WHAT IS A GROUP?

	$(1)(2)(3)$	$(1\ 2)$	$(1\ 3)$	$(2\ 3)$	$(1\ 2\ 3)$	$(1\ 3\ 2)$
$(1)(2)(3)$	$(1)(2)(3)$	$(1\ 2)$	$(1\ 3)$	$(2\ 3)$	$(1\ 2\ 3)$	$(1\ 3\ 2)$
$(1\ 2)$	$(1\ 2)$	$(1)(2)(3)$	$(1\ 2\ 3)$	$(1\ 3\ 2)$	$(1\ 3)$	$(2\ 3)$
$(1\ 3)$	$(1\ 3)$	$(1\ 3\ 2)$	$(1)(2)(3)$	$(1\ 2\ 3)$	$(2\ 3)$	$(1\ 2)$
$(2\ 3)$	$(2\ 3)$	$(1\ 2\ 3)$	$(1\ 3\ 2)$	$(1)(2)(3)$	$(1\ 2)$	$(1\ 3)$
$(1\ 2\ 3)$	$(1\ 2\ 3)$	$(2\ 3)$	$(1\ 2)$	$(1\ 3)$	$(1\ 3\ 2)$	$(1)(2)(3)$
$(1\ 3\ 2)$	$(1\ 3\ 2)$	$(1\ 3)$	$(2\ 3)$	$(1\ 2)$	$(1)(2)(3)$	$(1\ 2\ 3)$

Definition: Let G be a nonempty set and let * be a function with domain $G \times G$. Then the set G together with the function * is a *group* if and only if the following axioms are satisfied.

1. (*Closure*) For all $a,b \in G$, $a * b \in G$. (In other words, * is function from $G \times G \to G$.)

2. (*Associativity*) For all $a,b,c \in G$, $(a * b) * c = a * (b * c)$.

3. (*Identity*) There exists an element e in G called the *identity element* with the property that for any $a \in G$, $a * e = e * a$.

4. (*Inverse*) For any $a \in G$, there exists an element $a^{-1} \in G$ with the property that $a * a^{-1} = e = a^{-1} * a$.

Sometimes a group possesses a fifth property that we call *commutativity*, and when this happens the result is what we call either a *commutative* or *abelian group* (after the Norwegian mathematician Niels Henrik Abel (1802 – 1829) who can be said to have been one of the creators of group theory.)

(*Commutativity*) For all $a, b \in G$, $a * b = b * a$.

At this point, we should probably just look at several different examples of groups so that we can appreciate just how far reaching this concept is.

1. The real numbers under addition.

2. The non-zero real numbers under multiplication.

3. The positive real numbers under multiplication.

4. The complex numbers under addition.

5. The non-zero complex numbers under multiplication.

6. The rational numbers under addition.

7. The non-zero rational numbers under multiplication.

8. The positive rational numbers under multiplication.

9. The integers under addition.

1. The integers modulo *n* under addition (look it up, if you have to!).

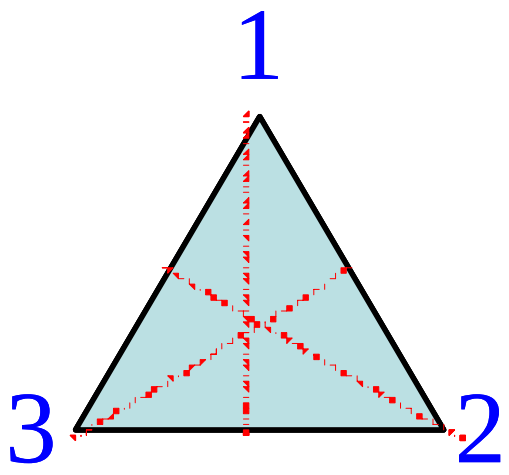
2. All 3×3 invertible matrices under matrix multiplication.

3. All 3×3 permutation matrices under matrix multiplication.

4. All permutations of 3 objects under multiplication of permutations.

5. All quadratic polynomials in one variable with integer coefficients (the operation is addition of polynomials).

6. The group of symmetries of an equilateral triangle. By symmetries we mean those rotations about a center or flips about an axis of symmetry that preserve the distance between points and that leave the triangle looking the same as what we started with. We multiply flips and rotations by simply following one by the other.



7. The group of symmetries associated with a frieze pattern such as the one below. In this case, we see a square pattern that is repeated four times in a cycle. We also see that that our basic shape has an additional mirror symmetry about a horizontal line going through its middle. Thus, we could take just the bottom half of that square and generate the whole pattern by doing translations to the right, and reflections about our axis of symmetry, and when we get to the rightmost end, we can just wrap back around to the beginning.

8. As you can see, most of the groups defined above are groups of numbers, but that is only because I am starting with what you are most familiar with. As I mentioned previously, anytime you have either permutations or symmetry involved, there's a group lurking in the background. For example, just consider the solutions to the quadratic equation $ax^2 + bx + c = 0$ that we get via the quadratic formula, $x = \frac{-b + \sqrt{b^2 - 4ac}}{2a}$ and $x = \frac{-b - \sqrt{b^2 - 4ac}}{2a}$. There is an obvious symmetry between these two solutions. In fact, if I define *F* to mean "flip the sign in front of the square root" and I define *I* to mean "do nothing at all," then we get the following multiplication table for the symmetry observed here.

	I	F
I	I	F
F	F	I

Even though this multiplication table is pretty elementary, it does define a group. Furthermore, it was by studying such symmetries related to the solutions of polynomial equations that Evariste Galois (1811 – 1832) was able to prove that there is no general algebraic formula for solving polynomial equations of degree 5 or higher. Now that is a result that depends on group theory that is far from trivial!

	I	F
I	I	F
F	F	I

The number of elements in a group G is called the *order* of the group, and for the most part we will focus in this book on finite groups. Thus, if a group contains n elements, then this is denoted by writing $|G| = n$.

Now let me show you a couple of theorems that apply to all groups, and remember, by proving these theorems for groups in general, we are simultaneously killing several groups of birds with one stone (metaphorically, that is). This is part of the power of group theory!

Theorem: Let G be a group. If $a,b \in G$, then $(ab)^{-1} = b^{-1}a^{-1}$.

Proof: To verify this, we simply need to show that $(ab)(b^{-1}a^{-1}) = e$. But this is obvious because $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = aa^{-1} = e$. Therefore, $(ab)^{-1} = b^{-1}a^{-1}$. □

Theorem: Let G be a group. If $a \in G$, then $(a^{-1})^{-1} = a$.

Proof: Since G is a group, $a^{-1}(a^{-1})^{-1} = e \Rightarrow a\left(a^{-1}(a^{-1})^{-1}\right) = ae \Rightarrow (aa^{-1})(a^{-1})^{-1} = ae$

$\Rightarrow e(a^{-1})^{-1} = ae \Rightarrow (a^{-1})^{-1} = a$. □