ABSTRACT ALGEBRA
TOPIC 4: GROUPS

PAUL L. BAILEY

1. Groups

1.1. **Definition of a Group.** Abstract mathematical objects are typically defined in terms of an underlying set and some additional structure on that set. In the case of groups, the additional structure is a single binary operation which is associative and admits an identity and inverses. The operation could normally be denoted as addition, multiplication, composition, or various other symbols; however, it is convenient and conventional to denote the operation by multiplication when speaking of groups in general. Thus statements of definitions, propositions, remarks, and so forth which apply to all groups are stated in this way, and the reader is asked to translate to the notation appropriate in a given example.

Definition 1. A *group* is a set G together with a binary operation

$$\cdot : G \times G \to G$$

such that

(G1) $g_1(g_2g_3) = (g_1g_2)g_3$ for all $g_1, g_2, g_3 \in G$ (associativity);
(G2) $\exists 1 \in G$ such that $1 \cdot g = g \cdot 1 = g$ for all $g \in G$ (existence of an identity);
(G3) $\forall g \in G \, \exists g^{-1} \in G$ such that $gg^{-1} = g^{-1}g = 1$ (existence of inverses).

Let G be group. We say that G is *abelian* if

(G4) $g_1g_2 = g_2g_1$ for all $g_1, g_2 \in G$ (commutativity).

We may identify a group in the form $(G, *, e)$, indicating that G is the underlying set, $*$ is the binary operation, and e is the identity element. However, the underlying set and the identity can actually be recovered from the binary operation itself, so indicating G and e is a courtesy. On the other hand, it is conventional to write "let G be a group"; this indicates that G is the underlying set under consideration, and $\cdot : G \times G \to G$ is the associative binary operator with identity denoted by 1 and the inverse of g denoted by g^{-1}.

Remark 1. (Generalized Associativity)
Let A be a set with a multiplicative binary operation, and let $a_1, \ldots, a_n \in G$. Since the operation is binary, we inductively define product without parentheses as

$$a_1a_2 \cdots a_n = (a_1a_2 \cdots a_{n-1})a_n;$$

that is, multiply from left to right.

Let $r, n \in \mathbb{N}$ with $1 < r < n$, and let G be a group with $g_1, \ldots, g_n \in G$. Since G is a group, the operation is associative by **(G1)**, and induction shows that

$$(g_1g_2 \cdots g_r)(g_{r+1}g_{r+2} \cdots g_n) = g_1g_2 \ldots g_rg_{r+1}g_{r+2} \ldots g_n.$$

Date: March 13, 2007.

Remark 2. (Uniqueness of Identity)
Let G be a group and suppose that $e, f \in G$ such that $eg = ge = g$ and $fg = gf = g$ for every $g \in G$. Then $e = ef = f$, so $e = f$. Thus the element 1 from **(G2)** is unique, and is called the *identity* of the group.

Remark 3. (Uniqueness of Inverses)
Let G be a group and let $g \in G$. Suppose that $a, b \in G$ such that $ag = ga = 1$ and $bg = gb = 1$. Then $a = a(gb) = (ag)b = b$, so $a = b$. Thus in the presence of associativity, the element g^{-1} from **(G3)** is unique, and is called the *inverse* of g.

Remark 4. (Standard Notation)
Standard conventions for binary operations written multiplicatively and additively are in force. Let G be a group, $g \in G$, and $n \in \mathbb{Z}$.

If the operation is "dot" $(\cdot)$, it is usually referred to as "multiplication", and the $\cdot$ is dropped from the notation whenever convenient. Also:

- the identity is denoted by 1 and is called "one";
- the inverse of g is denoted by g^{-1} and is called "g inverse";
- for $n = 0$, $g^n = 1$;
- for $n > 0$, $g^n = g \cdots g$ (n times);
- for $n < 0$, $g^n = (g^{-1})^{-n}$.

If the operation is "plus" $(+)$, it is usually referred to as "addition", and is assumed to be commutative, that is, $g + h = h + g$ for all $g, h \in G$. Also:

- the identity is denoted by 0 and is called "zero";
- the inverse of g is denoted by $-a$ and is called "negative g";
- for $n = 0$, $ng = 0$;
- for $n > 0$, $ng = g + \cdots + g$ (n times);
- for $n < 0$, $ng = (-n)(-g)$.

A group under addition is called an *additive group*.

1.2. **Properties of Groups.** We now list several properties that are common to all groups, and are easily derived from the definition. We list these properties in multiplicative notation, and ask the reader to convert from to additive notation where appropriate.

Proposition 1. (Cancelation Laws)
Let G be a group and let $g, h, k \in G$. Then

(a) *$gh = gk \Rightarrow h = k$ (left cancelation);*
(b) *$hg = kg \Rightarrow h = k$ (right cancelation).*

Proof. Keep in mind that the operation is not necessarily commutative. For **(a)**, multiply on the left by g^{-1}; for **(b)**, multiply on the right by g^{-1}. □

Proposition 2. (Exponential Properties)
Let G be a group. Let $g, h \in G$ and $m, n \in \mathbb{Z}$. Then

(a) $1^{-1} = 1$;
(b) $(g^{-1})^{-1} = g$;
(c) $(gh)^{-1} = h^{-1}g^{-1}$;
(d) $(g^n)^{-1} = g^{-n}$;
(e) $g^m g^n = g^{m+n}$;
(f) $(g^m)^n = g^{mn}$.

1.3. **Examples of Groups.** Understanding the theory of groups requires copious examples, and we give several now. The reader should keep these examples in mind throughout the course of the development of the general theory.

Example 1. The following are standard additive groups.

- $(\mathbb{Z}, +, 0)$, the integers under addition;
- $(\mathbb{Q}, +, 0)$, the rational numbers under addition;
- $(\mathbb{R}, +, 0)$, the real numbers under addition;
- $(\mathbb{C}, +, 0)$, the complex numbers under addition;

In each case, inverses are negatives. All additive groups are assumed be to abelian.

Example 2. Let n be a positive integer, and let $\mathbb{R}^n$ denote the set of ordered n-tuples of real numbers. Then $(\mathbb{R}^n, +, \vec{0})$ is an abelian group under vector addition, where $\vec{0}$ denotes the zero vector.

Example 3. Let M be a set admitting an associative binary operation with identity, and define

$$M^* = \{a \in M \mid a \text{ is invertible}\}.$$

Then M^* is a group. For example, standard sets produce these groups.

- $(\mathbb{Z}^*, \cdot, 1)$, the invertible integers under multiplication ($\mathbb{Z}^* = \{\pm 1\}$);
- $(\mathbb{Q}^*, \cdot, 1)$, the nonzero rational numbers under multiplication;
- $(\mathbb{R}^*, \cdot, 1)$, the nonzero real numbers under multiplication;
- $(\mathbb{C}^*, \cdot, 1)$, the nonzero complex numbers under multiplication.

In each case, inverses are reciprocals. Multiplicative groups are not assumed to be abelian, although these are abelian.

Example 4. Let $\mathbb{Z}_n$ denote the set of residues class modulo n. The set $\mathbb{Z}_n$ is a group under addition, with $\overline{0}$ the identity and $\overline{n-a}$ the inverse of $\overline{a}$. This abelian group contains n elements.

Example 5. Let $\mathbb{Z}_n^* = \{\overline{a} \in \mathbb{Z}_n \mid \gcd(a, n) = 1\}$. Then $\mathbb{Z}_n^*$ is a group under multiplication, with identity $\overline{1}$. The inverse of $\overline{a} \in \mathbb{Z}_n^*$ is $\overline{x}$, given from the Euclidean algorithm equation $ax + ny = 1$. This abelian group contains $\phi(n)$ elements.

Example 6. Let $\mathbb{U} = \{z \in \mathbb{C} \mid |z| = 1\}$ denote the unit circle in the complex plane. Then $\mathbb{U}$ is a group under multiplication. The set $\mathbb{U}$ is the image of the function

$$\operatorname{cis} : \mathbb{R} \to \mathbb{C} \quad \text{given by} \quad \operatorname{cis}\theta = \cos\theta + i\sin\theta.$$

Let $z_1, z_2 \in \mathbb{U}$. Then $z_1 = \operatorname{cis}\theta_1$ and $z_2 = \operatorname{cis}\theta_2$ for some $\theta_1, \theta_2 \in \mathbb{R}$. Using trigonometry, we have $z_1 z_2 = (\operatorname{cis}\theta_1)(\operatorname{cis}\theta_2) = \operatorname{cis}(\theta_1 + \theta_2)$. In particular,

$$\operatorname{cis}^n \theta = \operatorname{cis} n\theta.$$

Let $\mathbb{U}_n = \{\operatorname{cis}(2\pi k/n) \mid k \in \mathbb{Z}\}$. Then $\mathbb{U}_n$ is a group under multiplication containing n elements. Its elements are exactly the n^{th} roots of unity.

