Math 103 Notes

Modern Algebra

Summer Session 1 2021

Taught by Professor Kyle Meyer

Table of Contents

1 Review: Equivalence Relations **1**
1.1 Equivalence Relations . . . 1
1.1.1 Example: Relations . . . 1
1.2 Equivalence Relation Partitions . . . 2
1.3 Equivalence Relation Classes . . . 3
1.4 Summary . . . 4

2 Review: Congruences, Long Division, Modulo **5**
2.1 Congruence . . . 5
2.2 Congruence and Equivalence Relations . . . 5
2.3 Congruence and Partitions . . . 6
2.3.1 Well-Ordering Principle . . . 6
2.3.2 The Division Algorithm . . . 6

3 Binary Operations and Group Theory **7**
3.1 Binary Operations . . . 7
3.2 Properties of Binary Operations . . . 8
3.3 Groups . . . 9
3.3.1 Example: Addition . . . 9
3.3.2 Example: Multiplication . . . 10
3.3.3 Example: Addition and Modular Arithmetic . . . 10
3.3.4 Example: Multiplication and Modular Arithmetic . . . 11
3.4 Basic Properties of Groups . . . 11

1 Review: Equivalence Relations

We will go over topics covered in other courses that will be used in this course. We begin with the topic of equivalence relations.

1.1 Equivalence Relations

Let X be a non-empty set. Then, a **relation** over X is a subset R of $X \times X$. If $(x, y) \in R$, we say that x is R-related to y and write xRy.

So, for these relations, we should think about inequalities equalities, or congruences between integers.

Suppose R is a relation over X. Then:

- R is called **reflexive** if $\forall x \in X$, xRx. That is, every $x \in X$ is related to itself.
- R is called **symmetric** if $\forall x, y \in X$, $xRy \implies yRx$. In other words, if x is related to y, is y related to x?
- R is called **transitive** if $\forall x, y, z \in X$, xRy and yRz implies that xRz.

Definition 1.1: Equivalence Relation

R is called an **equivalence relation** if R is reflexive, symmetric, and transitive.

Remark: An equivalence relation is essentially an equality with respect to a certain measurement. In life, we often measure things or people with respect to properties (for example, scores or ratings). So, when we want to compare things, we pick a certain property and then, *from that point of view*, determine whether these things are equal. In this regard, equivalence relations are exactly equalities.

1.1.1 Example: Relations

Suppose X and Y are two non-empty sets and $f : X \to Y$ is a function. Let $\sim$ be the following relation over X:

$$\forall x_1, x_2 \in X \quad x_1 \sim x_2 \iff f(x_1) = f(x_2)$$

Then, $\sim$ is an equivalence relation[1].

Proof. We determine if an relation is an equivalence relation if it satisfies the three properties mentioned above.

- Reflexivity:
$$\forall x \in X, f(x) = f(x) \implies x \sim x$$
- Symmetric:
$$x_1 \sim x_2 \implies f(x_1) = f(x_2) \implies f(x_2) = f(x_1) \implies x_2 \sim x_1$$
- Transitive: We know that:
$$\forall x_1, x_2 \in X \qquad x_1 \sim x_2 \implies f(x_1) = f(x_2)$$
We also know that:
$$\forall x_2, x_3 \in X \qquad x_2 \sim x_3 \implies f(x_2) = f(x_3)$$
It follows that if $f(x_1) = f(x_2)$ and $f(x_2) = f(x_3)$, then $f(x_1) = f(x_3)$ and thus, $x_1 = x_3$. Namely, $x_1 \sim x_2$ and $x_2 \sim x_3$, then $x_1 \sim x_3$.

It follows that this is an equivalence relation. □

[1] Another way of interpreting this statement is as follows: x_1 is in relation to x_2 precisely when $f(x_1) = f(x_2)$. The claim here, then, is that this is an equivalence relation.

