show that composition actually defines a binary operation on $\mathrm{Symm}(X)$ by showing that the composition of two invertible functions is invertible. If $\sigma, \tau \in \mathrm{Symm}(X)$, then we can show that $(\sigma \circ \tau)^{-1} = \tau^{-1} \circ \sigma^{-1}$.

Next, we use the results of Exercise 3 in the first section to claim that $\circ$ is associative. It's identity is the identity function $\mathrm{id}_X : X \to X$, and by definition every element of $\mathrm{Symm}(X)$ is invertible with respect to composition.

Note that there is not a restriction that X has to be finite. Still, for any integer $n \geq 2$, we let $S_n = \mathrm{Symm}(\{1, 2, \ldots, n\})$. Let $\sigma \in S_n$. Then we can give an explicit description of σ by saying 1 goes to $\sigma(1)$, 2 goes to $\sigma(2)$, and so on until we have written down all values of σ for each element in the set X. For example, one possible element of S_6 is

$$\begin{array}{rcl} 1 & \to & 4 = \sigma(1) \\ 2 & \to & 1 = \sigma(2) \\ 3 & \to & 5 = \sigma(3) \\ 4 & \to & 2 = \sigma(4) \\ 5 & \to & 6 = \sigma(5) \\ 6 & \to & 3 = \sigma(6) \end{array}.$$

This notation is not very compact, especially as we consider larger n than 6. One way to make this more concise would be to write σ using a double-row notation that abbreviates the above table as follows:

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

In general, if $\sigma \in S_n$, we can write σ explicitly by

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}.$$

The double-row notation now gives us a way to compute compositions of permutations in a relatively simple way. For example, if $\tau \in S_6$ is given by

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

the we compute $\tau \circ \sigma$ as follows

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

where we include an intermediate step represented by the three rows, where the first and second rows represent σ, while the second and third rows represent τ. In this way, we can represent multiplication of elements of S_n. (For the purposes of making computations using this notation, we can rearrange the columns of this array as needed and this will still represent the same permutation.)

A more common notation is to use cycle notation. We first define a **cycle of length** k (where $1 \leq k \leq n$) as an element γ of S_n as an element that can be written in the form

$$\gamma = \begin{pmatrix} a & \gamma(a) & \gamma^2(a) & \cdots & \gamma^{k-1}(a) & b_1 & b_2 & \cdots & b_{n-k} \\ \gamma(a) & \gamma^2(a) & \gamma^3(a) & \cdots & a & b_1 & b_2 & \cdots & b_{n-k} \end{pmatrix}$$

where $b_1, b_2, \ldots, b_{n-k}$ are distinct integers between 1 and n that are not elements of the k element set $\{a, \gamma(a), \gamma^2(a), \ldots, \gamma^{k-1}(a)\}$. We will also refer to such a permutation as a **k-cycle**. For example,

$$\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 2 & 6 & 3 & 5 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 4 & 3 & 6 & 2 & 5 \\ 4 & 3 & 6 & 1 & 2 & 5 \end{pmatrix}$$

is a cycle of length 4 in S_6. We can abbreviate γ by using cycle notation and writing $\gamma = (1\ 4\ 3\ 6) \in S_6$. This is thought of as abbreviating the arrow diagram

$$1 \to 4 \to 3 \to 6 \to 1$$

with the understanding that for any element not mentioned in the cycle notation, γ sends that element to itself.

More generally, if γ is a k-cycle of S_n of the form

$$\gamma = \begin{pmatrix} a & \gamma(a) & \gamma^2(a) & \cdots & \gamma^{k-1}(a) & b_1 & b_2 & \cdots & b_{n-k} \\ \gamma(a) & \gamma^2(a) & \gamma^3(a) & \cdots & a & b_1 & b_2 & \cdots & b_{n-k} \end{pmatrix}$$

where $b_1, b_2, \ldots, b_{n-k}$ are distinct integers between 1 and n that are not elements of the k element set $\{a, \gamma(a), \gamma^2(a), \ldots, \gamma^{k-1}(a)\}$, then the **cycle notation** for γ is $\big(a\ \gamma(a)\ \gamma^2(a)\ \ldots\ \gamma^{k-1}(a)\big)$.

Cycle notation is more compact than the two row notation, but there are a few things to note about this notation.

- The identity of S_n is a 1-cycle that can be represented using any element of the set $\{1, 2, \ldots, n\}$. So $(1) = (2) = (3) = \cdots = (n)$ are all ways to represent the identity. (It is usually standard to write (1) for the identity, but this is not always the case.)
- Any k-cycle in S_n can be represented k ways using cycle notation. In particular, you can start the notation at any number mentioned in the cycle as long as the order of the following numbers remain intact. For example, in S_5 we have

$$(1\ 5\ 4) = (5\ 4\ 1) = (4\ 1\ 5) \neq (5\ 1\ 4).$$

- The inverse of a k-cycle $\gamma = (c_1\ c_2\ \ldots\ c_k)$ is just the k-cycle $(c_k\ c_{k-1}\ \ldots\ c_1)$.
- Not every permutation is a cycle. In fact, most permutations in S_n are not cycles. Still, we will see below that every permutation is a product of disjoint cycles (where we consider a k-cycle to be a product of cycles with only one factor). We say two cycles $\gamma = (c_1\ c_2\ \ldots\ c_k)$ and $\alpha = (a_1\ a_2\ \ldots\ a_t)$ are **disjoint** if $\{c_1, c_2, \ldots, c_k\} \cap \{a_1, a_2, \ldots, a_t\} = \emptyset$ and $k \geq 2, t \geq 2$.

Exercise 10: Let $\gamma = (1\ 3\ 7\ 4\ 2)$ and $\alpha = (5\ 4\ 6\ 1)$ be cycles in S_7. Express γ^2 and α^2 as a product of disjoint cycles. Express $\gamma\alpha$ as a product of disjoint cycles. Express $\alpha\gamma$ as products of disjoint cycles. Is $\gamma\alpha = \alpha\gamma$?

Lemma 3 *Let γ, α be two disjoint cycles in S_n. Then $\gamma\alpha = \alpha\gamma$.*

Exercise 11: Give a proof of the lemma above by considering 3 cases. If A is the set of elements mentioned in α and C is the set of elements mentioned in γ, then show $\gamma\alpha(j) = \alpha\gamma(j)$ when (a) $j \in A$, (b) $j \in C$, and (c) $j \notin A \cup C$.

Proposition 4 *Let $\sigma \in S_n$. Then σ can be expressed uniquely (up to ordering) as a product of disjoint cycles $\sigma = \gamma_1\gamma_2\cdots\gamma_r$ for some set of disjoint cycles $\gamma_1, \gamma_2, \ldots, \gamma_r \in S_n$ of length greater than 1. (Here we allow the possibility of $r = 1$.)*

Proof. Let $\sigma \in S_n$. If σ is the identity, then we write $\sigma = (1)$. If not, then there exists a smallest positive integer k_1 such that $\sigma^{k_1}(1) = 1$. Let $\alpha_1 = \big(1\ \sigma(1)\ \sigma^2(1)\ \ldots\sigma^{k_1-1}(1)\big)$ and let $A_1 = \{1, \sigma(1), \ldots, \sigma^{k-1}(1)\}$. If $A_1 = \{1, 2, \ldots, n\}$, then we are done and $\sigma = \alpha_1$. If not, then choose $a_2 \notin A_1$ and let k_2 be the smallest positive integer such that $\sigma^{k_2}(a_2) = a_2$ and let $\alpha_2 = \big(a_2\ \sigma(a_2)\ \sigma^2(a_2)\ \ldots\sigma^{k_2-1}(a_2)\big)$. Let $A_2 = \{a_2, \sigma(a_2), \ldots, \sigma^{k_2-1}(a_2)\}$. If $A_1 \cup A_2 = \{1, \ldots, n\}$, then we have $\sigma = \alpha_1\alpha_2$. If not, we select $a_3 \notin A_1 \cup A_2$ and continue as above.

Since $|A_j| \geq 1$ and the set $\{1, 2, \ldots, n\}$ has a finite number of elements, this process will stop after a finite number of times so that $\sigma = \alpha_1\alpha_2\cdots\alpha_t$. Now we omit all of the α_j that are 1-cycles to get $\sigma = \gamma_1\gamma_2\cdots\gamma_r$ for $r \leq t$.

To show this factorization is unique, assume $\sigma = \gamma_1\gamma_2\cdots\gamma_r = \beta_1\beta_2\cdots\beta_s$ for two sets of disjoint cycles. Let $j \in \{1, 2, \ldots, n\}$ and let γ' and β' be the cycles that have j mentioned in them. Then $\sigma(j) = \gamma_1\gamma_2\ldots\gamma_r(j) = \gamma'(j)$ and similarly $\sigma(j) = \beta'(j)$. Therefore, $(\gamma')^i(j) = \sigma^i(j) = (\beta')^i(j)$ for all i, hence $\gamma' = \big(j\ \sigma(j)\ \sigma^2(j)\ \ldots\ \sigma^{k_j-1}(j)\big) = \beta'$ where k_j is the smallest positive integer such that $\sigma^{k_j}(j) = j$. We do this for each $j \in \{1, 2, \ldots, n\}$ so that each γ cycle matches up with each β cycle to get uniqueness. ∎

We also develop a second way to characterize permutations. We call a 2-cycle in S_n a **transposition**. You can verify by direct computation that for any k-cycle $\gamma = (c_1\ c_2\ \ldots c_k)$ we have

$$\gamma = (c_1\ c_2\ \ldots\ c_k) = (c_1\ c_2)(c_2\ c_3)\cdots(c_{k-1}\ c_k) = (c_{k-1}\ c_k)(c_{k-2}\ c_k)\cdots(c_1\ c_k).$$

Hence, by the above proposition, every permutation can be written as a product of transpositions. Note that this product is not unique, as demonstrated above. It turns out that even the number of transpositions in this factorization is not unique. For example,

$$(1\ 2\ 3\ 4) = (1\ 2)(2\ 3)(3\ 4) = (1\ 3)(2\ 3)(1\ 2)(1\ 4)(1\ 3).$$

Still, if $\sigma \in S_n$ can be written as a product of an even number of transpositions, whenever σ is written as a product of transpositions there must be an even number of them. Similarly, if σ can be written as a product of an odd number of transpositions, whenever σ is written as a product of transpositions there must be an odd number of them. (The proof of this based on what we already know is a little long but not hard, so we will omit it for now.) Therefore, we define a permutation to be an **even permutation** if it can be written as a product of an even number of transpositions and a permutation to be an **odd permutation** if it can be written as a product of an odd number of transpositions. We define a function $\text{sgn} : S_n \to \{1, -1\}$ by letting $\text{sgn}(\sigma) = 1$ if σ is even and $\text{sgn}(\sigma) = -1$ if σ is odd.

