Algebraic Structure and Closure Operations
Summer MCTP Workshop
University of New Mexico

Janet Vassilev

July 5, 2012 – July 11, 2012

Contents

Chapter 1

Introduction

Welcome to the first week of the Summer MCTP Workshop at UNM. My goal for this course is to solidify your background in algebra through games and independent work. I like to think of Algebra (and all Mathematics for that matter) as a puzzle. Each new theorem and definition you learn can be thought of as a piece (or pieces) of some jigsaw puzzle where the jigsaw puzzle I am talking about is your algebra proof. Some pieces you can logically connect; others just don't fit. Sometimes, when you are assembling a jigsaw puzzle you think two pieces fit together, but later you see the color is wrong or the pieces just don't interlock correctly. These pieces that don't really fit together form a gap in your proof. You need to interlock different pieces instead to fill in this gap to finish the puzzle. I always feel satisfied when I finish a jigsaw puzzle. This is also how I feel when I finish a proof. Hopefully, this week you will gain an appreciation for algebra and proofs which will help you in all your mathematical endeavors.

You should know some basic proof techniques such as direct proofs, proofs by contradiction, proofs by induction and some basic facts about sets. Here are some facts that you may have proved in a previous math class:

- $\sum_{i=1}^{n} i = \dfrac{n(n+1)}{2}$.

- There are an infinite number of primes.

- If $f : A \to B$ and $g : B \to C$ are both one to one functions then $g \circ f : A \to C$ is a one to one function.

- The additive identity in a vector space is unique.

- The determinant of an orthogonal matrix is ± 1.

If you are not confident in your proof writing abilities, in the following sections I include a review of some of the basics. Learning to write proofs on your own takes time. Throughout the week we will be working either alone or in groups on various exercises, some of which will require proof writing skills. If proof writing is not one of your strengths let me know so I can pair you with someone appropriate.

1.1 Logic

In mathematics a firm grasp of logic is essential. A *statement* is a sentence which can be determined to be true or false.

Example 1.1 1. Every prime number besides 2 is odd. (This is a true statement.)

2. $2 + 3 \leq 10$. (This is a true statement.)

3. $4 + 5 < 9$. (This is a false statement.)

4. All sets have at least one element. (This is a false statement.)

5. $2x+4 = 10$. (This is not a statement since we cannot determine if it is true or false. If we knew $x = 4$, the sentence would be false. However, if $x = 3$, the sentence would be true. We call such a mathematical sentence a *conditional or variable statement.* When we quantify the variables that do not allow us to determine the truth or falsehood of a variable statement, the new quantified sentence becomes a statement. We will talk more on quantifying variable statements later.)

We will abbreviate statements by letters such as P, Q or R. A variable statement is usually written $P(x)$, $P(x, y)$ or $P(x_1, x_2, \ldots, x_n)$, depending on how many variables the sentence involves. The *negation* of a statement, P, is the new statement: It is not the case that P. This is usually written $\neg P$. For example, here are the negations of the above statements:

Example 1.2 1. It is not the case that every prime number besides 2 is odd. Equivalently, we could say, some prime besides 2 is even. Note both of these statements are false.

2. It is not the case the $2 + 3 \leq 10$ or $2 + 3 > 10$.

3. It is not the case that $4 + 5 < 9$ or $4 + 5 \geq 9$.

4. It is not the case that all sets have at least one element or some sets have no elements.

Most definitions and theorems in math rely on *conditional statements.* These statements take the the equivalent forms:

- If P then Q.
- P implies Q.
- Q if P.
- Q when P.
- P only if Q.
- A necessary condition for P is Q.

- A sufficient condition for Q is P.

Conditional statements are often abbreviated by $P \Rightarrow Q$. P is often called the *hypothesis* and Q is called the *conclusion.* If P is false then no matter what Q is, the statement $P \Rightarrow Q$ will be true. The only way a conditional statement is false is if Q is false and P is true because P being true implies that Q must be true.

Example 1.3 1. If $\frac{1}{2}$ is an integer, then any integer multiple of $\frac{1}{2}$ is an integer. (true)

2. If 2 is an integer, then $\frac{1}{2}$ is an integer. (false)

3. If $2 + 3 \leq 10$, then $4 + 5 > 7$. (true)

The common connectives for statements are *and* ($\wedge$) and *or* ($\vee$). If two statements P and Q are connected with the connective, and, then the connected statement $P \wedge Q$ is true when both P and Q are true. If one of P or Q is false, then $P \wedge Q$ is false. If two statements P and Q are connected with the connective, or, then the connected statement $P \vee Q$ is true when at least one of P or Q is true. The only scenario which would lead $P \vee Q$ to be false is if both P and Q are false.

Example 1.4 1. $2 + 3 \leq 10$ and $4 + 5 > 7$ is a true statement.

2. $2 + 3 \leq 10$ and $4 + 5 < 9$ is a false statement but $2 + 3 \leq 10$ or $4 + 5 < 9$ is a true statement.

3. $2 + 3 > 10$ or $4 + 5 < 9$ is a false statement.

To visualize the truth of compound and conditional statements, one may use a *truth table* which indicates the truth or the falsehood of a statement involving one or more statements in terms of the individual statements involved. We will abbreviate true by T and false by F.

P	Q	$P \wedge Q$
T	T	T
T	F	F
F	T	F
F	F	F

P	Q	$P \vee Q$
T	T	T
T	F	T
F	T	T
F	F	F

P	Q	$P \Rightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

Since the negation of a true statement is a false statement and vice versa, we see that the negations of the above statements are as follows:

P	Q	$\neg(P \wedge Q)$
T	T	F
T	F	T
F	T	T
F	F	T

P	Q	$\neg(P \vee Q)$
T	T	F
T	F	F
F	T	F
F	F	T

P	Q	$\neg(P \Rightarrow Q)$
T	T	F
T	F	T
F	T	F
F	F	F

Compare these to the following:

P	Q	$\neg P \vee \neg Q$
T	T	F
T	F	T
F	T	T
F	F	T

P	Q	$\neg P \wedge \neg Q$
T	T	F
T	F	F
F	T	F
F	F	T

P	Q	$P \wedge \neg Q$
T	T	F
T	F	T
F	T	F
F	F	F

We can see that the truth values of $\neg(P \wedge Q)$ and $\neg P \vee \neg Q$ are the same. We call these two statements equivalent because they have the same truth values. Similarly, $\neg(P \vee Q)$ is equivalent to $\neg P \wedge \neg Q$ and $\neg(P \Rightarrow Q)$ is equivalent to $P \wedge \neg Q$.

Note also that $P \Rightarrow Q$ is not equivalent to $Q \Rightarrow P$:

P	Q	$P \Rightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

P	Q	$Q \Rightarrow P$
T	T	T
T	F	T
F	T	F
F	F	T

We call $Q \Rightarrow P$ the *converse* of $P \Rightarrow Q$.

However, note that $P \Rightarrow Q$ is equivalent to $\neg Q \Rightarrow \neg P$:

P	Q	$P \Rightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

P	Q	$\neg Q \Rightarrow \neg P$
T	T	T
T	F	F
F	T	T
F	F	T

We call $\neg Q \Rightarrow \neg P$ the *contrapositive* of $P \Rightarrow Q$.

The statement $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$ is often written $P \Leftrightarrow Q$. We call $P \Leftrightarrow Q$ a *biconditional* statement and often write P if and only if Q or P is a necessary and sufficient condition for Q. The truth table for $P \Leftrightarrow Q$ follows:

P	Q	$P \Rightarrow Q$	$Q \Rightarrow P$	$P \Leftrightarrow Q$
T	T	T	T	T
T	F	F	T	F
F	T	T	F	F
F	F	T	T	T

1.2 Sets

A *set* is a collection of objects. For example $\{a, b, c\}$ is a set. The objects in a set are called *elements*. Order does not matter when you list the elements in a set. For example $\{a, b, c\}$ is the same set as both $\{b, a, c\}$ and $\{c, b, a\}$. Also, repetition of elements doesn't change a set. For example $\{a, b, c\}$ is the same as the set $\{a, a, b, c, c, c\}$. To indicate that an element x is a member of a set A, we write $x \in A$. To indicate that x is not a member of A, we write $x \notin A$.

We call two sets A and B *equal* if the elements of A and B are the same or equivalently all the elements of A are elements of B and all the elements of B are elements of A. The set with no elements is called *the empty set* which is either written $\emptyset$ or $\{\}$. Note that the set $\emptyset \neq \{\emptyset\}$, since the latter set has the empty set as a member, whereas the first set has no elements. We have seen above that we can describe a set by listing elements.

There are certain sets of numbers that you should be familiar with, for example:

- the counting numbers, $\mathbb{N} = \{1, 2, 3, \ldots\}$,
- the whole numbers, $\mathbb{N}_0 = \{0, 1, 2, 3, \ldots\}$,
- the integers, $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$,
- the rational numbers, $\mathbb{Q} = \{\frac{a}{b} \mid a, b \in \mathbb{Z} \text{ and } b \neq 0\}$,
- the real numbers, $\mathbb{R}$, and
- the complex numbers, $\mathbb{C}$.

Sometimes we describe a set using a variable statement, such as $A = \{x \mid P(x)\}$. We often call A of this form a *truth set* since the elements of A are the values of the variable x which make the variable statement $P(x)$ true.

Example 1.5 1. $\{n \mid n \text{ a prime number}\}$.

2. $\{x \mid 2x - 3 \geq 0\}$.

3. $\{x \mid x^2 + 3x - 28 = 0\}$.

Sometimes we specify a *domain* for x, a set where the variables x may be chosen from. For example $\{x \in \mathbb{N} \mid x^2+3x-28 = 0\} = \{4\}$ whereas $\{x \in \mathbb{Z} \mid x^2+3x-28 = 0\} = \{-7, 4\}$.

We say a set B is a *subset* of a set A if all the elements of B are elements of A and we denote B being a subset of A as $B \subseteq A$ or $B \subset A$. Note if $B \subseteq A$ and $x \in B$, then by definition, $x \in A$. If we want to indicate that B is a *proper* subset of A, a subset which is not equal to A itself, we write $B \subsetneq A$. To show that $A = B$ as sets it is necessary and sufficient to show that $A \subseteq B$ and $B \subseteq A$. If there are elements in B which are not in A we say that B is not a subset of A and we denote this as $B \not\subseteq A$. If $x \in B$ and $x \notin A$, then $B \not\subseteq A$.

We can denote subsets of a set A as truth sets $B = \{x \in A \mid P(x)\}$ for some variable statement $P(x)$. For example, you are probably familiar with intervals of the real line. Intervals are subsets of $\mathbb{R}$. The common interval notations are

- $(a, b) = \{x \in \mathbb{R} \mid a < x < b\}$.
- $(a, b] = \{x \in \mathbb{R} \mid a < x \leq b\}$.
- $[a, b) = \{x \in \mathbb{R} \mid a \leq x < b\}$.
- $[a, b] = \{x \in \mathbb{R} \mid a \leq x \leq b\}$.

The *power set*, of a set A, $P(A)$ is the set of all subsets of A. For example if $A = \{a, b, c\}$, $P(A) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, A\}$. Note that A has 3 elements and $P(A)$ has $8 = 2^3$ elements. In general, if A has n elements, the power set of A will have 2^n elements.

The common operations on sets are intersection, union and set difference. The *intersection* of two sets A and B is the set $A \cap B = \{x \mid x \in A \text{ and } x \in B\}$. The *union* of two sets A and B is the set $A \cup B = \{x \mid x \in A \text{ or } x \in B\}$. The *set difference* of A with B is the set $A \setminus B = \{x \mid x \in A \text{ and } x \notin B\}$.

Example 1.6 Let $A = \mathbb{Z}$, $B = (-2, 5]$ and $C = [2, 10)$.

1. $A \cap B = \{-1, 0, 2, 3, 4, 5\}$.
2. $A \setminus B = \{\dots, -4, -3, -2, 6, 7, 8, \dots\}$.
3. $B \cap C = [2, 5]$.
4. $B \cup C = (-2, 10)$.
5. $B \setminus C = (-2, 2)$.
6. $C \setminus B = (5, 10)$.

1.3 Quantifiers

When the truth of a variable statement, with variable x, (for example $x \geq 2$) we can make this sentence into a statement by *quantifying* x or specifying values for x. One way to quantify x is to list the values that x is allowed to be. For example, for $x = 3, 4$ or 5, $x \geq 2$. A variable statement $P(x)$ is *universally quantified* over a domain A if for every $x \in A$,$P(x)$, written $\forall x \in A,\ P(x)$. If $\forall x \in A,\ P(x)$ is true, this means that $P(x)$ is a true statement for each and every element $x \in A$. If the statement is false for at least one element $x \in A$, then $\forall x \in A,\ P(x)$ is false.

Example 1.7 1. $\forall x \in \mathbb{Z}$, $2x$ is an even number. (True)

2. $\forall x \in \mathbb{Q}$, $2x$ is an even number. (False, since $2 \cdot \frac{1}{2} = 1$ is odd and $2 \cdot \frac{1}{3}$ is not even an integer.)
3. $\forall x \in \mathbb{Z}$, $3x$ is an odd number. (False, since $3 \cdot 2 = 6$ is even.)

A variable statement $P(x)$ is *existentially quantified* over a domain A if for some $x \in A$, $P(x)$, written $\exists x \in A,\ P(x)$. The statement $\exists x \in A,\ P(x)$ is true if we can find at least one $x \in A$ so that the statement $P(x)$ is true. There may be some values of $x \in A$ where $P(x)$ is false.

Example 1.8 1. $\exists x \in \mathbb{Z}$, $2x$ is an even number. (True)

2. $\exists x \in \mathbb{Q}$, $2x$ is an even number. (True)
3. $\exists x \in \mathbb{Z}$, $x \in (0, 1)$. (False, since the elements of the interval $(0, 1)$ are not integers.)

Consider the negation of $\forall x \in A, P(x)$. If $P(x)$ were true for all $x \in A$ then $\forall x \in A, P(x)$ is a true statement. So $\neg(\forall x \in A, P(x))$ must be false. However, if $P(x)$ is false for at least one $x \in A$, then $\forall x \in A, P(x)$ is a false statement. Note that $\exists x \in A, (\neg P(x))$ is false if $P(x)$ is true for all $x \in A$ and is true if there is at least one $x \in A$ where $P(x)$ is false. Hence the statements, $\neg(\forall x \in A, P(x))$ and $\exists x \in A, (\neg P(x))$ are equivalent statements. Similarly, $\neg(\exists x \in A, P(x))$ and $\forall x \in A, (\neg P(x))$ are equivalent statements.

