A Crash Course In Group Theory (Version 1.0)

Part I: Finite Groups

Sam Kennerly

June 2, 2010

with thanks to Prof. Jelena Marićic, Zechariah Thrailkill, Travis Hoppe, Erica Caden, Prof. Robert Gilmore, and Prof. Mike Stein.

Contents

Why learn group theory? In short, the answer is: group theory is the systematic study of symmetry. When a physical system or mathematical structure possesses some kind of symmetry, its description can often be dramatically simplified by considering the consequences of that symmetry. Results from group theory can be very useful if (and only if) one understands them well enough to look them up and use them.

The purpose of these notes is to provide readers with some basic insight into group theory as quickly as possible. Prerequisites for this paper are the standard undergraduate mathematics for scientists and engineers: vector calculus, differential equations, and basic matrix algebra.

Simplicity and working knowledge are emphasized here over mathematical completeness. As a result, proofs are very often sketched or omitted in favor of examples and discussion. Readers are warned that these notes are not a substitute for a thorough study of modern algebra. Still, they may be helpful to scientists, engineers, or mathematicians who are not specialists in modern algebra. Readers who desire an in-depth study of the subject may find this document useful as an outline and/or a quick-reference guide.

Like any good mathematical game, group theory is almost cartoonishly simple at first but the most advanced results are nightmarishly complicated. For example, a team of mathematicians recently found all irreducible unitary representations of the "exceptional" Lie group E_8. The result was stored as one 453,060 x 453,060 matrix of polynomials requiring 60GB of disk space.

These notes will not attempt any such task. Rather, the goal is to summarize the most important definitions and results while keeping an eye out for possible uses in the physical sciences. Part I covers **finite groups**: groups with only a finite number of elements. Part II will cover **continuous groups**, but at the time of this writing, it is not finished yet.

1 Notation

Sections 1 and 2 are intended as background for those unfamiliar with formal logic and mathematical notation. Impatient readers are advised to skip directly to Section 3: Groups and refer back to these sections later as necessary.

Notational conventions used in this document:

Bold words indicate new definitions.
Italic words indicate terms defined later in the text.
"Quote marks" identify informal terminology.
SMALL CAPITAL LETTERS indicate informal definitions that are unconventional and/or lacking in mathematical rigor.

Set theory notation:

$\mathbb{Z}$	the set of all integers
$\mathbb{N}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$	the sets of natural, rational, real, and complex numbers.
$\mathbb{R}^2$	the set of all ordered pairs of real numbers, e.g. (-4.5, 7)
$\mathbb{R}^3$	the set of all ordered triplets of real numbers, e.g. (1, 2, 3)
$\mathbb{R}^n$	the set of all ordered n-tuplets of real numbers
$x \in S$	x is an element of the set S
$S_1 \cup S_2$	the set of elements in S_1 or S_2 or both
$S_1 \cap S_2$	the set of elements in S_1 and S_2
$S - \{x, y, z\}$	the set of all elements in S except x, y, and z.

Formal logic notation:

$\forall$	for all
$\exists$	there exists
:	such that
$\Rightarrow$	implies
$\Leftrightarrow$	is logically equivalent to
$\sim$	is proportional to
$\cong$	is isomorphic to

A slash through a symbol means the negation of that symbol:

$\nexists$	there does not exist
$\not\Rightarrow$	does not imply

Analysis notation:

$\|x\|$	absolute value of x: the positive square root of x^2
$[a, b]$	the real numbers between a and b including the endpoints: $a \leq x \leq b$
(a, b)	the real numbers between a and b not including the endpoints: $a < x < b$

Linear algebra notation:

$\hat{M}$	a matrix
M_{jk}	the element on the jth row and kth column of $\hat{M}$
$\hat{M}^T$	the transpose of $\hat{M}$ (formed by replacing every M_{jk} with M_{kj})
$\hat{M}^*$	the conjugate of $\hat{M}$ (formed by complex conjugating every element of $\hat{M}$)
$\hat{M}^\dagger$	the matrix adjoint to $\hat{M}$ (formed by transposing $\hat{M}^*$)
$\|x\rangle$	a vector (also represented as a column of components)
$\langle x\|$	the dual vector to $\|x\rangle$ (also represented as a row of components)
$\langle y\|x\rangle$	the inner product of $\langle y\|$ and $\|x\rangle$
$\|\|x\|\|^2$	the square magnitude of a vector x (also represented as $\langle x\|x\rangle$)
$\hat{M}\|x\rangle$	the vector formed by operating the matrix $\hat{M}$ on the column vector $\|x\rangle$
$\oplus$ or $\otimes$	direct sum or direct product of two groups

Some practice for readers unfamiliar with formal logic notation:

mathematical notation	English translation
$\nexists$ free lunch	There is no such thing as a free lunch.
$(x \in \{\text{things that glitter}\}) \not\Rightarrow (x = \text{gold})$	Not all that glitters is gold.
$(U \text{ thinks}) \Rightarrow \exists U$	U thinks, therefore U exists.
$\forall x \in \mathbb{Z}, (x > 0) \Rightarrow (x \in \mathbb{N})$	All positive integers are natural numbers.
$(\exists z \in \mathbb{Z} : x \div 2 = z) \Leftrightarrow (x \in 2\mathbb{Z})$	x divided by 2 is an integer if and only if x is even.

2 Set Theory

Set theory is an important and fascinating subject which, for the purposes of this document, we will almost completely ignore. A sincere and thorough investigation would lead us to deep problems in axiomatic mathematics about which the author is more or less ignorant.