6 Homomorphism and Isomorphisms

As with most mathematical objects, we can define functions between groups that are functions on the underlying sets but also relate the extra structure of the binary operations of the two groups involved. For example, in linear algebra, the natural functions we look at are linear transformations because they are functions that relate vector addition and scalar multiplication in the two vector spaces. So, if $T : V \to W$ is a linear transformation of vector spaces over the field F, then we know for all $x, y \in V$, $T(x+y) = T(x)+T(y)$ which relates the vector sum of V on the left side of this equation to the vector sum of W on the right side of this equation. Similarly for any $c \in F$, $T(cx) = cT(x)$ relates the scalar multiplication in V on the left with the scalar multiplication of W on the right side of the equation.

For groups, we only have one binary operation for each group, so we impose a condition similar to the one on vector sums with linear transformations.

Definition 4 *Let $(G, *)$ and $(H, \star)$ be groups. A function $\phi : G \to H$ is a* group homomorphism *if for all $x, y \in G$ we have*

$$\phi(x * y) = \phi(x) \star \phi(y).$$

Exercise 12: Let $n \geq 2$ be an integer. Show that the following functions are group homomorphisms:
(1) $\phi : \mathbb{Z} \to \mathbb{Z}_n$ where for each integer j we define $\phi(j)$ to be the remainder when j is divided by n.
(2) $\text{sgn} : S_n \to \{1, -1\}$, where $\{1, -1\}$ is considered a group under multiplication.
(3) Let $C_n = \langle a \rangle$ be a cyclic group of order n. Define $\phi : \mathbb{Z} \to C_n$ by $\phi(i) = a^i$ for all $i \in \mathbb{Z}$.
(4) The determinant function $\det : GL_n(\mathbb{R}) \to \mathbb{R}^\times$.

In general, we can say some things about group homomorphism that can be summarized in the proposition below.

Proposition 5 *Let G and H be groups and let $\phi : G \to H$ be a group homomorphism.*

1. *If e_G is the identity of G and e_H is the identity of H, then $\phi(e_G) = e_H$.*
2. *If $a \in G$, then $\phi(a^j) = \phi(a)^j$ for all $j \in \mathbb{Z}$.*
3. *If $a \in G$, then $\phi(a^{-1}) = \phi(a)^{-1}$.*

Proof. Let e_G be the identity of G. Then $e_G = e_G e_G$, so $\phi(e_G)e_H = \phi(e_G) = \phi(e_G e_G) = \phi(e_G)\phi(e_G)$, where e_H is the identity of H and the last equality follows since ϕ is a homomorphism. So we can apply the group cancellation law to the equality $\phi(e_G)e_H = \phi(e_G)\phi(e_G)$ to get $e_H = \phi(e_G)$ as claimed. Hence for any $a \in G$, we have $\phi(a^0) = \phi(e_G) = e_H = \phi(a)^0$.

Next, let j be a positive integer. Then $a^j = a \cdot a \cdot \ldots \cdot a$ (j times). So, by the property of being a homomorphism, $\phi(a^j) = \phi(a \cdot a \cdot \ldots \cdot a) = \phi(a) \cdot \phi(a) \cdot \ldots \cdot \phi(a) = \phi(a)^j$.

Also, $\phi(a)\phi(a^{-1}) = \phi(aa^{-1}) = \phi(e_G) = e_H = \phi(a)\phi(a)^{-1}$. Hence, again by group cancellation, $\phi(a^{-1}) = \phi(a)^{-1}$, which proves Part (3). Therefore, $\phi(a^{-j}) = \phi((a^{-1})^j) = \phi(a^{-1})^j = (\phi(a)^{-1})^j = \phi(a)^{-j}$, so the rest of Part (2) follows. ∎

Exercise 13: Let $C_n = \langle a \rangle$ be a cyclic group of order n. Prove that if G is a group and $b \in G$, then there is at most one homomorphism $\phi : C_n \to G$ such that $\phi(a) = b$. What condition must b satisfy in order for a group homomorphism $\phi : C_n \to G$ to exist such that $\phi(a) = b$?

Definition 5 *Let G and H be groups and let $\phi : G \to H$ be a group homomorphism. Let e_H be the identity element of H. Then the* kernel of ϕ *is the set*

$$\ker(\phi) = \{g \in G : \phi(g) = e_H\}.$$

Kernels of homomorphisms are analogous to the nullspace of a linear transformation and they are important because they are a measure of how much a homomorphism may "collapse" things. In particular, we have the following result.

Theorem 6 *Let G and H be groups with identities e_G and e_H, respectively and let $\phi : G \to H$ be a homomorphism of groups. Then ϕ is one-to-one if and only if* $\ker(\phi) = \{e_G\}$.

Proof. First, we assume ϕ is one-to-one. By Proposition 5, we know $\phi(e_G) = e_H$, so $e_G \in \ker(\phi)$. Now, if $g \in \ker(\phi)$, then $\phi(g) = e_H = \phi(e_G)$. Since ϕ is one-to-one, it follows that $g = e_G$. Therefore, the only element of $\ker(\phi)$ is e_G or $\ker(\phi) = \{e_G\}$.

Conversely, assume $\ker(\phi) = \{e_G\}$. Let $g_1, g_2 \in G$ be such that $\phi(g_1) = \phi(g_2)$. Then

$$e_H = \phi(g_1)^{-1}\phi(g_2) = \phi(g_1^{-1})\phi(g_2) = \phi(g_1^{-1}g_2).$$

Therefore, $g_1^{-1}g_2 \in \ker(\phi) = \{e_G\}$, so $g_1^{-1}g_2 = e_G \Rightarrow g_2 = g_1$. Hence ϕ is one-to-one. ∎

Exercise 14: Let G, H, and K be groups. Let $\phi : G \to H$ and $\psi : H \to K$ be homomorphisms. Prove that $\psi \circ \phi : G \to K$ is a homomorphism and that $\ker(\phi) \subseteq \ker(\psi \circ \phi)$.

As with linear transformations, the above theorem says that in order to test whether a group homomorphism is one-to-one, it is sufficient to only test whether the group homomorphism is one-to-one at the identity element e_H.

Definition 6 *Let G and H be groups and let $\phi : G \to H$ be a function. Then ϕ is an* isomorphism *if:*
(1) ϕ is a group homomorphism, and
(2) ϕ is one-to-one and onto (i.e., a bijection).
If there exists an isomorphism from G to H, we say that G is isomorphic to *H and write $G \cong H$.*

Note that one way to look at the definition of an isomorphism is to view it as a homomorphism that is invertible as a function. Therefore, if $\phi : G \to H$ is an isomorphism, the function $\phi^{-1} : H \to G$ exists, but potentially may not be a group homomorphism itself. We show in Theorem 7 below that ϕ^{-1} is indeed also an isomorphism.

Above, we talked about classifying groups up to some form of equivalence. To make this more precise, we would like to classify groups up to isomorphism. (So two groups will be "equivalent" when they are isomorphic.) We give some examples below.

Examples:

1. If G is a group, the identity function $\mathrm{id} : G \to G$ is an isomorphism so $G \cong G$.
2. If $C_n = \langle a \rangle$ is a cyclic group of order n, then the function $\phi : \mathbb{Z}_n \to C_n$ defined by $\phi(i) = a^i$ is an isomorphism, so $\mathbb{Z}_n \cong C_n$.
3. Let $\mathbb{R}^+$ be the group of all positive real numbers under multiplication. Define $\phi : \mathbb{R} \to \mathbb{R}^+$ by $\phi(x) = e^x$. Then ϕ is an isomorphism. (What is the inverse of ϕ?)

To go further with this idea of isomorphism as a type of equivalence, we now show that $\cong$ has the three properties of an equivalence relation. (A relation $\sim$ on a nonempty set A is an **equivalence relation** if for all $a, b, c \in A$ we have (1) $a \sim a$ (reflexive property), (2) if $a \sim b$ then $b \sim a$ (symmetric property) and (3) if $a \sim b$ and $b \sim c$ then $a \sim c$ (transitive property).)

Theorem 7 *Let G, H, and K be groups. Then*

1. *(Reflexivity) $G \cong G$.*
2. *(Symmetry) If $\phi : G \to H$ is an isomorphism, then $\phi^{-1} : H \to G$ is also an isomorphism. Therefore, $G \cong H \Rightarrow H \cong G$.*
3. *(Transitivity) If $\phi : G \to H$ and $\psi : H \to K$ are isomorphisms, then $\psi \circ \phi : G \to K$ is an isomorphism. Therefore, $G \cong H$ and $H \cong K$ imply $G \cong K$.*

Proof. (1) We noted above that the identity function $\mathrm{id} : G \to G$ is an isomorphism, hence by definition $G \cong G$.