Example 7. Let X be a set, and set $\operatorname{Sym}(X) = \{f : X \to X \mid f \text{ is bijective}\}$. Then $(\operatorname{Sym}(X), \circ, \mathrm{id}_X)$ is a nonabelian group under composition of functions, where $\mathrm{id}_X : X \to X$ is the identity function given by $\mathrm{id}_X(x) = x$.

Example 8. Let $X = \{1, \ldots, n\}$, and set $S_n = \operatorname{Sym}(X)$. Let $\epsilon = \mathrm{id}_X$, and write composition of functions multiplicatively. Then $(S_n, \cdot, \epsilon)$ is a nonabelian group containing $n!$ elements.

Example 9. Let $\mathcal{M}_{m\times n}(\mathbb{R})$ be the set of $m \times n$ matrices over the real numbers. Then $\mathcal{M}_{m\times n}(\mathbb{R})$ is an abelian group under matrix addition. The identity is the zero $m \times n$ matrix.

Example 10. Let $\mathbf{GL}_n(\mathbb{R})$ be the set of invertible $n \times n$ matrices over the real numbers. Then $\mathbf{GL}_n(\mathbb{R})$ is a nonabelian group under matrix multiplication. The identity is the identity $n \times n$ matrix. Note that $\mathbf{GL}_n(\mathbb{R}) = (\mathcal{M}_{n\times n}(\mathbb{R}))^*$.

Example 11. Let X be a set, and let $\mathcal{P}(X)$ denote the power set of X, which is the set of all subsets of X. If $A, B \subset X$, define the *symmetric difference* of A and B to be $A\triangle B$, given by

$$A\triangle B = (A \cup B) \smallsetminus (A \cap B);$$

Then $(\mathcal{P}(X), \triangle, \varnothing)$ is a group under symmetric difference. The identity is $\varnothing$, and the inverse of $A \in \mathcal{P}(X)$ is itself.

The next example can be used to show that $(\mathcal{P}(X), \triangle, \varnothing)$ is abelian.

Example 12. Let G be a group such that $g^2 = 1$ for every $g \in G$.
Show that G is abelian.

Solution. Let $g, h \in G$. Since $g^2 = 1$, multiplying both sides by g^{-1} gives $g = g^{-1}$. Similarly, $h = h^{-1}$.

Now $(gh)^2 = 1$, whence $gh = (gh)^{-1} = h^{-1}g^{-1} = hg$. Thus G is abelian. □

Definition 2. Let H and K be groups, written multiplicatively. The *product* of H and K is the set $G = H \times K$, together with multiplication defined by

$$(h_1, k_1)(h_2, k_2) = (h_1h_2, k_1k_2).$$

We we are working with two groups G and H written multiplicatively, we may distinguish the identity elements as 1_G and 1_H, respectively.

Proposition 3. *Let H and K be groups. Then $H \times K$ is a group.*

Proof. We verify the three properties of being a group.

(G1) Let $g_1, g_2, g_3 \in G$. Then there exist $h_1, h_2, h_3 \in H$ and $k_1, k_2, k_3 \in K$ such that $g_1 = (h_1, k_1)$, $g_2 = (h_2, k_2)$, and $g_3 = (h_3, k_3)$. Then

$$\begin{aligned}
(g_1g_2)g_3 &= ((h_1, k_1)(h_2, k_2))(h_3, k_3) && \text{by definition of the set } H \times K\\
&= ((h_1h_2)h_3, (k_1k_2)k_3) && \text{by definition of the operation on } H \times K\\
&= (h_1(h_2h_3), k_1(k_2k_3)) && \text{by associativity in } H \text{ and } K\\
&= (h_1, k_1)((h_2, k_2)(h_3, k_3)) && \text{by definition of the operation on } H \times K\\
&= g_1(g_2g_3) && \text{by definition of the set } H \times K.
\end{aligned}$$

(G2) The identity for $H \times K$ is $1_G = (1_H, 1_K)$. To verify this, let $g \in G$ so that $g = (h, k)$ for some $h \in H$ and $k \in K$. Then

$$g \cdot 1_G = (h, k)(1_H, 1_K) = (h \cdot 1_H, k \cdot 1_K) = (h, k) = g;$$
$$1_G \cdot g = (1_H, 1_K)(h, k) = (1_H \cdot h, 1_K \cdot k) = (h, k) = g.$$

(G3) Let $g \in G$, so that there exist $h \in H$ and $k \in K$ with $g = (h, k)$. Then $g^{-1} = (h^{-1}, k^{-1})$, since

$$(h, k)(h^{-1}, k^{-1}) = (hh^{-1}, kk^{-1}) = (1_H, 1_K) = 1_G;$$
$$(h^{-1}, k^{-1})(h, k) = (h^{-1}h, k^{-1}k) = (1_H, 1_K) = 1_G.$$

□

1.4. **Cayley Tables.** If A is a set with a binary operation, we can list this binary operation explicitly in a table. The elements of the set are listed vertically on the left and horizontally across the top to label the rows and columns. If a row is labeled a and a column is labeled b, the entry in this row and column is ab. This is called a *Cayley table*. Such a table defines the operation, and if the tables asserts that the operation satisfies the three group laws, then the table defines a group. Of course, this is only practical for relatively small groups.

Example 13. Let $K = \{e, a, b, c\}$. Define multiplication on K by

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Then K is a *Klein four* group; it is abelian.

Example 14. Let $Q = \{\pm 1, \pm i, \pm j, \pm k\}$. Define multiplication on Q by

$\cdot$	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	-1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	-1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	-1	1
k	$-k$	k	$-j$	j	i	$-i$	1	-1

Then Q is a *quaternion* group, which is nonabelian and satisfies

$$i^2 = j^2 = k^2 = -1, ij = k, jk = i, ki = j.$$

Example 15. We produce the Cayley table for $S_3 = \mathrm{Sym}(\{1, 2, 3\})$. This is a group with $3! = 6$ elements, and these elements are

$$S_3 = \{\epsilon, \texttt{(1 2 3)}, \texttt{(1 3 2)}, \texttt{(1 2)}, \texttt{(1 3)}, \texttt{(2 3)}\}.$$

Use cycle multiplication to determine products, such as `(1 2 3)(1 2)` = `(1 3)`.

$\cdot$	ϵ	`(1 2 3)`	`(1 3 2)`	`(1 2)`	`(1 3)`	`(2 3)`
`(1 2 3)`	`(1 2 3)`	`(1 3 2)`	ϵ	`(1 3)`	`(2 3)`	`(1 2)`
`(1 3 2)`	`(1 3 2)`	ϵ	`(1 2 3)`	`(2 3)`	`(1 2)`	`(1 3)`
`(1 2)`	`(1 2)`	`(2 3)`	`(1 3)`	ϵ	`(1 2 3)`	`(1 3 2)`
`(1 3)`	`(1 3)`	`(1 2)`	`(2 3)`	`(1 2 3)`	ϵ	`(1 3 2)`
`(2 3)`	`(2 3)`	`(1 3)`	`(1 2)`	`(1 3 2)`	`(1 2 3)`	ϵ

2. Subgroups

2.1. **Definition of Subgroup.** Every abstract mathematical object admits subobjects; in the case of groups, the subobjects are called subgroups, which are merely subsets of the original set which are themselves groups. The definition is designed to make proving a subset is a subgroup more transparent.

Definition 3. Let G be a group and let $H \subset G$.

We say that H is a *subgroup* of G, and write $H \leq G$, if

(S0) H is nonempty;
(S1) $h_1, h_2 \in H \Rightarrow h_1 h_2 \in H$;
(S2) $h \in H \Rightarrow h^{-1} \in H$.

Remark 5. (Subgroups are Groups)
These are exactly the conditions guaranteeing that a subgroup is a subset which is itself a group under the same binary operation. Conditions **(S1)** says that the operation is closed, that is, the restriction of the function $\cdot : G \times G \to G$ to $H \times H$ produces a function defined on $H \times H$, and **(S1)** ensures that the image of this function is contained in H, so we have an operation $\cdot : H \times H \to H$. Certainly, since the operation is the same, the associativity of this operation is inherited.

Condition **(S2)** says that the subset contains inverses. Finally, we note that, in the presence of **(S1)** and **(S2)**, property **(S0)** is equivalent to

(SO) $1 \in H$.

Indeed, if $1 \in H$, then H is nonempty. On the other hand, if H is nonempty, then H contains some element, say $h \in H$. Then $h^{-1} \in H$ by **(S2)**, so $1 = hh^{-1} \in H$ by **(S1)**.

Proposition 4. *Let G be a group and let $H \subset G$. Then $H \leq G$ if and only if*

(S0) *H is nonempty;*
(SI) $h_1, h_2 \in H \Rightarrow h_1 h_2^{-1} \in H$.

Proof.

($\Rightarrow$) Suppose $H \leq G$. Then H satisfies **(S0)** by hypothesis, and **(SI)** is an immediate combination of **(S1)** and **(S2)**.