In the interest of speed, we will make use of the following informal definitions. Readers interested in a rigorous discussion of these terms may want to consult a book on axiomatic set theory.

Definition 1. A **set** is a collection of things or ideas.[1] The individual contents of a set S are called **elements** of S. Sets are often indicated by writing their elements, or a description of their elements, in brackets.

Definition 2. The **empty** set has no elements. It is denoted $\emptyset$. Note that $\emptyset$ is not the same as $\{0\}$, the set containing only the element 0.

Definition 3. A **subset** of a set S is a set whose elements are all elements of S. Note that $\emptyset$ is a subset of any set S and that any set S is a subset of itself. S and $\emptyset$ are called **improper** subsets of S; any other subset of S is **proper**. "T is a proper subset of S" is denoted $T \subset S$.

Definition 4. A **map** $\Phi : A \to B$ is a method for associating elements of A to elements of B.

Definition 5. The **image** of a map Φ is the set of all $\Phi(a)$ where $a \in A$.

Definition 6. A map Φ from A to B is **onto** if every element in B is mapped to by at least one element of A: $\forall b \in B, \exists a \in A$ such that $b = \Phi(a)$. Φ is called a **surjection**.

Definition 7. A map Φ from A to B is **one-to-one** if no two or more elements in A are mapped to any one element in B: $\Phi(a) = \Phi(b) \Rightarrow a = b$. Φ is called an **injection**.

Definition 8. A map Φ from A to B is **invertible** if and only if every element of A is mapped to exactly one element of B and every element of B is mapped to by an element of A. In other words, an invertible map is one-to-one and onto. Invertible maps are also called **bijections**.

[1] Bertrand Russell used this definition in 1901 to construct the following paradox: Define S as { all sets which are not elements of themselves }. Now (S is an element of itself) $\Leftrightarrow$ (S is not an element of itself). Russell's Paradox is a disaster for my definition of set.

If Φ is invertible, then we can always define an **inverse map** Φ^{-1} such that $\Phi(a) = b \Leftrightarrow a = \Phi^{-1}(b)$ for all $a \in A$ and $b \in B$.

Examples and counterexamples:

$\Phi(x) = 2x - 3$ is an invertible map from $\mathbb{R}$ to itself. If we define $\Phi^{-1}(y) = \frac{1}{2}(y + 3)$, then $y = \Phi(x) \Leftrightarrow x = \Phi^{-1}(y)$ for all real x and y .

$\Phi(x) = x^2$ is not an invertible map from $\mathbb{R}$ to itself. Φ^{-1} is ambiguous because Φ is not one-to-one: $\Phi(2)$ and $\Phi(-2)$ are both 4, so $\Phi^{-1}(4)$ could be either. Φ also fails to be onto: it misses all the negative numbers.

$\Phi(x) = x^2$ *is* an invertible map from $\mathbb{R}^+$ to itself. ($\mathbb{R}^+$ is the set of all positive real numbers.) Its inverse map is of course $\Phi^{-1}(y) = \sqrt{y}$.

3 Groups

3.1 Definition of group

Definition 9. A **binary operator** from A to B maps an ordered pair of elements of A to one element of B. (A trinary operator maps an ordered triplet of elements of A to one element of B, and so on.)

Definition 10. A binary operator Φ is said to be **closed** on A if and only if $\Phi(a, b) \in A$ for all $a, b \in A$. (Equivalently, the image of Φ is a subset of A.)

You are probably familiar with many closed binary operators:
$+$ is a closed binary operator on $\mathbb{Z}$: $2 + 3 = 5$
$*$ is a closed binary operator on $\mathbb{Q}$: $\frac{1}{3} * \frac{3}{5} = \frac{1}{5}$
$\times$ (the vector cross product) is a closed binary operator on $\mathbb{R}^3$:
$(a, b, c) \times (x, y, z) = (bz - cy, cx - az, ay - bx)$

Examples of binary operators that are not closed:
$\div$ is not closed on $\mathbb{Z}$: $5 \div 2 = \frac{5}{2}$, which is not an integer
$\cdot$ is not closed on $\mathbb{R}^2$: $(a, b) \cdot (x, y) = ax + by$, which is not an element of $\mathbb{R}^2$

Definition 11. A **group** $(G, \star)$ consists of a set G and a binary operator $\star$ defined in such a way that the following four rules are true:

0) $\star$ is closed on G: if $a, b \in G$, then $(a \star b) \in G$
1) $\star$ is associative: if $a, b, c \in G$, then $(a \star b) \star c = a \star (b \star c)$
2) G contains the **identity** of $\star$: $\exists e \in G$ such that $\forall a \in G, (a \star e) = a$
3) Inverses exist: $\forall a \in G, \exists z \in G$ such that $(a \star z) = e$

Examples and counterexamples:

$(\mathbb{Z}, +)$ is a group:
1) $(a + b) + c = a + (b + c)$ for any integers a, b, c
2) $a + 0 = a$ for any integer a (0 is called the *additive identity*)
3) for every integer a, there is an integer $-a$ such that $a + (-a) = 0$

$(\mathbb{Z}, -)$ is not a group:
$(1 - 2) - 3 \neq 1 - (2 - 3)$. Subtraction is not associative, so rule 1 fails.

$(\mathbb{R}^3, \times)$ is not a group:
There is no "cross product identity" vector in $\mathbb{R}^3$, so rule 2 fails.