(2) Let $\phi : G \to H$ be an isomorphism and consider its inverse function $\phi^{-1} : H \to G$. We already know that ϕ^{-1} is a bijection since ϕ is a bijection. To show ϕ^{-1} is an isomorphism, let $x, y \in H$ and let $a = \phi^{-1}(x)$, $b = \phi^{-1}(y)$. Then we know $x = \phi(a)$ and $y = \phi(b)$. So

$$\phi^{-1}(xy) = \phi^{-1}(\phi(a)\phi(b)) = \phi^{-1}(\phi(ab)) = ab = \phi^{-1}(x)\phi^{-1}(y).$$

Therefore, ϕ^{-1} is a bijective homomorphism, or an isomorphism. Hence $H \cong G$ as claimed.

(3) By Exercise 14, $\psi \circ \phi$ is a group homomorphism. Furthermore, it is a standard result about functions that since ϕ and ψ are bijective, so is $\psi \circ \phi$. Therefore, $\psi \circ \phi : G \to K$ is an isomorphism, hence $G \cong K$. ∎

So, when two groups are isomorphic, they have the same algebraic structure. For example, if G and H are two isomorphic groups, then we know:
(1) The cardinalities of the underlying sets are the same: $|G| = |H|$
(2) G is abelian if and only if H is abelian (Why?)
(3) G is cyclic if and only if H is cyclic
(4) If $\phi : G \to H$ is an isomorphism, then for all $x \in G$ the order of $\phi(x)$ in H must equal the order of x in G.
We can use these properties to quickly determine that some groups are not isomorphic to each other. We give the following examples:

Example:

1. Note S_3 and S_4 are not isomorphic since $|S_3| = 3! = 6$ and $|S_4| = 4! = 24$.
2. We know S_3 and $\mathbb{Z}_6$ are not isomorphic since $\mathbb{Z}_6$ is abelian and S_3 is not.
3. We know that $\mathbb{R}$ and $\mathbb{R}^\times$ are not isomorphic since $\mathbb{R}^\times$ contains an element ($-1 \in \mathbb{R}^\times$) of order 2 and $\mathbb{R}$ does not.

Exercise 15: Let G and H be isomorphic groups. Prove observations (2) and (3) above. In particular, prove that G is abelian if and only if H is abelian and G is cyclic if and only if H is cyclic.

7 Subgroups

One of the important structures of groups is the lattice of subgroups. To find a lattice of subgroups, it is important first to be able to find and identify these subgroups. We start this section with a definition of a subgroup, then with some initial characterizations.

Definition 7 *Let G be a group with binary operation $*$ and let H be a subset of G. Then H is a* subgroup *of G if H is a group using the restriction of the binary operation $*$ to H.*

While the above definition is a good intuitive definition, it does not always work very well in proving something is a subgroup. Instead, we use the following characterizations.

Proposition 8 *Let H be a subset of the group G. Then H is a subgroup of G if and only if the following three conditions hold:*

1. *(Closure) for all $h_1, h_2 \in H$ we have $h_1 * h_2 \in H$.*
2. *(Identity) $e_G \in H$*
3. *(Inverses) if $h \in H$, then $h^{-1} \in H$.*

Proof. ($\Rightarrow$) Assume H is a subgroup of G. Then H must have the closure property (otherwise $*$ restricted to H would not be a binary operation). Since H is a group, it must have an identity, $e_H \in H$. So $e_H * e_H = e_H = e_H * e_G$ since e_H is the identity of H and e_G is the identity of G. By Group Cancellation, we get $e_H = e_G$, so $e_G \in H$. Finally, if $h \in H$ then h must have an inverse h' in H such that $hh' = e_H = e_G = hh^{-1}$. Again, by Group Cancellation, $h' = h^{-1} \in H$.

($\Leftarrow$) Now assume Closure, Identity, and Inverses as stated above. Then since $*$ is associative in G, it is certainly associative when restricted to elements of H. The rest of the assumed properties are the properties of a group, so H is a subgroup of G. ∎

The conditions in Proposition 8 can be shortened somewhat in the following Proposition.

Proposition 9 *Let G be a group and let H be a subset. Then H is a subgroup if*

1. *H is nonempty.*
2. *for all $x, y \in H$ we have $xy^{-1} \in H$.*

Proof. Assume the given two conditions. Since H is nonempty, we know there exists an $h \in H$. Therefore, by Condition (2), we have $(h)(h)^{-1} \in H$ or $e_G \in H$. Now, since $e_G \in H$ we know for any $a \in H$ we have $e_G a^{-1} \in H$ or $a^{-1} \in H$. Finally, let $h, a \in H$. We have already shown $a^{-1} \in H$ so, by Condition (2) we have $h(a^{-1})^{-1} \in H$ or $ha \in H$. Therefore, by Proposition 8, H is a subgroup of G. ∎

Every nontrivial group G has at least two subgroups, $\{e_G\}$ and G itself. We also make the following observation.

Lemma 10 *Let $\phi : G \to H$ be a group homomorphism and let $K = \ker(\phi)$. Then K is a subgroup of G.*

Proof. By Proposition 5, we know $e_G \in K$, so K is nonempty. Let $x, y \in K$. Then $\phi(xy^{-1}) = \phi(x)\phi(y)^{-1} = e_H e_H^{-1} = e_H$. Therefore, $xy^{-1} \in K$. Hence, by Proposition 9, K is a subgroup of G. ∎

So, looking at kernels of homomorphisms is one way to realize subgroups of a group. We look at a few examples below.

Examples: (1) Let $n > 1$ be an integer and consider the homomorphism $\pi_n : \mathbb{Z} \to \mathbb{Z}_n$ given by $\phi_n(j) = j \in \mathbb{Z}_n$. Then $\ker(\pi_n) = n\mathbb{Z} = \{jn : j \in \mathbb{Z}\}$, the set of all integral multiples of n. This shows that $n\mathbb{Z}$ is a subgroup of $\mathbb{Z}$ for any positive integer n. With a little more work we can show that for any integer n, $n\mathbb{Z}$ is a subgroup of $\mathbb{Z}$.
(2) Let n again be a positive integer and consider the determinant function $\det : GL_n(\mathbb{R}) \to \mathbb{R}^\times$. Since we know for any matrices $a, b \in GL_n(\mathbb{R})$ we have $\det(ab) = \det(a)\det(b)$, we see that det is a group homomorphism. The kernel of the determinant homomorphism is $\{g \in GL_n(\mathbb{R}) : \det(g) = 1\}$. We call this group the **special linear group of $n \times n$ matrices with entries in** $\mathbb{R}$ and denote it by $SL_n(\mathbb{R})$.
(3) Again, let $n \geq 2$ be an integer and consider the homomorphism $\text{sgn} : S_n \to \{1, -1\}$ given by

$$\text{sgn}(\sigma) = \begin{cases} 1 & \text{if } \sigma \text{ is even} \\ -1 & \text{if } \sigma \text{ is odd} \end{cases}$$

The kernel of this homomorphism is the group of all even permutations. We call this group the **alternating group on n letters** and denote it by A_n.

We can generalize Proposition 10 with the following exercise.

Exercise 16: Let $\phi : G \to H$ be a group homomorphism and let $G' \subseteq G$ and $H' \subseteq H$ be subgroups. Prove that $\phi^{-1}(H') = \{g \in G : \phi(g) \in H\}$ is a subgroup of G and $\phi(G') = \{h \in H : h = \phi(g) \text{ for some } g \in G'\}$ is a subgroup of H.

The above exercise shows that not only do homomorphisms relate the binary operations of the domain and codomain, it creates a relationship between the subgroups of the two groups.

We note not all subgroups of a group can be realized as the kernel of some homomorphism. Indeed, if we consider D_{10} where we denote the counterclockwise rotation by $2\pi/5$ radians about the center by r and the reflection about a line through a fixed vertex and the center of the regular pentagon, then one can easily check $\{1, s\}$ is a subgroup of D_{10}, but we claim that $\{1, s\}$ cannot be the kernel of some homorphism. To justify this claim, we make the observation that all kernels have an extra property, which we justify below.

Lemma 11 *Let $\phi : G \to H$ be a group homomorphism and let $K = \ker(\phi)$. Then for all $x \in K$ and $g \in G$, we have $gxg^{-1} \in K$.*

Proof. To show $gxg^{-1} \in K$, we need to show $\phi(gxg^{-1}) = e_H$. But

$$\phi(gxg^{-1}) = \phi(g)\phi(x)\phi(g)^{-1} = \phi(g)e_H\phi(g)^{-1} = e_H.$$

Hence $gxg^{-1} \in K$ as claimed. ∎

Definition 8 *Let H be a subgroup of a group G. Then H is a* normal subgroup *of G if for all $g \in G$ and $h \in H$ we have $ghg^{-1} \in H$.*

Going back to our claim that $\{1, s\} \subseteq D_{10}$ cannot be a kernel, we note that in D_{10} we have $rsr^{-1} = rsr^4 = sr^4r^4 = sr^8 = sr^3 \notin \{1, s\}$. Hence $\{1, s\}$ cannot be a kernel by Lemma 11.

This naturally leads to the question of how else we can find subgroups of a group. One place to start is to generalize the strategy in finding the subgroup $\{1, s\}$ of D_{10}. In particular, we have the following proposition.

Proposition 12 *Let G be a group and let $c \in G$. Then the set*

$$\langle c \rangle = \{c^j : j \in \mathbb{Z}\}$$

is a subgroup of G.

