

An Introduction to Groups

In a way, abstract algebra is the study of synthetic arithmetics (or man made arithmetics). Frequently, an arithmetic is invented to model physical phenomena but this is not always the case. We associate arithmetic with "numbers" and stereotypical operations with which we are comfortable (and by now don't think deeply about). An arithmetic can be invented for sets whose elements are not numbers. Operations can be invented that are much different than those that have been our experience (think of the invention of matrix multiplication). Usually when an arithmetic has been invented, it has to obey a minimal number of properties to be useful to mathematicians. The following definition unifies certain operations performed on certain sets.

Definition: A group is a set G endowed with a well defined closed binary operation \star such that:

1. \star is associative on G
2. there is an identity element e for \star in G
3. every element x in G possesses an inverse element in G denoted x^{-1} .

It is an easy trap to think that a set with an operation is a group if the system satisfies three criteria. Don't overlook the importance of closure and well defined in the definition. Notice also that we do not demand that \star be commutative on G . If it is, we refer to G as an abelian group (named after the famous Norwegian mathematician, Niels Henrik Abel (1802-1829)). Otherwise, we say that G is nonabelian.

Let's take a look at a system (a set with a well defined, closed binary operation) that constitutes a group but just might shake some of our assumptions concerning how arithmetic "has to work".

Let S be the set of all real numbers except -1 (why we prohibit -1 will be clear shortly). Let \star be defined by: $a \star b = a + b + ab$ for all a and b in S where $+$ represents the usual real number addition and ab represents the usual multiplication of real numbers a and b . For example, $3 \star 5 = 23$. This seems to be a "strange" arithmetic. Let's see how well behaved this system is by starting an investigation to determine whether or not this system constitutes a group.

Well Defined: Since usual addition and multiplication are well defined, we say that S "inherits" this property.

Closure: It is easy to overlook the necessity of examining closure. After all, $a + b + ab$ has to be a real number. However, we have prohibited -1 from being in the set S . We must determine whether $a \star b$ could ever equal -1 when $a \neq -1$ and $b \neq -1$.

If so, this would not be a closed system. Suppose a and b are in S and $a \star b = -1$.

$$\begin{aligned} \therefore a + b + ab &= -1 \\ \Rightarrow a + ab &= -b - 1 \\ \Rightarrow a(1 + b) &= -(b + 1) \\ \Rightarrow a &= -1 \\ \Rightarrow a &\text{ is not in } S \\ &\rightarrow \leftarrow \end{aligned}$$

(Notice that division by $1 + b$ is legitimized by the fact that b is in S and therefore can't equal -1). This establishes closure.

Associativity: For a, b , and c in S , we must examine the ATE:

$$(a \star b) \star c = a \star (b \star c)?$$

The left hand side becomes:

$$\begin{aligned} &(a \star b) \star c \\ &= (a + b + ab) \star c \\ &= a + b + ab + c + ac + bc + abc \end{aligned}$$

(Did you notice how important it was to think of $(a + b + ab)$ as a single number?)

The right hand side becomes:

$$\begin{aligned} &a \star (b \star c) \\ &= a \star (b + c + bc) \\ &= a + b + c + bc + ab + ac + abc \end{aligned}$$

Because real number addition is associative and commutative, the results from both sides are equal. This establishes associativity.

Existence of an Identity: Have you noticed that \star is a commutative binary operation? For this reason, if we can find a number $e \ni e \star x = x$ for all x in S then $x \star e$ would also equal x . Let's solve the equation $e \star x = x$ for e .

$$\begin{aligned} e \star x &= x \\ \Rightarrow e + x + ex &= x \\ \Rightarrow e + ex &= 0 \\ \Rightarrow e(1 + x) &= 0 \\ \Rightarrow e &= \frac{0}{1 + x} \text{ (which is defined because } x \text{ can't equal } -1) \\ \Rightarrow e &= 0 \\ \therefore 0 &\text{ acts as an identity for } \star. \end{aligned}$$

Try a few examples like $0 \star 5 = 0 + 5 + (0 \cdot 5) = 5$. Examples in an alien setting can sometimes be very revealing.