$(\mathbb{Q}, *)$ is almost a group, but not quite:

1) $(a * b) * c = a * (b * c)$ for all rationals a,b,c
2) $a * 1 = a$ for all rationals a (1 is called the *multiplicative identity*)
3) 0 does not have a multiplicative inverse in $\mathbb{Q}$: $0^{-1} \notin \mathbb{Q}$.
This looks silly, but it's important! Every operation in a group can be undone with an inverse operation. "Multiply by zero" is somehow too destructive; no inverse operation exists. For practice, check that we can form a group by removing 0 from $\mathbb{Q}$: $(\mathbb{Q} - \{0\}, *)$ is a group.

WARNING: It is very common to refer to the group $(\mathbb{Z}, +)$ as "the group $\mathbb{Z}$." Remember that a set without an operation is not a group! Sometimes it's obvious what is meant; $\mathbb{Z}$ can form a group under addition but not subtraction, multiplication, or division.

3.2 Isomorphic groups

Define the set $2\mathbb{Z} = \{$ all even integers $\}$. Is $(2\mathbb{Z}, +)$ a group?

First check that $+$ is closed on $2\mathbb{Z}$: $\forall a, b \in \mathbb{Z}, 2a + 2b = 2(a + b) \in 2\mathbb{Z}$
1) $+$ is still associative.
2) $0 \in 2\mathbb{Z}$, so the identity element exists.
3) $2a + (-2a) = 0$, so additive inverses exist.

As a group, $(2\mathbb{Z}, +)$ behaves identically to $(\mathbb{Z}, +)$. All we did was relabel the nonzero elements: rename $1 \to 2$, $2 \to 4$, etc. The elements still behave the same way: $6 + 7 = 13$ in $(\mathbb{Z}, +)$ and $12 + 14 = 26 =$ "13 renamed" in $(2\mathbb{Z}, +)$.

In general, to show that two groups behave the same, we must show there is a "relabeling map" from one to the other that does not change the group structure. In this case, $\Phi(a) = 2a$ is a relabeling map from $\mathbb{Z}$ to $2\mathbb{Z}$.

Definition 12. A **group homomorphism** is a map Φ from G to H compatible with the group operations of $(G, \star)$ and $(H, \heartsuit)$:
$\Phi(g_1) \heartsuit \Phi(g_2) = \Phi(g_1 \star g_2)$ for all $g_1, g_2 \in G$.

Definition 13. A **group isomorphism** is an invertible group homomorphism. If Φ is invertible, then Φ^{-1} is an isomorphism from $(H, \heartsuit)$ to $(G, \star)$. (To prove this, define $h_1 = \Phi(g_1)$, etc. and use the definitions of invertible map and group homomorphism.)

Definition 14. Two groups $(G, \star)$ and $(H, \heartsuit)$ are **isomorphic** to each other if a group isomorphism exists between them. Isomorphic groups in this document are denoted $(G, \star) \cong (H, \heartsuit)$ or sometimes $G \cong H$.

In our example, Φ was a map from $\mathbb{Z}$ to $2\mathbb{Z}$. Both groups used $+$ as their operation and $\Phi(a) = 2a$ is compatible: $2a + 2b = 2(a + b)\ \forall a, b \in \mathbb{Z}$. Φ is also invertible, so we conclude that the groups are isomorphic: $\mathbb{Z} \cong 2\mathbb{Z}$.

Mathematicians view isomorphic groups as identical structures with different labels on their elements and/or a different name for the operator. We can operate two elements of G together, or we can operate their "relabeled" counterparts in H, "un-label" the result back to G, and get the same answer: $g_1 \star g_2 = \Phi^{-1}(\Phi(g_1)\heartsuit\Phi(g_2))$. Invertibility is important if we want to say two groups are "the same."

3.3 Finite Groups

Definition 15. If $(G, \star)$ is a group, the **order** of this group is $|G|$, the number of elements in G. If $|G| \in \mathbb{N}$, G is called a **finite group**.

The groups $(\mathbb{Z}, +)$ and $(\mathbb{Q} - \{0\}, *)$ are not finite. Let's find some that are.

Definition 16. Define **modular addition** for any $n \in \mathbb{N}$: let $a + b$ (mod n) denote "the remainder when $a + b$ is divided by n." Define $\mathbb{Z}_n$ as the set of integers $\{0\ ...\ (n-1)\}$.

Note that $a + b$ (mod n) is a closed binary operation on $\mathbb{Z}_n$. Examples: $6 + 9\ (\text{mod } 10) = 5$, $2 + 2\ (\text{mod } 4) = 0$, $2^{100} + 1\ (\text{mod } 2) = 1$.

For any $n \in \mathbb{N}$, ($\mathbb{Z}_n$, + (mod n)) is a finite group.
1) + (mod n) is associative. $(a + b) + c = a + (b + c)$
2) 0 is the identity. $a + 0 = a$
3) the inverse of a is $n - a$. $[a + (n - a)]$ (mod n) $= n$ (mod n)$= 0$.
4) $|\mathbb{Z}_n|$ is a natural number by definition, so $\mathbb{Z}_n$ is finite.

Example: $\mathbb{Z}_4 = \{\ 0, 1, 2, 3\ \}$ has the following structure table:[2]

+ (mod 4)	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

How to read this table:
To find 1 + 2, find 1 in the left column and 2 in the top row. The result here is 3. Notice that the table is symmetric about its diagonal - this will not be true for all groups! Remember that in (mod 4) addition, 2+2 = 0, 2+3 = 1, and 3+3 = 2.

[2]Also known as a **Cayley table**. Arthur Cayley originally called them **squares**.