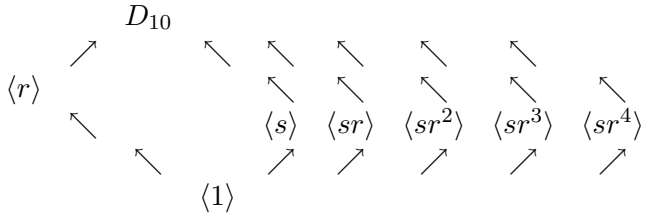
NOTE: We call the subgroup $\langle c \rangle$ the **cyclic subgroup of G generated by c.**

Proof. Note $e_G = c^0 \in \langle c \rangle$, by definition. So $\langle c \rangle$ is nonempty. Also, if $x, y \in \langle c \rangle$, then there exists integers i, j such that $x = c^i$ and $y = c^j$. So $xy^{-1} = c^i c^{-j} = c^{i-j}$. Since $i - j$ is also an integer, we get $xy^{-1} = c^{i-j} \in \langle c \rangle$. Hence, by Proposition 9, we have $\langle c \rangle$ is a subgroup of G. ∎

So, let us use the above proposition to analyze the subgroup structure of D_10. First, we note that $\{1\}$ and D_{10} itself are subgroups. Next, we choose an element of D_{10} and look at the cyclic subgroup it generates. So $\langle s \rangle = \{1, s\}$ since s has order 2. Next, we look at $\langle r \rangle = \{1, r, r^2, r^3, r^4\}$ since r has order 5. So now we look for an element not in one of the above sets. Take sr for example. Then $\langle sr \rangle = \{1, sr\}$ since sr has order 2 as well. We can continue this to find the remaining cyclic subgroups $\langle sr^2 \rangle$, $\langle sr^3 \rangle$, and $\langle sr^4 \rangle$.

The question then arises, are there any other subgroups? If H were a subgroup of D_{10} that was not one of the cyclic ones, then H would have to contain at least two nonidentity elements that are listed in two different cyclic subgroups. We first make the observation that if H contains r^i for some $1 \leq i \leq 4$, then H must contain all of $\langle r \rangle$. (You can check this directly.) Next, if H contains two elements of the form sr^i and sr^j with $0 \leq i < j \leq 4$, then H must contain $sr^i sr^j = s^2 r^{j-i} = r^{j-i} \neq 1$, so H must contain r itself. Once we know H contains r, then H must also contain $(sr^i)(r^{-1}) = s$. If H contains both r and s, then H must be all of D_{10}. (Why?) Similarly, if H contains r^i for $1 \leq i \leq 4$ and sr^j for some $0 \leq j \leq 4$, then H must also contain r, hence H contains $(sr^j)r^{-j} = s$ so we get H is all of D_{10}. Therefore, the only subgroups of D_{10} are the group itself, the trivial subgroup, and the cyclic subgroups listed above.

We can also draw a diagram indicating containment of subgroups as follows. (I apologize for the crudeness of this diagram in advance as drawing in LaTeX is somewhat time consuming.)



Exercise 17: Let G be a group.

1. Let H_1 and H_2 be subgroups of G. Prove that $H_1 \cap H_2$ is also a subgroup of G.
2. Generalize the above statement as follows. Let $\mathcal{S} = \{H_j : j \in J\}$ be a collection of subgroups of G. Prove that
$$H' = \bigcap_{j \in J} H_j$$
is also a subgroup of G. (Here, J can be any indexing set, including an uncountably infinite set.)
3. Recall that $2\mathbb{Z}$ and $3\mathbb{Z}$ are subgroups of $\mathbb{Z}$. Prove that $2\mathbb{Z} \cup 3\mathbb{Z}$ is NOT a subgroup of $\mathbb{Z}$.

8 Group Actions

Group actions are important constructs we can use to understand a group. When we were defining the dihedral groups, we used symmetries of regular n-gons. These symmetries were defined in terms of an action on the regular n-gon. Similarly, when we defined the symmetric group S_n, we used the set $\{1, 2, \ldots, n\}$ to define the symmetric group as invertible functions from this set to itself. In many other situations, we can use an auxillary set to help us understand the structure of a group. So we first make a formal definition of a group action.

Definition 9 *Let G be a group and let X be a nonempty set. A* **left action of G on X** *is a function $\cdot : G \times X \to X$ such that*

1. *$e_G \cdot x = x$ for all $x \in X$*
2. *for all $g_1, g_2 \in G$ and for all $x \in X$ we have $g_1 \cdot (g_2 \cdot x) = (g_1 g_2) \cdot x$.*

In this case, for each $x \in X$ we define the **orbit of** *x under this G action to be the set $G \cdot x = \{g \cdot x : g \in G\} \subseteq X$ and we define the* **stabilizer of** *x to be the set $G_x = \{g \in G : g \cdot x = x\}$.*

Note: Let G be a group. We can also define a right G-action on a nonempty set X by defining a function $* : X \times G \to X$ such that (1) $x * e_G = x$ for all $x \in X$ and (2) for all $g_1, g_2 \in G$ and $x \in X$ we have $(x * g_1) * g_2 = x * (g_1 g_2)$. Unless otherwise indicated, when we talk about a group action, we will assume it is a left group action.

Examples: (1) As in Section 4, let Δ_n be a regular n-gon with center at the origin. Then D_{2n} will act on Δ_n by $f \cdot x = f(x)$ for any symmetry f and any element $x \in \Delta_n$.
(2) More generally, if X is a nonempty set, we saw in Section 5 that $G = \text{Symm}(X)$ is a group. Therefore, we can define an action $\cdot : G \times X \to X$ by $\sigma \cdot x = \sigma(x)$ for all $\sigma \in G$ and $x \in X$. Of particular interest is when S_n acts on the set $\{1, 2, \ldots, n\}$ in this manner.
(3) Another standard action is if $G = GL_n(\mathbb{R})$ and $X = \mathbb{R}^n$, then $\cdot : GL_n(\mathbb{R}) \times \mathbb{R}^n \to \mathbb{R}^n$ is a left $GL_n(\mathbb{R})$-action on $\mathbb{R}^n$ when we define $g \cdot v = gv$ where gv denotes the standard matrix-vector product.

Lemma 13 *Let G be a group with a left action on a non-empty set X. Then for any $x \in X$, the stabilizer G_x of x is a subgroup of G.*

Proof. Since G acts on X, we know by definition $e_G * x = x$, so $e_G \in G_x$. Furthermore, if $g_1, g_2 \in G_x$ we see that $(g_1 g_2) * x = g_1 * (g_2 * x) = g_1 * x = x$, hence $g_1 g_2 \in G_x$. Finally, if $g \in G_x$, then $x = e_G * x = (g^{-1} g) * x = g^{-1} * (g * x) = g^{-1} * x$, so $g^{-1} \in G_x$. Hence, by Proposition 8, we have G_x is a subgroup of G. ∎

So, we can also find groups by looking at stabilizers. For example, if we consider the standard $GL_3(\mathbb{R})$-action on $\mathbb{R}^3$ and we let $x = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$, then we can find the stabilizer of x under this action to be

$$(GL_3(\mathbb{R}))_x = \left\{ \begin{bmatrix} 1 & a_{1,2} & a_{1,3} \\ 0 & a_{2,2} & a_{2,3} \\ 0 & a_{3,2} & a_{3,3} \end{bmatrix} : a_{2,2}a_{3,3} - a_{2,3}a_{3,2} \neq 0 \right\}.$$

Another such example is when we consider the above defined S_n-action on the set $X_n = \{1, 2, \ldots, n\}$ and look for the stabilizer of $n \in X_n$. This is the subgroup defined by $\{\sigma \in S_n : \sigma(n) = n\}$. So this is the subgroup of all permutations in S_n that permutes the elements $1, 2, \ldots, n-1$ but leaves n fixed. It is not hard to see that this stabilizer is a subgroup that is isomorphic to S_{n-1}.

One can prove some very interesting structure results about groups by considering the following standard actions of a group on itself.

Example: Let G be a group. The G can act on itself (i.e., by letting $X = G$) by **left multiplication** by defining $\cdot : G \times G \to G$ as $g \cdot x = gx$ where the right side of this equation uses the predefined binary operation of the group.

A second way G can act on itself is by **conjugation**, where we define $* : G \times G \to G$ by $g * x = gxg^{-1}$, where again the right side of this equation uses the binary operation of the group.

We comment that when we consider G acting on itself by conjugation, we have alternate names for both the orbits and the stabilizers of this action.

Definition 10 *Let G be a group acting on itself by conjugation. Let $x \in G$. Then the stabilizer of x under this action is called the* centralizer of x *and is denoted by $C_G(x)$. So*

$$C_G(x) = \{g \in G : g * x = x\} = \{g \in G : gxg^{-1} = x\} = \{g \in G : gx = xg\}.$$

We define the center of G *to be the set*

$$Z(G) = \{g \in G : gx = xg \text{ for all } x \in G\}.$$

We define the conjugacy class of x *to be orbit of x under the conjugation action.*

Note that it is not difficult to show from these definitions that for any group G we have

$$Z(G) = \bigcap_{x \in G} C_G(x).$$

When G is an abelian group, we see that $C_x(G) = G$ and $Z(G) = G$, so these concepts are not as useful as when they are applied to nonabelian groups.

Next, we prove a theorem that shows group actions have a corresponding group homomorphism lurking in the background.

Theorem 14 *Let G be a group and let X be a nonempty set. If G acts on X via $*$, then there exists a group homomorphism $\theta_* : G \to \text{Symm}(X)$ such that $g * x = \theta_*(g)(x)$ for all $g \in G$ and $x \in X$.*

Conversely, if $\theta : G \to \text{Symm}(X)$ is a homomorphism, then the function $*_\theta : G \times X \to X$ given by $g *_\theta x = \theta(g)(x)$ is a group action.

Proof. Let $*$ be an action of G on X. Define $\theta_* : G \to \text{Symm}(X)$ by $\theta_*(g)(x) = g * x$ for all $g \in G$, $x \in X$. (Recall, the group operation on $\text{Symm}(X)$ is composition of functions.) First, we need to show $\theta_*(g)$ is in $\text{Symm}(X)$ for every $g \in G$. But we can check using the properties of a group action that $\theta_*(g)^{-1} = \theta_*(g^{-1})$, so $\theta_*(g)$ is an invertible function, hence in $\text{Symm}(X)$.