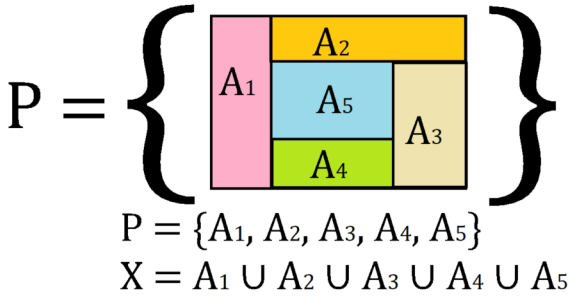
1.2 Equivalence Relation Partitions

Recall that P is called a **partition** of a non-empty set X if:

- Subsets: P consists of non-empty subsets of X.
- Disjointness: $A, B \in P$ and $A \neq B \implies A \cap B = \emptyset$. In other words, the subsets are disjoint.
- Covering: $\forall x \in X$, $\exists A \in P$ such that $x \in A$. In other words, every element in X will be in one of the subsets. Alternatively, $\bigcup_{A \in P} A = X$.

Remark:

- As mentioned, P is a set of sets. For instance, if we have $X = \{1, 2, 3\}$, one possible P is $P = \{\{1\}, \{2, 3\}\}$.
- Below is a visual diagram of what a partition may look like.



Suppose P is a partition of X. Then, we can get a classification function from X to P:

$$X \to P$$

$$x \mapsto [x]_P$$

Here, $[x]_P$ is the unique element of P which contains x. In other words, if we refer to the above diagram, we can think of $[x]_P$, a set, as one of the sets A_1, A_2, A_3, A_4, or A_5 which contains x. So, we can think of this function as saying that every $x \in X$ belongs to one of the sets $[x]_P$.

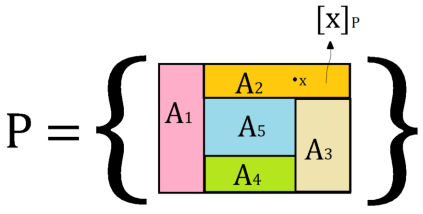
Notice that, because of the **covering** condition, x is contained in some element of P; additionally, because of the **disjointness** condition, x is in an unique element of P (i.e. it is in one of the sets which is in P). So, it follows that the function is well-defined.

By the previous example, $x \sim_P y \iff [x]_P = [y]_P$ is an equivalence relation. So, we obtain the following lemma.

Lemma 1.1

Suppose P is a partition of a non-empty set X. For $x, y \in X$, $x \sim y$ if x and y are in the same element of P. Then, $\sim$ is an equivalence relation.

Remark: Essentially, what this lemma is saying is that if $x \sim y$, then both x and y are in the same set which is in P. In other words, if we refer to the above diagram again, we can think of this situation as saying that both x and y are in one of A_1, A_2, A_3, A_4, or A_5. The diagram below complements the proof.



Proof. For $x \in X$, let $[x]_P$ to be the unique element of P which contains x. So, $x \mapsto [x]_P$ is a function from $X \to P$. By the previous example, $x \sim y \iff [x]_p = [y]_p$ is an equivalence relation over X. Notice that this means $x \sim y$ exactly when x and y are in the same element of P. □

1.3 Equivalence Relation Classes

Now, suppose that $\sim$ is the equivalence relation over a non-empty set X, we can partition X with respect to $\sim$.

For $x \in X$, we let $[x] = \{y \in X \mid y \sim x\}$ (all the elements that are $\sim$-related to x).[2] We call $[x]$ the **equivalence class of x with respect to $\sim$**. When $x \sim y$, we can say that x is equivalent to y with respect to $\sim$.

Proposition. *Suppose $\sim$ is an equivalence relation over a non-empty set X. Then, $\{[x] \mid x \in X\}$ is a partition of X.*

This proposition is essentially asking us to show the following properties:

- Covering: Every element of this set belongs to one of these equivalence classes.
- Disjointness: If we pick two equivalence classes, they do not intersect.