3.4 Cyclic Groups

The *cyclic* groups $\mathbb{Z}_n$ are especially straightforward: for any $n \in \mathbb{N}$, we can *generate* the entire group $\mathbb{Z}_n$ by operating 1 on itself repeatedly. Before introducing them, we pause for some new notation:

Definition 17. For any element a in a group $(G, \star)$, define the **powers** of a: $a^n = (a \star a \star \ldots \star a)$ where a appears in parentheses n times (and $n \in \mathbb{N}$).

WARNING: The notation $(a)(b)$ or ab is very common shorthand for $a \star b$ in group theory. This will look completely ridiculous when the operator being represented is addition: $(1)(3)$ means $(1+3)$, 2^5 means $(2+2+2+2+2)$, and so on. We adopt power notation for group operations now because it will be far more useful for matrix multiplication and symmetry transformations later.

Definition 18. Let a be an element of a group $(G, \star)$ and let d denote the identity of $(G, \star)$. The smallest natural number k such that $a^k = d$ is called the **order** of element a and is denoted $|a| = k$.

Definition 19. If the set $\{a, a^2, \ldots, a^k\}$ contains every element of G, then a is said to **generate** $(G, \star)$. If so, the order of the group G will be the same as the order of a. $|G| = |a| = k$.

Not all groups can be generated by repeated operations of the same element with itself. Groups that can be generated this way are called *cyclic*:

Definition 20. A finite group G of order n is called **cyclic** if it can be written $\{a, a^2, \ldots, a^n\}$ for some element $a \in G$.

Examples of cyclic groups:

The group $\mathbb{Z}_4$ can be written $\{1, 1^2, 1^3, 1^4\} = \{1, 2, 3, 0\}$. (As expected, power notation looks absurd when $+$ is the operation we're denoting.)

Cut a square out of cardboard and place it in front of you. Define $\curvearrowleft$ as the operation "rotate the square 90° counterclockwise." Define $\curvearrowleft^n$ to mean "do $\curvearrowleft$ n times." $\{\curvearrowleft, \curvearrowleft^2, \curvearrowleft^3, \curvearrowleft^4\}$ is a cyclic group. The group operation is "rotation composition" and the identity is $\curvearrowleft^4$. This group is isomorphic to $\mathbb{Z}_4$.

If $z \in \mathbb{C}$ and $z^n = 1$, z is called an **nth root of unity**. For any $n \in \mathbb{N}$, the nth roots of unity form a group under multiplication. For example, the fourth roots of unity $\{1, i, -1, -i\}$ are generated by i:

$\imath^1 = \imath, \imath^2 = -1, \imath^3 = -\imath, \imath^4 = 1$. This group is isomorphic to $\mathbb{Z}_4$.

If you've ever heard someone refer to $\imath$ as "a 90° rotation," this is what he/she meant! Generators are important and will show up later in new clothes as *Lie algebras*. For practice, find the 6th complex roots of unity. (Hint: Draw 30°-60°-90° triangles in the complex plane.)

You may have already conjectured the following theorem:

Theorem 1. *Every cyclic group of order n is isomorphic to $\mathbb{Z}_n$.*

Proof: Construct an isomorphism explicitly. $(G, \star)$ is a cyclic group of order $n \Leftrightarrow G = \{a, a^2, \ldots, a^n\}$ for some $a \in G$. Define $\Phi(a) = 1$, $\Phi(a^2) = 2, \ldots, \Phi(a^n) = n$. Then Φ is compatible: for any $j, k \in \mathbb{N}$, $\Phi(a^j \star a^k) = \Phi(a^{j+k}) = j + k \text{ (mod n)} = \Phi(a^j) + \Phi(a^k) \text{ (mod n)}$. Each element of G is mapped to exactly one element of $\mathbb{Z}^n$ and vice versa, so Φ is invertible. Therefore Φ is an isomorphism.

Mathematicians refer to all three of the examples above as the cyclic group of order 4. Each is isomorphic to the others regardless of what symbols are used to denote the elements or the group operation. The notation $\mathbb{Z}_n = \{a, a^2, \ldots, a^n\}$ is used here for any cyclic group of order n.

It is worth noting that there is another group of order 4 which is not cyclic. Alternately called the **Klein group**, the **Vierergruppe**,[3] or $\mathbb{Z}_2 \oplus \mathbb{Z}_2$, it is the smallest noncyclic group. All groups of order 4 are isomorphic to either $\mathbb{Z}_4$ or the Klein group. Its structure table is:

$\star$	1	i	j	k
1	1	i	j	k
i	i	1	k	j
j	j	k	1	i
k	k	j	i	1

Notice that every element is its own inverse and order of operations does not matter. The Klein group is isomorphic to the *direct sum* group $\mathbb{Z}_2 \oplus \mathbb{Z}_2$, to be defined in the next section.

Évariste Galois showed that this group guarantees the solvability of quartic (fourth-order) polynomials. Galois' research into higher-order polynomials is often considered the beginning of modern group theory.

[3]German for "four-ish group," or something like that. "Klein" is named for Felix Klein and is coincidentally the German word for "small."

4 More Groups

Notice what happens if we try to generate $\mathbb{Z}_4$ from the "wrong" element:

$0 + 0 = 0$ generates the set $\{ 0 \}$
$2 + 2 = 0, 0 + 2 = 2$ generates the set $\{ 0, 2 \}$
$3 + 3 = 2, 2 + 3 = 1, 1 + 3 = 0$ generates the set $\{ 2, 1, 0, 3 \} = \mathbb{Z}_4$

Apparently 3 is a perfectly good generator! The other two have "missed" some elements, but they have generated miniature groups of their own.