When combining existential and universal quantifiers, one must be careful with the order of quantification. Consider the statements:

Example 1.9

1. $\forall x \in \mathbb{R} \forall y \in \mathbb{R}, x + y = 0.$
2. $\exists x \in \mathbb{R} \forall y \in \mathbb{R}, x + y = 0.$
3. $\forall x \in \mathbb{R} \exists y \in \mathbb{R}, x + y = 0.$
4. $\exists x \in \mathbb{R} \exists y \in \mathbb{R}, x + y = 0.$

Clearly, (1) is false since $1 + 2 = 3 \neq 0$ is false. (2) is also false because there is no real number x such that $x + y = 0$ for all real y. However, (3) is true because for any x in (R), $-x$ is a real number that satisfies $x + -x = 0$. So we have found a y, $-x$, which satisfies the equality. (4) is also true.

1.4 Proof Techniques

The proof techniques that I am hoping you will be familiar with are

- Direct proofs.
- Disproof via counterexample.
- Proofs by contradiction.
- Proof by contrapositive.
- Existence proofs.
- Proofs involving cases.
- Proofs of equivalence.
- Mathematical induction.

I will include some examples.

Direct Proof

In a direct proof, we need to use definitions or theorems possibly along with computations to prove a statement is true. For example:

Example 1.10 Show that if m and n are both odd numbers, then mn is odd.

Proof: Since m is odd, there is an integer j such that $m = 2j + 1$. Similarly, since n is odd, there is an integer k such that $n = 2k + 1$.

$$\begin{aligned} mn &= (2j + 1)(2k + 1) \\ &= 4jk + 2j + 2k + 1 \\ &= 2(2jk + j + k) + 1. \end{aligned}$$

As j and k were integers, $2jk + j + k$ is also an integer. Hence, we have found an integer, $p = 2jk + j + k$ such that $mn = 2p + 1$. This implies that mn is odd. □

Disproofs by counterexample

One uses a counterexample to disprove a statement. It is enough to find one counterexample to show a statement is false. For example:

Example 1.11 Every prime number is odd.

This statement is false since 2 is a prime number which is even.

Proofs by contradiction

In a proof by contradiction, you have a statement such as $P \Rightarrow Q$. You assume both P is true and $\neg Q$ is true. Then you try to obtain a contradiction, a statement which is always false. The reason why this proof technique works is because $P \wedge \neg Q$ is the negation of $P \Rightarrow Q$. So if $P \wedge \neg Q$ is always false then $P \to Q$ must be true.

Example 1.12 If n is an integer such that $n + m = m = m + n$ for every $m \in \mathbb{Z}$, then $n = 0$.

Proof: Suppose not. There is an integer $n \neq 0$ such that $n + m = m = m + n$ for all integers m. Then $n + 0 = 0$. Since 0 is the additive identity, then $n + 0 = n$. This implies $n = 0$ which is a contradiction since $n \neq 0$ and $n = 0$ can't both be true at the same time. Hence, our assumption $n \neq 0$ can never hold and n must be 0. □

Proof by contrapositive

Recall that the statements $P \Rightarrow Q$ and $\neg Q \Rightarrow P$ are logically equivalent. Sometimes it is easier to show $\neg Q \Rightarrow P$.

Example 1.13 Suppose a, b and c are all real numbers and $a > b$. Show that if $ac \leq bc$ then $c \leq 0$.

Proof: Note that the contrapositive of the statement, if $ac \leq bc$ then $c \leq 0$ is the statement, if $c > 0$, then $ac > bc$. Since we know $a > b$, multiplying both sides of the inequality by the positive number c does not change the direction of the inequality, so $ac > bc$. Thus if $ac \leq bc$ that means that $c \leq 0$. □

Existence Proofs

For an existence proof, we need only show that there is some x in our domain of discourse such that the variable statement $P(x)$ is true.

Example 1.14 Suppose a and b are real numbers with $a > b$. Show there exists a real number x with $a < x < b$.

Proof: Note that $a = \frac{a}{2} + \frac{a}{2} < \frac{a}{2} + \frac{b}{2}$ since $a < b$. Also $\frac{a}{2} + \frac{b}{2} < \frac{b}{2} + \frac{b}{2} = b$. So if we take $x = \frac{a}{2} + \frac{b}{2}$, then we have found a real number with $a < x < b$. □

Proofs Involving cases

Suppose your are trying to prove a statement in the form $P \vee Q \Rightarrow R$. The following truth table shows that $P \vee Q \Rightarrow R$ is equivalent to $(P \Rightarrow R) \wedge (Q \Rightarrow R)$.

P	Q	R	$(P \vee Q) \Rightarrow R$	$(P \Rightarrow R) \wedge (Q \Rightarrow R)$
T	T	T	T	T
T	T	F	F	F
T	F	T	T	T
T	F	F	F	F
F	T	T	T	T
F	T	F	F	F
F	F	T	T	T
F	F	F	T	T

Hence, when trying to prove a statement involving a disjunction, we need to break the statement into cases, where we show that each statement in the hypothesis implies the conclusion. Sometimes this is called proof by exhaustion.

Example 1.15 Show that for every real number x, $x \leq |x|$.

Proof: Note that $|x| = x$ if $x \geq 0$ and $|x| = -x$ if $x < 0$. So we break the proof into the two cases: $x \geq 0$ and $x < 0$.
Case 1: If $x \geq 0$, then $|x| = x \geq x$ which is what we wanted to show.
Case 2: If $x < 0$, then $|x| = -x > 0$. However since $0 > x$, then $|x| > 0 > x$ implies $|x| \geq x$.
Hence, for all real x, $|x| \geq x$. □

Equivalence Proofs

If a statement is of the form $P \Leftrightarrow Q$, then either we can directly prove a chain of equivalent statements or we need to prove both $P \Rightarrow Q$ and $Q \Rightarrow P$.

The following statement can be proved using a chain of equivalent statements.

Example 1.16 For every integer n, n is odd if and only if $n - 1$ is even.

Proof: n is odd means there is an integer k such that $n = 2k + 1$. This is equivalent to the statement $n - 1 = 2k$ for some integer k. Which in turn, is equivalent to $n - 1$ being even.
□

The following is better suited for breaking the proof down into two directions:

Example 1.17 For sets A and B, $A \subseteq B$ if and only if $A \cap B = A$.

Proof: For the first direction, we need to show that if $A \subseteq B$, then $A \cap B = A$. Clearly $A \cap B \subseteq A$ by the definition of intersection of sets. We need to show that if $x \in A$, then $x \in A \cap B$. By our assumption $A \subseteq B$, if $x \in A \subseteq B$, then $x \in B$. Hence $x \in A$ and $x \in B$ implies that $x \in A \cap B$. Thus, $A \subseteq B$ implies $A \cap B = A$.

Now suppose $A \cap B = A$. Since $A \cap B \subseteq B$ by the definition of intersection, $A = A \cap B \subseteq B$, implies $A \subseteq B$. □

Mathematical Induction

The natural numbers $\mathbb{N}$ have a special property which we call well ordering. A set is *well ordered* if every subset has a smallest element. Because of this, if we are trying to prove statements about every natural number n or some subset of natural numbers greater than or equal to some natural number n_0, we can use
The Principle of Mathematical Induction: Let $P(n)$ be a variable statement with domain of discourse $\mathbb{N}$. Suppose $P(1)$ is true and when $P(n)$ is true then $P(n+1)$ is true. Then $P(n)$ is true for all integers n.

The reason this method of proof works is as follows: Suppose A is the set of natural numbers such that $P(n)$ is not true. Since A is a subset of the counting numbers, there is a smallest element $k \in A$, where $P(k)$ is false. Note that $k > 1$ since $P(1)$ is true. $k-1$ is not a member of A since k was the smallest element. Thus $P(k-1)$ is true. However, by the assumption that $P(n)$ is true implies that $P(n+1)$ is true, then $P(k-1)$ being true implies that $P(k)$ is true. Hence, contradicting the fact that $k \in A$. Hence, there is no natural number such that $P(n)$ is false. So $P(n)$ is true for all natural numbers.

Now that we know the principle works, let us see it in action.

Example 1.18 Show that $\sum\limits_{i=1}^{n} 2i - 1 = n^2$ for all natural number n.

Proof: The statement we are trying to prove is $P(n) := \sum\limits_{i=1}^{n} 2i - 1 = n^2$. Note that $P(1)$ corresponds to the statement $2 \cdot 1 - 1 = 1 = 1^2$ which is true. Now, let us assume $P(k)$ is true. In other words $\sum\limits_{i=1}^{k} 2i - 1 = k^2$. Let us add $2(k+1) - 1 = 2k + 1$ to both sides of this equality.

$$(\sum_{i=1}^{k} 2i - 1) + 2k + 1 = k^2 + 2k + 1$$

$$\sum_{i=1}^{k+1} 2i - 1 = (k+1)^2$$

Hence, using the principle of mathematical induction $\sum\limits_{i=1}^{n} 2i - 1 = n^2$ for all natural numbers n. □

Sometimes you cannot easily show that some variable statement $P(n)$ follows directly from $P(n-1)$. However it may easily follow from $P(k)$ for some $1 \leq k \leq n$. An alternate version of induction you may wish to employ is:
The Principle of Strong Mathematical Induction: Let $P(n)$ be a variable statement with domain of discourse $\mathbb{N}$. Suppose $P(1)$ is true and when $P(k)$ is true for all $1 \leq k \leq n$ then $P(n+1)$. Then $P(n)$ is true for all integers n.

Justifying the principle of strong mathematical induction works as a proof technique is very similar to the justification we gave above that induction is a valid method. Here is an example of how the principle works.

Example 1.19 Every natural number greater than 1 is either a prime or a product of two or more primes.

Proof: The first case is to check that 2 is is either a prime or a product of two or more primes. But 2 is a prime so this is true. Let us now assume that for $2 \leq k \leq n$, k is either a prime or a product of two or more primes. We want to see that $n+1$ is a either a prime or a product of two or more primes.
Case 1: If $n+1$ is prime, then we are done.
Case 2: If $n+1$ is not prime, then there exist c and d natural numbers with $2 \leq c, d \leq n$ and $n+1 = cd$. By assumption, both c and d are either primes or products of two or more primes. Hence, $n+1$ is a product of two or more primes.

By the principle of strong mathematical induction any natural number greater than one is a prime or a product of two or more primes. □

Chapter 2

The Hat Game – Intro to Linear Algebra over finite fields

Our first day starts with the Hat Game. In this game you are not competing against your fellow players, but with them for a group win. In the game, all players will blindfold themselves. Then each will have either a red or blue hat placed on his or her head. The players will remove their blindfolds and without communicating with the other players, they will jot down on a piece of paper either red, blue or pass. Red or blue means they think they have a red or blue hat on respectively. Pass means they didn't think they could determine their hat color. If at least one player guesses their hat color correctly and the remaining players either passed or guessed their hat colors correctly, then the team wins. If all the players pass or at least one player chooses the wrong hat color the team loses. Without knowing, some discrete math, the group's chances of winning are not too high.

We will play the three person game both to familiarize ourselves with playing the game and to learn the strategy to win as a group. To win the n person game, we will learn the basics about vector spaces over $\mathbb{Z}_2$ and error correcting codes, in particular Hamming Codes, to win the game with a very high probability.

2.1 The 3 person game

Break yourselves into groups of three. Before we play the game each group will have a strategy session on how the group will play. Since the whole group either wins or loses, it is essential that you come up with a good strategy playing by the rules. Remember, you cannot peak while your hat is being placed on your head and you cannot communicate with your teammates.

After the hats have been placed on the players' heads, each player has the option to guess a hat color or to pass by writing his guess on a piece of paper.

- **You win if:**

    1. at least one player guesses their hat color correctly **AND**
    2. all others either pass or guess correctly.

- **You lose if:**
  1. a hat color is guessed incorrectly **OR**
  2. all players pass.

Some of the strategies that your team might choose are:

1. Everybody guesses a hat color at random.
2. The team decides that two players will pass and one player will randomly decide on a hat color.
3. Each player on the team looks at the other players hats and bases his choice of hat color on what he sees.

Note that in the first scenario, the three guesses are independent. The probability of all three guessing the right color is $(\frac{1}{2})^3 = \frac{1}{8}$. In the second scenario, since two of the players pass and the third guesses, the probability is better: $\frac{1}{2}$. However, we can do better than that with the third scenario. Let R denote red, and B denote blue. The combinations are

RRR RRB RBR BRR

BBB BBR BRB RBB

3 out of 4 combinations are mixed. So if you see two blues, guess red, or if you see two reds, guess blue. However if you see red and blue, you should pass. This way the group wins 3 out of 4 times.

2.2 Vector spaces over general fields

Linear algebra is a valuable tool in most areas of mathematics. Vector spaces form the backbone of linear algebra and provide us with the algebraic structure for the subject. A vector space can be defined over any field. A *field* is a set F with two operations, addition $(+)$ and multiplication $(\cdot)$ satisfying the following properties:

- Addition and Multiplication are closed. For all $a, b \in F$ both $a + b$ and $a \cdot b$ are in F.
- Addition and Multiplication are commutative. For all $a, b \in F$, $a + b = b + a$ and $ab = ba$.
- Addition and Multiplication are associative. For all $a, b, c \in F$, $(a+b)+c = a+(b+c)$ and $(ab)c = a(bc)$.
- There exists both additive and multiplicative identities. For all $a \in F$ $0+a = a+0 = a$ and $a \cdot 1 = 1 \cdot a = a$.
- Additive inverses exist for all $a \in F$. For some $-a \in F$, $a + (-a) = -a + a = 0$.
- Multiplicative inverses exist for all nonzero $a \in F$. There exists $a^{-1} \in F$ such that $aa^{-1} = a^{-1}a = 1$.

The fields that you are most familiar with are $\mathbb{R}$, the real numbers; $\mathbb{C}$, the complex numbers; $\mathbb{Q}$, the rational numbers.