The following lemma follows from this proposition.

Lemma 1.2

$$x \sim y \iff [x] = [y]$$

Proof. We want to show that $[x] = [y] \implies x \sim y$. Recall that the equivalence class of x ($[x]$) and the equivalence class of y ($[y]$) are *sets* and, in particular, we know that $[x]$ consists of all elements that are related to x, including x. Since $\sim$ is reflexive, we know that:

$$x \sim x \implies x \in [x]$$

But, since $[x] = [y]$, then it follows that $x \in [y] \implies x \sim y$. Thus, $[x] = [y] \implies x \sim y$.

To show that $x \sim y \implies [x] = [y]$, we need to show equality of sets $[x] = [y]$. This means that it is necessary and sufficient to prove $[x] \subseteq [y]$ and $[y] \subseteq [x]$.

- To prove $[x] \subseteq [y]$, we let $z \in [x]$. This means that $z \sim x$. However, since $x \sim y$, by transitivity, it follows that $y \sim z$, which implies that $z \in [y]$. Hence, $[x] \subseteq [y]$.
- We note that $x \sim y \implies y \sim x$ by symmetry. Therefore, by the first bullet point, $[y] \subseteq [x]$.

So, it follows that $x \sim y \implies [x] = [y]$. □

Now that we proved the lemma, we can now prove the proposition.

Proof. As mentioned, we need to show that the covering and disjointness properties exist in this partition.

- Covering: $\forall x \in X$, we know that $x \sim x$ by the reflexive property (since $\sim$ is an equivalence relation). Thus, it follows that $x \in [x]$. This means that x is related to x and x is an equivalence class of x, so every element in X belongs to one of the equivalence classes. This implies that the $[x]$ sets are non-empty subsets and cover X.

[2] So, it's obvious that $[x] \subseteq X$.

- Disjointness: Suppose $z \in [x] \cap [y]$ (both equivalence classes are not disjoint). We need to show that they are equal. We know that:

$$z \in [x] \cap [y] \implies z \in [x] \implies z \sim x \implies [z] = [x]$$

$$z \in [x] \cap [y] \implies z \in [y] \implies z \sim y \implies [z] = [y]$$

Where the last two steps came from the lemma. Then, putting these two together, we have:

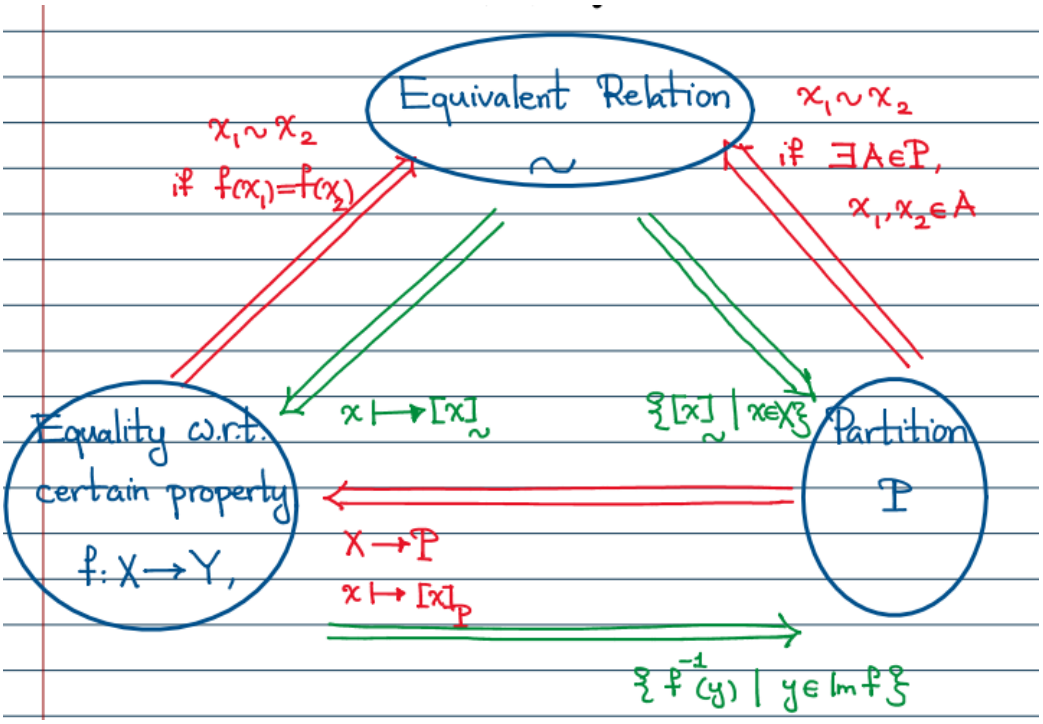
$$[z] = [x] \text{ and } [z] = [y] \implies [x] = [y]$$

