COMPUTATIONAL MATHEMATICS
TOPIC 33 - GROUPS

PAUL L. BAILEY

Abstract. We introduce some of the theory of groups which we will explore by writing software.

1. Groups

1.1. **Definition.** The most studied algebraic object with one operator is a group, which is a monoid in which each element has an inverse. For convenience, we will write generic groups using multiplicative notation.

Definition 1. A *group* $(G, \cdot, 1)$ consists of a nonempty set G together with a binary operation $\cdot : G \times G \to G$ satisfying

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

We recall that the identity and inverses are unique. Since a group is associative, parentheses are useless when writing operations with three or more elements. In general, groups are not commutative; we have a special name for the case that they are.

Definition 2. Let G be a group. We say the G is *abelian* if

- **(G4)** $g_1 g_2 = g_2 g_1$ for all $g_1, g_2 \in G$ (commutativity).

1.2. **Examples.** Understanding the theory of groups requires copious examples, and we give several now.

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 $(M, \cdot)$ be a multiplicative monoid, and set

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

Certainly the restriction of multiplication to M^* is still associative. Note that 1 is invertible, as it is its own inverse. Also, if g is invertible, then g^{-1} is also invertible, with inverse g. Thus M^* is closed under inverses, so M^* is a group.

Date: Sunday, February 24, 2019.

Example 3. The following are standard multiplicative groups.

- $(\mathbb{Z}^*, \cdot, 1)$, the integers under addition (how big is this?);
- $(\mathbb{Q}^*, \cdot, 1)$, the rational numbers under addition;
- $(\mathbb{R}^*, \cdot, 1)$, the real numbers under addition;
- $(\mathbb{C}^*, \cdot, 1)$, the complex numbers under addition.

In each case, inverses are reciprocals. Not all multiplicative groups are abelian, but these are.

Example 4. Let $\mathbb{Z}_n$ denote the set of residues classes of integers 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 X be a set, and set $\mathrm{Sym}(X) = \{f : X \to X \mid f \text{ is bijective}\}$. Then $(\mathrm{Sym}(X), \circ, \mathrm{id}_X)$ 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 7. Let $X = \{1, \ldots, n\}$, and set $S_n = \mathrm{Sym}(X)$. Let $\epsilon = \mathrm{id}_X$, and write composition of functions multiplicatively. Then $(S_n, \cdot, \epsilon)$ is a nonabelian group containing $n!$ elements.

Example 8. 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 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. If $m = n$, we may shorten this to $\mathcal{M}_n(\mathbb{R})$.

Example 10. Let $\mathbf{GL}_n(\mathbb{R}) = \mathcal{M}_n(\mathbb{R})^*$ 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.

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.

1.3. **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 12. Let $\mathbb{Z}_{10}^* = \{1, 3, 7, 9\}$; this is a group under multiplication. One computes the following Cayley table.

$\cdot$	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

Then $\mathbb{Z}_{10}^*$ is a *cyclic group* of order four, which means that each member is a power of one the elements (in this case, either 3 or 7).

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

1.4. **Commuting Elements.** Let G be a group. If $a, b \in G$, we say that a and b *commute* if $ab = ba$. There are many important groups which contain very few elements that commute; it is worthwhile to mention a couple of properties of commuting elements.

Proposition 1. *Let G be a group and let $a, b \in G$. Then a and b commute if and only if $(ab)^n = a^n b^n$ for all $n \in \mathbb{N}$.*

Proof. If a and b commute, the $(ab)^n = a^n b^n$. This follows from successive usage of associative and commutative properties; for example, $(ab)^2 = (ab)(ab) = ((ab)a)b = (a(ba))b = (a(ab))b = (a^2 b)b = a^2 b^2$. This may be written more formally using induction.

If $(ab)^2 = a^2 b^2$, then a and b commute; to see this, write $abab = aabb$, multiply on the left by a^{-1} to get $a^{-1}abab = a^{-1}aabb$, so that $bab = abb$. Now multiply on the right by b^{-1} to get $babb^{-1} = abbb^{-1}$, so that $ba = ab$. □

Example 16. Let $\alpha, \beta \in S_5$ be given by $\alpha =$ `(1 2 3)` and $\beta =$ `(4 5)`. Then $\alpha^3 = \epsilon$ and $\beta^2 = \epsilon$, so $(\alpha\beta)^6 = \alpha^6\beta^6 = \epsilon$; this is because disjoint cycle commute.