Definition 21. If $(G, \star)$ is a group, H is some subset of G, and $(H, \star)$ is a group, then $(H, \star)$ is called a **subgroup** of $(G, \star)$. If H is a proper subset of G, then $(H, \star)$ is a **proper subgroup** of $(G, \star)$.

To prove that a subset H forms a subgroup, use the "Subgroup Test": show that $(a, b \in H) \Rightarrow (a \star b^{-1} \in H)$. Note that we already know $\star$ is associative. Be sure that H contains the identity of $(G, \star)$ so that $a \star a^{-1} \in H$.

Example: $\{ 0, 2 \}$ is a group under the operation + (mod 4). It is a proper subgroup of $\mathbb{Z}_4$ and is isomorphic to $\mathbb{Z}_2$.

Example: $\{ 0 \}$ is a group under + (mod 4). It is isomorphic to the group $\mathbb{Z}_1$ (often called the **trivial group**). Any group with one element is (trivially) cyclic and therefore isomorphic to $\mathbb{Z}_1$.

Theorem 2. *Every subgroup of a cyclic group is cyclic. $\mathbb{Z}_j$ is isomorphic to a subgroup of $\mathbb{Z}_n$ if and only if j is a factor of n.*

Theorem 3. *If $(G, \star)$ is finite and $(H, \star)$ is a subgroup, then $|H|$ is a factor of $|G|$. The order of every element in G is a factor of $|G|$. [Szekeres]*

We will see many more examples of subgroups in the next sections.

4.1 Factor Groups

Definition 22. Let $(H, \star)$ be a subgroup of $(G, \star)$. For any element $a \in G$, define the **left coset** aH to be the set $\{a \star h_0, a \star h_1, a \star h_2, \dots\}$ where h_0 is the identity and the other h_j are all the other elements of H.

Example: $H = \{0, 2\}$ is a subgroup of $\mathbb{Z}_4$. Its left cosets are
$0H = \{0, 2\}, 1H = \{1, 3\}, 2H = \{2, 0\}, 3H = \{3, 1\}$.

In this example, $0H$ and $2H$ are different names for the set $\{0, 2\}$ and $1H$ and $3H$ are different names for the set $\{1, 3\}$. Also notice that the cosets of H **partition** G; they split it into sets that do not overlap. Keep in mind that each coset of H is a subset of G, but not necessarily a subgroup of $(G, \star)$. In our example, $\{1, 3\}$ is not a subgroup of $\mathbb{Z}_4$.

Definition 23. Define **right cosets** of H in G: $Ha = \{a, h_1 \star a, h_2 \star a, \dots\}$. A subgroup H is **normal** if $aH = Ha$ for all $a \in G$.

The left and right cosets of $\{0, 2\}$ in $\mathbb{Z}_4$ are equal because the operation $+$ (mod n) is *commutative*: $a + b = b + a$ always. Operations that do not commute can sometimes cause "abnormal" subgroups.[4]

If a group $(G, \star)$ has a normal subgroup $(H, \star)$, we can try to "factor out" the behavior of H to form a simpler group. This new group will have cosets of H as its elements and a new operation $\diamond$ defined as follows:

Definition 24. Let $(G, \star)$ have a normal subgroup $(H, \star)$. Define the **coset operation** $\diamond$: $aH \diamond bH = (a \star b)H = \{a \star b, a \star b \star h_1, a \star b \star h_2, \dots\}$ where a, b are any two elements of G and the h_j are all the elements of H. The cosets of H under the operation $\diamond$ form a group called the **factor group** G/H, pronounced "G modulo H" or "G slash H."

Example: The cosets of $H = \{0, 2\}$ in $\mathbb{Z}_4$ are $0H$ and $1H$ from above. $\{0H, 1H\}$ under $\diamond$ forms the factor group $\mathbb{Z}_4/H$. Its structure table is:

$\diamond$	$0H$	$1H$
$0H$	$0H$	$1H$
$1H$	$1H$	$0H$

$$0H \diamond 0H = (0+0)H = 0H$$
$$0H \diamond 1H = (0+1)H = 1H$$
$$1H \diamond 0H = (1+0)H = 1H$$
$$1H \diamond 1H = (1+1)H = 2H = 0H$$

This structure table looks exactly like the table for $\mathbb{Z}_2$, so $\mathbb{Z}_4/H$ is isomorphic to $\mathbb{Z}_2$. Earlier we showed that H itself is also isomorphic to $\mathbb{Z}_2$. Abusing our notation somewhat, we can write $\mathbb{Z}_4/\mathbb{Z}_2 \cong \mathbb{Z}_2$.

Definition 25. Every group $(G, \star)$ contains itself and $\mathbb{Z}_1$ as factor groups. If no other factor group can be defined, then $(G, \star)$ is a **simple** group.

"Simple" is a dangerous term. A "monster group" has been discovered which is simple and of order 808,017,424,794,512,875,886,459,904,961,710 757,005,754,368 billion. In retrospect, "prime" might have been a better name for an unfactorable group.

[4] A noncommutative group with no abnormal subgroups is called **Hamiltonian** after Sir William Rowan Hamilton and his famous example, the *quaternion group* $\mathbb{Q}_8$.

4.2 Direct Products and Direct Sums

Factor groups can be used to break a group apart into simpler groups. Similarly, we can define *direct product* groups that combine two groups to make a more complicated one:

Definition 26. Given two groups $(G, \star)$ and $(H, \heartsuit)$, a new group called the **direct product group** $(G, \star) \otimes (H, \heartsuit)$ can be constructed. The elements are ordered pairs (g, h) where $g \in G$ and $h \in H$ and the operation $\times$ is defined $(g_1, h_2) \times (g_2, h_2) = (g_1 \star g_2, h_1 \heartsuit h_2)$.