We have established the existence of an identity.

Inverses: Let $x \in S$. Does x^{-1} exist? If so $x \star x^{-1} = e$. However, we know from the previous discussion that $e = 0$ (exploration to find an identity must precede any discussion of inverses). \therefore we must solve $x \star x^{-1} = 0$ for x^{-1} .

$$\begin{aligned} \text{If } x \star x^{-1} &= 0 \\ \text{then } x + x^{-1} + x \cdot x^{-1} &= 0 \\ \Rightarrow x^{-1} + xx^{-1} &= -x \\ \Rightarrow x^{-1}(1 + x) &= -x \\ \Rightarrow x^{-1} &= \frac{-x}{1+x} \end{aligned}$$

Notice that this last expression is always defined since if $x \in S$ then $x \neq -1$.

$8^{-1} = \frac{-8}{9}$ and $(-5)^{-1} = \frac{5}{4}$ by our formula for x^{-1} . (It is highly recommended that you compute $8 \star (-\frac{8}{9})$ and $(-5) \star \frac{5}{4}$ and verify that both result in 0 the identity.

Since $\frac{-x}{x+1}$ is always defined, we have established that every element in S has an inverse (and we have also obtained a formula to find it).

We have covered all the bases. This system is a group. Specifically, it is an infinite abelian group.

Let's consider some infinite systems with which you are familiar:

1. The non-zero reals under multiplication is a group.
2. The set of all integers under addition is a group.
3. The set of all integers under multiplication is not a group (one problem is that 4 has no inverse because $\frac{1}{4}$ is not an integer).
4. The set of real numbers under subtraction is not a group (one problem is that subtraction is not associative).
5. The set of non-singular matrices under matrix multiplication is a group.
6. The set of all even integers under addition is a group.

Finite groups can sometimes be quite confusing for a new student of abstract algebra. The elements generally are formal symbols and the definitions of the various

binary operations (which we will now call from time to time "group operators") can seem to be quite unintuitive.

We formally adopt two conventions:

1. $a \cdot b$ and ab will be acceptable substitutes for $a \star b$ (as previously discussed).
2. the symbol x^n will represent $\underbrace{x \cdot x \cdot x \cdot \dots \cdot x}_n$.
 n factors

Let's meet our first finite group. It's name is the dihedral-three group and we symbolize it: D_3 . As a set, $D_3 = \{e, a, b, b^2, ab, ab^2\}$. We call the number of elements in a finite group its order. The order of D_3 is 6 and this is symbolized: $o(D_3) = 6$. However, D_3 also is endowed with a group operator. To accomplish this we start with a set of "defining equations" for this operator. Such a set constitutes just enough facts to completely fill in an operation table for the group. Our defining equations are:

1. e acts as an identity
2. $a^2 = e$
3. $b^3 = e$
4. $ba = ab^2$

An operation table would look like:

D_3	e	a	b	b^2	ab	ab^2
e						
a						
b					?	
b^2						
ab						
ab^2						

We will adopt the convention that the question mark in this table represents the answer to $b \cdot ab$ and not $ab \cdot b$. In other words, to complete any blank we compute the row label operating on the left and the column label operating on the right. The defining equations along with our conventions allow us to fill in this much of the table immediately:

D_3	e	a	b	b^2	ab	ab^2
e	e	a	b	b^2	ab	ab^3
a	a	e	ab	ab^2		
b	b	ab^2	b^2	e		
b^2	b^2		e			
ab	ab					
ab^2	ab^2					

Can we assume D_3 is associative? If it is not, then D_3 will not be a group. If we assume associativity in the construction of this table, we will need to find a procedure to confirm associativity at the end of the construction. Proceeding with this in mind, let's compute some of our blanks.