We showed that $[x] \cap [y] \neq \emptyset \implies [x] = [y]$, the contrapositive of the disjointness property.

Thus, the proof is complete. □

1.4 Summary

The following diagram provides a brief summary of what we've learned[3]



[3]This diagram was taken from Professor Alireza Salehi Golsefidy's notes.

2 Review: Congruences, Long Division, Modulo

In this section, we discuss congruences, long division, and modulo.

2.1 Congruence

The set of integers is denoted by $\mathbb{Z}$. For $a, b \in \mathbb{Z}$, we say that a divides b and write $a|b$ if $b = ak$ for some $k \in \mathbb{Z}$. Suppose n is a non-zero integer. Then, we say that a is **congruent** to b modulo n and write one of the following if $n|(a-b)$:

$$a \equiv b \pmod{n}$$

$$a \overset{n}{\equiv} b$$

One way to think of this is through a clock. A clock has n numbers (usually 12 numbers). Then, a and b will be on the same spot. For instance, suppose we have 9PM (denoted by the 21st hour). Then, we know that:

$$21 \equiv \boxed{9} \pmod{12}$$

In other words, the hour hand for 9PM will be in the same position as 9AM.

2.2 Congruence and Equivalence Relations

Lemma 2.1

$\overset{n}{\equiv}$ is an equivalence relation over $\mathbb{Z}$.

Proof. Recall that something is an equivalence relation if it satisfies the three properties mentioned in definition 1.1. So, we need to show that $\overset{n}{\equiv}$ satisfies these.

- Reflexive: For every $a \in \mathbb{Z}$, we know that $a - a = 0$ is a multiple of n as $n \cdot 0 = 0$. Hence, $a \overset{n}{\equiv} a$.
- Symmetric: We have that:

$$\begin{aligned} a \overset{n}{\equiv} b &\implies n|(a-b) \\ &\implies \exists k \in \mathbb{Z}, a - b = nk \\ &\implies b - a = n\underbrace{(-k)}_{\text{In } \mathbb{Z}} \\ &\implies b \overset{n}{\equiv} a \end{aligned}$$

- Transitive: We know that:

$$a \overset{n}{\equiv} b \implies n|(a-b) \implies \exists k \in Z, a - b = nk$$

We also know that:

$$b \overset{n}{\equiv} c \implies n|(b-c) \implies \exists l \in \mathbb{Z}, b - c = nl$$

Combining the statements, we now have:

$$(a-b) + (b-c) = nk + nl \implies a - c = n\underbrace{(k+l)}_{\text{In } \mathbb{Z}} \implies a \overset{n}{\equiv} c$$

Thus, $\overset{n}{\equiv}$ is an equivalence class. □

2.3 Congruence and Partitions

As we have seen earlier, every equivalent relation gives us a **partition** and an **equality function**. For $a \in \mathbb{Z}$, the equivalent class of a with respect to $\overset{n}{\equiv}$ is called the **mod-n residue class of** a and is denoted by $[a]_n$. By the results that we proved for equivalence relations, we have that:

- $\{[a]_n \mid a \in \mathbb{Z}\}$ is a partition of $\mathbb{Z}$; and
- $a \overset{n}{\equiv} b \iff [a]_n = [b]_n$

The partition $\{[a]_n \mid a \in \mathbb{Z}\}$ is denoted by $\mathbb{Z}_n$ and it is called **the set of integers modulo** n. Notice that:

$$\begin{aligned} b \in [a]_n &\iff b \overset{n}{\equiv} a \\ &\iff n|(b-a) \\ &\iff \exists k \in \mathbb{Z}, b - a = nk \\ &\iff \exists k \in \mathbb{Z}, b = a + nk \\ &\iff b \in \{a + nk \mid k \in \mathbb{Z}\} \quad \text{Arithmetic Progression} \end{aligned}$$

To understand the set $\mathbb{Z}_n$ better, we recall the well-ordering principle and the long division property of integers. One of the important properties of positive integers is the **well-ordering principle**. This principle can be viewed as an axiom that we assume $\mathbb{Z}$ has.

2.3.1 Well-Ordering Principle

Every non-empty subset of the set $\mathbb{Z}_{\geq 0}$ of non-negative integers has a minimum. Using the well-ordering principle, we can prove the division algorithm.

2.3.2 The Division Algorithm

For every $a \in \mathbb{Z}$, $b \in \mathbb{Z} - \{0\}$, there is a unique pair (q, r) of integers such that:

$$a = bq + r \qquad 0 \leq r \leq |b|$$

3 Binary Operations and Group Theory

We want to explore the idea behind *algebraic structures*. In particular, we want to explore these structures in more detail compared to earlier courses (either in past college or high school algebra classes).

To do this, we need to think about *what* algebra really is. We might think about solving equations like $x^2 + 3x + 5 = 0$ for x. In particular, what is really happening here?

Well, there are a couple of operations going on. Specifically, we have *addition* and *multiplication*.

$$x \cdot x + 3 \cdot x + 5 = 0$$

We now want to examine these operations. Both of these operations $(+, \cdot)$ take in two numbers and output one number. The question we might have, then, is: how can we can generalize these operations?

3.1 Binary Operations

A **binary operation** is a way of taking in two values and outputting one value. Of course, we might now ask: what can these values be? These values can come from any specific set.

For example, we can consider addition over the integers ($\mathbb{Z}$). The sum of two integers is an integer. Similarly, we could consider multiplication over the integers. Again, the product of two integers is an integer. We could also consider multiplication or addition over the real, rational, or complex numbers.

The idea is that whatever "type" we give our binary operation, we will get that same "type" for our output. To formalize this, we have the following definition:

Definition 3.1: Binary Operation

A binary operation $*$ over a set S is a function mapping $f : S \times S \to S$. For each $(a, b) \in S \times S$, we will denote the element $*((a, b))$ of S by $a * b$.[a]

[a] As a side note, in this class, $a * b$ is equivalent to $f(a, b)$ and $b * a$ is equivalent to $f(b, a)$.

We also introduce the notion of closure, which will be used later.

Definition 3.2: Closure

Let $*$ be a binary operation on S and let H be a subset of S. The subset H is **closed under** $*$ if for all $a, b \in H$ we also have $a * b \in H$. In this case, the binary operation on H given by restricting $*$ to H is the **induced operation** of $*$ on H.

Anything that is "like" addition or multiplication is probably a binary operation. For example, let's consider **matrices**.