($\Leftarrow$) Suppose that H satisfies **(S0)** and **(SI)**. Since H is nonempty, let $h \in H$; then $hh^{-1} = 1 \in H$. Thus $1 \cdot h^{-1} = h^{-1} \in H$, so H satisfies **(S2)**.

Let $h_1, h_2 \in H$. Then $h_1 (h_2^{-1})^{-1} = h_1 h_2 \in H$, so H satisfies **(S1)**. □

Proposition 5. *Let G be a group and let $H \subset G$. Then $H \leq G$ if*

(S0) *H is nonempty;*
(S1) $h_1, h_2 \in H \Rightarrow h_1 h_2 \in H$;
(SF) *H is finite.*

Proof. It suffices to show that in the presence of properties **(S0)** and **(S1)**, property **(SF)** implies property **(S2)**.

By **(S0)**, H is nonempty, so let $h \in H$. Let A be the subset of G given by $A = \{h^n \mid n \in \mathbb{N}\}$. By **(S1)**, $A \subset H$, so by **(SF)**, A is finite. Thus $h^n = h^m$ for some $m < n$. Thus $h^{n-m} = h^n (hm)^{-1} = 1$. Therefore $h^{n-m-1} h = 1$, so $h^{-1} = h^{n-m-1} \in A \subset H$, and H satisfies **(S2)**. □

2.2. **Examples of Subgroups.** We now list examples of subgroups; some examples apply to specific groups, whereas others are general principles, in the sense that certain types of subgroups appear in every group.

Example 16. Let G be a group. Then $\{1\} \leq G$ and $G \leq G$.

Definition 4. Let G be a group and let $H \leq G$. We say that H is *proper* is $H \neq G$, and we say that H is *trivial* if $H = \{1\}$.

We are often interested in proper nontrivial subgroups.

Example 17. The groups $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ are subgroups of $\mathbb{C}$ under addition. The groups $\mathbb{Q}^*, \mathbb{R}^*, \mathbb{U}$ are subgroups of $\mathbb{C}^*$ under multiplication.

Example 18. The groups $\mathbb{U}_n$ are subgroups of $\mathbb{U}$ under multiplication. If m and n are positive integers, $\mathbb{U}_m \leq \mathbb{U}_n$ if and only if $m \mid n$.

Example 19. Let $n \in \mathbb{Z}$ and set

$$n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}.$$

Thus $n\mathbb{Z}$ is a subgroup of $\mathbb{Z}$ under addition.

Given two subgroups of a group G, we can form a new subgroup of G by taking the intersection.

Proposition 6. *Let G be a group and let $H, K \leq G$. Then $H \cap K \leq G$.*

Proof. We verify properties **(S0)**, **(S1)**, and **(S2)**.

(S0) Since $H, K \leq G$, we have $1 \in H$ and $1 \in K$. Thus $1 \in H \cap K$.

(S1) Let $a, b \in H \cap K$. Then $a, b \in H$ and $a, b \in K$, Since H and K are closed under multiplication, $ab \in H$ and $ab \in K$. Thus $ab \in H \cap K$.

(S2) Let $a \in H \cap K$. Then $a \in H$ and $a \in K$. Since H and K are closed under inverses, $a^{-1} \in H$ and $a^{-1} \in K$. Thus $a^{-1} \in H \cap K$. □

If G is a group, the intersection of any number of subgroups of G is itself a subgroup; this generalizes the last proposition.

Proposition 7. *Let G be a group and let $\mathcal{H}$ be a nonempty collection of subgroups of G. Then $\cap\mathcal{H}$ is a subgroup of G.*

Proof. Since $1 \in H$ for every $H \in \mathcal{H}$, we see that $1 \in \cap\mathcal{H}$. Let $h_1, h_2 \in \cap\mathcal{H}$. Then $h_1, h_2 \in H$ for every $H \in \mathcal{H}$. Then $h_1 h_2^{-1} \in H$ for every $H \in \mathcal{H}$ because each H is a subgroup. Thus $h_1 h_2^{-1} \cap \mathcal{H}$. Therefore $\cap\mathcal{H} \leq G$. □

Example 20. Let $m, n \in \mathbb{Z}$ and let $d = \gcd(m, n)$.
Then $d\mathbb{Z} = m\mathbb{Z} \cap n\mathbb{Z}$, so $d\mathbb{Z} \leq m\mathbb{Z}$ and $d\mathbb{Z} \leq n\mathbb{Z}$.

Given a group G and an element $g \in G$, we can construct the smallest subgroup of G which contains g.

Proposition 8. *Let G be a group and let $g \in G$. Set*

$$\langle g \rangle = \{g^k \mid k \in \mathbb{Z}\}.$$

Then $\langle g \rangle \leq G$.

Proof. Since $1 = g^0$, $1 \in \langle g \rangle$. If $g^m, g^n \in \langle g \rangle$, then $g^m g^n = g^{m+m} \in \langle g \rangle$. Finally, if $g^m \in \langle g \rangle$, then $(g^m)^{-1} = g^{-m} \in \langle g \rangle$. This verifies properties **(S0)**, **(S1)**, and **(S2)**. □

2.3. **Subgroups of S_n.** Small nonabelian groups are most conveniently realized as subgroups of S_n, and are often written in terms of one or two elements of the group, where every other element of the group is a product of these.

Example 21. The *symmetric group on n points* is S_n.

Example 22. The *cyclic group on n points*, denoted C_n, is the smallest subgroup of S_n containing the cycle $\rho =$ `(1 2 ...n)`; it consists of all powers of ρ, so

$$C_n = \{\epsilon, \rho, \rho^2, \ldots, \rho^{n-1}\}.$$

For example,

- $C_2 = \{\epsilon, $`(1 2)`$\}$;
- $C_3 = \{\epsilon, $`(1 2 3)`$, $`(1 3 2)`$\}$;
- $C_4 = \{\epsilon, $`(1 2 3 4)`$, $`(1 3)(2 4)`$, $`(1 4 3 2)`$\}$.

Example 23. View the group S_3 as the set of rigid motions of a regular triangle. Label the vertices `1`, `2`, and `3`. One rotation of the triangle is the permutation $\rho =$ `(1 2 3)`; then $\rho^2 =$ `(1 3 2)` and ρ^3 is the identity ϵ. If we let τ denote reflection across the line through vertex `1` and the midpoint of the opposite side, then $\tau =$ `(2 3)`. Then

$$S_3 = \{\epsilon, \rho, \rho^2, \tau, \tau\rho, \tau\rho^2\},$$

and we compute its Cayley table using the fact that $\rho\tau = \tau\rho^2$.

$\cdot$	ϵ	ρ	ρ^2	τ	$\tau\rho$	$\tau\rho^2$
ϵ	ϵ	ρ	ρ^2	τ	$\tau\rho$	$\tau\rho^2$
ρ	ρ	ρ^2	ϵ	$\tau\rho^2$	τ	$\tau\rho$
ρ^2	ρ^2	ϵ	ρ	$\tau\rho$	$\tau\rho^2$	τ
τ	τ	$\tau\rho$	$\tau\rho^2$	ϵ	ρ	ρ^2
$\tau\rho$	$\tau\rho$	$\tau\rho^2$	τ	ρ^2	ϵ	ρ
$\tau\rho^2$	$\tau\rho^2$	τ	$\tau\rho$	ρ	ρ^2	ϵ

Example 24. Let D_4 denote the set of rigid motions of a square. We label the vertices `1`, `2`, `3`, and `4` to realize D_4 as a subgroup of S_4. Let $\rho =$ `(1 2 3 4)` be rotation by 90°, and let $\tau =$ `(2 4)` be reflection across the line through `1` and `3`. Then $\rho^2 =$ `(1,3)(2,4)`, $\rho^3 =$ `(1 4 3 2)`, $\tau\rho =$ `(1 4)`(23), $\tau\rho^2 =$ `(1 3)`, and $\tau\rho^3 =$ `(1 2)(3 4)`. Then

$$D_4 = \{\epsilon, \rho, \rho^2, \rho^3, \tau, \tau\rho, \tau\rho^2, \tau\rho^3\}.$$

One may use the fact that ρ^2 commutes with every element of D_4, and that $\tau\rho = \rho^3\tau$ to compute the entire Cayley table of D_4.

Example 25. The *dihedral group on n points*, denoted D_n, the subgroup of S_n containing $2n$ elements which represents the set of rigid motions of a regular n-gon. If $\rho =$ `(1 2 ... n)` is rotation and τ is reflection through the line contain vertex `1`, then

$$D_n = \{\epsilon, \rho, \rho^2, \ldots, \rho^{n-1}, \tau, \tau\rho, \tau\rho^2, \ldots, \tau\rho^{n-1}\}.$$

In the case $n = 3$, we have $S_3 = D_3$; for larger n, D_n is a proper subgroup of S_n.