However, note that if $\alpha =$ `((1 2 3)` and $\beta =$ `(2 5)`, these cycles do not commute, and

$$\alpha\beta = \texttt{(1 2 5 3)} \text{ and } (\alpha\beta)^6 = (\alpha\beta)^2 = \texttt{(1 5)(2 3)}.$$

Example 17. In the group $\mathbf{GL}_3(\mathbb{R})$, the scalar matrices are those of the form $\lambda I = \begin{bmatrix} \lambda & 0 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \lambda \end{bmatrix}$. A scalar matrix commutes with any other matrix; in fact, these are the *only* matrices which commute with every other matrix.

One can tell if a group is abelian by looking at its Cayley table; if the Cayley table is symmetric across its diagonal, then the operation is commutative.

Example 18. The quaternion group is not abelian. Indeed, the only elements which commute with every other element are 1 and -1.

Proposition 2. *Let G be a group such that $g^2 = 1$ for every $g \in G$.*
Then G is abelian.

Proof. 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. □

Example 19. In the group $(\mathcal{P}(X), \triangle, \varnothing)$, if $A \subset X$, we have $A^2 = A \triangle A = \varnothing$; thus, by Prop 2, this group is abelian.

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)** $h \in H \Rightarrow h^{-1} \in H$.

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. We note that, in the presence of **(S1)** and **(S2)**, property **(S0)** is equivalent to the presence of $1 \in H$.

(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 3. *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 20. 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 21. 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 22. 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.

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

Proposition 4. *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 5. *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 23. 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 6. *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)**. □

2.4. **Product of Groups.** 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 7. *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

$$\begin{aligned}
(g_1 g_2)g_3 &= ((h_1, k_1)(h_2, k_2))(h_3, k_3) && \text{by definition of the set } H \times K \\
&= ((h_1 h_2)h_3, (k_1 k_2)k_3) && \text{by definition of the operation on } H \times K \\
&= (h_1(h_2 h_3), k_1(k_2 k_3)) && \text{by associativity in } H \text{ and } K \\
&= (h_1, k_1)((h_2, k_2)(h_3, k_3)) && \text{by definition of the operation on } H \times K \\
&= g_1(g_2 g_3) && \text{by definition of the set } H \times K.
\end{aligned}$$

(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

$$\begin{aligned}
g \cdot 1_G &= (h, k)(1_H, 1_K) = (h \cdot 1_H, k \cdot 1_K) = (h, k) = g; \\
1_G \cdot g &= (1_H, 1_K)(h, k) = (1_H \cdot h, 1_K \cdot k) = (h, k) = g.
\end{aligned}$$

(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

$$\begin{aligned}
(h, k)(h^{-1}, k^{-1}) &= (hh^{-1}, kk^{-1}) = (1_H, 1_K) = 1_G; \\
(h^{-1}, k^{-1})(h, k) &= (h^{-1}h, k^{-1}k) = (1_H, 1_K) = 1_G.
\end{aligned}$$

□

Let G and H be groups. Define

$$\widehat{G} = \{(g, 1_) \in G \times H \mid g \in G\} \text{ and } \widehat{H}\{(1_G, h) \in G \times H \mid h \in H\}.$$

Then $\widehat{G}$ and $\widehat{H}$ are subgroups of $G \times H$ which "look exactly like" G and H.

2.5. **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 24. The *symmetric group on n points* is S_n.

Example 25. 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 26. 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 27. 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 28. 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 29. 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 30. 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 31. Consider the group $\mathbb{Z}$ under addition. Then $\langle 2 \rangle = 2\mathbb{Z}$, the set of even integers.

Example 32. The modular integers $\mathbb{Z}_n$ for a cyclic group generated by $\overline{0}$.

Example 33. 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.

Proposition 8. *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 9. *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 $H = \langle g^k \rangle$. □

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 10. *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 11. *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 12. *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 13. *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 14. *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 15. *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 16. *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 17. *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 18. *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 19. *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 34. 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 35. 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 36. 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 37. 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.

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 20. *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 21. *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 22. *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 23. *Let $\phi : G \to H$ be a homomorphism and let $g \in G$ be an element of finite order. Then* $\operatorname{ord}(\phi(g)) \mid \operatorname{ord}(g)$.

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

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 *isomorphism* is a bijective homomorphism. If there exists an isomorphism from a group G to a group H, we say that G and H are *isomorphic*, and write $G \cong H$.