Let $\mathbb{Z}_2$ be the set $\{0, 1\}$ with addition and multiplication defined as follows:

$$0 + 0 = 1 + 1 = 0 \text{ and } 0 + 1 = 1 + 0 = 1$$

$$0 \cdot 0 = 0 \cdot 1 = 1 \cdot 0 = 0 \text{ and } 1 \cdot 1 = 1.$$

We can easily verify that $\mathbb{Z}_2$ also is a field. In fact, $\mathbb{Z}_p = \{0, 1, 2, \ldots, p-1\}$ is also a field with addition defined as $a + b := r_+$ where r_+ is the remainder when $a + b$ is divided by p and multiplication is defined as $ab := r_\times$ where $r_\times$ is the remainder when ab is divided by p. If a field F has $m < \infty$ elements, we call F a *finite field.*

Now consider the set $F^n = \{(a_1, a_2, \ldots, a_n) | a_i \in F\}$ with addition defined componentwise. For any $\alpha \in F$ and $v := (v_1, \ldots, v_n) \in \mathbb{Z}_2^n$ we define $\alpha v := (\alpha v_1, \ldots, \alpha v_n)$. This multiplication is called scalar multiplication. The addition and scalar multiplication on F^n satisfy the following properties for all $u, v, w \in F^n$ and all $\alpha, \beta \in F$:

A1. $v + w = w + v$ (The commutative law for addition).

A2. $u + (v + w) = (u + v) + w$ (The associative law for addition).

A3. Let $\mathbf{0} = (0, 0, \ldots, 0)$. $\mathbf{0} + v = v + \mathbf{0} = v$ (The additive identity property).

A4. $v + v = \mathbf{0}$ (The additive inverse property.)

S1. $\alpha(v + w) = \alpha v + \alpha w$

S2. $(\alpha + \beta)v = \alpha v + \beta v$.

S3. $(\alpha\beta)v = \alpha(\beta v)$.

S4. $1v = v$.

Definition 2.1 *If V is a set with a closed addition which satisfies A1-A4 above and a scalar multiplication of F with V which satisfies S1-S4 above, then we call V a F-vector space.*

The structure we gave to F^n endows F^n as a F-vector space. Since $\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$, we can think of $\mathbb{R}^n$ as both a $\mathbb{R}$-vector space and $\mathbb{Q}$-vector space. However, $\mathbb{R}^n$ is not a $\mathbb{C}$-vector space since multiplying a real number by a complex number is complex so the scalar multiplication will not be closed over $\mathbb{R}^n$.

If F is a finite field with q elements, then the vector spaces, F^n will have q^n elements. For example $\mathbb{Z}_2^n$ will have 2^n elements and $\mathbb{Z}_3^n$ will have 3^n elements.

The elements of any vector space are called *vectors.* Suppose we have m vectors $v_1, \ldots, v_m \in F^n$ and m scalars $a_1, \ldots, a_m \in F^n$, then $a_1v_1 + a_2v_2 + \cdots + a_mv_m$ is called a F-*linear combination* of $v_1, \ldots, v_m$. A set of vectors $v_1, \ldots, v_m \in \mathbb{Z}_2^n$ *spans* F^n if any vector in F^n can be expressed as a linear combination of $v_1, \ldots, v_m$. A set of vectors $v_1, \ldots, v_m \in F^n$ are *linearly independent* if the only linear combination $a_1v_1 + a_2v_2 + \cdots + a_mv_m = (0, 0, \ldots, 0)$ is when $a_1 = a_2 = \cdots = a_m = 0$. If a set of vectors in F^n is both linearly independent and spans F^n then we say that $v_1, \ldots, v_n$ form a *basis* for F^n. Let e_i be the n-tuple with 1 in the ith spot and 0's elsewhere. Note that $a_1e_1 + a_2e_2 + \cdots a_ne_n = (a_1, a_2, \ldots, a_n)$ which is a random vector in F^n so any vector in F^n can be expressed as a linear combination of $e_1, e_2, \ldots, e_n$. Also if $a_1e_1 + a_2e_2 + \cdots a_ne_n = (a_1, a_2, \ldots, a_n) = (0, \ldots, 0)$, this implies $a_1 = a_2 = \cdots = a_n = 0$ so $e_1, \ldots e_n$ are linearly independent. Thus the e_i's form a basis of F^n.

A subset W of F^n is a *subspace* if $v + w \in W$ for all $v, w \in W$ and $\alpha v \in W$ for all $\alpha \in F$ and $v \in W$.

Note for a finite field F with q elements, the order of any subspace W of F^n will have q^k elements for $0 \leq k \leq n$. To see this, suppose $F = \{0 = \alpha_0, 1 = \alpha_1, \ldots, \alpha_{q-1}\}$. Note that if $v \in W$ is a nonzero vector, $\{\alpha_j v\}_{0 \leq j \leq q-1}$ gives us q distinct vectors that are in W. Now if $v_1, \ldots, v_k$ form a basis for W, then every vector in W is of the form $\beta_1v_1 + \beta_2v_2 + \cdots \beta_kv_k$. Thus there are q^k vectors in W. So clearly any subspace of $\mathbb{Z}_2^n$ has 2^k some $0 \leq k \leq n$.

Examples

- $V = \{(0,0,0), (1,1,1)\}$ is a subspace of $\mathbb{Z}_2^3$.
- $V = \{(0,0,0,0,0,0,0), (1,0,0,1,1,0,1),$
  $(0,1,0,1,0,1,1), (0,0,1,0,1,1,1),$
  $(1,1,0,0,1,1,0), (1,0,1,1,0,1,0),$
  $(0,1,1,1,1,0,0), (1,1,1,0,0,0,1)\}$ is a subspace of $\mathbb{Z}_2^7$

A *linear map* or *linear transformation* $A : F^n \to F^m$ satisfies $A(v + w) = A(v) + A(w)$ and $A(\alpha v) = \alpha A(v)$ for all $v, w \in F^n$ and $\alpha \in F$. For ease of working with linear transformations, we usually we represent A by an $m \times n$ matrix which is an array $A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}$

and v by a column vector which is an $n \times 1$ matrix. $m \times n$ matrices can be added together componentwise and they are multiplied as follows:

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} \begin{pmatrix} b_{11} & b_{12} & \cdots & a_{1r} \\ b_{21} & b_{22} & \cdots & a_{2r} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \cdots & a_{nr} \end{pmatrix} = \begin{pmatrix} c_{11} & c_{12} & \cdots & c_{1r} \\ c_{21} & c_{22} & \cdots & c_{2r} \\ \vdots & \vdots & \ddots & \vdots \\ c_{m1} & c_{m2} & \cdots & c_{mr} \end{pmatrix}$$

where $c_{ij} = \sum\limits_{k=1}^{n} a_{ik}b_{kj}$. Note this is the sum of the componentwise product of the ith row of A with the jth column of B.

For example over the reals,

$$\begin{pmatrix} 2 & 2 & 0 & 1 \\ 3 & 0 & 1 & 4 \end{pmatrix} \begin{pmatrix} 1 & 3 & 0 \\ 0 & 2 & 1 \\ 2 & 2 & 5 \\ 4 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 6 & 11 & 4 \\ 21 & 15 & 13 \end{pmatrix}$$

Here is a linear transformations represented via matrix multiplication. $A : \mathbb{Z}_2 \to \mathbb{Z}_2^3$ defined by $A(z) = (z, z, z)$ can be represented by the matrix $A = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$ and $Az = (zzz)$.

Also the linear transformation $A : \mathbb{Z}_2^3 \to \mathbb{Z}_2^7$ defined by $A(a, b, c) = (a, b, c, a + b + c, a + b, a + c, b + c)$ can be represented by the matrix

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

Note that $A \begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} a \\ b \\ c \\ a+b+b \\ a+b \\ a+c \\ b+c \end{pmatrix}$.

2.3 Hamming Codes: An example of Error Correcting Codes

When sending data, there may be noise. This can alter the message sent. Computers use binary, Sequences of 0's and 1's. A *word* is a sequence of n 0's and 1's. We can think of it as an element of $\mathbb{Z}_2^n$. Sending a word over a noisy circuit, did the receiver receive the correct word? He won't know, unless ... We agree to some error correcting scheme. This involves encoding words using a linear map $E : \mathbb{Z}_2^n \to \mathbb{Z}_2^{n+m}$. $E(v)$ is called a *code word*.

For example, let $E : \mathbb{Z}_2 \to \mathbb{Z}_2^3$ given by $E(a) = aaa$. If the receiver receives 101 he knows that he needs to change the middle digit to 1 and he decodes the message as 1. If the receiver receives 001 he knows that he needs to change the last digit to 0 and he decodes the message as 0. Sending three digits for every one can be unwieldy and it uses unnecessary memory. As more than one error in a longer word is less probable, many encoding maps address correcting one error only.

The Hamming (7,4) code has 16 words of length 4.

0000, 0001, 0010, 0100, 1000, 1111, 1110, 1101,

1011, 0111, 0011, 0101, 1001, 1100, 1010, 0110.

Let $E : \mathbb{Z}_2^4 \to \mathbb{Z}_2^7$ be the map given by

$$E = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}^T$$

There are 16 codewords which make up a subspace of $\mathbb{Z}_2^7$. 0000000, 0001011, 0010101, 0100110, 1000111, 1111111, 1110100, 1101010,

1011001, 0111000, 0011110, 0101101, 1001100, 1100001, 1010010, 0110011.

The matrix
$$H = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$
will correct one bit errors. Let w be the word received.

- If $Hw = 111$ the error in first slot.
- If $Hw = 110$ the error in second slot.
- If $Hw = 101$ the error in third slot.
- If $Hw = 011$ the error in fourth slot.
- If $Hw = 100$ the error in fifth slot.
- If $Hw = 010$ the error in sixth slot.
- If $Hw = 001$ the error in seventh slot.
- If $Hw = 000$ no error.

The Hamming $(2^n - 1, 2^n - 1 - n)$ code has $2^n - 1$ distinct words of length n different from 0. We use them to form columns in the error correcting matrix: $H = (A|I)$, A an $n \times 2^n - 1 - n$ matrix. Let $E = \begin{pmatrix} I \\ A \end{pmatrix}$. E is a $2^n - 1 \times 2^n - 1 - n$ matrix which encodes words of length $2^n - 1 - n$. There are 2^{2^n-1-n} code words in $\mathbb{Z}_2^{2^n-1}$. The ratio of code words to words is
$$\frac{2^{2^n-1-n}}{2^{2^n-1}} = \frac{1}{2^n}.$$
So the ratio of non-codewords to words is $\dfrac{2^n - 1}{2^n}$.

2.4 Hamming Codes and the Hat Game

Playing the Hat Game with $2^n - 1$ players. Fix a Hamming Error Check Matrix. Order the players. Don't deviate the order. Errors occur at a rate of $\dfrac{2^n - 1}{2^n}$. Denote red hats as 1's and blue hats as 0's. You see all hats but your own. The ith player sees $a_1 a_2 \dots \hat{a}_i \dots a_{2^n-1}$. The ith player will

- Compute $H(a_1 a_2 \dots 0 \dots a_n)$
- Compute $H(a_1 a_2 \dots 1 \dots a_n)$
- If both are nonzero, pass.

- If $H(a_1a_2\dots 0\dots a_n) = \overline{0}$, guess red.
- If $H(a_1a_2\dots 1\dots a_n) = \overline{0}$, guess blue.

In this way the team can win $\dfrac{2^n-1}{2^n}$ times.

Example 2.2 Playing the 7 person game:

Our Hamming Error check matrix is

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

Suppose the hats are distributed as follows:

red blue red red blue red red

This corresponds to the word 1011011

All players compute

$$\begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix} (1011011)^T = (010).$$

Player one computes

$$\begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix} (0011011)^T = (101)$$

and passes.

Player two computes

$$\begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix} (1111011)^T = (100)$$

and passes.

Player three computes

$$\begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix} (1001011)^T = (111)$$

and passes.

Player four computes

$$\begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix} (1010011)^T = (001)$$

and passes.

Player five computes

$$\begin{pmatrix}1&1&1&0&1&0&0\\1&1&0&1&0&1&0\\1&0&1&1&0&0&1\end{pmatrix}(1011111)^T=(110)$$

and passes.

Player six computes

$$\begin{pmatrix}1&1&1&0&1&0&0\\1&1&0&1&0&1&0\\1&0&1&1&0&0&1\end{pmatrix}(1011001)^T=(000)$$

and guesses correctly
red blue red red blue red red.

Player seven computes

$$\begin{pmatrix}1&1&1&0&1&0&0\\1&1&0&1&0&1&0\\1&0&1&1&0&0&1\end{pmatrix}(1011010)^T=(011)$$

and passes.

Now we will play in your groups of seven with the following configurations:

1. red red red blue red blue blue
2. blue blue red red blue red blue
3. blue blue blue blue red red red

2.5 Playing the Game

What do you notice about the Hamming (7,4) error correcting matrix? In particular, if you look at the columns in pairs, what can you say? They are linearly independent in pairs. In fact, there is no column that we could add to the error correcting matrix so that it would be linearly independent with the rest. Unfortunately $2^r - 1 \neq 19$ for any positive integer r. In our case, $2^5 - 1 > n > 2^4 - 1$? The best strategy is to use the $(2^4 - 1, 2^4 - 1 - 4)$ Hamming code. In otherwords, ignore the last 4 players. You will win with a probability of $\dfrac{15}{16}$.

Exercise 2.1 Come up with a Hamming (15,11) code which you can use for a hat game with 15 people. We will use this for our game.

Exercise 2.2 Using the Hamming (15,11) code that you came up with in the above problem, determine who if anyone should guess their hat color for the following hat placements:

red red blue blue blue red red blue red blue red red red blue red
blue blue red red blue red blue red red red blue red red red blue
blue red blue red red blue red blue red red red red blue red blue

What would you do if there were three hat colors instead of two? We certainly can't win with such a high probability, but we can use Hamming Codes. Let $\mathbb{Z}_3$ be the set $\{0, 1, 3\}$ with addition and multiplication defined as follows:

$$0+0=1+2=2+1=0 \text{ and } 0+1=1+0=2+2=1 \text{ and } 0+2=2+0=1+1=2$$

$$0 \cdot 0 = 0 \cdot 1 = 1 \cdot 0 = 0 \cdot 2 = 2 \cdot 0 = 0 \text{ and } 1 \cdot 1 = 2 \cdot 2 = 1 \text{ and } 1 \cdot 2 = 2 \cdot 1 = 2.$$

Now consider the set $\mathbb{Z}_3^n = \{(a_1, a_2, \ldots, a_n) | a_i \in \mathbb{Z}_3\}$ which is a $\mathbb{Z}_3$-vector space. We can also form Hamming codes in this setting. A Hamming code over $\mathbb{Z}_3$ will be a code in $\mathbb{Z}_3^n$ where $n = \frac{3^r-1}{2}$ for some positive integer r. We can form the error correcting matrix here, just like for the binary Hamming codes, by finding an $n \times r$ matrix where every pair of columns are linearly independent. For example, if $r = 2$, then $n = 4$ and our error correcting matrix is $\begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \end{pmatrix}$.