$$a \cdot (ab) = (a \cdot a) \cdot b = e \cdot b = b$$

$$b^2 \cdot b^2 = b^2 \cdot (b \cdot b) = (b^2 \cdot b) \cdot b = e \cdot b = b$$

$$(ab) \cdot (ab) = a \cdot (b \cdot (ab)) = a \cdot ((ba) \cdot b) = a \cdot ((ab^2) \cdot b) =$$

$$a \cdot (a \cdot (b^2 \cdot b)) = a \cdot (a \cdot e) = a \cdot a = e$$

$$b^2 \cdot (ab) = (b^2 \cdot a) \cdot b = ((b \cdot b) \cdot a) \cdot b = (b \cdot (ba)) \cdot b = (b \cdot (ab^2)) \cdot b =$$

$$((b \cdot a) \cdot b^2) \cdot b = (b \cdot a)(b^2 \cdot b) = b \cdot a = ab^2$$

Using similar manipulations, the entire table can be completed as follows:

D_3	e	a	b	b^2	ab	ab^2
e	e	a	b	b^2	ab	ab^3
a	a	e	ab	ab^2	b	b^2
b	b	ab^2	b^2	e	a	ab
b^2	b^2	ab	e	b	ab^2	a
ab	ab	b^2	ab^2	a	e	b
ab^2	ab^2	b	a	ab	b^2	e

Does this represent a group? The issue of well defined will be a given. The issue of closure is settled by simply noting that every answer in the group table is one of the original six elements. The existence of an identity is settled in the defining equations. A close inspection of the group table reveals that every element has an inverse.

To be precise:

$$\begin{aligned}e^{-1} &= e \\ a^{-1} &= a \\ b^{-1} &= b^2 \\ (b^2)^{-1} &= b \\ (ab)^{-1} &= ab \\ (ab^2)^{-1} &= ab^2\end{aligned}$$

The issue of associativity is all that remains. Using only the table we have constructed, let's consider:

$$b \cdot (a \cdot ab^2) \stackrel{?}{=} (b \cdot a) \cdot ab^2$$

The left side becomes:

$$b \cdot (a \cdot ab^2) = b \cdot b^2 = e$$

The right side becomes:

$$(b \cdot a) \cdot ab^2 = ab^2 \cdot ab^2 = e$$

This establishes our equation but not the issue of associativity. An example is not a proof. The ATE demands that $x \star (y \star z) = (x \star y) \star z$ for every $x, y,$ and z in D_3 . Since x can be any of six elements, y can be any of six elements and z can be any of six elements, combinatorics tells us that there are $6^3 = 216$ different equations that must be verified to establish associativity. There exists computer software that can rapidly test all 216 equations. Indeed, each one is correct. By exhausting all combinations, D_3 can be proven to be associative. Therefore, D_3 is a group. More specifically, D_3 is a finite, nonabelian ($a \cdot b \neq b \cdot a$) group.

D_3 is one member of a "family" of nonabelian groups: the dihedral groups. Let's construct D_4 . What do you think the set of elements we'll use could be? The set is $\{e, a, b, b^2, b^3, ab, ab^2, ab^3\}$ and therefore $\circ(D_4) = 8$. What is an appropriate collection of defining equations? You may have already guessed correctly:

1. e acts as an identity
2. $a^2 = e$
3. $b^4 = e$
4. $ba = ab^3$

With these defining equations (and our experience in constructing D_3), we can compute any product in D_4 . For example:

$$b \cdot (ab^2) = (ba) \cdot b^2 = (ab^3) \cdot b^2 = a(b^3 \cdot b^2) = ab.$$

Now, state the elements in D_5 and D_6 along with the defining equations for these groups. Complete group tables for D_4 , D_5 and D_6 and place these (along with the D_3 group table) on four 3" X 5" index cards. (You have probably noticed that the dihedrals are an infinite family and that $|D_n| = 2n \forall n$). We are going to construct a "library" of finite groups. These will be extremely useful as examples of new concepts, insight into new Theorems, counterexamples of false propositions, etc. In this text you will be asked to refer to this "library" frequently. The rest of this chapter will be used to construct a significant number of groups that we can add to our library.