To show θ_* is a homomorphism, let $g_1, g_2 \in G$. Then for all $x \in X$ we have

$$\theta_*(g_1g_2)(x) = (g_1g_2) * x = g_1 * (g_2 * x) = \theta_*(g_1)(g_2 * x) = \theta_*(g_1)(\theta_*(g_2)(x)) = \theta_*(g_1)\theta_*(g_2)(x)$$

hence $\theta_*(g_1g_2) = \theta_*(g_1)\theta_*(g_2)$. Therefore, θ_* is a homomorphism.

Conversely, assume $\theta : G \to \text{Symm}(X)$ is a homomorphism. Define $*_\theta : G \times X \to X$ by $g *_\theta x = \theta(g)(x)$ for all $g \in G$ and $x \in X$. Then, since θ is a homomorphism, $\theta(e_G) = \text{id}$, hence $e_G *_\theta x = \text{id}(x) = x$ for all $x \in X$. Furthermore, for any $g_1, g_2 \in G$ and $x \in X$, we have

$$(g_1g_2) *_\theta x = \theta(g_1g_2)(x) = \theta(g_1)\theta(g_2)(x) = \theta(g_1)(g_2 *_\theta x) = g_1 *_\theta (g_2 *_\theta x).$$

Therefore $*_\theta$ is a group action of G on X. ∎

So the above Theorem shows that group actions on X and homomorphisms with codomain $\text{Symm}(X)$ are equivalent. If $* : G \times X \to X$ is an action of the group G on the set X, we define the **kernel of the action** $*$ to be $\ker(\theta_*)$. In DF they characterize the kernel of the action as the set $\{g \in G : g * x = x \text{ for all } x \in X\}$. These definitions are equivalent. (Why?)

For example, for the S_n action on the set $\{1, 2, \ldots, n\}$, the kernel of this action is just the trivial subgroup $\{(1)\}$. When $GL_n(\mathbb{R})$ acts on itself by conjugation, the kernel of this action is going to be the set $\{cI_n : c \in \mathbb{R}^\times\}$. When an action has the trivial subgroup as its kernel, we say this action is **faithful**.

Exercise 18: Let G be a group.

1. Prove that the set of isomorphisms from G to itself is a subgroup of $\text{Symm}(G)$. We call this the **group of automorphisms of** G and we denote it by $\text{Aut}(G)$.
2. Let $*$ be the group action of G acting on itself by conjugation. Prove that $\theta_*(G) \subseteq \text{Aut}(G)$.
3. Let $\mathcal{S}_G$ be the set of subgroups of G. Use Exercise 16 to prove that the function $\star : G \times \mathcal{S}_G \to \mathcal{S}_G$ given by $g \star H = gHg^{-1} = \{ghg^{-1} : h \in H\}$ for any $g \in G$ and any subgroup $H \in \mathcal{S}_G$ defines a G-action on $\mathcal{S}_G$.

As a corollary of the above theorem, we get Cayley's Theorem.

Corollary 15 (Cayley's Theorem) *Let G be a group. Then G is isomorphic to a subgroup of* $\text{Symm}(G)$.

Proof. Let $\cdot : G \times G \to G$ be the action of G acting on itself by left multiplication. By Theorem 14, we have a corresponding homomorphism $\theta_\cdot : G \to \text{Symm}(G)$. By Exercise 16, $\theta_\cdot(G)$ is a subgroup of $\text{Symm}(G)$. Finally, since for any $(g, x) \in G \times G$ we have $g \cdot x = gx = x \Rightarrow g = e_G$ by Group Cancellation, the kernel of this group action is trivial, hence $\theta_\cdot$ is injective by Theorem 6. So we can define an isomorphism $\bar{\theta} : G \to \theta_\cdot(G)$ by $\bar{\theta}(g) = \theta_\cdot(g)$ for all $g \in G$. So $G \cong \theta_\cdot(G)$. ∎

Cayley's Theorem is a good news/bad news situation. The good news is if we completely understand the groups $\text{Symm}(X)$ for any set X, then we understand all groups. The bad news is completely understanding $\text{Symm}(X)$ for all sets X is as difficult as understanding the structure of all groups.

Finally, we can realize normalizers of subgroups as stabilizers of the group action defined in Exercise 18. We first define a normalizer.

Definition 11 *Let G be a group and let H be a subgroup of G. The* normalizer of H in G *is the set*

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

Exercise 19: Let H be a subgroup of a group G. As in Exercise 17, let $\mathcal{S}_G$ be the set of subgroups of G and let $\star : G \times \mathcal{S}_G \to \mathcal{S}_G$ be the group action on $\mathcal{S}_G$ defined by conjugation. Prove that $N_G(H)$ is the stabilizer of H under the action $\star$, hence $N_G(H)$ is a subgroup of G. If H is a normal subgroup of G, what is $N_G(H)$?

Exercise 20: Let G act on a set X and let $x, y \in X$ be such that x and y are in the same G-orbit. Prove that the stabilizers G_x and G_y are conjugate. (In other words, prove that there exists a $g \in G$ such that $G_y = gG_xg^{-1}$.)

Exercise 21: Let $G = GL_3(\mathbb{C})$ and let $X = M_3(\mathbb{C})$.

1. Prove that G acts on X by conjugation.
2. Find the kernel of the above action.
3. Let $A = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{bmatrix} \in M_3(\mathbb{C})$. Find the stabilizer of A under the conjugation action. How does this compare with the centralizer of A in $GL_3(\mathbb{C})$?
4. Let $T = \left\{ \begin{bmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{bmatrix} : abc \neq 0 \right\} \subseteq GL_3(\mathbb{C})$. Prove that T is a subgroup of $GL_3(\mathbb{C})$ and find the normalizer of T in $GL_n(\mathbb{C})$.
5. Classify the G-orbits in X. (HINT: Think Jordan-Canonical Forms.)

Exercise 22: Let V be an n-dimensional vector space over $\mathbb{R}$ and let $\mathcal{L}(V)$ be the group of invertible linear transformations from V to V. Prove that $\mathcal{L}(V) \cong GL_n(\mathbb{R})$. (You can cite results from a linear algebra text to prove this.)

9 Cyclic Groups Revisited

Recall that we defined a group G to be cyclic if there exists and element $c \in G$ such that $G = \langle c \rangle = \{c^j : j \in \mathbb{Z}\}$. We want to classify all subgroups of cyclic groups. First we note that for $G = \langle c \rangle$, there exists a function $\phi : \mathbb{Z} \to G$ given by $\phi(j) = c^j$ for all $j \in \mathbb{Z}$. We make the following observations about this homomorphism.

Lemma 16 *Let $G = \langle c \rangle$ be a cyclic group. Then there exists a surjective homomorphism $\phi : \mathbb{Z} \to G$ defined by $\phi(j) = c^j$ for all $j \in \mathbb{Z}$. Furthermore, if G has infinite order, then ϕ is an isomorphism so $G \cong \mathbb{Z}$. If G has order $n < \infty$, then $\ker(\phi) = n\mathbb{Z}$ and ϕ induces an isomorphism $\bar{\phi} : \mathbb{Z}_n \to G$.*

Proof. We first show that ϕ is a homomorphism. But if $i, j \in \mathbb{Z}$, then $\phi(i + j) = c^{i+j} = c^i c^j = \phi(i)\phi(j)$, so ϕ is a group homomorphism. To prove ϕ is surjective, let $x \in G = \langle c \rangle$. Then, since G is cyclic with generator c, we have $x = c^j$ for some $j \in \mathbb{Z}$. Therefore $x = \phi(j)$, so ϕ is surjective as claimed.

Now we assume G has infinite order and we compute the kernel of ϕ. If $j \in \ker(\phi)$, then $c^j = e_G \Rightarrow c^{|j|} = e_G$, so we can assume $j \geq 0$. If $j \neq 0$, then by the Division Algorithm, for every $k \in \mathbb{Z}$, we can write $k = qj + r$ for some $0 \leq r < j$, so $\phi(k) = c^k = c^{qj+r} = (c^j)^q c^r = c^r$. Therefore, $G = \phi(\mathbb{Z}) = \{e_H, c, c^2, \ldots, c^{j-1}\}$, which contradicts the assumption that G is infinite. Therefore, $\ker(\phi) = \{0\}$, hence by Theorem 6, ϕ is injective as well as surjective. Since ϕ is bijective, it is an isomorphism as claimed.

Next, if $|G| = n < \infty$, then we see that $\phi(n) \in \ker(\phi)$ since $c^n = e_G$. Furthermore, for any $k \in \mathbb{Z}$ we have $k = qn + r$ for some integers q, r such that $0 \leq r < n$, so $\phi(k) = c^k = c^{qn+r} = (c^n)^q c^r = c^r$. Therefore, $\phi(k) = e_G$ if and only if $r = 0$ which means k is a multiple of n. Hence $\ker(\phi) = n\mathbb{Z}$.

Now define $\bar{\phi} : \mathbb{Z}_n \to G$ by $\bar{\phi}(j) = c^j$. Then we see that for any $0 \leq i, j \leq n - 1$, we have $\bar{\phi}(i)\bar{\phi}(j) = c^i c^j = c^{i+j}$. Since c has order n, we have $c^{i+j} = c^{i+j-n}$, so $c^{i+j} = \bar{\phi}(i + j)$ and $\bar{\phi}$ is a homomorphism. Furthermore, it is easy to see $\bar{\phi}$ is surjective. Finally, we have $\ker(\bar{\phi}) = \ker(\phi) \cap \mathbb{Z}_n = \{0\}$, hence by Theorem 6, $\bar{\phi}$ is injective, hence an isomorphism. ∎

So, if we are to analyze the subgroups of an infinite cyclic group, it is sufficient to analyze the subgroups of $\mathbb{Z}$. We have also seen that any set of the form $n\mathbb{Z}$ (where n is a nonnegative integer) is a subgroup of $\mathbb{Z}$. We now show these are the only subgroups of $\mathbb{Z}$.