Exercise 2.3 Come up with a way to play the hat game with three colors (red, blue and yellow) with four people which will win 4 in 9 times. Then play the game a few times.

Exercise 2.4 Find an error correcting matrix for the Hamming ${}_3(13, 10)$ Code. With what probability will you win the three color hat game, using the Hamming ${}_3(13, 10)$ Code? Play the game a few times with this code.

Chapter 3

Torus games: Relations and Functions

For those of you who play video games, you may be familiar with asteroids. My brother used to play it when he was a child. The goal is to shoot down as many asteroids as you can without getting hit. The space ship moves around the screen. If you move to the right edge of the screen seeming to exit the screen you will suddenly reappear on the left edge of the screen. Similarly if you exit upwards, you reappear at the bottom. Asteroids is an example of a torus game. A torus is essentially the surface of a donut; however, we can realize the torus on a sheet of paper, by identifying the two side edges and the two top edges. We will talk more about this identification later today, but I want you all to first get used to playing a game on the torus.

Everyone knows how to play standard tic-tac-toe. One player is x's and the other o's. On each player's turn, the players place their mark in one of the squares on a 3 × 3 grid. A player wins if he or she has three of his or her marks on some line (a row, column, or diagonal). To play tic-tac-toe on the torus, again, a player wins as long as he or she has three of his or her marks on some line. However, now the lines continue to the through the identification of the top and bottom edges and through the identification of the side edges. For example, the following are winning games for the person playing with x's:

x	o	o
		x
	x	

	x	o
	o	x
x		

Exercise 3.1 1. What other configurations can you think of are also winning games?

2. If the first player plays optimally, will he or she always win?

We will discuss relations to solidify the mathematics that is going on behind this torus tic-tac-toe. And we can use this mathematics to learn a new variant of the game.

3.1 Relations

If A and B are sets, the cartesian product of A and B, denoted

$$A \times B = \{(a,b) \mid a \in A \text{ and } b \in B\}.$$

A *relation* from A to B is a subset R of $A \times B$. If a pair $(a,b) \in R$, sometimes we express this as aRb, indicating that a is related to b via this relation. $(a,b) \in R$ and aRb can be used interchangeably. If $A = B$, we often say that a relation from A to A is a *relation on* A. Some examples of relations are:

Example 3.1

1. Let $A = \{a,b,c\}$ and $B = \{1,2,3\}$ a relation from A to B is $R = \{(a,1),(a,3),(b,2)\}$.
2. Let $A = B = \mathbb{R}$. A relation $' <'$ on $\mathbb{R}$ is $' <' = \{(a,b) \mid a < b\}$. Here, one would probably prefer to express the relation on $\mathbb{R}$ just using $a < b$.
3. Let A be any set and $P(A)$, the power set of A. Define the relation from A to $P(A)$ by $S = \{(a,B) \mid a \in B\}$. Suppose for example that $A = \{1,2\}$, then we have $S = \{(1,\{1\}),(1,\{1,2\}),(2,\{2\}),(2,\{1,2\})\}$.

Exercise 3.2 Let $A = \{1,2\}$ and $B = \{a,b\}$. Give all possible relations from A to B.

Exercise 3.3 Think of three different relations on $\mathbb{R}$.

Some special sets related to a relation R from A to B are *the domain* of R, which is the set

$$\text{Dom}(R) := \{a \in A \mid (a,b) \in R\}$$

and the *range* of R, which is the set

$$\text{Ran}(R) := \{b \in B \mid (a,b) \in R\}.$$

For the relation $R = \{(a,1),(a,3),(b,2)\}$ from $A = \{a,b,c\}$ to $B = \{1,2,3\}$, the domain is $\{a,b\}$ and the range is $\{1,3,2\}$.

Exercise 3.4

1. Give a relation from $A = \{a,b,c\}$ to $B = \{1,2,3\}$ which has domain $\{a,c\}$ and range $\{2,3\}$.
2. Give a relation from $A = \{a,b,c\}$ to $B = \{1,2,3\}$ which has domain $\{a,b,c\}$ and range $\{1\}$.

Exercise 3.5 Find the domain and the range of the following relations:

1. Let $R = \{(x,y) \in \mathbb{R}^2 \mid x^2 + 4y^2 = 4\}$.
2. For a set $A = \{a,b,c,d\}$, the relation on the power set of A defined by

$$S = \{(B,C) \mid B \subseteq C \text{ and } B \text{ has at most 2 elements and } C \text{ has at least 2 elements}\}.$$

If R is a relation from A to B and S is a relation from B to C, we can define the *composition* $S \circ R$ to be the relation from A to C defined by

$$S \circ R := \{(a, c) \mid (a, b) \in R \text{ and } (b, c) \in S \text{ for some } b \in B\}.$$

Also the *inverse relation* of a relation R from A to B is the relation

$$R^{-1} = \{(b, a) \mid (a, b) \in R\}.$$

Example 3.2 Let $A = \{1, 2, 3\}$ and $B = \{a, b, c, d\}$. Suppose $R = \{(1, a), (1, b), (3, a), (3, d)\}$ is a relation from A to B and $S = \{(a, b), (a, d), (b, c)\}$ is a relation on B.

1. The relation $S \circ R = \{(1, b), (1, d), (1, c), (3, b), (3, d)\}$.

2. The relation $R^{-1} = \{(a, 1), (a, 3), (b, 1), (d, 3)\}$.

3. The relation $R^{-1} \circ S = \{(a, 1), (a, 3)\}$.

Exercise 3.6 Let $A = \{1, 2, 3, 4\}$ and $B = \{a, b\}$. Suppose $R = \{(1, a), (1, b), (2, a), (3, a)\}$ is a relation from A to B and $S = \{(a, 2), (b, 3)), (b, 4)\}$ is a relation from B to A. Find the following relations.

1. The relation $S \circ R$.

2. The relation S^{-1}.

3. The relation R^{-1}.

4. The relation $R^{-1} \circ S^{-1}$.

Exercise 3.7 Let R and S be relations from A to B. Prove the following:

1. $(R^{-1})^{-1} = R$.

2. If $R \subseteq S$, then $R^{-1} \subseteq S^{-1}$.

3. $(R \cap S)^{-1} = R^{-1} \cap S^{-1}$.

Now let us focus on relations on a set A. If R is a relation on A, there are 4 properties that R may satisfy.

- R is *reflexive* if $(a, a) \in R$ for all $a \in A$.
- R is *symmetric* if $(a, b) \in R$, then $(b, a) \in R$.
- R is *antisymmetric* if $(a, b) \in R$ and $(b, a) \in R$ then $a = b$.
- R is *transitive* if $(a, b) \in R$ and $(b, c) \in R$, then $(a, c) \in R$.

Example 3.3 1. The identity on A which is the relation defined by $i_A = \{(a, a) \mid a \in A\}$ is reflexive, symmetric, antisymmetric and transitive.

2. The relation $R = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x \leq y\}$ is reflexive, antisymmetric and transitive but not symmetric.

3. The relation $R = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid x + y \text{ is even}\}$ is reflexive, symmetric and transitive but not antisymmetric.

4. The relation $R = \{(1, 2), (2, 1)\}$ on $A = \{1, 2\}$ is symmetric but not reflexive, transitive nor antisymmetric.

5. The relation $R = \{(1, 2), (2, 3), (1, 3)\}$ on $A = \{1, 2, 3\}$ is transitive but not reflexive nor symmetric. R is trivially antisymmetric because for every$(a, b) \in R$ and $(b, a) \notin R$.

6. The relation $R = \{(1, 1), (1, 2), (2, 1), (2, 2), (2, 3), (3, 3)\}$ on $A = \{1, 2, 3\}$ is reflexive but not symmetric, antisymmetric, nor transitive.

A nice visual way to indicate a relation R on a finite set A is through a table. The set values listed to the left of the table are the ones taken to be the first element in the ordered pair in the relation and the set values above the table are the ones from the second element in the ordered pair. If there is an x in a cell, that means the ordered pair indicated by the row and column is included in the relation:

The relation $R = \{(a, b), (a, c), (b, b), (c, c)\}$ on $A = \{a, b, c\}$ can be expressed by the following table:.

R	a	b	c
a		x	x
b		x	
c			x

Exercise 3.8 Give examples of relations R on the set $A = \{a, b, c\}$ which satisfy the following properties:

1. R is reflexive only.

2. R is transitive only.

3. R is symmetric only.

4. R is only reflexive and symmetric.

5. R is only reflexive and transitive.

6. R is only symmetric and transitive.

Exercise 3.9 Let R be a relation on A

1. Show that R is reflexive if and only if $i_A \subseteq R$.

2. Show that R is symmetric if and only if $R = R^{-1}$.

3. Show that R is transitive if and only if $R \circ R \subseteq R$.

Exercise 3.10 Let R_1 and R_2 be relations on A

1. If R_1 and R_2 are reflexive determine if $R_1 \cap R_2$ or $R_1 \cup R_2$ are reflexive.
2. If R_1 and R_2 are symmetric determine if $R_1 \cap R_2$ or $R_1 \cup R_2$ are symmetric.
3. If R_1 and R_2 are antisymmetric determine if $R_1 \cap R_2$ or $R_1 \cup R_2$ are antisymmetric.
4. If R_1 and R_2 are transitive determine if $R_1 \cap R_2$ or $R_1 \cup R_2$ are transitive.

3.2 Equivalence Relations

An *equivalence relation* is a relation R on a set A which satisfies the reflexive, symmetric and transitive properties. For equivalence relations, we often use the symbol $\sim$ to indicate the relation R. For example, instead of writing $(a, b) \in R$, we write $a \sim b$. When we discussed relations on a set A with various properties above we noted that

$$R = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid a + b \text{ is even}\}$$

has the three properties that define an equivalence relation. Hence, R is an equivalence relation on $\mathbb{Z}$.

The torus that we have been using for our games can be described by the equivalence relation on $\mathbb{R} \times \mathbb{R}$ given by $(x, y) \sim (z, w)$ if and only if $z - x$ and $w - y$ are both integers or $\sim = \{((x, y), (z, w)) \mid z - x \in \mathbb{Z} \text{ and } w - y \in \mathbb{Z}\}$. Note: This is an equivalence relation since for every element (x, y) of $\mathbb{R} \times \mathbb{R}$ $x - x = 0 = y - y$ so $(x, y) \sim (x, y)$ implying $\sim$ is reflexive. Also if $(x, y) \sim (z, w)$, then $z - x = n$ for some integer n and $w - y = m$ for some integer m. Thus $x - z = -n \in \mathbb{Z}$. and $y - w = -m \in \mathbb{Z}$. Thus showing that $(z, w) \sim (x, y)$ which means $\sim$ is symmetric. Now, to see that $\sim$ is transitive, we consider $(x, y) \sim (z, w)$ and $(z, w) \sim (u, v)$. These imply that there exists integers n, m, ℓ, k, such that $z - x = n$, $w - y = m$, $u - z = \ell$ and $v - w = k$. Putting these together we get $u - z + z - x = \ell + n \in \mathbb{Z}$ and $v - w + w - y = k + m \in \mathbb{Z}$, showing that $\sim$ is transitive.

An equivalence relation that is handy to know for algebra and number theory is equivalence modulo n on the integers. We say that $a \equiv b \mod n$ if $a - b$ is a multiple of n or in other words, $a - b = nk$ for some integer k. Clearly, $a \equiv a \mod n$ since $a - a = 0 = n \cdot 0$. Also if $a \equiv b \mod n$, then $a - b = nk$ for some $k \in \mathbb{Z}$ so $b - a = n(-k)$ which implies $b \equiv a \mod n$ and $\equiv \mod n$ is symmetric. If $a \equiv b \mod n$ and $b \equiv c \mod n$, then there exists k and ℓ integers, with $a - b = nk$ and $b - c = n\ell$. Putting these together we see that $a - c = a - b + b - c = n(k + \ell)$ showing that $\equiv \mod n$ is transitive.

When an equivalence relation $\sim$ is defined on a set A, we can discuss the equivalence classes of A defined by $\sim$. The *equivalence class* of $a \in A$ is the set

$$[a] = \{y \in A \mid y \sim a\}.$$

A *partition* of a set A is a collection of subsets $A_1, A_2, \ldots, A_n$ of A, such that $A = A_1 \cup A_2 \cup \cdots \cup A_n$ and $A_i \cap A_j = \emptyset$ for all $i \neq j$.

Theorem 3.4 *The equivalence classes of A defined by an equivalence relation $\sim$ partition A. Also for any partition $P = \{A_i \mid i \in I\}$ of A, we can define an equivalence relation $\sim_P$ given by $a \sim_P b$ if and only if a and b are in the same subset A_i of the partition P for some $i \in I$.*

Proof: Suppose first that $\sim$ is an equivalence relation on a set A. Note that for every $a \in A$ we know that $a \sim a$ so $a \in [a]$. So $\bigcup\limits_{a \in A} [a] = A$. Suppose $a \neq b$, we need to show either $[a] = [b]$ or $[a]$ and $[b]$ are distinct equivalence classes. Suppose $[a] \cup [b] \neq \emptyset$. Then there is an $x \in [a] \cap [b]$. Since $x \in [a]$ and $x \in [b]$, then $x \sim a$ and $x \sim b$. Since $\sim$ is an equivalence relation, then $a \sim x$ and $b \sim x$. Putting together $b \sim x$ and $x \sim a$ we see that $b \in [a]$. Since for all $x \in [b]$, we know that $x \sim b$. Again using the transitive property, we see that for all $x \in [b]$, $x \sim a$. Thus $[b] \subseteq [a]$. Similarly, we can see that $[a] \subseteq [b]$. Hence, $[a] = [b]$.

Now suppose that $P = \bigcup\limits_{i \in I} P_i$ is a partition of A. Define an equivalence relation by $a \sim_P b$ if a and b are in the same subset of the partition P. Note that $\sim_P$ is reflexive since a can only be in one subset of the partition. $\sim_P$ is also symmetric because if a and b are in the same subset of the partition P, then $a \sim_P b$ and $b \sim_P b$. Now suppose $a \sim_P b$ and $b \sim_P c$. This implies that there is a P_i so that both $a, b \in P_i$ and a P_j so that $b, c \in P_j$. Since $b \in P_i$ and $b \in P_j$, then $b \in P_i \cap P_j$. Since P is a partition, this implies that $P_i = P_j$ and $a, b, c \in P_i$. Hence, $a \sim_P c$ and $\sim_P$ is transitive. $\square$

The set of all equivalence classes of A under the equivalence relation $\sim$ is denoted $A/\sim$. For example the torus is $T = \mathbb{R}^2/\sim$ and the congruence classes modulo n is $\mathbb{Z}_n = \mathbb{A}/\equiv$ which we usually denote using the remainders modulo n or $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$.