Example 26. The *alternating group on n points*, denoted A_n, is the smallest subgroup of S_n which contains all of the three-cycles. For example, $A_3 = C_3$, and

$$A_4 = \{\epsilon, \texttt{(1 2 3)}, \texttt{(1 3 2)}, \texttt{(1 2 4)}, \texttt{(1 4 2)}, \texttt{(2 3 4)}, \texttt{(2 4 3)},$$
$$\texttt{(1 2)(3 4)}, \texttt{(1 3)(2 4)}, \texttt{(1 4)(2 3)}\}.$$

3. Cyclic Groups

3.1. **Definition of Cyclic Group.** A cyclic group is a group generated by a single element. In multiplication notation, this means that every element in the group is a power of the generator; in additive notation, this means that every element in the group is a multiple of the generator.

Definition 5. Let G be a group. We say that G is *cyclic* if there exists $g \in G$ such that $G = \langle g \rangle$. In this case, we say that g *generates* G.

Example 27. The integers $\mathbb{Z}$ form a cyclic group; since every element of $\mathbb{Z}$ is a multiple of 1, 1 is a generator, so $\mathbb{Z} = \langle 1 \rangle$. Note the -1 is the only other generator.

Example 28. The modular integers $\mathbb{Z}_n$ for a cyclic group generated by $\overline{1}$.

Example 29. Let $\zeta = \text{cis}(2\pi/n)$. Then $\mathbb{U}_n = \langle \zeta \rangle$.

Example 30. Let $\rho = \texttt{(1 2 3)} \in S_3$, so that $\rho^2 = \texttt{(1 3 2)}$. Let $C_3 = \{\epsilon, \rho, \rho^2\}$. Then $C_3 \leq S_3$, and $C_3 = \langle \rho \rangle = \langle \rho^2 \rangle$.

The last three examples are examples of finite cyclic groups; the name "cyclic" comes from this case. Note that if G is a group and $g \in G$. then $\langle g \rangle$ is a subgroup of G which is cyclic, known as the *cyclic subgroup generated by* g.

Example 31. Consider the group $\mathbb{Z}$ under addition. Then $\langle 2 \rangle = 2\mathbb{Z}$, the set of even integers.

Example 32. Let $\zeta \in \mathbb{C}^*$ be given by $\zeta = \text{cis}(2\pi/30)$. Then $\langle \zeta \rangle \leq \mathbb{C}^*$ is $\langle \zeta \rangle = \mathbb{U}_{30}$. Now $\zeta^6 \in \mathbb{U}_{30}$, and $\langle \zeta^6 \rangle \leq \mathbb{U}_{30}$ is $\langle \text{cis}(2\pi/5) \rangle = \mathbb{U}_5$.

Proposition 9. *Let G be a cyclic group. Then G is abelian.*

Proof. Since G is cyclic, $G = \langle g \rangle$ for some $g \in G$. Then any element in G is of the form g^n for some $n \in \mathbb{Z}$. Thus if $i, j \in \mathbb{Z}$, then g^i and g^j are two arbitrary elements of G. Clearly, $g^i g^j = gg...g$ (i+j times) $= g^j g^i$. □

Proposition 10. *Let G be a cyclic group and let $H \leq G$. Then H is cyclic.*

Proof. Let g be a generator for G. Then every element in G is of the form g^k for some $k \in \mathbb{Z}$.

If H is trivial, then $H = \langle 1 \rangle$ is cyclic. Suppose that H is nontrivial and let $h \in H \setminus \{1\}$. Then $h = g^k$ for some $k \in \mathbb{Z}$. If $k < 0$, then $h^{-1} = g^{-k} \in H$; thus H contains an element of the form g^k where k is a positive integer.

Let k be the smallest positive integer such that $g^k \in H$. Let $h \in H$; then $h = g^l$ for some $l \in \mathbb{Z}$. There exist unique $q, r \in \mathbb{Z}$ such that $l = kq + r$ where $0 \leq r < k$. Then

$$h = g^l = g^{kq+r} = (g^k)^q g^r.$$

Since $g^k \in H$, we have $g^r \in H$. But r is nonnegative and less then k, so we must have $r = 0$. Thus $h = (g^k)^q$, which proves that $H = \langle g^k \rangle$. □

Proposition 11. *Let G be a group. Then G is the union of cyclic groups.*

Proof. Let G be a group. Then $\langle g \rangle \leq G$ for any $g \in G$ so that $G = \cup_{g \in G} \langle g \rangle$. □

3.2. **Order of an Element.** The order of an element is the length of the cycle it creates when it is multiplied by itself. It is possible that the order is infinite, in which case there really is not a cycle; otherwise, however, powers of the element eventually loop back on themselves, thus creating a cycle of a given length.

Definition 6. Let $g \in G$. The *order of* g, denoted $\text{ord}(g)$, is the smallest positive integer $n \in \mathbb{Z}$ such that $g^n = 1$, if such an integer exists; otherwise, $\text{ord}(g) = \infty$. An *exponent* of g is any positive integer $k \in \mathbb{N}$ such that $g^k = 1$.

Proposition 12. *Let G be a group and let $g \in G$ with $\text{ord}(g) = n < \infty$. Then*

(a) *$i, j \in \{0, \ldots, n-1\}$ and $g^i = g^j \Rightarrow i = j$;*
(b) *$\langle g \rangle = \{1, g, g^2, \ldots, g^{n-1}\}$;*
(c) *$|\langle g \rangle| = \text{ord}(g)$;*
(d) *$|G| = \text{ord}(g)$ if and only if $G = \langle g \rangle$.*

Proof. Let $i, j \in \mathbb{N}$ with $0 \leq i \leq j < n$. Suppose that $g^i = g^j$. Then $g^{j-i} = 1$, and $j - i$ is a nonnegative integer. But $j - i < n$, and n is the smallest positive integer such that $g^n = 1$. Thus $j = i$. This shows that $\{1, g, g^2, \ldots, g^{n-1}\} \subset \langle g \rangle$ is a collection of n distinct elements. If $k \geq n$, then there exist unique integers $q, r \in \mathbb{Z}$ such that $k = nq + r$ with $0 \leq r < n$. Now $g^k = g^{nq+r} = (g^n)^q g^r = 1^q \cdot g^r = g^r$; this shows that $1, g, \ldots, g^{n-1}$ is a complete list of the elements in $\langle g \rangle$, and $|\langle g \rangle| = \text{ord}(g)$.

If $|G| = \text{ord}(g)$; since $\langle g \rangle \leq G$ and $|\langle g \rangle| = \text{ord}(g)$, we see that $G = \langle g \rangle$. On the other hand, we have already seen that if $G = \langle g \rangle$, then $|G| = \text{ord}(g)$. □

Proposition 13. *Let G be a group and let $g \in G$ with $\text{ord}(g) = n < \infty$. Let $m \in \mathbb{Z}$. Then*

$$g^m = 1 \quad \Leftrightarrow \quad n \mid m.$$

Proof. Suppose that $g^m = 1$. There exist unique integer $q, r \in \mathbb{Z}$ with $0 \leq r < n$ such that $m = nq + r$. Then

$$g^m = g^{nq+r} = g^{nq} g^r = (g^n)^q g^r = 1^q \cdot g^r = g^r.$$

But r is nonnegative and less than n; since n is the smallest positive integer such that $g^n = 1$, we must have $r = 0$. Conversely, suppose that n divides m. Then $m = qn$ for some $q \in \mathbb{Z}$, so $g^m = g^{qn} = (g^n)^q = 1^q = 1$. □

Proposition 14. *Let G be a group and let $g \in G$ with $\text{ord}(g) = n < \infty$. Let $m \in \mathbb{Z}$. Then $\langle g \rangle = \langle g^m \rangle$ if and only if $\gcd(m, n) = 1$.*

Proof. There exist unique integers $q, r \in \mathbb{Z}$ such that $m = qn + r$ with $0 \leq r < n$. Since $g^n = 1$, we see that $g^m = g^r$. Without loss of generality, assume that $0 < m < n$.

Suppose that $\gcd(m, n) = d > 1$. Then $m = kd$ and $n = ld$ for some integers $k, l > 1$. Then $(g^m)^l = g^{nk} = 1$, so $\text{ord}(g^m) < n$, which shows that $\langle g^m \rangle$ is properly contained in $\langle g \rangle$.

Suppose that $\gcd(m, n) = 1$. Then there exist $x, y \in \mathbb{Z}$ such that $mx + ny = 1$. Let g^k be an arbitrary member of $\langle g \rangle$. Then $g^k = g^{(mx+ny)k} = g^{mxk} g^{nyk} = g^{mxk}$. This shows that $\langle g \rangle \subset \langle g^m \rangle$. The opposite inclusion is obvious, so $\langle g \rangle = \langle g^m \rangle$. □

Proposition 15. *Let G be a group and let $g \in G$ with $\text{ord}(g) = n < \infty$. Let $d, m \in \mathbb{Z}$ be positive with $d = \gcd(m, n)$. Then $\text{ord}(g^m) = \frac{n}{d}$.*

Proof. Exercise. □

Proposition 16. *Let G be a cyclic group with $|G| = n < \infty$.*

(a) *If $H \leq G$, then $|H|$ divides $|G|$.*

(b) *If $d \mid n$, then there exists a unique subgroup $H \leq G$ such that $|H| = d$.*

Proof. Let g be a generator for G; then $\text{ord}(g) = n$.