- Addition of matrices of a fixed dimension. More specifically, the set of $n \times m$ matrices (here, n and m are fixed positive integers) over the integers, rationals, reals, or complex numbers under matrix addition is a binary operation.

$$\begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \end{bmatrix} + \begin{bmatrix} b_{11} & b_{12} & b_{13} \\ b_{21} & b_{22} & b_{23} \end{bmatrix} = \begin{bmatrix} a_{11} + b_{11} & a_{12} + b_{12} & a_{13} + b_{13} \\ a_{21} + b_{21} & a_{22} + b_{22} & a_{23} + b_{23} \end{bmatrix}$$

- Multiplication of matrices of a fixed dimension. More specifically, the set of $n \times n$ matrices (square matrices). We could also just multiply a $(n \times m)$ matrix by a $(k \times l)$ matrix assuming $m = k$ (otherwise, multiplying these two matrices will result in undefined behavior).

So far, we considered binary operations on infinite sets in which we need some sort of formula to describe (e.g. $f_{\cup}(A, B) = A \cup B$). Now, if we have a finite set, we could define a binary operation exhaustively by just saying what the binary operation does on every pair of entries.

For example, given the set $S = \{a, b, c, d, e\}$. We can define a binary operation on S with the below (random) table (first entry on left side, second entry on top side).

	a	b	c	d	e
a	a	c	d	d	e
b	b	c	c	b	a
c	d	e	e	b	b
d	a	a	a	c	a
e	b	b	c	c	d

Denote the binary operation to be #.

- What is $c\#d$? The answer is b.
- What is $e\#((a\#b)\#c)$? The answer is d.
- Suppose we have $X\#a = a$. What is X? The answer is $X = a, d$.

3.2 Properties of Binary Operations

What properties could binary operations have?[4]

- **Commutativity:** A binary operation is commutative if the order of the two inputs does not matter. For example, if f is a function corresponding to a binary operation, then:

  $$f(a, b) = f(b, a) \quad \forall a, b \in S$$

  More commonly:

  $$a * b = b * a \quad \forall a, b \in S$$

  For example, addition or multiplication of numbers is commutative. Unions and intersections of sets is also commutative. *However*, matrix multiplication is *not* commutative. Our example above is also not commutative.

- **Associativity:** A binary operation is associative if the order of applying the operation (in a string) does not matter. Specifically:

  $$(a * b) * c = a * (b * c) \quad \forall a, b, c \in S$$

  Which means that we can write $a * b * c$ without ambiguity.

  For example, addition or multiplication of numbers is associative. Addition or multiplication of matrices is also associative. Our example above is not associative.

- **Identity:** A binary operation has a two-sided identity element and a two-sided inverse for every element.

  More specifically, we say that ϵ is a left identity if $f(\epsilon, s) = s$ for all $s \in S$. ϵ is a right identity if $f(s, \epsilon) = s$ for all $s \in S$. Then, ϵ is a two-sided identity if it is both a left identity and right identity.

  For example, 0 is a two-sided identity for addition and 1 is a two-sided identity for multiplication. For matrix addition, the zero-matrix is a two-sided identity. For matrix multiplication, the matrix with

[4] In this course, we will consider binary operations with all the properties excluding commutativity.

ones on the diagonal and zeros everywhere else is the identity element. In our example above, # does not have a left or right identity.

Given a two-sided identity, we can also consider the idea of an inverse. In addition, this is the negative/negation. In multiplication, this is the reciprocal. The additive inverse of x is $-x$. The multiplicative inverse of x is $\frac{1}{x}$ (for all $x \neq 0$).

For a general binary operation $f : S \times S \to S$ with a two-sided identity ϵ, an element $s \in S$ has a two-sided inverse if there exists an element $t \in S$ such that:

$$\underbrace{f(s,t)}_{\text{Right Inverse}} = \overbrace{f(t,s)}^{\text{Left Inverse}} = \epsilon$$

So, a property for binary operations would be for every element to have a two-sided inverse, which requires a two-sided identity element.

Remark: Commutativity does not imply associativity.

3.3 Groups

Of course, the properties of binary operations that were discussed just now are very much applicable in something called **groups**.