Exercise 3.11 Find all equivalence relations on $\{a, b, c, d\}$

Exercise 3.12 Suppose that n is a positive integer. Show that if $a \equiv b \bmod n$ and $c \equiv d \bmod n$, then $a + c \equiv b + d \bmod n$ and $ac \equiv bd \bmod n$. This implies that addition and multiplication are well defined on $\mathbb{Z}_n$.

Exercise 3.13 Let R_1 and R_2 be equivalence relations on A. Determine if $R_1 \cap R_2$ or $R_1 \cup R_2$ are equivalence relations

3.3 Partial Orders

A relation R on A is called a *partial order* on A if R is reflexive, antisymmetric and transitive. We will typically denote a partial order R on A by (A, R). We often write aRb for $(a, b) \in R$, when R is a partial order. Some partial orders you should be familiar with are $(\mathbb{R}, \leq)$ and $(P(A), \subseteq)$. Also $(\mathbb{N}, |)$ where $a \mid b$ means a divides b, is a partial order on the natural numbers.

Exercise 3.14 Let R_1 and R_2 be a relations on A. Are $R_1 \cap R_2$ or $R_1 \cup R_2$ partial orders?

Exercise 3.15 Show the only relation which is both an equivalence relation and a partial order is the identity relation.

We call a partially ordered set (A, R) a *total order* if for every $a, b \in A$ aRb or bRa. For example $(\mathbb{R}, \leq)$ is a total order but $(\mathbb{N}, |)$ is not a total order. Why?

Exercise 3.16 Suppose R is a total order on A and S is a total order on B. Define the following relations on $A \times B$: $T := \{((a,b),(a',b')) \in (A \times B)^2 \mid aRa' \text{ and } bSb'\}$ and $L := \{((a,b),(a',b')) \in (A \times B)^2 \mid aRa' \text{ and if} a = a' \text{ then } bSb'\}$. Decide if either T or L are total orders on $A \times B$.

When you have a partial order (A, R) and a subset B of A, we define $b \in B$ to be the *smallest element* or *minimum* of B if $(b, x) \in R$ for all $x \in B$. B does not necessarily have a smallest element. If this element exists, we denote it $\min B$.

Example 3.5 Suppose $A = \{a, b, c\}$ and our partial order is $(P(A), \subseteq)$. Let $B = \{\{a\}, \{b\}, \{c\}\}$. Since $\{a\}$, $\{b\}$ and $\{c\}$ are incomparable as sets, then B has no smallest element. Whereas the set $C = \{\{a\}.\{a,b\}, \{a,c\}, A\}$ has smallest element $\{a\}$.

In contrast, we say $b \in B$ is a *minimal element* if there exists no $x \in B$, with $(x, b) \in R$. In the previous example, B has minimal elements $\{a\}, \{b\}, \{c\}$. Note that if there is a smallest element b of B then b is a minimal element.

We define $b \in B$ to be the *largest element* or *maximum* of B if $(x, b) \in R$ for all $x \in B$. B does not necessarily have a largest element. If this element exists, we denote it $\max B$.

Example 3.6 Again using the set $A = \{a, b, c\}$ and partial order is $(P(A), \subseteq)$. Let $B = \{\{a\}, \{b\}, \{c\}\}$. Since $\{a\}$, $\{b\}$ and $\{c\}$ are incomparable as sets, then B has no largest element. Whereas the set $C = \{\{a\}.\{a,b\}, \{a,c\}, A\}$ has largest element A.

In contrast, we say $b \in B$ is a *maximal element* if there exists no $x \in B$, with $(b, x) \in R$. In the previous example, B has maximal elements $\{a\}, \{b\}, \{c\}$. Similarly if there is a largest element b of B then b is a maximal element.

Exercise 3.17

1. Let $(\mathbb{N}, |)$ be our partially ordered set. Set $B = \{2, 3, 5, 6, 10, 30\}$ and $C = \{1, 3, 7, 15, 21\}$.
   (a) Determine the minimal and maximal elements B.
   (b) Does B have a minimum or maximum?
   (c) Determine the minimal and maximal elements C.
   (d) Does C have a minimum or maximum?
2. Let $A = \{a, b, c\}$ and our partially ordered set is $(P(A), \subseteq)$. Set $B = \{\{a\}, \{a,b\}, \{a,c\}, \{b,c\}\}$ and $C = \{\emptyset, \{b\}, \{a,b\}, \{a,c\}, A\}$.
   (a) Determine the minimal and maximal elements B.
   (b) Does B have a minimum or maximum?
   (c) Determine the minimal and maximal elements C.
   (d) Does C have a minimum or maximum?
3. Let $(P(\mathbb{N}), \subseteq)$ be our partially ordered set. Let $B = \{A \subseteq \mathbb{N} \mid A \text{ has at least 4 elements}\}$ and $C = \{A \subseteq \mathbb{N} \mid A \text{ has at most 3 elements}\}$.

(a) Determine the minimal and maximal elements B.

(b) Does B have a minimum or maximum?

(c) Determine the minimal and maximal elements C.

(d) Does C have a minimum or maximum?

We say y is a *lower bound* for the subset B of A with respect to the partial order R if $(y,b) \in R$ for all $b \in B$. If B has a lower bound, we say that B is *bounded from below.* Suppose $L \subseteq A$ is the set of all lower bounds of B. We say that y is the *greatest lower bound* or *infimum* (or *inf* for short) of B if y is the largest element of L. We say y is an *upper bound* for the subset B of A with respect to the partial order R if $(b,y) \in R$ for all $b \in B$. If B has an upper bound, we say B is *bounded from above.* Suppose $U \subseteq A$ is the set of all upper bounds of B. We say that y is the *least upper bound* or *supremum* (or *sup* for short) of B if y is the smallest element of U. If a subset B bounded from above and below, we say B is *bounded.* Otherwise, we say that B is *unbounded.*

Example 3.7 Again using the set $A = \{a,b,c\}$ and partial order is $(P(A), \subseteq)$. Let $B = \{\{a\},\{b\},\{c\}\}$. The only lower bound of B is $\emptyset$. Hence, $\emptyset$ is the greatest lower bound of A. Also the only upper bound of B is A itself, since no other subset contains all the subsets $\{a\},\{b\}$ and $\{c\}$. So A is the least upper bound of B. Whereas the set $C = \{\{a\}.\{a,b\},\{a,c\},A\}$ has lower bounds $\emptyset$ and $\{a\}$ and $\{a\}$ is the greatest lower bound of C. The least upper bound (and only upper bound) of C is again A.

Exercise 3.18 For the partially ordered sets in Exercise 3.17, determine the least upper bounds and greatest lower bounds if they exist.

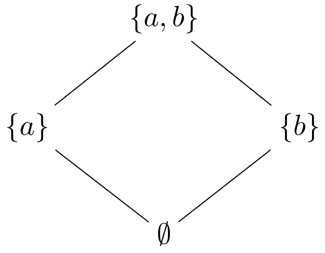
A *Hasse diagram* is a visualization of a finite partially ordered set (A,R) such that

- There is a vertex for every element of A.

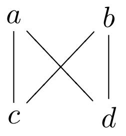
- If $(a,b) \in R$, then the vertex for b is positioned higher than the vertex of a.

- If $(a,b) \in R$, $a \neq b$ and there is no $c \in A$ so that $(a,c) \in R$ and $(c,b) \in R$, then there is a line drawn from a to b.

For example, here is the Hasse diagram for the partially ordered set $(P(\{a,b\},\subseteq)$:



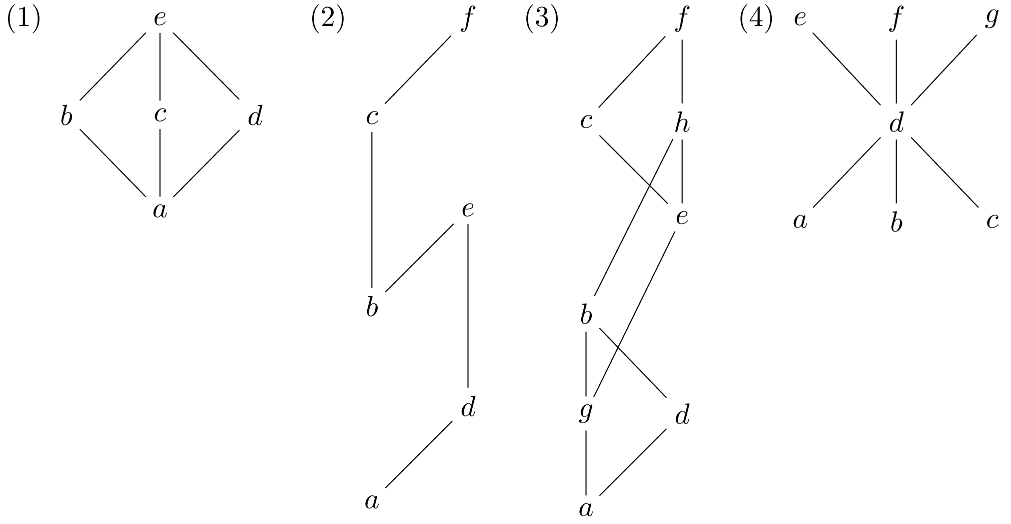
We can now use Hasse diagrams to describe partially ordered sets. Suppose $A = \{a,b,c,d\}$. Consider the Hasse diagram for A:



This describes the partial ordering: $R = \{(a,a), (b,b), (c,a), (c,b), (c,c), (d,a), (d,b), (d,d)\}$.

For $B = \{a, b, c\}$, we see that $cRx = c$ for any $x \in B$. Thus c is the smallest element of B. However, a and b are both maximal elements which are not largest elements.

Exercise 3.19 For the following Hasse diagrams, determine the minimal elements, maximal elements, minimum, and maximum (the last two only if they exist).



A partially ordered set (A, R) is called a *lattice* if for every a and b in A the subset $\{a, b\}$ has both a least upper bound and a greatest lower bound. We denote the least upper bound of a and b, $a \vee b$ and the least upper bound of a and b is denoted as $a \wedge b$. The real numbers under the partial order $\leq$ is a lattice since $a \vee b = \max\{a, b\}$ and $a \wedge b = \min\{a, b\}$. The natural numbers under division is also a lattice. However, in this case $a \vee b$ is the least common multiple of a and b and $a \wedge b$ is the greatest common divisor of a and b. A lattice (A, R) is called a *complete lattice* if every subset B of A has both a greatest lower bound and a least upper bound. Neither of the above examples are complete lattices. $(\mathbb{R}, \leq)$ is not complete since any unbounded subset of $\mathbb{R}$ has either no least upper bound or no greatest lower bound. $(\mathbb{N}, |)$ is not complete since any infinite subset of $\mathbb{N}$ has no least upper bound. However, any subset of $\mathbb{N}$ will have a greatest lower bound. The lattice given by $(P(\{a, b\}, \subseteq)$ is a complete lattice.

Exercise 3.20 For the diagrams in Exercise 3.19, determine if any are lattices.

Exercise 3.21 Show any bounded lattice is complete.

3.4 Functions

A *function* from A to B is a relation f from A to B satisfying the property that for every $x \in A$, there exists exactly one $y \in B$ so that $(x, y) \in f$, we usually express this as $f(x) = y$.

Example 3.8 1. $R = \{(1,2), (2,1), (2,3)\}$ is a relation from $A = \{1,2\}$ to $B = \{1,2,3\}$ which is not a function.

2. $f = \{(x, \frac{x}{2}) \mid x \in \mathbb{Z}\}$ is a function from $\mathbb{Z}$ to $\mathbb{Q}$. However it is not a function from $\mathbb{Z}$ to $\mathbb{Z}$ since for x odd, $\frac{x}{2}$ is not an integer. We usually write this function $f : \mathbb{Z} \to \mathbb{Q}$ given by the formula $f(x) = \frac{x}{2}$.

If f is a function from A to B, we often write $f : A \to B$ to express that f is a function. The *domain* of f is A and the *codomain* of f is B. The *range* of f is the set $\{y \in B \mid y = f(x) \text{ for some } x \in A\}$. Note that the range is a subset of the codomain B and need not be all of B. For example $f : \mathbb{Z} \to \mathbb{Z}$ given by $f(n) = 2n$ has codomain $\mathbb{Z}$ but the range of f is the set of even integers.

Some special functions to be aware of are:

- $i : A \to A$ given by $i(x) = x$ is call the identity function.
- If $A \subseteq B$, the map $i_A : A \to B$ defined by $i_A(x) = x$ is called the inclusion map from A to B.
- If $C \subseteq A$, the restriction of $f : A \to B$ to C is $f\mid_C : C \to B$ defined by $f\mid_C(x) = f(x)$ for all $x \in C$.

If $C \subseteq A$, the *image of* C *under* f, denoted $f(C) = \{y \in B \mid f(x) = y \text{ for some } x \in C\}$. If $D \subseteq B$, the *preimage of* D *under* f, denoted $f^{-1}(D) = \{x \in A \mid f(x) \in D\}$.

Exercise 3.22 Suppose $f : \mathbb{R}^2 \to \mathbb{R}$ is the function defined by $f(x, y) = x^2 + y^2$.

1. What is the image of $C = \{(x, y) \mid -1 \le x \le 2, 0 \le y \le 3\}$?
2. What is the preimage of $D = \{x \mid -2 \le x \le 4\}$?

A function f from A to B is *injective* or *one to one* if for every $x \neq y$ in A $f(x) \neq f(y)$ or equivalently if $f(x) = f(y)$ then $x = y$. A function f from A to B is *surjective* or *onto* if the range of f is B. A function f from A to B is *bijective* if f is both one-to-one and onto.

Example 3.9 1. $f : \mathbb{Z} \to \mathbb{Z}$ defined by $f(n) = 2n$ is one to one but not onto.

2. $g : \mathbb{Z} \to \mathbb{Z}$ defined by $g(n) = \begin{cases} n \text{ if } n \text{ is odd} \\ \frac{n}{2} \text{ if } n \text{ is even} \end{cases}$ is onto but not one to one.

3. $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = 2x$ is bijective.

Exercise 3.23 Suppose $f : A \to B$ and $g : B \to C$ are functions.

1. If f and g are both injective, show $g \circ f$ is injective.
2. If f and g are both surjective, show $g \circ f$ is surjective.
3. If $g \circ f$ is bijective, show f is injective and g is surjective.
4. Give an example of functions g and f so that f is injective only and g is surjective only and $g \circ f$ is bijective.