Before we proceed, an examination of an important property of groups will be extremely useful to us. The following Theorem is called the Right Hand Cancellation Law and abbreviated in the rest of this text as RHC.

Theorem: If G is a group and a, b and c are elements of G , if $ac = bc$ then $a = b$.

Proof: We are given: $ac = bc$

$$\Rightarrow (ac)c^{-1} = (bc)c^{-1} \text{ (well-defined)}$$

$$\Rightarrow a(cc^{-1}) = b(cc^{-1}) \text{ (associativity)}$$

$$\Rightarrow ae = be \text{ (definition of an inverse)}$$

$$\Rightarrow a = b \text{ (definition of an identity)}$$

QED

As we gain a comfort level with group theory, we will cease annotating the reasons for each step in a group theoretic proof. As you probably guessed, there exists a similar Theorem called LHC. It states that whenever $ca = cb$ then $a = b$. You may have already observed the effects of RHC and LHC. Look across any row of a dihedral group or down any column of a dihedral group. Notice anything? No duplication! No row contains the same element twice nor does any column. This is a result of LHC and RHC (LHC controls that fact that there isn't row duplication while RHC governs the columns). We can capitalize on this fact in the following way: if we are constructing a finite group table and have filled in every entry on a row except one, we can deduce what that final entry must be.

Let's construct a new family of groups. The first group in the family is called the Klein-four group, which we will denote K_4 . The elements of K_4 will be: e, p, q, r . The defining equations for K_4 are:

1. e acts as an identity
2. $x^2 = e$ for all x

The defining equations fill this much of the group table:

K_4	e	p	q	r
e	e	p	q	r
p	p	e		
q	q		e	
r	r			e

Let's consider the product $p \cdot q$. The result can't be p or e because that would create row duplication. The result also can't be q since that would create column duplication. We can deduce that the answer must be r . Further, the last element in the p row is now determined. It must be q . By similar reasoning, the entire chart must be:

K_4	e	p	q	r
e	e	p	q	r
p	p	e	r	q
q	q	r	e	p
r	r	q	p	e

This table represents a group (every necessary condition is observed). Did you notice that every element is its own inverse? Every element is said to be self invertible.

We will now use set theory to construct the rest of this family. Let S be a set. The power set of S (denoted $\mathcal{P}(S)$) is defined to be the collection of all subsets of S . For example, if $S = \{a, b\}$ then $\mathcal{P}(S) = \{\{a\}, \{b\}, S, \emptyset\}$. Remember that any set is a subset of itself and the null set is a subset of every set. Let's define the following binary operator on this particular power set:

If H and G are elements of $\mathcal{P}(S)$, $H \star G$ is defined to be $(H \cup G) - (H \cap G)$. You are probably familiar with set union and set intersection. Set subtraction may be new to you. If C and D are sets, $C - D$ is defined to be the set of elements that are in C but are not in D . $\{1, 2, 7, 8, 9\} - \{5, 7, 8, 15\} = \{1, 2, 9\}$

Returning to our development and our power set $\mathcal{P}(S) = \{\{a\}, \{b\}, S, \emptyset\}$, let's compute $\{a\} \star \{b\}$.

$$\{a\} \star \{b\} = (\{a\} \cup \{b\}) - (\{a\} \cap \{b\}) = \{a, b\} - \emptyset = \{a, b\}$$

As a second example, let's compute

$$\{b\} \star S = \{\{b\} \cup S\} - \{\{b\} \cap S\} = S - \{b\} = \{a\}.$$

Let's compute a table for this power set endowed with this binary operator:

	\emptyset	$\{a\}$	$\{b\}$	S
\emptyset	\emptyset	$\{a\}$	$\{b\}$	S
$\{a\}$	$\{a\}$	\emptyset	S	$\{b\}$
$\{b\}$	$\{b\}$	S	\emptyset	$\{a\}$
S	S	$\{b\}$	$\{a\}$	\emptyset

At a glance at this table reveals that if \emptyset were relabeled e , $\{a\}$ relabeled p , $\{b\}$ relabeled q and S were relabeled q , this table would match K_4 . When two tables differ only in labeling, we say that they are isomorphic copies of each other. For now, they can be thought of as the same group with different labels. A formal development of the idea of an isomorphism will occur later in this text.