Example: $\mathbb{R}^+$, the set of all positive real numbers, forms a group under multiplication. The set $\mathbb{R}^+ \otimes \mathbb{R}^+$ consists of all ordered pairs (x, y) where x and y are positive real numbers. Define $(x, y) * (a, b) = (xa, yb)$ to form the group $(\mathbb{R}^+ \otimes \mathbb{R}^+, *)$. $(1, 1)$ is the identity and $(x, y)^{-1} = (x^{-1}, y^{-1})$.

The direct product group $G \otimes H$ will always contain a normal subgroup isomorphic to G and another one isomorphic to H. To see this, let 1_g and 1_h denote the identities of G and H and consider the sets $\{(g, 1_h)\}$ and $\{(1_g, h)\}$ where g is any element of G and h is any element of H. These two sets form subgroups isomorphic to G and H respectively.

Definition 27. If the operations of G and H are denoted by addition (rather than multiplication or some other symbol), the term **direct sum** is used instead of direct product. Direct sums are denoted $G \oplus H$. It is conventional to reserve the symbol + only for *commutative* operations.

Notice that $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ consists of the elements $\{(0, 0), (1, 0), (0, 1), (1, 1)\}$. If the elements are renamed $\{1, i, j, k\}$, their structure table is identical to that of the Klein group from before and so Klein $\cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$.

WARNING: Since we know that $\mathbb{Z}_4/\mathbb{Z}_2 \cong \mathbb{Z}_2$, it is very tempting to write $\mathbb{Z}_4 \cong \mathbb{Z}_2 \otimes \mathbb{Z}_2$. Don't do it! Not only are we using bad notation by representing additive groups with $\otimes$, but $\mathbb{Z}_2 \otimes \mathbb{Z}_2$ is not isomorphic to $\mathbb{Z}_4$. Direct products do not "undo" factor groups.

In the next section we will see that $D_3/\mathbb{Z}_3 \cong \mathbb{Z}_2$ and $\mathbb{Z}_6/\mathbb{Z}_3 \cong \mathbb{Z}_2$ despite the fact that D_3 and $\mathbb{Z}_6$ are not isomorphic. While there is a close analogy between factoring groups and factoring natural numbers, be careful not to take the analogy too far!

4.3 Noncommutative Groups

So far, every group operation we have seen obeys the commutative property: $a \star b = b \star a$ for any $a, b \in G$. Not all groups behave this way.

Definition 28. A group $(G, \star)$ in which $a \star b = b \star a$ for all $a, b \in G$ is called **commutative** or **Abelian**.[5]

Theorem 4. *All cyclic groups are commutative.*

Proof: Any cyclic group $(G, \star)$ has a generator a such that every element of G can be written as a^j for some $j \in \mathbb{N}$. Thus the result of any operation can be written as $a^j \star a^k = a^{j+k} = a^{k+j} = a^k \star a^j$ for some $j, k \in \mathbb{N}$.

Essentially, a commutes with itself and therefore so do the elements it generates. Noncyclic groups can also be commutative, but many are not.

Example: The set of all 3x3 real matrices with nonzero determinant form a group under the operation of matrix multiplication. (Any square matrix has a multiplicative inverse if and only if its determinant is not zero.) This group is called $GL(3, \mathbb{R})$, the *General Linear 3-dimensional real group.* Some elements of $GL(3, \mathbb{R})$ commute, but these two certainly don't:

$$\begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ -1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -1 & 0 \\ 0 & 0 & 1 \\ -1 & 0 & 0 \end{pmatrix}$$

Now multiply the first two matrices in reverse order:

$$\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ -1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

Reversing the order of operations does not give the same result!

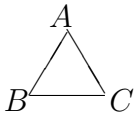
Experiment: The *Special Orthogonal group* $SO(3)$ of all possible rotations in a 3-dimensional vector space is noncommutative. Find an object that is not perfectly symmetrical and choose three directions x,y, and z that are perpendicular to each other. Rotate an object 90° counterclockwise as seen by someone looking in the positive-y direction. Now rotate the object 90° counterclockwise as seen by someone looking in the positive-z direction.

[5]Named after Norwegian mathematician Niels Henrik Abel, pronounced "ah-bell".

Draw a sketch of the object. Return the object to its original position and repeat, but this time do the z-axis rotation first. Is the object oriented the same way as before? (Hint: No.)

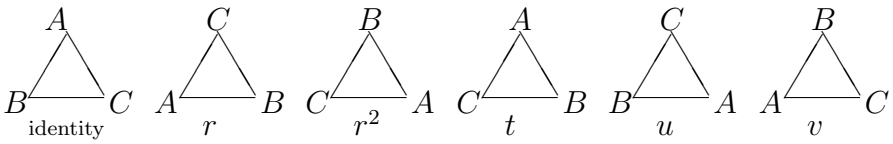
$SO(3)$ is extremely important in theoretical physics and chemistry, but for now, we will set it aside and practice on finite groups. The symmetry groups of regular 2D polygons are called the *dihedral groups* D_n and are never commutative.[6] The smallest noncommutative group (i.e. the one with the fewest elements) is D_3, the symmetry group of an equilateral triangle.

Experiment: Construct a cardboard model of a triangle and pretend it is absolutely perfect, with equal 60° angles and equal sides. Label the vertices A,B, and C. Set the triangle on the desk in front of you like this:



If the triangle is left flat on the table, it can be rotated 120°, 240°, or 360°, or integer multiples of those. Name those transformations $\{r, r^2, r^3\}$. Since r^3 is equivalent to "don't touch the triangle," let's rename it "the identity transformation" and write $r^3 = 1$.