Chapter 4

The Game of Set – Binary operations and new algebraic structures

The game SET is a card game using a special deck of cards. Each card has four characteristics: symbol, color, number and filling. Each of these characteristics can take on one of the three possible values:

1. **Symbol:** Each card contains either ovals, squiggles or diamonds.
2. **Color:** The color of the symbols are either red, green or purple.
3. **Number:** There are either 1,2 or 3 symbols on each card.
4. **Filling:** The symbols on each card are either filled in (solid), unfilled or striped.

A collection of three cards is a ”Set” if for each of the four characteristics, all three cards share the same value or they are all different values.

Since there are 4 properties and each property can take on three different values we can represent each card as an element in $\mathbb{Z}_3^4$. The first copy of $\mathbb{Z}_3$ will represent the symbol, the second the color, the third the number and the fourth the filling:

Symbol	Label	Color	Label	Number	Label	Shading	Label
oval	1	red	1	1	1	solid	1
squiggle	2	green	2	2	2	empty	2
diamond	0	purple	0	3	0	striped	0

An alternate version of the game is SUPERSET. A *superset* is a set of four cards such that there is a unique card not among these four so that precisely two sets would be formed with this card.

4.1 Binary Operations

A binary operation on a set S is a function $* : S \times S \to S$. In other words, for every $a, b \in S$, $*(a, b)$ written $a * b$ is a unique element of S. For example, addition, subtraction and multiplication on either the integers or the real numbers are binary operations. Division on the set of integers is not a binary operations since $1 \div 2$ is not an integer. Division is also not a binary operation on the set of real numbers since division by zero is not defined.

Exercise 4.1 (a) Give some examples of binary operations on $\mathbb{Z}$ and $\mathbb{R}$ other than addition, subtraction and multiplication.

(b) Give an example of a set which has division as a binary operation.

(c) Give some other examples of binary operations on sets other than $\mathbb{Z}$ and $\mathbb{R}$.

If $A \subseteq S$, we say $*$ is *closed* on A if for all $a, b \in A$, $a * b \in A$. In particular, $*|_A$ is also a binary operation on A.

Exercise 4.2 (a) Can you think of any subsets of $\mathbb{Z}$ for which addition is closed?

(b) Can you think of any subsets of $\mathbb{Z}$ for which multiplication is closed?

(c) Can you think of any subsets of $\mathbb{Z}$ for which subtraction is closed?

(d) Answer the same questions for $\mathbb{R}$.

A binary operation $*$ on S is *commutative* if $a * b = b * a$ for every $a, b \in S$. A binary operation $*$ on S is associative if $a * (b * c) = (a * b) * c$ for all $a, b, c \in S$.

Exercise 4.3 For all the binary operations you came up with, which ones are commutative and which ones are associative?

If S is a finite set, you can represent any binary operation on S via a table. For example if $S = \{a, b\}$, there are 16 binary operations

*	a	b
a	a	a
b	a	a

○	a	b
a	a	a
b	a	b

•	a	b
a	a	a
b	b	a

◇	a	b
a	a	b
b	a	a

△	a	b
a	b	a
b	a	a

▽	a	b
a	a	a
b	b	b

◁	a	b
a	a	b
b	a	b

▷	a	b
a	b	a
b	a	b

♣	a	b
a	a	b
b	b	a

♡	a	b
a	b	a
b	b	a

♠	a	b
a	b	b
b	a	a

✠	a	b
a	a	b
b	b	b

©	a	b
a	b	a
b	b	b

♭	a	b
a	b	b
b	a	b

♮	a	b
a	b	b
b	b	a

♯	a	b
a	b	b
b	b	b

Exercise 4.4 Which of these binary operations are commutative? Which ones are associative?

A binary operation $*$ on S has an *identity* if there exists an element $e \in S$ so that $e * x = x * e = x$ for all $x \in S$. If $*$ has an identity e on S, then we say $x \in S$ has a $*$-*inverse* if there exists a $s \in S$ such that $s * x = x * s = e$.

Exercise 4.5 (a) Which of the above binary operations have identities?

(b) For those binary operations with identities, which elements have inverses?

Let us define a binary operation on $\mathbb{Z}_3^4$ which represents our Set deck. Let x denote (x_1, x_2, x_3, x_4) and y denote (y_1, y_2, y_3, y_4). We will define $x * y = (2(x_1 + y_1), 2(x_2 + y_2), 2(x_3 + y_3), 2(x_4 + y_4))$.

Exercise 4.6 Suppose that $x = (1,1,1,1)$, $y = (0,0,2,2)$, $z = (1,2,0,1)$, $w = (0,2,2,1)$. Compute $x * y$, $x * z$, $x * w$, $y * z$, $y * w$ and $z * w$. Is there anything special about these products?

Exercise 4.7 (a) Is $*$ commutative?

(b) Is $*$ associative?

(c) Does $*$ have an identity?

(d) Do inverses exist in $\mathbb{Z}_3^4$?

Exercise 4.8 Show that $x * (x * y) = y$ and $(x * y) * y = x$.

Exercise 4.9 Show that if $x * y = x * z$ then $y = z$. This is called left cancelation.

Exercise 4.10 Prove that if $x, y, z \in \mathbb{Z}_3^4$ then $(z * x) * (z * y) = z * (x * y)$.

Exercise 4.11 Show that the map $T_w : \mathbb{Z}_3^4 \to \mathbb{Z}_3^4$ defined by $T_w(x) = w{*}x$ is a permutation, i.e. T_w is a one to one and onto map.

Exercise 4.12 Suppose that $U \subseteq \mathbb{Z}_3^4$. We say U is *product-free* if $xy \notin U$ whenever $x, y \in U$. If U is product-free, show that $xU = \{x * s \mid s \in U\}$ is also product-free.

Exercise 4.13 Prove that if U is product-free and $x \in U$, then $xU \cap U = \{x\}$.

Note that if the cards only had one property (i.e. only symbol, only color, only number or only shading) then a product-free set would consist of two cards, for example {oval, diamond}. We can indicate this by one line of a tic-tac-toe grid x | | x If the cards had only two properties, for example symbol and color, then a product-free set would consist of 4 cards. An example of this would be {red oval, red diamond, purple oval, purple diamond}. We can indicate this on a tic-tac-toe grid

x		x
x		x

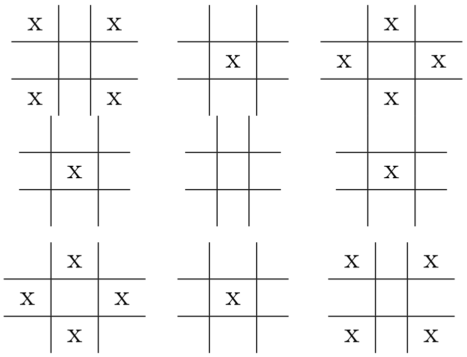
If the cards had only three properties, for example symbol, color and number, then a product-free set would consist of 9 cards. An example of this would be {one red oval, one red diamond, one purple oval, one purple diamond, two green squiggles, three red squiggles, three green ovals, three green diamonds, three purple squiggles }. We can indicate this on three tic-tac-toe grids.

x		x
x		x

	x	

	x	
x		x
	x	

If the cards have all four properties, then a product-free set would consist of 20 cards. An example of this would be {one red solid oval, one red solid diamond, one purple solid oval, one purple solid diamond, two green solid squiggles, three red solid squiggles, three green solid ovals, three green solid diamonds, three purple solid squiggles, one green empty squiggle, three green empty squiggles, one red striped squiggle, one green striped oval, one green striped diamond, one purple striped squiggle, two green striped squiggles, three re striped ovals three purple striped diamonds, three red striped diamonds, three purple striped diamonds }. We can indicate this on four tic-tac-toe grids.



It is very difficult to prove that maximal collection of cards which doesn't contain a set must be 20. If there were 5 properties in the game set instead of 4, then the maximal product free set would have 45 cards. If there are 6 or more properties, the maximal product free set is not known.

4.2 Algebraic structures

An *algebraic structure* is a set together with one or more binary operations. If $*_1, \dots, *_n$ are binary operations on S, we indicate the algebraic structure by $(S, *_, \dots, *_n)$. First let us discuss some algebraic structures with one binary operation. A set S with a single binary operation $*$, $(S, *)$ is called a *magma*. A magma $(S, *)$ with an identity is called a *unital magma*. A *semigroup*, $(S, *)$, is a magma which is associative. A *monoid* is a semigroup with an identity. A *group* is a monoid $(S, *)$ in which all elements have inverses.

Example 4.1 *1.* $(\mathbb{N}, +)$ *is a semigroup.*

2. $(\mathbb{N}_0, +)$ *is a monoid.*

3. $(\mathbb{Z}, +)$ *is a group.*

4. $(\mathbb{Z}, \times)$ *is a monoid.*

5. $(\mathbb{R}, \times)$ *is a monoid.*

6. $(\mathbb{R} \setminus \{0\}, \times)$ *is a group.*

7. $(\mathbb{Z}_n, +)$ *is a group.*

8. $(\mathbb{Z}_n \setminus \{0\}, \times)$ *is a monoid.*

9. *For any set S, $(P(S), \cup)$ is a monoid with $\emptyset$ the identity. Similarly, $(P(S), \cap)$ is a monoid with S the identity.*

All of the examples above are commutative. A commutative group is called an *abelian group* after the mathematician Abel.

Suppose $S = \{a, b, c\}$ and the binary operation $*$ is given by the following table:

*	a	b	c
a	a	b	c
b	b	b	b
c	c	c	c

Exercise 4.14 Show that $*$ is associative. Thus $(S, *)$ is a semigroup. Is $(S, *)$ a monoid? Is $(S, *)$ a group? How could you alter the binary operation $*$, so that $(S, *)$ is a semigroup but not a monoid?

Exercise 4.15 Show that every magma with one element is a commutative group.

Exercise 4.16 Determine if every commutative magma with two elements is a semigroup.

Exercise 4.17 Show that every group $(S, *)$ with identity e which satisfies the property $x*x = e$ for all $x \in S$ is an abelian group. If $(S, *)$ is a monoid satisfying the same property, must $(S, *)$ be commutative?

An algebraic structure $(S, *, \circ)$ with two binary operations $*$ and $\circ$ which satisfy the distributive properties:

$$a \circ (b * c) = (a \circ b) * (a \circ c) \qquad (a * b) \circ c = (a \circ c) * (b \circ c)$$

is called a *ringoid.* A *semiring* is a ringoid for which both $(S, *)$ and $(S, \circ)$ are semigroups. A *ring* is a semiring for which $(S, *)$ is an abelian group. Usually the operations in a ring are called addition $(+)$ and multiplication $(\cdot)$ and we denote a ring $(S, +, \cdot)$. The additive identity is called zero (0). Depending on who you talk to, some mathematicians add the additional property that a ring $(S, +, \cdot)$ has a multiplicative identity or in other words $(S, \cdot)$ is a monoid. If you want to be assured your ring has a multiplicative identity, you may always call such a ring a *ring with unity.* If the multiplication on a ring is commutative, we call the ring a *commutative ring.* If $(S, +, \cdot)$ is a commutative ring with unity so that $(S \setminus \{0\})$ is also an abelian group, we call $(S, +, \cdot)$ a *field.* We say an element x in a ring $(S, +, \cdot)$ is a *zero divisor* if there exists $0 \neq y \in S$ with $x \cdot y = 0$. A commutative ring with no zero divisors is called an *integral domain.*

Example 4.2 1. $(\mathbb{N}, +\cdot)$ *is a semiring.*

2. $(\mathbb{N}_0, +, \cdot)$ *is a semiring with unity.*

3. $(\mathbb{Z}, +\times)$ *is a domain.*

4. $(2\mathbb{Z}, +\times)$ *is a commutative ring without unity.*

5. $(\mathbb{R}, +, \times)$ *is a field.*

6. $(\mathbb{R}^2, +, \times)$ *where addition and multiplication are defined component-wise is a ring which is neither a domain nor field.*

7. $(\mathbb{Z}_n, +, \cdot)$ *is a commutative ring and if* n *is prime it is a field.*

8. *For any set* S*,* $(P(S), \cup, \cap)$ *is a semiring.*

Exercise 4.18 An element a in a ring $(S, +, \cdot)$ is *idempotent* if $a^2 = a$. Show that the subset of all idempotent elements is a submonoid of $(S, \cdot)$.

Exercise 4.19 A ring $(R, +, \cdot)$ is *a Boolean ring* if x is idempotent for all $x \in R$. Show that $(R, +, \cdot)$ is a commutative ring.

Exercise 4.20 Show that a field $(F, +, \cdot)$ has exactly two idempotent elements.

Exercise 4.21 An element a in a ring $(S, +, \cdot)$ is *nilpotent* if $a^n = 0$ for some $n \in \mathbb{N}$. Show that if a and b are nilpotent, so is $a + b$.

4.3 Subgroups, Ideals and Homomorphisms

For every magma $(S, *)$, if there is a subset H for which $(H, *)$ is also a magma then we call H a submagma. Note that as long as $*$ is closed on H, then $*$ will be a function from $H \times H$ to H, so we need only check closure of $*$ to see that H is a submagma. For all of the magmas we discussed earlier, there is a corresponding submagma. A *subsemigroup* of a semigroup $(S, *)$ is a subset H, so that $(H, *)$ is also a semigroup.

Example 4.3 $\{2, 3, 4, \ldots n \ldots\}$ *is a subsemigroup of* $\mathbb{N}$.
$\{3, 5, 6, 8, 9, 10, \ldots, \}$ *is a subsemigroup of* $\mathbb{N}$.

A submonoid of a monoid $(S, *)$ is a subset H where $(H, *)$ is a monoid. If H is a subset of a monoid $(S, *)$ on which $*$ is closed, to assure that $(H, *)$ is a submonoid, we need to check that H also contains an identity. A subgroup of a group $(G, *)$ is a subset H where $(H, *)$ is a group. If H is a subset of a group $(S, *)$ on which $*$ is closed, to assure that $(H, *)$ is a subgroup, we need to check that H also contains an identity and inverses are present for all the members of H. However a quick way to check this in one step is that $a * b^{-1} \in H$ for all $a, b \in H$. Since a group $(G, *)$ is also a monoid and a semigroup, we can find submonoids and subsemigroups of G. Consider $(\mathbb{R}, +)$. $(\mathbb{N}, +)$ is a subsemigroup of $(\mathbb{R}, +)$ and $(\{0, 2, 4, 5, 6, \rightarrow\}, +)$ is a submonoid of $(\mathbb{R}, +)$.