Let $H \leq G$. Then H is cyclic, so $H = \langle h \rangle$ for some $h \in G$. Since G is cyclic, $h = g^m$ for integer m with $0 \leq m \leq n$. Let $k = \text{ord}(g^m)$; we have seen that k divides $n = |G|$. This proves **(a)**.

Suppose that $d \mid n$; then $n = dk$ for some $k \in \mathbb{N}$. Let $l = \text{ord}(g^k)$. Then $(g^k)^d = g^n = 1$, so l divides d. If $\text{ord}(g^k) = l$, then $g^{kl} = (g^k)^l = 1$, so n divides kl. Thus d divides l, so $l = d$. Thus $\langle g^k \rangle$ is a subgroup of G of order d.

To see that this subgroup is unique, let H be a subgroup of G of order d. Then H is cyclic, so $H = \langle g^m \rangle$ for some integer m with $0 \leq m < n$. Then $\text{ord}(g^m) = d$ so that $g^{md} = 1$; thus n divides md, that is, k divides m. Thus $g^m \in \langle g^k \rangle$, and since both groups have order d, we see that $\langle g^m \rangle = \langle g^k \rangle$. □

Proposition 17. *Let G be a group and let $h, k \in G$ be elements of finite order. Suppose that* $\gcd(\text{ord}(h), \text{ord}(k)) = 1$. *Then $\langle h \rangle \cap \langle k \rangle = \{1\}$.*

Proof. Let $g \in \langle h \rangle \cap \langle k \rangle$. Then $\text{ord}(g) | \text{ord}(h)$ and $\text{ord}(g) | \text{ord}(k)$, so that $\text{ord}(g)$ divides $\gcd(\text{ord}(h), \text{ord}(k)) = 1$. Therefore $\text{ord}(g) = 1$, so $g = 1$. □

3.3. **Order of Commuting Elements.** If two element do not commute, it is difficult to predict the order of the product. There are groups containing two element of order two whose product has infinite order. However, if the elements commute, we can predict the order of the product with some accuracy.

Definition 7. Let G be a group and let $h, k \in G$. We say that h and k *commute* if $hk = kh$. We synonymously say that h *centralizes* h or k *centralizes* h.

Proposition 18. *Let G be a group and let $h, k \in G$ be elements of finite order which commute. Suppose that $\langle h \rangle \cap \langle k \rangle = \{1\}$.*
Then $\text{ord}(hk) = \text{lcm}(\text{ord}(h), \text{ord}(k))$.

Proof. Exercise. □

Proposition 19. *Let G be a group and let $h, k \in G$ be elements of finite order which commute. Suppose that* $\gcd(\text{ord}(h), \text{ord}(k)) = 1$.
Then $\text{ord}(hk) = \text{ord}(h)\text{ord}(k)$.

Proof. Since the orders of h and k are relatively prime, their cyclic subgroups intersect trivially. Then $\text{ord}(hk) = \text{lcm}(\text{ord}(h), \text{ord}(k)) = \text{ord}(h)\text{ord}(k)$. □

4. Homomorphisms

4.1. **Definition of Homomorphism.** Abstract mathematics consists of the study of objects with certain structures, and the functions between them that in some way preserve these structures. For example, given two ordered sets, we may wish to understand the increasing or decreasing functions between them. In the case of groups, the structure is the binary operation, and the functions preserving that structure are called homomorphisms.

Definition 8. Let G and H be a groups. A *group homomorphism* from G to H is a function $\phi : G \to H$ such that

$$\phi(g_1 g_2) = \phi(g_1)\phi(g_2) \text{ for any } g_1, g_2 \in G.$$

Proposition 20. *Let $\phi : G \to H$ be a homomorphism. Then*

- **(a)** $\phi(1_G) = 1_H$*;*
- **(b)** $\phi(g^{-1}) = \phi(g)^{-1}$ *for every $g \in G$;*
- **(c)** $\phi(g^n) = \phi(g)^n$ *for every $g \in G$ and $n \in \mathbb{Z}$.*

Proof. We have $\phi(1_G) = \phi(1_G \cdot 1_G) = \phi(1_G)\phi(1_G)$. Multiplying both sides by $\phi(1_G)^{-1}$ in H, we have $1_H = \phi(1_G)$.

Let $g \in G$. Then $1_H = \phi(1_G) = \phi(g^{-1}g) = \phi(g)\phi(g^{-1})$. Multiplying both sides by $\phi(g)^{-1}$ in H yields $\phi(g)^{-1} = \phi(g^{-1})$.

If $n > 0$, **(c)** follows from the definition of homomorphism by induction. Combine this with **(a)** and **(b)** for the cases where $n \leq 0$. We acknowledge that **(c)**, in the stated form, actually includes **(a)** and **(b)**. □

Proposition 21. *Let $\phi : G \to H$ be a homomorphism and let $K \leq G$.*
Then $\phi \restriction_K : K \to H$ is a homomorphism.

Proof. This is obvious. □

4.2. **Examples of Homomorphisms.** We list a few well known examples of homomorphisms; more examples will arise as we build the theory.

Example 33. Define a function

$$f : \mathbb{Z} \to \mathbb{Z} \quad \text{given by} \quad f(a) = 2a.$$

Then $f(a + b) = 2(a + b) = 2a + 2b$, so f is a homomorphism by the distributive property. The image of f is the even integers.

Example 34. Let $n \in \mathbb{Z}$, $n \geq 2$, and define a function

$$\xi_n : \mathbb{Z} \to \mathbb{Z}_n \quad \text{by} \quad \xi_n(a) = \overline{a}.$$

Then ξ_n is a homomorphism. This is because we successfully defined addition in $\mathbb{Z}_n$ by $\overline{a} + \overline{b} = \overline{a + b}$.

Example 35. Define a function

$$T : \mathbb{R}^3 \to \mathbb{R}^3 \quad \text{by} \quad T(x, y, z) = (z, x, y).$$

This linear transformation is a homomorphism of the group of vectors under addition. Geometrically, this is rotation around the line $x = y = z$ by 120°.

Example 36. Define a function

$$\exp : \mathbb{R} \to \mathbb{R}^* \quad \text{by} \quad \exp(x) = e^x.$$

Then exp is a homomorphism from the real under addition to the nonzero reals under multiplication, because $e^{x+y} = e^x e^y$. The image of exp is $\mathbb{R}^>$, the positive real numbers.

Example 37. Define a function

$$\text{cis} : \mathbb{R} \to \mathbb{C}^* \quad \text{by} \quad \text{cis}(\theta) = \cos\theta + i\sin\theta.$$

Then cis is a homomorphism, because $\text{cis}(\theta_1 + \theta_2) = \text{cis}(\theta_1)\,\text{cis}(\theta_2)$. The image of cis is $\mathbb{U}$, the unit circle in the complex plane.

Example 38. Define a function

$$f : \mathbb{C} \to \mathbb{C} \quad \text{by} \quad f(x+iy) = x - iy.$$

This is complex conjugation, and it is a homomorphism of the additive structure of $\mathbb{C}$. If we restrict to $\mathbb{C}^*$, complex conjugation is a homomorphism of the multiplicative structure.

4.3. **Properties of Homomorphisms.** The homomorphic image of a subgroup is a subgroup, and the homomorphic preimage of a subgroup is a subgroup. Composition of homomorphisms is a homomorphism. The order of a homomorphic image of an element divides the order of the element. We now show these basic facts.

Proposition 22. *Let $\phi : G \to H$ be a homomorphism and let $K \leq G$. Then $\phi(K) \leq H$.*

Proof. We verify the three properties of a subgroup.

(S0) Since K is a subgroup of G, $1_G \in K$. Since $\phi(1_G) = 1_H$, $1_H \in \phi(K)$.

(S1) Let $h_1, h_2 \in \phi(K)$. Then there exist $k_1, k_2 \in K$ such that $\phi(k_1) = h_1$ and $\phi(k_2) = h_2$. Let $k = k_1k_2$, and since K is a subgroup, $k \in K$; we have $\phi(k) = \phi(k_1k_2) = \phi(k_1)\phi(k_2) = h_1h_2$, which shows that $h_1h_2 \in \phi(K)$.

(S2) Let $h \in \phi(K)$. Then $h = \phi(k)$ for some $k \in K$. Since K is a subgroup, $k^{-1} \in K$, and $\phi(k^{-1}) = \phi(k)^{-1} = h^{-1}$, so $h^{-1} \in \phi(K)$. □

Proposition 23. *Let $\phi : G \to H$ be a homomorphism and let $K \leq H$. Then $\phi^{-1}(K) \leq G$.*

Proof. We verify the three properties of a subgroup.