Proposition 24. *Let G be a group. Then* $\mathrm{id}_G : G \to G$ *is an isomorphism.*

Proof. This is obvious. □

Proposition 25. *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 $h_1h_2 = \phi(g_1)\phi(g_2) = \phi(g_1g_2)$. Thus $\phi^{-1}(h_1h_2) = g_1g_2 = \phi^{-1}(h_1)\phi^{-1}(h_2)$. □

Proposition 26. *Let $\phi : G \to H$ and $\psi : H \to K$ be isomorphisms. Then $\psi \circ \phi : G \to K$ is an isomorphism.*

Proof. We have seen that the composition of homomorphisms is a homomorphism, and that the composition of bijective functions is bijective. Thus the result. □

The three propositions above infer that isomorphism is an equivalence relation on any collection of groups; that is,

(a) $G \cong G$;
(b) $G \cong H$ implies $H \cong G$;
(c) $G \cong H$ and $H \cong K$ implies $G \cong K$.

Example 38. 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 $(\mathbb{R}, +, 0) \cong (\mathbb{R}^>, \cdot, 1)$.

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 27. *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 39. 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 40. 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 28. *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. Permutation Representations

Groups were originally invented (discovered?) in the context of permutation groups. Later, the concept was generalized to use the definition we have given on the first page. Eventually, Cayley showed that the generalization actually did not introduce any new groups (up to isomorphism).

Let X be any set. A *permutation* of X is a bijective function $X \to X$. The composition of permutations of X is another permutation of X. Composition is associative. The identity map of X onto itself is a permutation of X, and the inverse of a permutation is a permutation.

The *symmetry group* of X is

$$\mathrm{Sym}(X) = \{\alpha : X \to X \mid \alpha \text{ is bijective } \};$$

this is a group under composition.

A *symmetry group* is a subgroup of $\mathrm{Sym}(X)$, for some X. Next we show that every finite group is isomorphic to a symmetry group.

Proposition 29 (Cayley's Theorem)**.** *Let G be a group. For each $g \in G$, define a function*

$$\phi_g : G \to G \quad \textit{given by} \quad \phi_g(x) = gx.$$

Then ϕ_g is bijective. Define a function

$$\Phi : G \to \mathrm{Sym}(G) \quad \textit{given by} \quad \Phi(g) = \phi_g.$$

Then Φ is an injective group homomorphism, and G is isomorphic to $\Phi(G) \leq \mathrm{Sym}(G)$.

Proof. For each $g, x \in G$, we have $\phi_{g^{-1}} \circ \phi_g(x) = \phi_{g^{-1}}(gx) = g^{-1}gx = x$, so $\phi_{g^{-1}} \circ \phi_g$ is the identity function; thus ϕ_g is invertible, and is therefore bijective.

To show that Φ is a homomorphism, let $g, h \in G$. Select $x \in G$ and compute

$$\begin{aligned}\Phi(gh)(x) = \phi_{gh}(x) = (gh)x = g(hx) = g\phi_h(x) = \phi_g(\phi_h(x)) \\ = \phi_g \circ \phi_h(x) = (\Phi(g)) \circ \Phi(h))(x);\end{aligned}$$

since this is the case for all $x \in G$, we have $\Phi(gh) = \Phi(g) \circ \Phi(h)$, so Φ is a homomorphism.

Finally, suppose that $g, h \in G$ such that $\Phi(g) = \Phi(h)$, so that $\phi_g = \phi_h$ as functions. Then $\phi_g(1) = \phi_h(1)$, that is, $g = h$.

If we restrict the codomain of Φ to the image of G, we obtain an isomorphism $\Phi : G \to \mathrm{Sym}(G)$. Thus $G \cong \Phi(G)$; that is, G is isomorphic to a symmetry group. □

Consider the case where X is finite, say of cardinality n. An *enumeration* of X is an injective function $f : X \to \{1, \ldots, n\}$. If α is a permutation of X, then $f \circ \alpha \circ f^{-1}$ is a permutation of $\{1, \ldots, n\}$. This gives a function $\mathrm{Sym}(X) \to S_n$ which is a group homomorphism. In other words, symmetry groups in $\mathrm{Sym}(X)$ may be viewed as subgroups of S_n.

An *embedding* is an injective group homomorphism. The image of the domain is a subgroup of the codomain which is isomorphic to the domain. Cayley's Theorem states that G embeds into $\mathrm{Sym}(G)$, and if G is finite, if we enumerate G, this produces an embedding of G into S_n.

Let G be a group. A *permutation representation* of G is a group homomorphism $\phi : G \to S_n$. This representation is *faithful* if ϕ is injective. The image of ϕ is a subgroup of S_n, and if ϕ is faithful, $\phi(G)$ is isomorphic to G.

Department of Mathematics and CSci, BASIS Scottsdale
Email address: paul.bailey@basised.com