For every ringoid $(S, *, \circ)$, if there is a subset H for which $(H, *, \circ)$ is also a ringoid then we call H a subringoid. Note that as long as $*$ and $\circ$ are closed on H, then $*$ and $\circ$ will be a functions from $H \times H$ to H, so we need only check closure of $*$ and $\circ$ to see that H is a subringoid. For all of the ringoids we discussed earlier, there is a corresponding subringoid. A *subsemiring* of a semiring $(S, *, \circ)$ is a subset H, so that $(H, *, \circ)$ is also a semiring. A *subring* of a ring $(S, +, \cdot)$ is a subset H, so that $(H, +, \cdot)$ is also a ring. If H is a subset of a ring $(S, +, \cdot)$ on which addition and multiplication are closed, to assure that $(H, +, \cdot)$ is a subring, we need to check that $(H, +)$ forms a group structure which we can do by checking closure of subtraction for all $a, b \in H$. We can similarly define subdomains and subfields. Any ring can have subringoids, subsemirings and subrings.

Exercise 4.22 1. Take any field and give some examples of subfields, subdomains, subsemirings inside of it.

2. Show that any subring of a field must be a subdomains.

Let H be a subset of a magma $(S, *)$, such that $s * h \in H$ and $h * s \in H$ for all $s \in S$, then we say that H is an *ideal* of S.

Exercise 4.23 Show that if $(G, *)$ is a group then the only ideal of $(G, *)$ is itself.

However, when $(S, *)$ is a semigroup, we have proper ideals. For example, in the semigroup $\{3, 5, 6, 8, 9, 10, \ldots,\}$, $\{6, 8, 9, 10, \ldots,\}$ is an ideal.

In a ring $(S, +, \cdot)$ we define an ideal to be a subset H so that $(H, +)$ is an abelian group and $(H, \cdot)$ is an ideal in $(S, \cdot)$.

A function $f : (S, *) \to (T, \circ)$ between two magmas is a homomorphism if $f(a * b) = f(a) \circ f(b)$ for all $a, b \in S$. We use homomorphisms to compare common properties of various magmas. A function $f : (S, *, \circ) \to (T, \star, \bullet)$ between two ringoids is a homomorphism if $f(a * b) = f(a) \star f(b)$ and $f(a \circ b) = f(a) \bullet f(b)$ for all $a, b \in S$.

Exercise 4.24 Let G and G' be semigroups and H is a subsemigroup in G and I is an ideal in G. Suppose $f : G \to G'$ is a semigroup homomorphism.

1. Show that $f(H)$ is a subsemigroup of G'.

2. Is $f(I)$ an ideal in G'?

Exercise 4.25 Let G and G' be semigroups and H is a subsemigroup in G' and I is an ideal in G'. Suppose $f : G \to G'$ is a semigroup homomorphism.

1. Show that $f^{-1}(H)$ is a subsemigroup of G.

2. Is $f^{-1}(I)$ an ideal in G?

Chapter 5

Postage Stamp Problem – A focus on Numerical Semigroups

5.1 Postage Stamp Problem

As you know the post office only has certain denominations of stamps. They keep changing so I don't know what they are at present. I just buy the forever stamps. However, imagine twenty years ago when they didn't have forever stamps and you wanted to post a package for \$2.25. Suppose you had 29 cent stamps and 23 cent stamps, can you post the package with exact postage with these denominations? For what value of n, will you be able to make exact postage for every package of value n or greater? This is called the postage stamp problem for obvious reasons. Of course, this problem has many variants. The key to the problem is numerical semigroups.

Exercise 5.1 The martian monetary system uses colored beads instead of coins. A blue bead is worth 3 martian credits and a red bead is worth 5 martian credits.

1. Find a value n so that you can pay for everything with exact credits for every value greater than or equal to n.

2. Prove that this is the case.

3. Are there any values of n that would be impossible to pay with the blue and red beads? If so, what are they?

4. Suppose the beads were worth 3 credits and 6 credits instead of 5, what values could you pay for in this case? Which values are impossible?

Exercise 5.2 Generalize the postage stamp problem for integers n and m. In particular, for what values of m and n can you find an integer k, so that you can pay exact postage for all integer values greater than or equal to k cents? Can you express this integer k in a nice way in terms of m and n?

Exercise 5.3 In an ancient society grey stones were worth 3 credits, black stones were worth 5 credits and white stones were worth 7 credits.

1. Find a value n so that you can pay for everything with exact credits for every value greater than or equal to n.
2. Prove that this is the case.
3. Are there any values of n that would be impossible to pay with the blue and red beads? If so, what are they?
4. Suppose the beads were worth 3 credits and 6 credits instead of 5, what values could you pay for in this case? Which values are impossible?

Exercise 5.4 Is there a formula $f(x, y, z)$ that works for all relatively prime triples, n_1, n_2, n_3, such that $k = f(n_1, n_2, n_3)$?

5.2 Invariants on Numerical Semigroups

A numerical semigroup is a submonoid of $\mathbb{N}_0$ such that the complement $\mathbb{N}_0 \setminus H$ is a finite set. Every numerical semigroup S admits a finite system of generators, $a_1, a_2, \ldots, a_n \in S$ such that $S =< a_1, a_2, \ldots, a_n >= \{\lambda_1 a_1 + \cdots + \lambda_n a_n \mid \lambda_1, \ldots \lambda_n \in \mathbb{N}_0\}$. We say that S is minimally generated by $a_1, \ldots, a_n$ if no smaller subset $b_1, \ldots, b_m$ generate S, i.e. $S \neq < b_1, \ldots b_m >$, $m < n$. We usually list the generators in increasing order: $a_1 < a_2 < \cdots < a_n$. We call a_1 the *multiplicity* of S and denote it $m(S) = a_1$. The embedding dimension of S is $n := e(S)$. In general $e(S) \leq m(S)$. If $e(S) = m(S)$, we say that S has *maximal embedding dimension*. The set $G(S) := \mathbb{N}_0 \setminus S$ is called the *set of gaps* of S and the cardinality of $G(S)$ is called the *genus* of S, denoted $g(S)$. The largest integer of $G(S)$ is called the *Frobenius* of S denoted $F(S)$. Notice that every $n \geq F(S) + 1$ is a member of S. We call $F(S) + 1$ the conductor of S and denote it $c(S)$. If we are writing the numerical semigroup as a set, we often use an arrow after $c(S)$ to indicate that all positive integers past $c(S)$ are elements of S.

Example 5.1 1. $S =< 2, 3 >= \{0, 2, \rightarrow\}$. The numerics for this semigroup are $m(S) = e(S) = 2$, $G(S) = \{1\}$, $g(S) = 1 = F(S)$ and $c(S) = 2$.

2. $S =< 3, 5, 7 >= \{0, 3, 5, \rightarrow\}$. The numerics for this semigroup are $m(S) = e(S) = 3$, $G(S) = \{1, 2, 4\}$, $g(S) = 3$, $F(S) = 4$ and $c(S) = 5$.

3. $S =< 4, 7, 10 >= \{0, 4, 7, 8, 10, 11, 12, 14, \rightarrow\}$. The numerics for this semigroup are $m(S) = 4$, $e(S) = 3$, $G(S) = \{1, 2, 3, 5, 6, 9, 13\}$, $g(S) = 7$, $F(S) = 13$ and $c(S) = 14$.

Exercise 5.5 Determine the multiplicity, embedding dimension, the gaps, the genus, the Frobenius and the conductor of the following numerical semigroups:

1. $< 3, 7, 8 >$.
2. $< 4, 5, 11 >$.
3. $< 5, 8, 12 >$.

Exercise 5.6 Compare $< 5, 7, 9 >$ with $< 5, 7, 9, 11 >$.

We say a numerical semigroup S is *symmetric* if for every $z \in \mathbb{Z}$, either $z \in S$ or $F(S) - z \in S$.

Exercise 5.7 Show that if S is symmetric $2g(S) = F(S) + 1$. (Think of an appropriate bijection.)

We say a numerical semigroup S is *pseudo-symmetric* if for every $z \in \mathbb{Z}$ and $z \neq \frac{F(S)}{2}$, then either $z \in S$ or $F(S) - z \in S$.

Exercise 5.8 Show that if S is psuedo-symmetric $2g(S) = F(S) + 2$. (Think of an appropriate bijection.)

We say an integer x is a *pseudo-Frobenius number* of S if $x \notin S$ and $x + h \in S$ for all nonzero $h \in S$. We will denote the pseudo-Frobenius numbers of S by $PF(S)$. The cardinality of $PF(S)$ is called the type of S, denoted $t(S)$.

Exercise 5.9 Find the pseudo-Frobenius numbers and types of the following numerical semigroups:

1. $< 3, 5, 7 >$
2. $< 4, 7, 10, 13 >$
3. $< 3, 7, 8 >$
4. $< 5, 9, 11 >$

The *Apery set* of n in S is the set $\mathrm{Ap}(S, n) = \{h \in S \mid h - n \notin S\}$.

Exercise 5.10 Find the Apery sets of the following semigroups with respect to $m(S)$ for each semigroup S:

1. $< 3, 5, 7 >$
2. $< 4, 7, 10, 13 >$
3. $< 3, 7, 8 >$
4. $< 5, 9, 11 >$

Exercise 5.11 Define $\leq_S$ be the relation on S defined by $a \leq_S b$ if $b - a \in S$.

1. Show that $\leq_S$ is a partial ordering on S.
2. Use $\leq_S$ to show that $PF(S) = \{\omega - n \mid \omega \text{ is maximal with respect to } \leq_S \text{ in } \mathrm{Ap}(S, n)\}$.

For any numerical semigroup S we say that a subset I of $\mathbb{Z}$ is a *relative ideal of S* if $I + S \subseteq I$ and $h + I = \{h + i \mid i \in I\} \subseteq S$ for some $h \in S$. An *ideal* of S is a relative ideal of S which is a subset of S.

Exercise 5.12 Show that if I and J are relative ideals of S that $I - J = \{z \in \mathbb{Z} \mid z + J \subseteq I\}$ is a relative ideal of S.

We call the ideal $M = S \setminus \{0\}$, the *maximal ideal* of S.

Exercise 5.13 Show that $M - M = S \cup PF(S)$.

Exercise 5.14 Show that $M - M$ is a numerical semigroup.

Exercise 5.15 Determine $M - M$ for each of the following semigroups:

1. $< 3, 5, 7 >$

2. $< 4, 7, 10, 13 >$

3. $< 3, 7, 8 >$

4. $< 5, 9, 11 >$

The relative ideal $S - I$ is called the *dual* of I. An ideal I is called a *bidual* if $S - (S - I) = I$. The dual of S is $S - M$.

Exercise 5.16 Show that $S - M = M - M$ is a numerical semigroup.

The set $K_S := \{F(S) - z \mid z \notin S\}$ is called the *canonical ideal* of S.

Exercise 5.17 Show that K_S is a relative ideal of S and $S \subseteq K_S$.

Exercise 5.18 Determine K_S for each of the following semigroups:

1. $< 3, 5, 7 >$

2. $< 4, 7, 10, 13 >$

3. $< 3, 7, 8 >$

4. $< 5, 9, 11 >$

Exercise 5.19 Define $N(S) = \{h \in S \mid h < F(S)\}$.

1. Show that if $h \in N(S)$, then $F(S) - h \notin S$.

2. Show that if $h \in PF(S) \setminus \{F(S)\}$, then $F(S) - h \notin S$.

3. Define a map from $\theta : N(S) \cup (PF(S) \setminus \{F(S)\}) \to G(S)$ defined by $\theta(h) = F(S) - h$. Use this map to show the inequality $2g(S) \geq F(S) + t(S)$.

A numerical semigroup S is *almost symmetric* if $2g(S) = F(S) + t(S)$.

Exercise 5.20 Show that if S is symmetric or pseudo-symmetric then S is almost symmetric.

Exercise 5.21 Suppose that S is almost symmetric. Show that $K_S \subseteq M - M$.

Let $0 < h_0 < h_1 < \cdots h_n = c(S)$ be the smallest elements of S and let $n = n(S)$ be the number of elements of S smaller than $F(S)$. For each $i \geq 0$, define the ideal $S_i = \{h \in S \mid h \geq h_i\}$ and the relative ideal $S(i) = S - S_i$.

Exercise 5.22 Show that $S(i) = S_i - S_i$ and $S(i)$ is a semigroup. Then determine what $S(0)$, $S(1)$ and $S(n)$ are.

Define the cardinality of $S(i) \setminus S(i-1)$ by $t_i(S)$. The sequence $(t_1(S), t_2(S), \ldots, t_n(S)$ is called the *type sequence* of S.

Exercise 5.23 1. What is the type sequence of a symmetric semigroup?

2. What is the type sequence of a pseudo-symmetric semigroup?

Exercise 5.24 Let S be a numerical semigroup. Show that S is an almost symmetric with maximal embedding dimension if and only if $M - M$ is symmetric.

5.3 Semigroup Rings

Let k be a field such as $\mathbb{Z}_2$ or $\mathbb{R}$. The ring of formal power series is

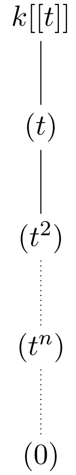
$$k[[t]] = \{\sum_{n=0}^{\infty} a_n t^n \mid a_n \in k\}.$$

Note that all polynomials with coefficients in k are contained in $k[[t]]$.