(S0) Since K is a subgroup of H, $1_H \in K$, and since $\phi(1_G) = 1_H$, $1_G \in \phi^{-1}(K)$.

(S1) Let $g_1, g_2 \in \phi^{-1}(K)$. Then there exist $k_1, k_2 \in K$ such that $\phi(g_1) = k_1$ and $\phi(g_2) = k_2$. Since ϕ is a homomorphism and K is a subgroup, $\phi(g_1g_2) = \phi(g_1)\phi(g_2) = k_1k_2 \in K$. Thus $g_1g_2 \in \phi^{-1}(K)$.

(S2) Let $g \in \phi^{-1}(K)$. Then $\phi(g) = k$ for some $k \in K$, and since $K \leq H$, $k^{-1} \in K$. Thus $\phi(g{-}1) = \phi(g)^{-1} = k^{-1} \in K$, so $g^{-1} \in \phi^{-1}(K)$. □

Proposition 24. *Let $\phi : G \to H$ and $\psi : H \to K$ be homomorphisms. Then $\psi \circ \phi : G \to K$ is a homomorphism.*

Proof. If $g \in G$, then $\psi \circ \phi(g)$ means $\psi(\phi(g))$. Let $g_1, g_2 \in G$. Then

$$\psi(\phi(g_1g_2)) = \psi(\phi(g_1)\phi(g_2)) = \psi(\phi(g_1))\psi(\phi(g_2)).$$

□

Proposition 25. *Let $\phi : G \to H$ be a homomorphism and let $g \in G$ be an element of finite order. Then* $\mathrm{ord}(\phi(g)) \mid \mathrm{ord}(g)$.

Proof. Let $\mathrm{ord}(g) = n$. Then $\phi(g)^n = \phi(g^n) = \phi(1_G) = 1_H$. Thus n is an exponent of $\phi(g)$. □

Proposition 26. *Let G and H be groups with $g \in G$ and $h \in H$.*
If $\mathrm{ord}(h) \mid \mathrm{ord}(g) < \infty$, *or* $\mathrm{ord}(g) = \infty$, *then the function*

$$\phi : \langle g \rangle \to \langle h \rangle \quad \text{by} \quad \phi(g^k) = h^k$$

is a well-defined homomorphism.

Proof. Suppose ϕ is well-defined; then $\phi(g^i g^j) = \phi(g^{i+j}) = h^{i+j} = h^i h^j = \phi(g^i)\phi(g^j)$, so ϕ is a homomorphism. If $\mathrm{ord}(g) = \infty$, then ϕ is necessary well-defined, since there is only one way to write an element of $\langle g \rangle$ as g^k. Thus suppose $\mathrm{ord}(g) < \infty$.

Let $n = \mathrm{ord}(g)$ and $m = \mathrm{ord}(h)$. Since $m \mid n$, there exists $l \in \mathbb{Z}$ such that $n = mk$. To see that ϕ is well-defined, suppose that $g^i = g^j$; we wish to show that $h^i = h^j$. Now $g^{j-i} = 1$, so $n \mid j - i$, so $j - i = nl$ for some $l \in \mathbb{Z}$. Thus $h^{j-i} = h^{nl} = h^{mkl} = (h^m)^k l = 1^{kl} = 1$. □

Corollary 1. *The homomorphic image of a cyclic group is cyclic.*

4.4. **Definition of Isomorphism.** Of particular concern are those structure preserving functions that are bijective, because this sets up a correspondence between the objects which allows us to see that they are "essentially the same"; a change of notation makes them the same.

Definition 9. An injective homomorphism is called a *monomorphism*. A surjective homomorphism is called an *epimorphism*. A bijective homomorphism is called an *isomorphism*. If there exists an isomorphism between the groups G and H, we say that G and H are *isomorphic*, and write $G \cong H$.

Proposition 27. *Let G be a group. Then* $\mathrm{id}_G : G \to G$ *is an isomorphism.*

Proof. This is obvious. □

Proposition 28. *Let $\phi : G \to H$ be an isomorphism.*
Then $\phi^{-1} : H \to G$ is an isomorphism.

Proof. By definition, ϕ is bijective, so it is invertible. Let $h_1, h_2 \in H$. Since ϕ is bijective, there exist unique $g_1, g_2 \in G$ such that $\phi(g_1) = h_1$ and $\phi(g_2) = h_2$. Then $h_1 h_2 = \phi(g_1)\phi(g_2) = \phi(g_1 g_2)$. Thus $\phi^{-1}(h_1 h_2) = g_1 g_2 = \phi^{-1}(h_1)\phi^{-1}(h_2)$. □

Proposition 29. *Let $\mathcal{G}$ be a collection of groups.*
Then isomorphism is an equivalence relation on $\mathcal{G}$.

Proof. The identity map on a group establishes the reflexivity of isomorphism. The symmetry relation is established by the fact that bijective maps are invertible. The transitivity relation is given by the fact that the composition of homomorphisms is a homomorphism, and the composition of bijections is a bijection. □

Example 39. The function $\exp : \mathbb{R} \to \mathbb{R}^>$ is an isomorphism from the additive group of real numbers to the multiplicative group of positive real numbers, with inverse $\log : \mathbb{R}^> \to \mathbb{R}$. Thus $(\mathbb{R}, +, 0) \cong (\mathbb{R}^>, \cdot, 1)$.

Example 40. The function $f : \mathbb{Z}_n \to \mathbb{U}_n$, given by $f(\overline{k}) = \operatorname{cis}(2\pi k/n)$ is well-defined, and is an isomorphism from the additive group of integers modulo n to the multiplicative group of n^{th} roots of unity. Thus $(\mathbb{Z}_n, +, \overline{0}) \cong (\mathbb{U}_n, \cdot, 1)$.

4.5. **Kernels.** Homomorphisms are consistent in the sense that the cardinalities of the preimages of any two points are the same. This is a major theme in algebra, and we begin to develop it now. We start by showing the a homomorphism is injective if and only if its kernel is trivial.

Definition 10. Let $\phi : G \to H$ be a homomorphism.

The *kernel* of ϕ is the subset of G denoted by $\ker(\phi)$ and defined by

$$\ker(\phi) = \{g \in G \mid \phi(g) = 1_H\}.$$

Proposition 30. *Let $\phi : G \to H$ be a homomorphism. Then $\ker(\phi) \leq G$.*

Proof. The kernel of ϕ is the preimage of the trivial subgroup $\{1_H\} \leq H$, and as such, it is a subgroup of the domain G. □

Example 41. Consider the homomorphism $\xi : \mathbb{Z} \to \mathbb{Z}_n$ given by $\xi(a) = \overline{a}$. Then $\xi(a) = 0$ if and only if $a \equiv 0 \pmod{n}$, that is, if a is a multiple of n. Thus the kernel of ξ is

$$\ker(\xi) = n\mathbb{Z} = \{a \in \mathbb{Z} \mid a = nb \text{ for some } b \in \mathbb{Z}\}.$$

Example 42. Consider the homomorphism $\operatorname{cis} : \mathbb{R} \to \mathbb{U}$. Now $\operatorname{cis}\theta = 0$ if and only if $\theta = 2\pi k$ for some integer k. The kernel of cis, then, is the subgroup of $\mathbb{R}$ given as

$$\ker(\operatorname{cis}) = 2\pi\mathbb{Z} = \{x \in \mathbb{R} \mid x = 2\pi k \text{ for some } k \in \mathbb{Z}\}.$$

Example 43. Consider the linear transformation $T : \mathbb{R}^3 \to \mathbb{R}^3$ given as projection onto the xy-plane. Then T is a homomorphism of additive groups, and the kernel of T is the z-axis.

Proposition 31. *Let $\phi : G \to H$ be a homomorphism.*
Then ϕ is injective if and only if $\ker(\phi) = \{1_G\}$.

Proof.
($\Rightarrow$) Suppose the ϕ is injective. Since the identity of G maps to the identity of H, no other element of G may map to the identity of H.
($\Leftarrow$) Suppose that $\ker(\phi)$ is trivial. Then

$$\begin{aligned}
\phi(g_1) = \phi(g_2) &\Leftrightarrow \phi(g_1)\phi(g_2)^{-1} = 1_H \\
&\Leftrightarrow \phi(g_1)\phi(g_2^{-1}) = 1_H \\
&\Leftrightarrow \phi(g_1 g_2^{-1}) = 1_H \\
&\Leftrightarrow g_1 g_2^{-1} = 1_G \\
&\Leftrightarrow g_1 = g_2.
\end{aligned}$$

□

5. Cosets

5.1. **Definition of Cosets.** The preimages of points in the image of a homomorphism are examples of cosets, and they are "translations" of the kernel. We give the general definition of cosets, and eventually see how they are translations of a kernel exactly when they are translations of what is known as a normal subgroup.

Definition 11. Let G be a group and $H \leq G$. Let $g \in G$.