Definition 3.3: Group

A group is a set G, closed under a binary operation $*$, satisfying the three properties:

1. Associativity: For all $a, b, c \in G$, we have:
$$(a * b) * c = a * (b * c)$$
2. Identity Element: There is an element $\epsilon \in G$ such that for all $x \in G$:
$$\epsilon * x = x * e = x$$
3. Inverse: Corresponding to each $a \in G$, there is an element $a' \in G$ such that:
$$a * a' = a' * a = \epsilon$$

Remark: Notationally, this can be represented by $(G, *)$ or $\langle G, * \rangle$. This is saying that we are pairing a set with a binary operation.

3.3.1 Example: Addition

For example, the integers under addition are a group. Notationally, this is represented by $(\mathbb{Z}, +)$.

- It's obvious that addition is associative. That is:
$$(a + b) + c = a + (b + c) = a + b + c$$
- The identity element is 0. This is because:
$$0 + x = x + 0 = x$$

- The inverse is $-x$. This is because:

$$x + (-x) = (-x) + x = 0$$

We also know that the reals, rationals, or complex numbers under addition are also groups. Notationally, this is represented by $(\mathbb{R}, +)$, $(\mathbb{Q}, +)$, or $(\mathbb{C}, +)$, respectively.

3.3.2 Example: Multiplication

Let's now consider multiplication. In particular, multiplication does give a binary operation over $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$. It's obvious that this is associative and 1 is the two-sided identity element. However, what about the inverse?

- If we try to take the integers under multiplication as a group, then we'll run into problems. This is because the multiplicative inverse of every integer except ± 1 is not an integer. For example, if we tried 2, then the multiplicative inverse of 2 is $\frac{1}{2}$. However, $\frac{1}{2} \notin \mathbb{Z}$.

- Rational numbers are closer. For instance, $\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}$. However, this is only defined if $a \neq 0$. The solution is to remove 0. Define $\mathbb{Q}^*$ to be the non-zero rational numbers (i.e. $\mathbb{Q}^* = \mathbb{Q} - \{0\}$). Then, $(\mathbb{Q}^*, \cdot)$ is a group. Similarly, we can make $\mathbb{R}$ and $\mathbb{C}$ groups under multiplication by removing 0.

  We note that this change does not affect the closure property because we can only achieve $a \cdot b = 0$ if and only if $a = 0$ or $b = 0$. Since $a \notin \mathbb{R} - \{0\}$ and $b \notin \mathbb{R} - \{0\}$ (or $\mathbb{Q}$ or $\mathbb{C}$), then we are still closed and our binary operation is still well-defined.

3.3.3 Example: Addition and Modular Arithmetic

More examples of groups come from modular arithmetic. For instance, consider addition modulo n for some integer n. The set that we're going to be working with is *equivalence classes* modulo n. Recall that[5]:

$$[0]_n = \overline{0} = \{\dots, -3n, -2n, -n, 0, n, 2n, 3n, \dots\}$$
$$[1]_n = \overline{1} = \{\dots, 1-3n, 1-2n, 1-n, 1, 1+n, 1+2n, 1+3n, \dots\}$$
$$[2]_n = \overline{2} = \{\dots, 2-3n, 2-2n, 2-n, 2, 2+n, 2+2n, 2+3n, \dots\}$$
$$\vdots$$
$$[n-1]_n = \overline{n-1} = \{\dots, -n-1, -1, n-1, 2n-1, \dots\}$$

We define our binary operation on the set of equivalence classes $\{\overline{0}, \overline{1}, \overline{2}, \dots, \overline{n-1}\}$. What properties does this have? We know that modulo n addition on these equivalence classes is:

- Associative (and commutative).
- It has identity $\overline{0}$. If you have equivalence class $\overline{k}$ (for $k \geq 1$), then the inverse if $\overline{n-k}$ for $1 \leq k \leq n-1$ so that $1 \leq n-k \leq n-1$. We note that:

$$\overline{k} + \overline{n-k} = \overline{0} \pmod{n}$$
$$k + (n-k) = n \in \overline{0}$$

- $\overline{0}$ is the inverse of $\overline{0}$.