Lemma 17 *Let H be a subgroup of $\mathbb{Z}$. Then there exists a nonnegative integer n such that $H = n\mathbb{Z}$.*

Proof. Let H be a subgroup of $\mathbb{Z}$. If $H = \{0\}$, then $H = 0\mathbb{Z}$. So assume $H \neq \{0\}$. Then there exists a nonzero integer $a \in H$, so $-a \in H$ as well. Hence H contains a positive integer. By the Well Ordering Axiom, there exists a smallest positive integer in H, which we will call n. Then, by closure, we know $n\mathbb{Z} \subseteq H$. We claim that $H \subseteq n\mathbb{Z}$ as well. Indeed, if $x \in H$ but $x \notin n\mathbb{Z}$, then there exists integers q and r such that $x = qn + r$ and $1 \leq r < n$. Hence, since $r = x - qn$, we see that $r \in H$ with $0 < r < n$. This contradicts the assumption that n was the smallest positive element of H. Therefore, $x \in n\mathbb{Z}$, so $H \subseteq n\mathbb{Z} \subseteq H \Rightarrow H = n\mathbb{Z}$. ∎

Next, we make the following observation. Let $n\mathbb{Z}$ and $k\mathbb{Z}$ be two subgroups of $\mathbb{Z}$. Then we have

$$n\mathbb{Z} \subseteq k\mathbb{Z} \Leftrightarrow k|n(\text{i.e., } n \text{ is a multiple of } k).$$

It is then not hard to show that for any two nontrivial subgroups $n\mathbb{Z}$ and $m\mathbb{Z}$ that

$$n\mathbb{Z} \cap m\mathbb{Z} = \text{lcm}(n, m)\mathbb{Z} \text{ and } n\mathbb{Z} + m\mathbb{Z} = \gcd(n, m)\mathbb{Z},$$

where $n\mathbb{Z} + m\mathbb{Z} = \{in + jm : i, j \in \mathbb{Z}\}$ is the smallest subgroup of $\mathbb{Z}$ containing both m and n.

So, we can classify the maximal subgroups of $\mathbb{Z}$ fairly quickly. (Here, a proper subgroup H of a group G is **maximal** if for every subgroup K of G such that $H \subseteq K \subseteq G$, we have $K = H$ or $K = G$.) One can use the divisibility condition above to conclude the maximal subgroups of $\mathbb{Z}$ are precisely the subgroups of the form $p\mathbb{Z}$ when p is a prime.

Our next question asks, what about the subgroup structure when G is a finite, cyclic group. Assume G has order $n < \infty$ and let H be a subgroup of G. Then, by Exercise 16, we know the inverse image $\phi^{-1}(H)$ of H under the homomorphism ϕ defined in Lemma 16 is a subgroup of $\mathbb{Z}$, hence by Lemma 17, $\phi^{-1}(H) = k\mathbb{Z}$ for some nonnegative integer k. Furthermore, since $e_G \in H$, we know

$$n\mathbb{Z} = \ker(\phi) = \phi^{-1}(e_G) \subseteq \phi^{-1}(H) = k\mathbb{Z}.$$

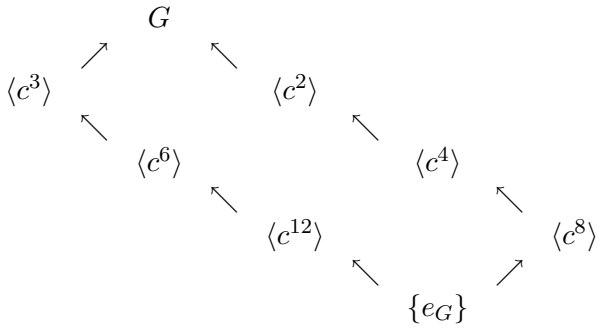
Therefore, we know $k|n$. Furthermore, since ϕ is surjective, we have $\phi(\phi^{-1}(H)) = H$. (Why?) So $H = \phi(k\mathbb{Z}) = \langle c^k \rangle$. Hence we conclude the following.

Proposition 18 *Let $G = \langle c \rangle$ be a finite, cyclic group of order n and let H be a subgroup of G. Then $H = \langle c^k \rangle$ for some integer k that divides n. Furthermore, for any k that divides n, the subgroup $H = \langle c^k \rangle$ is a subgroup of G of order (n/k).*

Example: Let $G = \langle c \rangle$ be a cyclic group of order 24. Since the positive divisors of 24 are $1, 2, 3, 4, 6, 8, 12, 24$, the subgroups of G are

$$\langle c \rangle, \langle c^2 \rangle, \langle c^3 \rangle, \langle c^4 \rangle, \langle c^6 \rangle, \langle c^8 \rangle, \langle c^{12} \rangle, \langle c^{24} \rangle = \{e_G\}.$$

The inclusion of these subgroups can be diagrammed as follows:



Exercise 23: Let $G = \langle c \rangle$ be a cyclic subgroup of order 60. Find all subgroups of G and draw a diagram or lattice of these subgroups indicating inclusions.

So, it follows from Lemma 17 and Proposition 18 that any subgroup of a cyclic group is also cyclic. Furthermore, if $G = \langle c \rangle$ is a cyclic group of order n, it follows from Proposition 18 that there is exactly one subgroup of G whose order is the divisor k of n. The question then remains, if $1 < j < n$, which subgroup is $\langle c^j \rangle$ when j is not a divisor of n? This is determined by the order of c^j.

Lemma 19 *Let $G = \langle c \rangle$ be a cyclic group of order n and let $1 \leq j \leq n-1$. Then $\langle c^j \rangle = \langle c^d \rangle$, where $d = gcd(j, n)$.*

Proof. Since G is a finite group and let $d = \gcd(j, n)$. Then since $d|j$ we have $c^j \in \langle c^d \rangle$ so $\langle c^j \rangle \subseteq \langle c^d \rangle$. Furthermore, by the Euclidean Algorithm, there exist integers a and b such that $aj + bn = d$. So

$$c^d = c^{aj+bn} = (c^j)^a (c^n)^b = (c^j)^a (e_G)^n = (c^j)^a \in \langle c^j \rangle$$

which implies $\langle c^d \rangle \subseteq \langle c^j \rangle \subseteq \langle c^d \rangle$. Hence $\langle c^j \rangle = \langle c^d \rangle$. ∎

Note, a consequence of Lemma 19 is that c^j is a generator of G if and only if $\gcd(j, n) = 1$.

10 Equivalence Relations, Equivalence Classes, and Orbits

In this section, we first review the definition of an equivalence relation and equivalence classes. After this review, we see how we can use the action of a group G on a set X to define an equivalence relation on X for which the equivalence classes are precisely the G-orbits in X.

Definition 12 *Let X be a nonempty set. A* relation on X *is a subset $R \subseteq X \times X$. We denote this relation elementwise with the symbol $\sim_R$ by defining $x \sim_R y \Leftrightarrow (x, y) \in R$ for all $x, y \in X$.*

The relation $\sim_R$ is an equivalence relation *if for all $x, y, z \in X$ we have*

1. *(Reflexivity) $x \sim_R x$*
2. *(Symmetry) If $x \sim_R y$ then $y \sim_R x$*
3. *(Transitivity) If $x \sim_R y$ and $y \sim_R z$, then $x \sim_R z$*

In general, if R defines an equivalence relation, we usually abbreviate $\sim_R$ by $\sim$ when there is no confusion. If $\sim$ is an equivalence relation on a set X, for every $x \in X$ we can define the **equivalence class of** x by letting

$$[x] = \{y \in X : x \sim y\}$$

and we denote the set of equivalence classes in X under $\sim$ by $X/\sim$.

Examples of equivalence relations are equality on a set, congruence of triangles in the plane, and similarity of triangles in the plane. One important special case of equivalence classes come from group actions.

Lemma 20 *Let the group G act on a nonempty set X and for any $x, y \in X$ define $x \sim y$ if and only if there exists a $g \in G$ such that $y = g * x$. Then $\sim$ is an equivalence relation on X and the equivalence classes are precisely the orbits of G in X.*

Proof. To prove $\sim$ is an equivalence relation, we show the three properties of an equivalence relation. First, $x \sim x$ since $x = e_G * x$. Next, if $x \sim y$ then $y = g * x$ for some $g \in G$, so $g^{-1} * y = g^{-1}g * x = x \Rightarrow y \sim x$. Finally, if $x \sim y$ and $y \sim z$, then $y = g_1 * x$ and $z = g_2 * y$ for some $g_1, g_2 \in G$. Therefore, $z = g_2 * y = g_2 * (g_1 * x) = (g_2 g_1) * x$, so $x \sim z$. Hence $\sim$ is an equivalence relation.

Next, let $x \in X$. Then the equivalence class of x under $\sim$ is

$$[x] = \{y \in X : x \sim y\} = \{y \in X : y = g * x \text{ for some } g \in G\} = \{g * x : g \in G\} = G * x.$$

∎

An example of the above lemma is when we consider the conjugation action of $GL_n(F)$ on $M_n(F)$, where F is any field. In this situation, we say that two matrices A and B are **similar** if and only if there exists a $g \in GL_n(F)$ such that $B = gAg^{-1}$. Since similarity defined in this way comes from a $GL_n(F)$-action on $M_n(F)$, similarity is an equivalence relation.

In general, one can prove that if $\sim$ is an equivalence relation on X, then the equivalence classes under $\sim$ partition X in that the union of the equivalence classes is all of X and the equivalence classes are pairwise disjoint. We take the time to prove this in the special case of the orbits of a group action.