The *left coset* at g of H in G is the set

$$gH = \{gh \mid h \in H\}.$$

The *right coset* at g of H in G is the set

$$Hg = \{hg \mid h \in H\}.$$

Proposition 32. *Let G be a group and $H \leq G$. Let $g, g_1, g_2 \in G$. Then*

(a) $g \in gH$;
(b) $g \in Hg$;
(c) $gH = H \Leftrightarrow g \in H$;
(d) $Hg = H \Leftrightarrow g \in H$;
(e) $g_1H = g_2H \Leftrightarrow g_1^{-1}g_2 \in H$;
(f) $Hg_1 = Hg_2 \Leftrightarrow g_2g_1^{-1} \in H$.

Proof. First note that since $1 \in G$, H is a coset of H in G, specifically, $H = 1H$. Also $g \in gH$ since $g = g \cdot 1$. This proves **(a)**.

Thus if $gH = H$, then $g \in H$.

If $g \in H$, then $gH \subset H$ by closure, because H is a group. Since g^{-1} is also in H, we have $g^{-1}H \subset H$, so $H \subset gH$; thus $gH = H$. This proves **(c)**.

If $g_1H = g_2H$, then $H = g_1^{-1}g_2H$, so $g_1^{-1}g_2 \in H$. If $g_1^{-1}g_2 \in H$, then $g_1^{-1}g_2H = H$, so $g_2H = g_1H$. This proves **(e)**.

The proofs for right cosets are analogous. □

Definition 12. Let G be a group and let $H \leq G$. Let $g_1, g_2 \in G$.

We say that g_1 and g_2 are *left congruent modulo H* if $g_1^{-1}g_2 \in H$.

We say that g_1 and g_2 are *right congruent modulo H* if $g_1g_2^{-1} \in H$.

Proposition 33. *Let G be a group and $H \leq G$. Then left and right congruence modulo H is an equivalence relation.*

Proof. Let $g \in G$. Then $g^{-1}g = 1 \in H$, so g is left congruent to itself modulo H. Thus left congruence is reflexive.

Let $g_1, g_2 \in G$. Suppose that $g_1^{-1}g_2 \in H$. Thus $g_2^{-1}g_1 = (g_1^{-1}g_2)^{-1} \in H$ since H is closed under inverses. Thus left congruence is symmetric.

Let $g_1, g_2, g_3 \in G$. Suppose that $g_1^{-1}g_2 \in H$ and $g_2^{-1}g_3 \in H$. Then $g_1^{-1}g_3 = g_1^{-1}g_2g_2^{-1}g_3 \in H$ since H is closed under multiplication. Thus left congruence is transitive.

The proof for right congruence is analogous. □

Corollary 2. *Let G be a group and let $H \leq G$. Then the collection of left (right) cosets of H in G partition G.*

5.2. **Lagrange's Theorem.** We now show that the size of a subgroup divides the size of a group; this is known as Lagrange's Theorem. Thus the size of a cyclic group is the order of a generator; for this reason, the word order has come to mean the cardinality of a group.

Definition 13. Let G be a group. The *order* of G is $|G|$.

Proposition 34. *Let G be a group and let $H \leq G$. Let $g \in G$. Then the maps*

$$\lambda_g : H \to gH \text{ given by } \phi(h) = gh$$

and

$$\rho_g : H \to Hg \text{ given by } \phi(h) = hg$$

are bijective.

Proof. Let $gh \in gH$; then $h \mapsto gh$, so λ_g is surjective. Let $gh_1, gh_2 \in gH$; then $h_1 = h_2$ by cancelation, so λ_g is injective. The proof for ρ_g is analogous. □

Corollary 3. *Let G be a group and let $H \leq G$. Let $g \in G$. Then*

$$|gH| = |Hg| = |H|.$$

Definition 14. Let G be a group and $H \leq G$. The collection of left cosets of H in G is called the *left coset space* of H in G. The collection of right cosets of H in G is called the *right coset space* of H in G.

Proposition 35. *Let G be a group and $H \leq G$. Then there is a correspondence between the left and right coset spaces of H in G given by*

$$gH \leftrightarrow Hg^{-1}.$$

Proof. The map $\phi : gH \mapsto Hg^{-1}$ is well-defined and injective:

$$\begin{aligned} g_1H = g_2H &\Leftrightarrow g_2^{-1}g_1H = H \\ &\Leftrightarrow g_2^{-1}g_1 \in H \\ &\Leftrightarrow Hg_2^{-1}g_1 = H \\ &\Leftrightarrow Hg_2^{-1} = Hg_1^{-1}. \end{aligned}$$

Since $\phi(g^{-1}H) = Hg$, the map is surjective. □

Corollary 4. *Let G be a group and $H \leq G$. Then the left coset space of H in G and the right coset space of H in G have the same cardinality.*

Definition 15. Let G be a group and let $H \leq G$. The *index* of H is G is the cardinality of the left coset space of H in G, and is denoted by $[G : H]$.

Theorem 1. (Lagrange's Theorem)
Let G be a finite group and $H \leq G$. Then $|G| = |H|[G : H]$.

Proof. The cardinality of each left coset is the cardinality of H. There are $[G : H]$ of these in G. Since these cosets form a partition of G, the result follows. □

Proposition 36. *Let G be a finite group and let $g \in G$.*
Then $\mathrm{ord}(g)$ *divides* $|G|$.

Proof. Since $\langle g \rangle \leq G$ and $\mathrm{ord}(g) = |\langle g \rangle|$, the result follows from Lagrange's Theorem. □

Proposition 37. *Let G be a finite group such that $|G|$ is prime.*
Then G is cyclic.

Proof. Let G be a group of order p, where p is prime. Let $p \in G$. Then $\mathrm{ord}(g)||G|$ so $\mathrm{ord}(g) = p$ or $\mathrm{ord}(g) = 1$. Thus if $g \neq 1$ then $G = \langle g \rangle$. □

5.3. **The Exponent of a Group.** If every element in a group G has finite order, it is possible that there is a single positive integer k which is an exponent for every element in the group; that is $g^n = 1$ for every $g \in G$, whatever the order of g. Certainly, if this happens, the order of g will divide n.

Definition 16. Let G be a group. The *exponent* of G is the smallest positive integer $n \in \mathbb{N}$ such that $g^n = 1$ for every $g \in G$, if such an integer exists. The exponent of G is denoted by $\exp(G)$.

Proposition 38. *Let G be a finite abelian group.*
Then G has an element of order $\exp(G)$.

Proof. Let $\exp(G) = p_1^{a_1} \dots p_n^{a_n}$ be the unique factorization of $\exp(G)$ into powers of distinct primes. Let g be an element of G of largest order, and suppose that $\mathrm{ord}(g) < \exp(G)$. Then $\mathrm{ord}(g) = p_1^{b_1} \dots p_n^{b_n}$, where $0 \leq b_i \leq a_i$, because $\mathrm{ord}(g) | \exp(G)$. We assume that at least one of the b_i's is less than a_i; without loss of generality, $b_1 < a_1$.

Now for some element $h \in G$, $\mathrm{ord}(h) = p_1^{c_1} \dots p_n^{c_n}$ where $c_1 > b_1$; otherwise, $p_1^{b_1} p_2^{a_2} \dots p_n^{a_n}$ would be an exponent for every element in G. Now $g' = g^{p_1^{b_1}}$ has order $p_2^{b_2} \dots p_n^{b_n}$ and $h' = h^{p_2^{c_2} \dots p_n^{c_n}}$ has order $p_1^{c_1}$. Then $g'h'$ has order $p_1^{c_1} p_2^{b_2} \dots p_n^{b_n}$, which is greater than $\mathrm{ord}(g)$, a contradiction. □

Proposition 39. *Let G be a finite abelian group.*
Then G is cyclic if and only if $|G| = \exp(G)$.

Proof. If G is cyclic with generator g, then $|G| = \mathrm{ord}(g)$. For $g^n \in G$, $(g^n)^{\mathrm{ord}(g)} = 1$, so $\mathrm{ord}(g)$ is an exponent of g^n. But nothing smaller than $\mathrm{ord}(g)$ is an exponent of g. Thus $\exp(G) = \mathrm{ord}(g)$.

Now suppose that $|G| = \exp(G)$. Then G has an element g of order $|G|$. Then G is generated by g. □

6. Quotients

6.1. **Normal Subgroups.** We wish to put a group structure on the left coset space of a subgroup in a group. This requires that the subgroup has the property of normality.

Definition 17. Let G be a group and $H \leq G$. We say that H is a *normal* subgroup, and write $H \triangleleft G$, if $gH = Hg$ for every $g \in G$.

Proposition 40. *Let G be a group and let $H \leq G$. The following conditions are equivalent:*

(1) *$gH = Hg$ for every $g \in G$;*
(2) *$g^{-1}Hg = H$ for every $g \in G$;*
(3) *$g^{-1}Hg \subset H$ for every $g \in G$.*

Proof. That **(1)** $\Leftrightarrow$ **(2)** and **(2)** $\Rightarrow$ **(3)** are obvious.