We denote this group as $(\mathbb{Z}_n, + \pmod{n})$, where $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}$. When it is clear, we can drop the lines.

[5] In general, $[a]_n = \overline{a} = \{x \in \mathbb{Z} \mid x \equiv a \mod n\}$

3.3.4 Example: Multiplication and Modular Arithmetic

Could we do multiplication modulo n as a group? Well, multiplication modulo n on the set $\mathbb{Z}_n$ is an associative, commutative, binary operation with identity $\overline{1}$. However, inverses are potentially an issue ($\overline{0}$ specifically will be an issue). Can we fix this by removing all uninvertible elements?

- Yes, but can we characterize uninvertible elements? Well, the greatest common divisor of two integers is a linear combination. This is useful because we can think about $\gcd(k, n)$ where $k \in \{1, \ldots, n-1\}$. Specifically, if $\gcd(k, n) = 1$, then $ak + bn = 1$ implies that $\overline{a} \cdot \overline{k} = \overline{1} \pmod{n}$. In other words, k is invertible if $\gcd(n, k) = 1$.
- What if $\gcd(k, n) > 1$? If k was invertible under multiplication modulo n, then $\overline{a}\overline{k} = \overline{1} \pmod{n}$. But, that would mean that there is a linear combinations of a and k that is equal to 1. Thus, k is invertible under multiplication modulo n if and only if $\gcd(k, n) = 1$.

Let's now consider only taking equivalence classes $\overline{k}$ where $\overline{k}$ is relatively prime for n. We will now make the claim that $(U(n), \cdot \pmod{n})$ is a group. We know that this is associative and commutative, we justified that it has an inverse and an identity element. However, is this still closed?

More formally, why do we have closure of the binary operations? We could think about this in several ways. We could give a proof that the product two integers that are relatively prime to n is still relatively prime to n, or we can think about this more algebraically: namely, we can justify that the product of two invertible equivalence classes is also invertible.

If k_1, k_2 are both invertible, then $k_1 k_2$ is also invertible. Why is this the case? Well, k_1 and k_2 being invertible means that there is some value k_1^{-1} and k_2^{-1}. So, let's consider $k_2^{-1}k_1^{-1}$. We know that:

$$\begin{aligned}(k_1k_2)\left[k_2^{-1}k_1^{-1}\right] &= k_1\left[k_2k_2^{-1}\right]k_1^{-1}\\ &= k_1\epsilon k_1^{-1}\\ &= k_1k_1^{-1}\\ &= \epsilon\end{aligned}$$

3.4 Basic Properties of Groups

- Uniqueness of the Identity.

  Could we have two unique two-sided identities in a group G? No. If we assume by contradiction that we had ϵ_1 and ϵ_2, both of which are unique two-sided identity elements. Then, we know that $\epsilon_1\epsilon_2 = \epsilon_2$ since ϵ_1 is an identity. But, since ϵ_2 is also an identity, then $\epsilon_1\epsilon_2 = \epsilon 1$. So, it follows that ϵ_1 and ϵ_2 are not unique.

- Uniqueness of Inverses.

  If g_1, g_2 are both inverses of some element h, then:

  $$g_1h = \epsilon = g_2h$$

  Additionally, we know that:

  $$\begin{aligned}g_1(hg_2) &= g_1\epsilon = g_1\\ (g_1h)g_2 &= g_2\epsilon = g_2\end{aligned}$$

  So, it follows that $g_1 = g_2$. Thus, an element h will have a unique inverse.

- Cancellation.

  Suppose we have the expression $ga = gb$. This implies that $a = b$.

  Proof. We know that $gag^{-1} = gbg^{-1} \iff \epsilon a = \epsilon b \iff a = b$. □

  Remark: Although $ga = gb$, $ga \neq bg$ (ga is not necessarily equal to bg).