Now let's construct the second group in this family called K_8 .

$$\text{Let } S = \{a, b, c\}$$

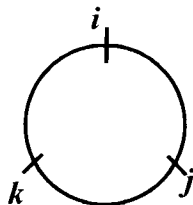
$$\mathcal{P}(S) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, S\}$$

(You may have learned in a course covering combinatorics that if a finite set contains n elements then its power set contains 2^n elements). We define the group operator on $\mathcal{P}(S)$ the same way we did previously: If G and H are in $\mathcal{P}(S)$, $G \star H = (G \cup H) - (G \cap H)$. With some labor on your part, you will be able to confirm the following table:

K_8	\emptyset	$\{a\}$	$\{b\}$	$\{c\}$	$\{a, b\}$	$\{a, c\}$	$\{b, c\}$	S
\emptyset	\emptyset	$\{a\}$	$\{b\}$	$\{c\}$	$\{a, b\}$	$\{a, c\}$	$\{b, c\}$	S
$\{a\}$	$\{a\}$	\emptyset	$\{a, b\}$	$\{a, c\}$	$\{b\}$	$\{c\}$	S	$\{b, c\}$
$\{b\}$	$\{b\}$	$\{a, b\}$	\emptyset	$\{b, c\}$	$\{a\}$	S	$\{c\}$	$\{a, c\}$
$\{c\}$	$\{c\}$	$\{a, c\}$	$\{b, c\}$	\emptyset	S	$\{a\}$	$\{b\}$	$\{a, b\}$
$\{a, b\}$	$\{a, b\}$	$\{b\}$	$\{a\}$	S	\emptyset	$\{b, c\}$	$\{a, c\}$	$\{c\}$
$\{a, c\}$	$\{a, c\}$	$\{c\}$	S	$\{a\}$	$\{b, c\}$	\emptyset	$\{a, b\}$	$\{b\}$
$\{b, c\}$	$\{b, c\}$	S	$\{c\}$	$\{b\}$	$\{a, c\}$	$\{a, b\}$	\emptyset	$\{a\}$
S	S	$\{b, c\}$	$\{a, c\}$	$\{a, b\}$	$\{c\}$	$\{b\}$	$\{a\}$	\emptyset

Following the pattern established by K_4 and K_8 , K_{16} can be constructed from the power set of $\{a, b, c, d\}$ using the usual operator. In fact there is a K group for every power of 2 ($K_{32}, K_{64}, K_{128}, \dots$). This family of groups differs from the dihedral family in many respects. One of which is that each group in this family is abelian. Finite abelian groups have symmetry with respect to their main diagonals. For K_8 , note that the fourth result (starting at the top) of the $\{a\}$ column matches the fourth result (starting at the left) of the $\{a\}$ row. Now try this for other matched rows and columns. The K family also enjoys the fact that each element is self invertible. That means that $x^2 = e$ for every $x \in K_n$ or, in other words, $x^{-1} = x$ for every $x \in K_n$. In D_3 , only e, a, ab , and ab^2 were self invertible.

Let's pause from our study of families of finite groups. We now explore an interesting group that is not a member of a larger family. It is called the quaternion group and is denoted Q_8 . You may recall from Calculus (or Linear Algebra) the unit vectors i, j and k that constitute the standard basis for Euclidean three-space. The cross product of any two of these vectors can be remembered by forming the "clock":



If the order of the product (from left to right) corresponds to a clockwise movement, the result is the third member of the "clock". For example, $j \times k = i$. If the order of the product corresponds to a counterclockwise movement, the result is the negative of the third. For example, $k \times j = -i$. Q_8 borrows these results to form a part of its group table.