Lemma 21 *Assume the group G acts on the nonempty set X and let $x, y \in X$. Then either $G*x = G*y$ or $G * x \cap G * y = \emptyset$.*

Proof. Assume $G * x \cap G * y \neq \emptyset$. Then there exists a $z \in G * x \cap G * y$, so there exist $g_1, g_2 \in G$ such that $g_1 * x = z = g_2 * y \Rightarrow y = g_2^{-1} g_1 * x$ and $x = g_1^{-1} g_2 * y$. So, let $y' \in Gy$. Then $y' = g' * y$ for some $g' \in G$. Hence $y' = g' * y = g' g_2^{-1} g_1 * x \in G * x$. Therefore, $G * y \subseteq G * x$. Similarly, for any $x' \in G * x$, there exists a $g \in G$ such that $x' = g * x = g g_1^{-1} g_2 * x \in G * y$. Hence we get $G * x \subseteq G * y \subseteq G * x \Rightarrow G * x = G * y$. ∎

Now let H be a subgroup of a group G. Then H acts on G by left multiplication, hence this action defines an equivalence relation on G where the equivalence class of an element $a \in G$ is the orbit $Ha = \{ha : h \in H\}$. Since the element $a \in G$ is written on the right with this notation, we call the H-orbit the **right H-coset of a in G**. We define the **index of H in G** to be the number of distince right H-cosets in G and we denote the index of H in G by $[G : H]$.

Corollary 22 *Let H be a subgroup of a group G. Then for any two right H-cosets Ha and Hb we have either $Ha = Hb$ or $Ha \cap Hb = \emptyset$.*

Proof. This follows directly from Lemma 21 by noting that each right coset is the H-orbit in G under the left multiplication action. ∎

Next, we need a quick technical lemma to prove Lagrange's Theorem.

Lemma 23 *Let H be a subgroup of a group G and let $a \in G$. Then the function $f : H \to Ha$ defined by $f(h) = ha$ is a bijection.*

Exercise 24: Prove Lemma 23.

We saw with a cyclic group of order n that for each divisor of n there exists a unique subgroup of that order. While this is not true for arbitrary finite groups, we can relate the order of the subgroups of a group to the divisors of the order of the whole group. This gives us Lagrange's Theorem.

Theorem 24 (Lagrange's Theorem) *Let G be a finite group of order n and let H be a subgroup of G. Then the order of H must be a divisor of n.*

Proof. Let H be a subgroup of G, where $|G| = n$. Since H acts on G by left multiplication, G is the union of the right cosets of H. By Lemma 21, we can choose $a_1, a_2, \ldots, a_r \in G$ such that $Ha_i = Ha_j \Leftrightarrow i = j$ and $G = \bigcup_{i=1}^{r} Ha_i$. Since the Ha_i are pairwise disjoint, $|G| = |Ha_1| + |Ha_2| + \cdots + |Ha_r|$. But, by Lemma 23, we have $|Ha_i| = |H|$ for all $1 \leq i \leq r$. Therefore, $|G| = |H|r$, hence $|H|$ divides $|G|$. ∎

Lagrange's Theorem is a tremendous help when looking for subgroups of a finite group as it narrows our search down to subgroups whose orders are divisors of the total order of the group. Note that unlike the cyclic case, this does not say that for every divisor there is a subgroup.

Exercise 25: Use Lagrange's Theorem to prove that if G is a finite group of order n and $a \in G$, then the order of a must be a divisor of n.

Corollary 25 *Let G be a finite group of prime order p. Then G is cyclic and $G \cong \mathbb{Z}_p$.*

Proof. Let G be a group of prime order p and let $c \in G$ be chosen so that $c \neq e_G$. Then $H = \langle c \rangle$ is a subgroup of G. Since $c \neq e_G$, we know $|H| > 1$. Since p is prime, Lagrange's Theorem gives us that

$|H| = p = |G|$, so $\langle c \rangle = G$. ∎

It also follows from Lagrange's Theorem that if H is a subgroup of a *finite* group G, then

$$[G : H] = \frac{|G|}{|H|}.$$

Note that it is still possible for an infinite group to have a subgroup of finite index. Indeed, if we look at $G = \mathbb{Z}$ and $H = 3\mathbb{Z}$, then $[\mathbb{Z} : 3\mathbb{Z}] = 3$ even though both $|G|$ and $|H|$ are infinite.

10.1 Right vs. Left

Let us still consider the case when H is a subgroup of a group G. Most texts will use left H-cosets to prove results analogous to the results we have proven above for right H-cosets. We include this short subsection to make this correspondence more explicit.

First we note that we can define a different H-action on G by letting $* : H \times G \to G$ be given by $h * g = gh^{-1}$. Indeed, to show $*$ is an H-action, first note for all $g \in G$ we have $e_G * g = ge_G = g$ and for any $h_1, h_2 \in H$ and $g \in G$ we have

$$h_1 * (h_2 * g) = h_1 * (gh_2^{-1}) = (gh_2^{-1})h_1^{-1} = g(h_1h_2)^{-1} = (h_1h_2) * g.$$

Therefore, for any element $a \in G$, we can define the **left H-coset of a in G** to be the H-orbit of a in G under the $*$-action. Therefore, we find that Corollary 22 and Lemma 23 hold for left cosets as well as right cosets. In addition, the following exercise (Exercise 12 in §3.2 of DF) gives us a bijection between left H-cosets and right H-cosets in G.

Exercise 26: (DF, §3.2, Exercise 12) Let H be a subgroup of a group G. Prove that the function $f : G \to G$ given by $f(x) = x^{-1}$ sends each left H-coset to a right H-coset (i.e., for any left coset aH, the image $f(aH)$ is a right H-coset). Furthermore, show the induced map ϕ from the set of left H-cosets to the set of right H-cosets given by $\phi(aH) = f(aH)$ is a bijection.

As a result, we can define the index $[G : H]$ to be either the number of left H-cosets in G or the number of right H-cosets in G, as these are equal due to the above exercise.

11 Cartesian Products of Groups

In this section we review the Cartesian Product construction of a group. Let us start with two groups, G and H with operations $\cdot$ and $*$, respectively. Then we can define the Cartesian Product of G and H as sets by

$$G \times H = \{(g, h) : g \in G, h \in H\}.$$

To make this a group, we define a binary operation $\star$ on $G \times H$ as follows. For any $(g_1, h_1), (g_2, h_2) \in G \times H$ we define

$$(g_1, h_1) \star (g_2, h_2) = (g_1 \cdot g_2, h_1 * h_2).$$

This will turn out to be a group. So for example, $\mathbb{Z}_4 \times S_3$ would be a group where for any $i, j \in \mathbb{Z}_5$ and any $\sigma, \tau \in S_3$ and we would have $(i, \sigma) \star (j, \tau) = (i + j, \sigma\tau)$.

More generally, let J be an arbitrary (possibly finite or uncountably infinite) nonempty set and for every $j \in J$, let G_j be a group with binary operation $*_j$. Then we define the Cartesian Product $\Pi = \prod_{j \in J} G_j$ to be the set of functions $a : J \to \bigcup_{j \in J} G_j$ such that $a(j) = a_j \in G_j$. In addition, if $a, b \in \Pi = \prod_{j \in J} G_j$, we can define $a \star b$ to be the function $a \star b(j) = a_j *_j b_j$ for all $j \in J$. We now prove that Π is a group.

Proposition 26 *Let J be a nonempty set and for each $j \in J$, let G_j be a group. Then $\Pi = \prod_{j\in J} G_j$ is a group under the binary operation $\star$ defined above.*

Proof. First, we need to show that the binary operation $\star$ is well-defined, but this follows directly from the definition. To show associativity, note that for any $a, b, c \in \Pi$ and for any $j \in J$ we have

$$a\star(b\star c)(j) = a(j)*_j(b\star c)(j) = a(j)*_j(b(j)*_j c(j)) = (a(j)*_j b(j))*_j c(j) = (a\star b)(j)*_j c(j) = (a\star b)\star c(j),$$

so $a \star (b \star c) = (a \star b) \star c$.

Next, for each $j \in J$, let $e_j \in G_j$ be the identity element. Then we can define the function $e : J \to \bigcup_{j\in J} G_j$ by $e(j) = e_j$ for all $j \in J$. Then for any $a \in \Pi$ we have for each $j \in J$ that $a \star e(j) = a(j) *_j e_j = a(j) = e_j *_j a(j) = e \star a(j)$, hence $a \star e = a = e \star a$ and $e \in \Pi$ is the identity.

Finally, to show inverses, let $a \in \Pi$ and define $a' \in \Pi$ by letting $a'(j) = a(j)^{-1}$ for all $j \in J$. Then for each $j \in J$ we have $a\star a'(j) = a(j) *_j a(j)^{-1} = e_j = a(j)^{-1} *_j a(j) = (a'\star a)(j)$. Hence $a\star a' = e = a'\star a$, so a' is an inverse for a. Therefore, Π is a group under the $\star$ operation. ∎

Notation: If $\{G_j : j \in J\}$ is a set of groups with indexing set J, and $a \in \prod_{j\in J} G_j$, then we usually denote $a(j)$ by a_j. Furthermore, we will sometimes denote the function a by $(a_j)_{j\in J}$.

Example: (1) Let $G = \mathbb{Z}_4$ and $H = S_3$. Then $G \times H$ is a group of order 24 and for any $(i, \sigma), (j, \tau) \in \mathbb{Z}_4 \times S_3$ we have $(i, \sigma) \star (j, \tau) = (i + j, \sigma\tau)$. In particular, $(2, (1\ 2)) \star (3, (2\ 3)) = (2 + 3, (1\ 2)(2\ 3)) = (1, (1\ 2\ 3))$.
(2) If we let $J = \mathbb{R}$ and let G_j be the additive group $\mathbb{R}$ for all $j \in \mathbb{R}$, then $\mathcal{F} = \prod_{j\in\mathbb{R}} \mathbb{R}$ is the set of functions from $\mathbb{R}$ to $\mathbb{R}$. So for any $f, g \in \mathcal{F}$, we define $f + g$ to be the function given by $(f + g)(j) = f(j) + g(j)$ for all $j \in \mathbb{R}$.

Lemma 27 *Let J be a nonempty set and, for each $j \in J$ let G_j be a group with subgroup H_j. Then*

$$H = \prod_{j\in J} H_j = \left\{ a \in \prod_{j\in J} G_j : a(j) \in H_j \text{ for all } j \in J \right\}$$

is a subgroup of $G = \prod_{j\in J} G_j$.