If we allow operations in three dimensions, the triangle can also be flipped in three different ways. Flip over the triangle so that the top point is unmoved and call this transformation t (for "top vertex"). Flips around the other two vertices will be named u and v as shown below:



Now define $(a \triangleright b)$ to mean "do transformation b, then do transformation a to the result." (The notation may look backwards, but it will be useful for matrix transformations later.) The set of all six transformations $\{1, r, r^2, t, u, v\}$ forms a group under the operation $\triangleright$, called "transformation composition." The group is called D_3 and its structure table is:

[6] We could define commutative groups D_1 and D_2, but no 1- or 2-sided polygons exist.

$\triangleright$	1	r	r^2	t	u	v
1	1	r	r^2	t	u	v
r	r	r^2	1	v	t	u
r^2	r^2	1	r	u	v	t
t	t	u	v	1	r	r^2
u	u	v	t	r^2	1	r
v	v	t	u	r	r^2	1

This structure table is not symmetric because D_3 is not a commutative group. Be sure to read the table in the correct order: the result of $r \triangleright t$ is listed in row r, column t and it is v. Check the accuracy of the table by drawing triangles or using the cardboard model.

For practice, we will now find all subgroups and factor groups of D_3. Notice that the product of two rotations is always another rotation: $\{1, r, r^2\}$ looks promising as a potential subgroup. Apply the Subgroup Test: for any two rotations a and b, is $a \triangleright b^{-1}$ a rotation? Yes! The inverse of r is r^2, the inverse of r^2 is r, and the product of two rotations is another rotation. Also, the identity is contained in $\{1, r, r^2\}$, so $\{1, r, r^2\}$ is a subgroup. In fact, it's a cyclic group of order 3 because r generates $\{1, r, r^2\}$.

Stare at the structure table for D_3 and look for other subgroups. $\{1, t\}$ is a subgroup: it includes 1 and it passes the Subgroup Test. Similarly, $\{1, u\}$ and $\{1, v\}$ are each subgroups. Because there are only 6 elements in D_3, it's not hard to see that no other proper subgroups exist. ($\{1\}$ is not proper!)

Are these subgroups normal? If so, we can use them to build factor groups. Look at the rotation subgroup first: denote $\{1, r, r^2\}$ as H and use the structure table to find its left and right cosets aH and Ha for all $a \in G$:

$1H = \{1, r, r^2\} \qquad rH = \{r, r^2, 1\} \qquad r^2H = \{r^2, 1, r\}$

$tH = \{t, tr, tr^2\} = \{t, u, v\} \qquad uH = \{u, ur, ur^2\} = \{u, v, t\}$
$vH = \{v, vr, vr^2\} = \{v, t, u\}$

The left cosets are apparently $1H = \{1, r, r^2\}$ and $tH = \{t, u, v\}$; the other left cosets are each equivalent to one of these. We have partitioned D_3 into a "rotation coset" $1H$ and a "flip coset" tH. Check the right cosets $H1$ and Ht to see if H is normal:

$H1 = \{1, r, r^2\} = 1H$ (of course! 1 commutes with everything.)
$Ht = \{t, rt, r^2t\} = \{t, v, u\} = tH$.

H is a normal subgroup, so we can define the factor group D_3/H by using the coset operation $\diamond$ as before: $aH \diamond bH = (ab)H = \{ab1, abr, abr^2\}$.

Written out completely, we have:

$1H \diamond 1H = 1H \qquad 1H \diamond tH = tH \qquad tH \diamond 1H = tH$
$tH \diamond tH = (t^2)H = \{t^2, t^2r, t^2r^2\} = \{1, r, r^2\} = 1H$

The structure table of D_3/H looks like either of these:

$\diamond$	$1H$	tH
$1H$	$1H$	tH
tH	tH	$1H$

or

$\diamond$	rotations	flips
rotations	rotations	flips
flips	flips	rotations

The factor group D_3/H has only two elements, so it is isomorphic to $\mathbb{Z}_2$. H is known to be isomorphic to $\mathbb{Z}_3$, so we feel justified writing $D_3/\mathbb{Z}_3 \cong \mathbb{Z}_2$.

Exercise: Show that these subgroups of D_3 are <u>not</u> normal: $\{1, t\}$, $\{1, u\}$, $\{1, v\}$. These subgroups cannot be used to form factor groups of D_3.

Be careful not to assume that $\mathbb{Z}_3 \otimes \mathbb{Z}_2 \cong D_3$. The group $\mathbb{Z}_6$ also can be factored $\mathbb{Z}_6/\mathbb{Z}_3 \cong \mathbb{Z}_2$. If groups factored the way natural numbers do, we could conclude that $D_3 \cong \mathbb{Z}_6$, which is wrong! $\mathbb{Z}_6$ is cyclic and D_3 is <u>not</u>; D_3 is not even commutative. Apparently $(G/H \cong K) \not\Rightarrow (G \cong H \otimes K)$.