In the complex number system, i has a different meaning. In that system $i^2 = -1$. Q_8 not only borrows that result, but extends it in its defining equations to $j^2 = -1$ and $k^2 = -1$ also. Finally, Q_8 borrows 1 and -1 from the real number system and endows them with their usual real number system multiplicative properties. The set for Q_8 is: $\{1, -1, i, -i, j, -j, k, -k\}$. The defining equations are:

- (a) 1 acts as an identity
- (b) $(-1)^2 = 1$
- (c) $(-1) \cdot x = -x$ and $x \cdot (-1) = -x$ for all x
- (d) $i^2 = j^2 = k^2 = -1$
- (e) i, j , and k obey the "clock" product rules.

While the results in the Q_8 operating table may seem intuitively obvious, to obtain them from the defining equations can be tedious. For example:

$$\begin{aligned}
 -j \cdot i &= ((-1) \cdot j) \cdot i = (-1)(j \cdot i) = (-1)(-k) = \\
 &= (-1)((-1) \cdot k) = ((-1) \cdot (-1))k = 1 \cdot k = k
 \end{aligned}$$

The complete Q_8 table is as follows:

Q_8	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

You should verify these results and add the table to your library. The number of equations needed to establish associativity for this table is $8^3 = 512$. Notice that each element has an inverse (for example: $(-j)^{-1} = j$).

Q_8 can be modeled by the following eight 2×2 matrices over the complex number system: $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$, $\begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}$, $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$, $\begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}$, $\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$ and $\begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}$. Try identifying each of these with one of our elements in Q_8 . Check the various combinations of products of these matrices using matrix multiplication.

In order to create the next family of groups, we need to study an important concept in mathematics. Given a set S , a relation on S is any set of ordered pairs (x, y) where $x \in S$ and $y \in S$. Relations are often defined by some rule that allows their construction. For example, if S is the set of positive integers we could define a relation to be the set of all ordered pairs (x, y) such that x is a divisor of y . Because of this "rule", $(2, 6)$ is in the relation but $(2, 7)$ is not. Our generic symbol for a relation will be R . It will be used two different ways that hopefully won't be ambiguous in context. The symbol aRb will be read " a relates to b ". Similarly, $(a, b) \in R$ will mean the ordered pair (a, b) is a member of the relationship being examined. Even though R is being used in two ways, the two uses are extremely similar. In our previous example, we could say $2R6$ (or $(2, 6) \in R$) but $2R7$ (or $(2, 7) \notin R$).

You have already been introduced to numerous relations in mathematics. They include "less than" on the set of real numbers, "is parallel to" for lines in a plane, and many more. There are numerous properties that a given relationship may or may not possess. We will focus on three. A relation is said to be reflexive if and only if aRa for every a in S . In the real number system, the relationship $<$ is not reflexive. The reflexive property can be troublesome for beginners. For example, let S be the set $\{1, 2, 3\}$. Let R be defined by, xRy iff x is a divisor of $y + 2$. It is true that $1R1$ since 1 is a divisor of 3. It is also true that $2R2$ since 2 is a divisor of 4. However, $3\not R3$ (3 is not a divisor of 5) and the relationship fails to be reflexive.

A relation is said to be symmetric iff whenever aRb then bRa . Notice that unlike the previous property, this property is essentially a conditional statement. If $a\not Rb$, that's fine. We only are concerned when a does relate to b . Our "is less than" relation on the real number system is not symmetric. $3 < 5$ but $5 \not< 3$. In our example in the last paragraph $1R2$ but $2\not R1$. This relation is not symmetric.