Proof. Note that since H_j is a subgroup of G_j for all $j \in J$, $e_j \in H_j$ for all $j \in J$, hence $e \in H$. Furthermore, if $a, b \in H$, then $a(j), b(j) \in H_j$ for all $j \in J$. Hence $a(j)b(j)^{-1} \in H_j$ for all $j \in J$ by Proposition 9, so $ab^{-1} \in H$. Therefore, by Proposition 9, we have H is a subgroup of G. ∎

We note that not all subgroups of $\prod_{j\in J} G_j$ are of the above form. Indeed, consider the group $\mathbb{Z}_4\times\mathbb{Z}_2$. We have the cyclic subgroup $\langle(2, 1)\rangle = \{(0, 0), (2, 1)\}$ which is not of the given form. Still, using Lemma 27 we see that $\{0\} \times \mathbb{Z}_2$, $\mathbb{Z}_4 \times \{0\}$, $2\mathbb{Z}_4 \times \{0\}$, and $2\mathbb{Z}_4 \times \mathbb{Z}_2$ are all proper subgroups of $\mathbb{Z}_4 \times \mathbb{Z}_2$.

If J is a nonempty set and $\{G_j : j \in J\}$ is a set of groups, then we can define a subset of $\prod_{j\in J} G_j$ by

$$\coprod_{j\in J} G_j = \left\{ a \in \prod_{j\in J} G_j : a(j) = e_j \text{ for all but finitely many } j \in J \right\},$$

which we call the **coproduct** of the set $\{G_j : j \in J\}$. If J is a finite set, then the coproduct and the product are the same set, so we typically only consider the coproduct when J is infinite.

Lemma 28 *Let J be a nonempty set and let $\{G_j : j \in J\}$ be a set of groups. Then the coproduct $\coprod_{j\in J} G_j$ is a subgroup of the product $\prod_{j\in J} G_j$.*

Proof. Again, we use Proposition 9. First, it is clear that $e \in \coprod_{j\in J} G_j$, so the coproduct is nonempty. Next, let $a, b \in \coprod_{j\in J} G_j$. Define $J_a = \{j \in J : a(j) \neq e_j\}$, $J_b = \{j \in J : b(j) \neq e_j\}$ and $J_{ab^{-1}} = \{j \in J : a(j)b(j)^{-1} \neq e_j\}$. Clearly $J_{ab^{-1}} \subseteq J_a \cup J_b$. Since a and b are in the coproduct, both J_a and J_b are finite sets, hence $J_{ab^{-1}}$ is finite. Therefore $ab^{-1} \in \coprod_{j\in J} G_j$. So, by Proposition 9, $\coprod_{j\in J} G_j$ is a subgroup of $\prod_{j\in J} G_j$. ∎

12 Classifying Groups of Small Order

In this section, we look at classifying all groups of order 7 or smaller. It follows from Corollary 25 that any group of order 2, 3, 5, or 7 must be cyclic, hence isomorphic to $\mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_5$, or $\mathbb{Z}_7$, respectively. Therefore, we are left with considering the groups of order 4 and order 6.

Let us start with the groups of order 4. Let G be a group of order 4. By Exercise 25, the order of the elements in G are either 1, 2, or 4. Only the identity element e has order 1. If G has an element of order 4, then G must be cyclic, hence $G \cong \mathbb{Z}_4$. If G does not have an element of order 4, then G must have three distinct elements of order 2, say a, b, and c. By group cancellation, $ab \neq a$, $ab \neq b$, and since a has order 2, $e = aa$, hence $ab \neq aa = e$. Therefore, $ab = c$. By a similar argument, $ba = c$ as well. Hence if we define a bijective function $\phi : G \to \mathbb{Z}_2 \times \mathbb{Z}_2$ by

x	e	a	b	ab
$\phi(x)$	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$

it is not hard to check that ϕ is also a homomorphism, hence an isomorphism.

Next, we assume G is a group of order 6, but is not cyclic. (If G is cyclic, then $G \cong \mathbb{Z}_6$.) Therefore, the only orders an element of G can have are 1 (which is only the identity), 2, and 3. Assume G only has elements of order 2. Then for any two distinct elements $a, b \in G$ we have $e = (ab)^2$, so $(ab) = (ab)^{-1} = b^{-1}a^{-1} = ba$ and we get G must be abelian. Hence the set $\{e, a, b, ab\}$ is a subgroup of G of order 4, which contradicts Lagrange's Theorem. Therefore, G must contain an element of order 3, call it a. Then $a^2 = a^{-1} \neq a$ is another element of order 3. If G has an element $b \notin \langle a \rangle$ of order 3, then we have at least 5 distinct elements $\{e, a, a^2, b, b^2\} \subseteq G$. Now consider ab. Using group cancellation, we see that $ab \notin \{e, a, a^2, b, b^2\}$, hence is a new element. Similarly, $a^2b \notin \{e, a, a^2, b, b^2\}$ and $a^2b \neq ab$. Therefore, we now have 7 distinct elements in a group of order 6, which is a contradiction.

So we know that if G is not cyclic, then G has exactly two elements of order 3, which we have denoted as a and a^2. All of the other elements must have order 2. Let us label the remaining elements b, c, and d. Then ba must be either c or d. Let us choose $ba = c$. If $ab = c = ba$ as well, then c will be an element of order 6, which contradicts our assumption that G is not cyclic. Therefore, $ab = d$. So $ba^2 = d$ as well since all other possibilities lead to a contradiction using group cancellation. Similarly, $a^2b = c$. It then follows that G is generated by an element a of order 3 and an element b of order 2 such that $ba = a^2b$. Therefore, we can construct an isomorphism $\phi : G \to D_6$ where $\phi(a) = r$ and $\phi(b) = s$. Since $D_6 \cong S_3$, we get $G \cong S_3$.

We note that we had a choice of letting $ba = c$. One can ask, what happens if we let $ba = d$ instead? In this case, one can run the exact same argument with $ab = c = ba^2$ and $ba = d = a^2b$.

The next case to consider is groups of order 8. We will delay the proof of this classification until later. We have seen all the isomorphism types for groups of order 8 except for one known as the quaternion group, Q. We introduce this group now.

The **quaternion group** Q is the group of order 8 consisting of the set

$$Q = \{\mathbf{1}, -\mathbf{1}, \mathbf{i}, -\mathbf{i}, \mathbf{j}, -\mathbf{j}, \mathbf{k}, -\mathbf{k}\}$$

where we can view Q as a subgroup of $GL_2(\mathbb{C})$ given by letting

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

$$\mathbf{j} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, -\mathbf{j} = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \mathbf{k} = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}, -\mathbf{k} = \begin{bmatrix} 0 & -i \\ -i & 0 \end{bmatrix}.$$

Therefore, Q is a nonabelian group whose center is $\{\mathbf{1}, -\mathbf{1}\}$ and every element outside the center of Q has order 4.

We now give a table of isomorphism types of groups of order 15 or less. Like with groups of order 8, we delay the classification of groups of order 8 or more until we develop a few more tools.

Order	Isomorphism Types
1	$\{e\}$
2	$\mathbb{Z}_2$
3	$\mathbb{Z}_3$
4	$\mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_2$
5	$\mathbb{Z}_5$
6	$\mathbb{Z}_6$, S_3
7	$\mathbb{Z}_7$
8	$\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, D_8, Q
9	$\mathbb{Z}_9$, $\mathbb{Z}_3 \times \mathbb{Z}_3$
10	$\mathbb{Z}_{10}$, D_{10}
11	$\mathbb{Z}_{11}$
12	$\mathbb{Z}_{12}$, $\mathbb{Z}_6 \times \mathbb{Z}_2$, $\mathbb{Z}_4 \times \mathbb{Z}_3$, D_{12}, A_4
13	$\mathbb{Z}_{13}$
14	$\mathbb{Z}_{14}$, D_{14}
15	$\mathbb{Z}_{15}$

13 Normal Subgroups and Quotient Groups

In Section 10, we introduced the concept of right and left cosets of a given subgroup of a group. In this section we consider the question if we can define a binary operation on these sets of cosets to define a group that somehow relates to the original group we started with.

First, we start with an example. Consider the group homomorphism $\phi : \mathbb{Z}_2 \times \mathbb{Z}_4 \to \mathbb{Z}_2 \times \mathbb{Z}_2$ given by

$$\phi(i,j) = \begin{cases} (i,j) & \text{if } j = 0,1 \\ (i,j-2) & \text{if } j = 2,3 \end{cases}$$

One can check that ϕ is a homomorphism with kernel $H = \{(0,0),(0,2)\} = \{0\} \times 2\mathbb{Z}$, with cosets

$$H, \quad (1,0)+H, \quad (0,1)+H, \quad (1,1)+H.$$

Furthermore, one can check the inverse image or fiber $\phi^{-1}(i,k)$ of $(i,k) \in \mathbb{Z}_2 \times \mathbb{Z}_2$ is exactly the coset $(i,k)+H$. Therefore, since we have a one-to-one correspondence between the fibers of ϕ and the cosets of H, we can borrow the binary operation on the codomain $\mathbb{Z}_2 \times \mathbb{Z}_2$ to create a binary operation on the H-cosets in $\mathbb{Z}_2 \times \mathbb{Z}_4$. In particular, we define the sum of $(i,j)+H$ and $(i',j')+H$ to be the H-coset corresponding to the fiber of $\phi(i,j)+\phi(i',j') \in \mathbb{Z}_2 \times \mathbb{Z}_2$. This is a little roundabout, but can be visualized by the following diagram:

$$\begin{array}{ccc} ((i,j)+H)+((i',j')+H) & \longrightarrow & \phi(i,j)+\phi(i',j') \\ & & \downarrow \\ \phi^{-1}(k,\ell) & \longleftarrow & (k,\ell) = \phi(i,j)+\phi(i',j') \end{array}$$