Suppose that $g^{-1}Hg \subset H$ for every $g \in G$. Let $g \in G$; then $g^{-1} \in G$, so $gHg^{-1} \subset H$. Thus $H \subset g^{-1}Hg$. □

Proposition 41. *Let G be a group. Then $G \triangleleft G$ and $1 \triangleleft G$.*

Proposition 42. *Let G be a group and let $\mathcal{N}$ be a collection of normal subgroups of G. Then $\cap\mathcal{N}$ is a normal subgroup of G.*

Proof. Let $\mathcal{N} = \{H_\alpha \triangleleft G \mid \alpha \in A\}$, where A is some indexing set. Then for any $g \in G$, $g^{-1}(\cap_{\alpha\in A} H_\alpha)g = \cap_{\alpha\in A} g^{-1}H_\alpha g = \cap_{\alpha\in A} H_\alpha$. □

Proposition 43. *Let G be an abelian group and let $H \leq G$. Then $H \triangleleft G$.*

Proof. For $H \triangleleft G$ and $g \in G$, $h \in H$ we have $gh = hg$. Thus $gH = Hg$. □

Proposition 44. *Let $\phi : G \to H$ be a homomorphism and let $K = \ker(\phi)$. Then $K \triangleleft G$.*

Proof. We have $\phi(g^{-1}Kg) = \phi(g)^{-1}\phi(K)\phi(g) = \phi(g)^{-1} \cdot 1_H \cdot \phi(g) = 1_H$. Thus $g^{-1}Kg \subset K$. □

Definition 18. Let G be a group and let $X, Y \subset G$. Set

$$XY = \{xy \in G \mid x \in X \text{ and } y \in Y\} \quad \text{and} \quad X^{-1} = \{x^{-1} \in G \mid x \in X\}.$$

Proposition 45. *Let G be a group and let $H, K \leq G$. Then $HK \leq G$ if and only if $HK = KH$.*

Proof. If $M \leq G$, then $M^{-1} = M$. Thus if $HK \leq G$, then $HK = (HK)^{-1} = K^{-1}H^{-1} = KH$.

Suppose $HK = KH$. Let $h_1, h_2 \in H$ and $k_1, k_2 \in K$ so that h_1k_1 and h_2k_2 are arbitrary members of HK. Since $HK = KH$, there exists $k_3 \in K$ such that $k_1h_2 = h_2k_3$. Then $h_1k_1h_2k_2 = h_1h_2k_3k_2 \in HK$.

Let $h \in H$ and $k \in K$ so that hk is an arbitrary member of HK. Then $(hk)^{-1} = k^{-1}h^{-1} \in KH = HK$. Thus $HK \leq G$. □

Proposition 46. *Let G be a group, $H \leq G$, and $K \triangleleft G$. Then $HK = KH$, and $HK \leq G$.*

Proof. We have $hK = Kh$ for every $h \in H$, so $HK = KH$. Thus $HK \leq G$ by the previous proposition. □

6.2. **Factor Groups.** We are now in a position to show that multiplication of cosets of a normal subgroup produces a new group.

Proposition 47. *Let G be a group and $H \triangleleft G$. Denote the collection of left cosets of H in G by G/H. Define a binary operation on G/H by*

$$(g_1H) \cdot (g_2H) = (g_1g_2)H.$$

Then $\cdot$ is well defined, and G/H is a group under this operation, with identity element H and inverses $(gH)^{-1} = g^{-1}H$.

Proof. To see that this operation is well defined, let $g_1, g_2 \in G$ be such that $g_1H = g_2H$. Then $g_2^{-1}g_1 \in H$ and $g_1^{-1}g_2 \in H$. Let gH be another coset. Then $(g_1H)(gH) = g_1gH$ by definition. But $g_1gH = g_1gHH$ because $HH = H$. Since H is normal, $gHH = HgH$. Thus $g_1gH = g_1gHH = g_1HgH = g_2HgH = g_2gHH = g_2gH$.

The operation is associative by the associativity of G. □

Definition 19. Let G be a group and $H \triangleleft G$. The left coset space of H in G is denoted G/H. Then G/H with the binary operation defined above is called the *quotient group*, or *factor group* of G over H. This group is known as G *modulo* H.

Proposition 48. *Let G be a group and $H \triangleleft G$. Define $\beta : G \to G/H$ by $\beta(g) = gH$. Then β is a surjective homomorphism with kernel H.*

Proof. Let $g_1, g_2 \in G$. Note that $HH = H$ and that $g_2H = Hg_2$ because $H \triangleleft G$. Thus

$$\beta(g_1g_2) = g_1g_2H = g_1g_2HH = g_1Hg_2H = \beta(g_1)\beta(g_2).$$

It is clear that β is surjective. □

Remark 6. Thus the kernel of every homomorphism is normal, and every normal subgroup is the kernel of a homomorphism.

6.3. **Isomorphism Theorems.** Quotients give us a way to understand homomorphic images, and vice versa, through the following important theorems.

Theorem 2. (First Isomorphism Theorem)
Let $\phi : G \to H$ be a group homomorphism with kernel K. Let $\beta : G \to G/K$ be the canonical homomorphism. Let $\overline{\phi} : G/K \to H$ be given by $\overline{\phi}(gK) = \phi(g)$. Then

- **(a)** *$\overline{\phi}$ is a well defined injective homomorphism;*
- **(b)** *$\phi = \overline{\phi} \circ \beta$;*
- **(c)** *if ϕ is surjective, then $\overline{\phi}$ is bijective, and $G/K \cong H$.*

Proof. To show that $\overline{\phi}$ is well-defined and injective, let $g_1, g_2 \in G$ so that g_1H and g_2H are arbitrary members of G/K. Then

$$\begin{aligned} g_1K = g_2K &\Leftrightarrow g_2^{-1}g_1 \in K \\ &\Leftrightarrow \phi(g_2^{-1}g_1) = 1_H \\ &\Leftrightarrow \phi(g_1) = \phi(g_2). \end{aligned}$$

Also $\overline{\phi}$ is a homomorphism because ϕ is. That $\phi = \overline{\phi} \circ \psi$ is true by definition. It is clear that if ϕ is surjective, then so is $\overline{\phi}$, in which case $\overline{\phi}$ is bijective, so it is an isomorphism. □

Theorem 3. (Second Isomorphism Theorem)
Let G be a group, $H \leq G$, and $K \triangleleft G$. Then $HK \leq G$, $H \cap K \triangleleft H$, and

$$\frac{HK}{K} \cong \frac{H}{H \cap K}.$$

Proof. We have already seen that $HK \leq G$ and $H \cap K \leq H$. Let $h \in H$; then $h^{-1}(H \cap K)h = h^{-1}Hh \cap h^{-1}Kh = H \cap K$, so $H \cap K \triangleleft H$.

Let $\overline{H} = H/(H \cap K)$. Let $\phi : HK \to \overline{H}$ be given by $hk \mapsto \overline{h}$.

This map is a homomorphism:

$$\phi(h_1k_1h_2k_2) = \phi(h_1h_2k_3k_2) = \overline{h_1h_2}$$

for some $k_3 \in K$ because $h_2K = Kh_2$.

Note that for $k \in K$, $\phi(k) = \overline{1}$. Thus $\ker(\phi) = K$.

This map is clearly onto, so by the first isomorphism theorem the induced map $\overline{\phi}$ is an isomorphism. This is exactly the isomorphism we seek. □

Theorem 4. (Third Isomorphism Theorem)
Let G be a group with normal subgroups K and H and suppose that $K \leq H$. Then

$$\frac{G/K}{H/K} \cong \frac{G}{H}.$$

Proof. Let $\phi : G/K \to G/H$ be given by $gK \mapsto gH$. This map is well defined since $K \subset H$. It is a homomorphism since $H \triangleleft G$. It is clearly onto and its kernel is H/K. □

6.4. **Correspondence Theorems.** The subgroups of a homomorphic images correspond to the subgroups of the domain which contain the kernel.

Proposition 49. *Let $\phi : G \to H$ be a surjective homomorphism with kernel K Let $\mathcal{S}$ be the collection of subgroups of G which contain K and let $\mathcal{T}$ be the collection of subgroups of H. Define*

$$\Phi : \mathcal{S} \to \mathcal{T} \quad \text{by} \quad \Phi(S) = \phi(S).$$

Then Φ is an inclusion preserving bijection.

Corollary 5. *Let G be a group and let $K \triangleleft G$. Let $\mathcal{S}$ be the collection of subgroups of G which contain K and let $\mathcal{T}$ be the collection of subgroups of G/K. If $S \leq G$, set $S/K = \{sK \mid s \in S\}$. Define*

$$\Phi : \mathcal{S} \to \mathcal{T} \quad \text{by} \quad \Phi(S) = S/K.$$

Then Φ is an inclusion preserving bijection.

Department of Mathematics and CSci, Southern Arkansas University
E-mail address: plbailey@saumag.edu