A relation is said to be transitive iff whenever aRb and bRc then aRc . In our "is less than" example on the real number system, we already know that if $a < b$ and $b < c$ then $a < c$. This is an example of a transitive relation. Let's return to the set $S = \{1, 2, 3\}$ and the relation xRy iff x is a divisor of $y + 2$. $3R1$ (3 is a divisor of 3) and $1R2$ (1 is a divisor of 4). If the relation was transitive we would be able to deduce that $3R2$. However, 3 is not a divisor of 4. Therefore, this relation on this set is not transitive.

A relation on a set is said to be an equivalence relation if it enjoys all three properties: the reflexive, symmetric and transitive properties. You have encountered numerous equivalence relations in your math courses. To name just two: "is equal to" is an equivalence relation on the set of real numbers and "is congruent to" is an equivalence relation on the set of triangles in a plane.

We want to study a very special relation defined on the integers. We will say that a is congruent to $b \pmod{5}$ iff $a - b = 5q$ for some integer q . If a is congruent to $b \pmod{5}$, we will write $a \equiv b \pmod{5}$. For example, $-2 \equiv 8 \pmod{5}$ since $-10 = 5(-2)$. As another example, $8 \not\equiv 1 \pmod{5}$ since $7 \neq 5q$ for any integer q (while it is true that $7 = 5(\frac{7}{5})$, $\frac{7}{5}$ is not an integer).

We will now prove that congruence $\pmod{5}$ is an equivalence relation.

Reflexive Property

Is $a \equiv a \pmod{5}$ for every integer a ? This is the same as asking whether $0 = 5q$ for some integer q no matter what value a takes on. Since 0 is an integer, if we let $q = 0$ the question is answered affirmatively and the relation has been shown to be reflexive.

Symmetry Property

If $a \equiv b \pmod{5}$ is $b \equiv a \pmod{5}$?

We are given that $(a - b) = 5q$ for some integer q :

$$b - a = -5q$$

$$\Rightarrow b - a = 5(-q)$$

Since $-q$ must also be an integer, $b \equiv a \pmod{5}$

Transitive Property

Suppose $a \equiv b \pmod{5}$. and $b \equiv c \pmod{5}$

Is $a \equiv c \pmod{5}$? We know from the given that $a - b = 5q_1$ and $b - c = 5q_2$ for some integers q_1 and q_2 .

$$\therefore (a - b) + (b - c) = 5q_1 + 5q_2$$

$$\Rightarrow a - c = 5(q_1 + q_2)$$

Since $q_1 + q_2$ must be an integer, we have proven that $a \equiv c \pmod{5}$ establishing the transitive property.

You may have noticed that if a and b are positive integers, $a \equiv b \pmod{5}$ if and only if a and b have the same remainder when divided by 5. We will return to this relation shortly, but first we have to examine an important aspect of equivalence relations generally.

Let R be an equivalence relation on a set S . Let $x \in S$. The "equivalence class generated by x " is defined to be the set of all elements y in S such that xRy and is denoted $[x]$. In other words:

$$[x] = \{y \mid y \in S \text{ and } xRy\}$$

Theorem: If R is an equivalence relation on a set S and if $a \in S$ and $b \in S$ then $[a] = [b]$ or $[a] \cap [b] = \emptyset$ (This states that two equivalence classes are either equal or disjoint).

Proof: If $[a] \cap [b] = \emptyset$, we are done. Suppose $[a] \cap [b] \neq \emptyset$. We must show that $[a] = [b]$. Since $[a]$ and $[b]$ are sets, how do we prove they are equal? You may recall that two sets are equal iff whenever an element is in the first, then it is also in the second and whenever an element is in the second it must also be in the first.

We know $[a] \cap [b] \neq \emptyset \therefore \exists z$ such that $z \in [a]$ and $z \in [b]$. $\therefore aRz$ and bRz . By symmetry, we also note that zRa and zRb .

Let x be any element of $[a]$.

$$\therefore aRx$$

$$\Rightarrow xRa$$

Since xRa and aRz and since R is transitive, we know xRz . Since xRz and zRb , we know xRb . $\therefore bRx \therefore x$ is an element of $[b]$.