What does the real $\mathbb{Z}_3 \otimes \mathbb{Z}_2$ look like? First, let's use the $\oplus$ notation instead of $\otimes$ because we're using $+$ as our operator. Elements of $\mathbb{Z}_3 \oplus \mathbb{Z}_2$ look like this: $(0,0), (0,1), (1,0), (1,1), (2,0), (2,1)$

The operation for $\mathbb{Z}_3 \oplus \mathbb{Z}_2$ is strange: the left elements are added (mod 3) and the right elements are added (mod 2): $(a, b) \star (x, y) = (a + x \pmod 3 , b + y \pmod 2)$. The structure table looks like:

$\star$	(0,0)	(0,1)	(1,0)	(1,1)	(2,0)	(2,1)
(0,0)	(0,0)	(0,1)	(1,0)	(1,1)	(2,0)	(2,1)
(0,1)	(0,1)	(0,0)	(1,1)	(1,0)	(2,1)	(2,0)
(1,0)	(1,0)	(1,1)	(2,0)	(2,1)	(0,0)	(0,1)
(1,1)	(1,1)	(1,0)	(2,1)	(2,0)	(0,1)	(0,0)
(2,0)	(2,0)	(2,1)	(0,0)	(0,1)	(1,0)	(1,1)
(2,1)	(2,1)	(2,0)	(0,1)	(0,0)	(1,1)	(1,0)

This table is symmetric about its diagonal, so order of operations does not matter. $\mathbb{Z}_3 \oplus \mathbb{Z}_2$ is commutative.

Exercise: Show that $\mathbb{Z}_3 \oplus \mathbb{Z}_2$ is cyclic of order 6 and therefore $\mathbb{Z}_3 \oplus \mathbb{Z}_2 \cong \mathbb{Z}_6$. Construct an isomorphism explicitly. (Hint: Pick an element of $\mathbb{Z}_3 \oplus \mathbb{Z}_2$ and

operate it on itself repeatedly. Keep trying until you find an element that generates the entire group. Map that element to a generator of $\mathbb{Z}_6$.)

4.4 Permutation Groups

Definition 29. If a set S has a finite number of elements, then any invertible map from S to itself is called a **permutation** of S.

Informal Definition: If some number of things are arranged in a specific order, a permutation is a way of rearranging those things.

Instead of drawing triangles (or constructing a cardboard model) to study D_3, we could have simply written down the letters $\{A, B, C\}$ and every possible permutation of them:

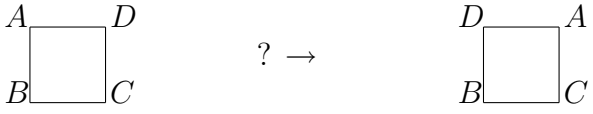
permutation	(A,B,C)	(C,A,B)	(B,C,A)	(A,C,B)	(C,B,A)	(B,A,C)
name	1	r	r^2	t	u	v

These ordered triplets form a group under the operation of **permutation composition**: $a \triangleright b =$ "do permutation b, then do permutation a to the result." This group is isomorphic to D_3 and an isomorphism is shown explicitly in the table above. Groups formed by permutations are important enough to have their own name:

Definition 30. For any $n \in \mathbb{N}$, define the **symmetric group** S_n as the set of all permutations of n distinct elements under the operation of permutation composition.

WARNING: The name "symmetric group" does not imply that the structure tables of S_n are symmetric! If $n > 2$, then S_n is not commutative and thus its structure table is not symmetric.

S_3, the group of all permutations of 3 elements, is isomorphic to D_3, the symmetry group of a regular triangle. Can we extrapolate and claim that D_4 is isomorphic to S_4? No! Construct a cardboard square and label its vertices $\{A, B, C, D\}$. Consider the permutation (A,B,C,D) $\rightarrow$ (D,B,C,A):



This transformation would require an exceptionally flexible square! D_4 is not isomorphic to S_4, but D_4 is isomorphic to a subgroup of S_4. All

symmetry transformations of a square can be represented by permutations of 4 elements, but not all permutations of 4 elements represent symmetries of a square. This conclusion is a special case of the following theorem:

Theorem 5. *Every finite group is isomorphic to a subgroup of some S_n.*

We are now ready, at last, to give an informal definition of finite group:

Informal Definition: A finite group is a list of things together with several ways to rearrange those things and instructions about how to put them back where they started.

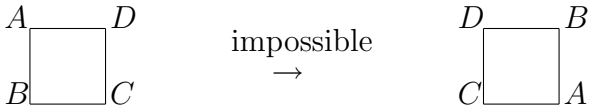
There are 6 distinct permutations of 3 elements and 24 distinct permutations of 4 elements. For any $n \in \mathbb{N}$, it is well known that the order of S_n is n **factorial**: $n! = n * (n-1) * (n-2) * \cdots * 2 * 1$. Thus, given a finite group, we can know everything about it by choosing a large enough n, writing out all $n!$ elements of S_n, and looking for subgroups.

Faced with this task, we now declare ourselves experts at finite group theory and abandon the subject. Here are more exercises to fill space:

Definition 31. A **derangement** of an ordered n-tuple $(a_1, a_2, \ldots, a_n)$ is a permutation ϕ that maps no element to itself: $\forall k \in \mathbb{N} : k \leq n, \phi(a_k) \neq a_k$.

Example: The two non-identity rotations of our cardboard triangle represent derangements of (A,B,C): (C,A,B) and (B,C,A). The non-identity rotations of any regular n-sided polygon will always represent a subset of the derangements of an ordered list of n elements.

Exercise: Write down all 9 derangements of (A,B,C,D). Label the vertices of a square with the letters ABCD. Which derangements represent symmetries of the square shown below? (Hint: Some of the derangements are impossible transformations of the square. Here is one of them:)



(A,B,C,D) (D,C,A,B)

Exercise: Rubik's group - the group of all operations on a Rubik's cube that do not involve disassembling the cube - is a subgroup of S_{48} with 43,252,003,274,489,856,000 elements. Scramble a Rubik's cube and solve it.