The argument that every element in $[b]$ is also an element of $[a]$ is similar to the above argument and left to the student.

$$\therefore [a] = [b]$$

QED

Let's compute some equivalence classes for the integers ($\text{mod } 5$) relation.

$$[0] = \{\dots, -15, -10, -5, 0, 5, 10, 15, \dots\}$$

(It should be no surprise that $0 \in [0]$.)

This relation is reflexive.)

$$[1] = \{\dots, -14, -9, -4, 1, 6, 11, \dots\}$$

$$[2] = \{\dots, -13, -8, -3, 2, 7, 12, \dots\}$$

$$[3] = \{\dots, -12, -7, -2, 3, 8, 13, \dots\}$$

$$[4] = \{\dots, -11, -6, -1, 4, 9, 14, \dots\}$$

If we compute the union of the sets, we will obtain the set of all integers. Any other equivalence class must be identical to one of these by our Theorem. For example, $[9] = [4]$.

We will define a binary operator on the set $\{[0], [1], [2], [3], [4]\}$. Define $[x] \star [y]$ to be $[x + y]$. You may be concerned about closure. For example, by our definition, $[3] \star [4] = [7]$ which is not in our set. However, $[7] = [2]$. $\therefore [3] \star [4] = [2]$. In this manner, \star is a closed binary operation on our set. This set and its operator is called the integers ($\text{mod } 5$) under addition and symbolized \mathbb{Z}_5 . For convenience in constructing the table, we will denote $[0]$ as 0, $[1]$ as 1, etc. You must recall that each element in this chart symbolizes an infinite set.

\mathbb{Z}_5	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

This is a group. Every element has an inverse (check for yourself). There are 125 equations to test for associativity and they all work basically because associativity is

inherited from the real number system. Closure is obvious from a glance at our table and by our previous discussion. 0 acts as our identity.

We could have just as easily developed the integers (*mod* 4). The table is:

\mathbb{Z}_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

Notice that this is not an isomorphic copy of K_4 since every element is not self invertible. For completeness, we even have a group \mathbb{Z}_1 . Its rather abbreviated table is:

\mathbb{Z}_1	0
0	0

You should create cards for \mathbb{Z}_1 , \mathbb{Z}_2 , \mathbb{Z}_3 , \mathbb{Z}_4 , \mathbb{Z}_5 , and \mathbb{Z}_6 . Add these to your library.

Returning to the equivalence classes [0], [1], [2], [3] and [4] generated by congruence (*mod* 5), let's attempt to generate a new group by defining:

$$[x] \star [y] = [x \cdot y].$$

It is immediately obvious that this won't work unless we delete [0] because of violations of RHC and LHC. $[0] \star [2] = [0] \star [3]$ but $[2] \neq [3]$. Therefore our set becomes $\{[1], [2], [3], [4]\}$. The table for our operation would be:

	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

This is a group. However, we will discover that this group has occurred elsewhere in our work. To dramatize the difficulties encountered when using multiplication, let's consider the equivalence classes generated by congruence (*mod* 6). If we delete [0] (and we must) we are left with $\{[1], [2], [3], [4], [5]\}$.

Again we attempt $[x] \star [y] = [x \cdot y]$. A table would be:

	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

While there exists an identity (namely 1), this is clearly not a group. Let's list all the violations we can find:

- (1) Closure is violated ($2 \star 3 = 0$ which is not in the set being used)
- (2) 2, 3 and 4 do not have inverses (1 is the identity)
- (3) LHC is violated ($3 \cdot 3 = 3 \cdot 5$)
- (4) RHC is violated ($1 \cdot 2 = 4 \cdot 2$)

Using multiplication on the integers ($\text{mod } n$) does not create a group if n is not a prime number. If n is a prime number, a group is formed but not a group that will interest us in the early stages of this course.