Theorem 5.2 *The nonzero ideals of $k[[t]]$ can all be expressed in the form (t^n) for some $n \geq 0$.*

Proof: Let I be a nonzero ideal of $k[[t]]$. First we will show that I must be generated by exactly one element. Let $f = \sum_{n=0}^{\infty} a_n t^n$ be an element of I such that n is the smallest nonnegative integer such that $a_n \neq 0$ and $a_i = 0$ for all $i \leq n$ and among all $g \in I$ the first nonzero term of g has exponent greater than or equal to n. We claim that $I = (t^n)$. Note that $f = t^n(\sum_{i=0}^{\infty} a_{n+i}t^i)$. Thus $f \in (t^n)$. For any $g \in I$, $g = \sum_{i=0}^{\infty} c_{i+n}t^{n+i}$ by the way we chose f. Thus $g \in (t^n)$ also. Thus $I \subseteq (t^n)$. Now I claim that $t^m \in (f)$ for all $m > n$. Since $f = t^n(\sum_{i=0}^{\infty} a_{n+i}t^i)$. Note that $g = \sum_{i=0}^{\infty} a_{n+i}t^i$ is a unit. Suppose $(\sum_{i=0}^{\infty} b_i t^i)(\sum_{i=0}^{\infty} a_{n+i}t^i) = 1$. Then we can recursively find b_i in terms of the a_{n+i}. First $b_0 = a_n^{-1}$. Then $a_{n+1}b_0 + a_n b_1 = 0$ implies that $b_1 = -a_{n+1}a_n^{-2}$. Knowing b_j in terms of a_{n+i} for $0 \leq i \leq j < k$ and using $a_n b_k + a_{n+1}b_{k-1} + \cdots + a_{n+k}b_0 = 0$, we see we can solve b_k in terms of a_{n+i} for $0 \leq i \leq k$. Thus $\sum_{i=0}^{\infty} a_{n+i}t^i$ has an inverse. So $t^m = t^{m-n}g^{-1}f$ implies that $t^m \in (f)$ and in particular $(t^n) \subseteq (f)$. Thus $(t^n) = (f)$. □

This implies that the ideals of $k[[t]]$ are a totally ordered lattice. The Hasse diagram looks like:



A semigroup ring is the subring of $k[[t]]$ generated by the powers in a numerical semigroup$S$, denoted $k[[t^S]]$. For example if $S =< 2,3 >$, the semigroup ring generated by S is $k[[t^2,t^3]]$ which contains all power series that have 0 as the coefficient of t. For example, $1+t^2+t^3+t^4+\cdots$. The semigroup ring generated by $< 3,5,7 >$ contains all power series that have no t, t^2 nor t^4 in their expansion.

Although the ideals of $k[[t^S]]$ form a lattice, the lattice is much more complicated than the partially ordered set given by the semigroup itself. Since the coefficients of k complicate things slightly.

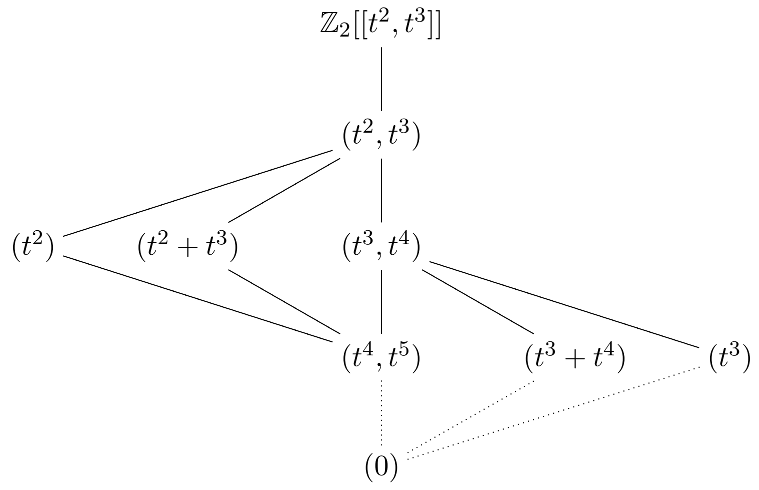
Theorem 5.3 *The nonzero ideals of $k[[t^2,t^3]]$ are of the form (t^n,t^{n+1}) or (t^n+at^{n+1}) for $n \geq 2$ and for some $a \in k$.*

Proof: Suppose $0 \neq f \in R$. Thus, after multiplying by a nonzero element of k, $f = t^n + a_1t^{n+1} + a_2t^{n+2} + \cdots$ for $n \geq 2$. We will show that $t^m \in (f)$ for $m \geq n+2$. Hence, $t^n + a_1t^{n+1} \in (f)$. Similarly, $t^m \in (t^n + a_1t^{n+1})$ for $m \geq n+2$. Hence, $f \in (t^n + a_1t^{n+1})$.

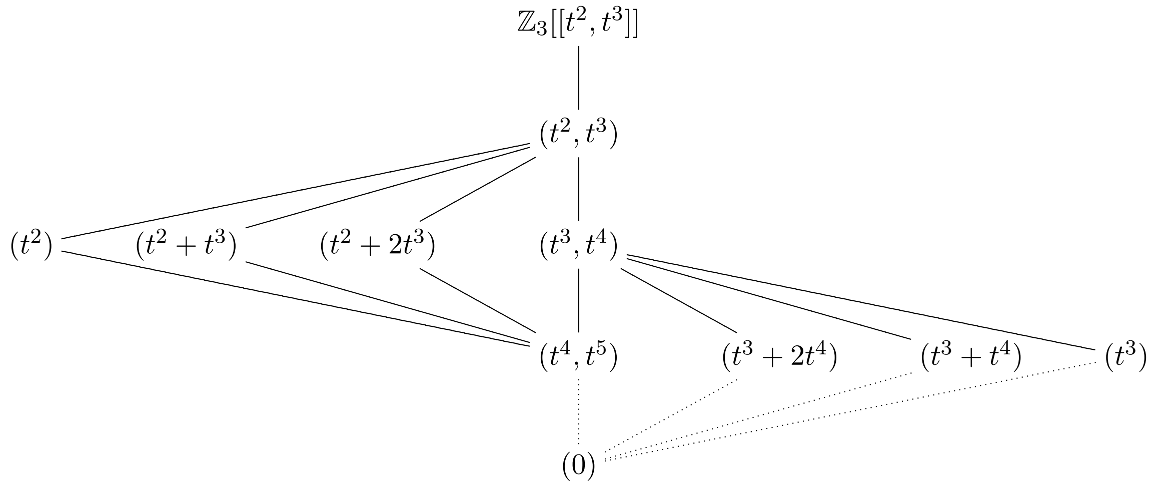
Let $g \in k[[t]]$. Note that $t^{m-n}g \in k[[t^2,t^3]]$. Hence, if g is a unit in $k[[t]]$, then $t^{m-n}g^{-1} \in k[[t^2,t^3]]$ also. In $k[[t]]$, $f = t^n(1 + a_1t + a_2t^2 + \cdots) = t^ng$. Note that $t^{m-n}g^{-1}f = t^m$. Similarly $t^m \in (t^n + a_1t^{n+1})$. Since $f - (t^n + a_1t^{n+1}) = a_2t^{n+2} + a_3t^{n+3} + \cdots \in (f) \bigcap (t^n + a_1t^{n+1})$, we see that $(t^n + a_1t^{n+1}) = (f)$. Hence, all principal ideals of $k[[t^2,t^3]]$ have the form $(t^n + at^{n+1})$.

Suppose, I is not principal. As $t^m \in (t^n + at^{n+1})$ for $m \geq n+2$, then I can be generated by at most 2 elements of the form $(t^n + at^{n+1}, t^m + bt^{m+1})$ where $m = n$ or $m = n+1$. If $m = n$, then $t^{n+1} \in I$ which also implies that $t^n \in I$. Hence $I = (t^n, t^{n+1})$. If $m = n+1$, then $t^{n+2} \in (t^n + at^{n+1}) \subseteq I$ as in the principal case above. However, $t^{n+1} = t^{n+1} + bt^{n+2} - bt^{n+2} \in I$ and once again $t^n \in I$. Hence, $I = (t^n, t^{n+1})$. □

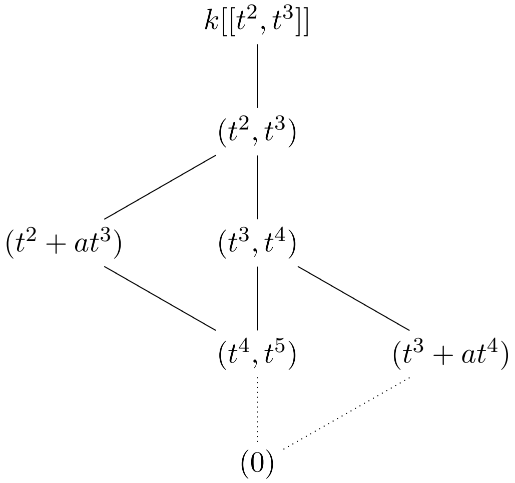
For example, suppose $k = \mathbb{Z}_2$, then the Hasse diagram for the lattice for $\mathbb{Z}_2[[t^2,t^3]]$ looks like



The Hasse diagram for the lattice for $\mathbb{Z}_3[[t^2, t^3]]$ looks like



We will represent the lattice for $k[[t^2, t^3]]$ by



where the nodes with $(t^n + at^{n+1})$ have the cardinality of k incomparable vertices there.

Exercise 5.25 State and prove a Theorem similar to Theorem 5.3 for the ideals of $k[[t^2,t^5]]$. Then come up with a Hasse Diagram that represents the relationships between the ideals in $k[[t^2,t^5]]$.

Exercise 5.26 State and prove a Theorem similar to Theorem 5.3 for the ideals of $k[[t^3,t^4,t^5]]$. Then come up with a Hasse Diagram that represents the relationships between the ideals in $k[[t^3,t^4,t^5]]$.

Here is a translation of the terminology we discussed for numerical semigroups S in the language of semigroup rings $k[[t^S]]$. The multiplicity of $k[[t^S]]$ is precisely $m(S)$. Similarly the embedding dimension of $k[[t^S]]$ is $e(S)$. The Frobenius of $k[[t^S]]$ is $F(S)$; however, the conductor or $k[[t^S]]$ is $(t^{c(S)}, t^{c(S)+1}, \ldots, t^{c(s)+m(S)-1})$. We say a semigroup ring $k[[t^S]]$ is Gorenstein if its defining semigroup is symmetric. We say a semigroup ring $k[[t^S]]$ is almost Gorenstein if its defining semigroup is pseudo-symmetric. Let $k((t)) = \{\sum\limits_{n\in\mathbb{Z}} a_n t^n \mid$ for some $m \in \mathbb{Z}a_i = 0$ for all $i < m\}$. A *fractional ideal* of $k[[t^S]]$ is a subset J of $k((t))$ such that $Jk[[t^S]] \subseteq J$. Define $(I :_{k((t))} J) = \{f \in k((t)) \mid fJ \subseteq I\}$.

Exercise 5.27 Show that if I and J are fractional ideals in $k[[t^S]]$ then $(I :_{k((t))} J)$ is a fractional ideal of $k[[t^S]]$.

The dual of I is $(S :_{k((t))} I)$. The canonical ideal of $k[[t^S]]$ is the fractional ideal generated by $t^{F(S)-z}$ for all $z \notin S$.

Chapter 6

Closure Operations

6.1 The basics

Let $(A, \leq)$ be a partially ordered set. A closure operation on A is a function $c : A \to A$, such that

1. $a \leq c(a)$ (expansive),
2. If $a \leq b$, then $c(a) \leq c(b)$ (order preserving), and
3. $c(c(a)) = c(a)$ (idempotent).

We say a is c-closed if $c(a) = a$.

The identity function is a closure operation. If $(A \leq)$ is a complete lattice with sup $A = M$, then the function $f(a) = M$ for all $a \in A$ is a closure operation.

Exercise 6.1 1. Give some examples of closures on $(\mathbb{N}, \leq)$.

2. Give some examples of closures on $(\mathbb{R}, \leq)$.

3. Give some examples of closures on $(\{a, b, c\}, R)$ where R is given by the table

R	a	b	c
a	x	x	
b		x	
c		x	x

Although we see that closure operations operations can be defined on partially ordered set, the most interesting closure operations are defined on the partially ordered set of ideals in magmas or ringoids. Since we spent a day talking about numerical semigroups, we will focus on closure operations defined on the ideals (or relative ideals) of a numerical semigroup. The set of ideals $I(S)$ of a numerical semigroup S is a partially ordered set under containment. In fact, $I(S)$ is a lattice. Also, if we take any element $s \in S$, $s + I = \{s + i \mid i \in I\}$ is also an ideal of S so is in $I(S)$. Since any intersection of ideals is an ideal, we can prove the following:

Theorem 6.1 *Let S be a numerical semigroup and $c : I(S) \to I(S)$ be a closure operation on the ideals of S. Let I be an ideal and $\{I_\alpha\}_{\alpha\in\mathcal{A}}$ a set of ideals.*

1. *If every I_α is c-closed, then $\bigcap\limits_{\alpha\in\mathcal{A}} I_\alpha$ is c-closed.*
2. *$\bigcap\limits_{\alpha\in\mathcal{A}} c(I_\alpha)$ is c-closed.*
3. *$c(I)$ is the intersection of all c-closed ideals that contain I.*
4. *$c(\sum\limits_{\alpha\in\mathcal{A}} c(I_\alpha)) = c(\sum\limits_{\alpha\in\mathcal{A}} I_\alpha)$.*

Proof: (1) For $\beta \in \mathcal{A}$, we have $\bigcap\limits_{\alpha\in\mathcal{A}} I_\alpha \subseteq I_\beta$. Since c is order preserving $c(\bigcap\limits_{\alpha\in\mathcal{A}} I_\alpha) \subseteq c(I_\beta) = I_\beta$. Since this holds for any $\beta \in \mathcal{A}$, then $c(\bigcap\limits_{\alpha\in\mathcal{A}} I_\alpha) \subseteq \bigcap\limits_{\beta\in\mathcal{A}} I_\beta = \bigcap\limits_{\alpha\in\mathcal{A}} I_\alpha$.

(2) This follows directly from part (1).

(3)Let J be an ideal so that $I \subseteq J = c(J)$. By order preservation, $c(I) \subseteq c(J) = J$. Thus if $\mathcal{A}$ is the set of all c-closed ideals containing I, then $c(I) \subseteq \bigcap\limits_{J\in\mathcal{A}} J$. But $c(c(I)) = c(I)$ implies that $c(I) \in \mathcal{A}$. Hence, we conclude that $\bigcap\limits_{J\in\mathcal{A}} J \subseteq c(I)$. Putting these containments together we conclude that $c(I) = \bigcap\limits_{J\in\mathcal{A}} J$.

(4) By the extension property $I_\alpha \subseteq c(I_\alpha)$ implies $\sum\limits_{\alpha\in\mathcal{A}} I_\alpha \subseteq \sum\limits_{\alpha\in\mathcal{A}} c(I_\alpha)$. Now by order preservation, $c(\sum\limits_{\alpha\in\mathcal{A}} I_\alpha) \subseteq c(\sum\limits_{\alpha\in\mathcal{A}} c(I_\alpha))$. Also $I_\beta \subseteq \sum\limits_{\alpha\in\mathcal{A}} I_\alpha \subseteq c(\sum\limits_{\alpha\in\mathcal{A}} I_\alpha)$ implies $c(I_\beta) \subseteq c(c(\sum\limits_{\alpha\in\mathcal{A}} I_\alpha)) = c(\sum\limits_{\alpha\in\mathcal{A}} I_\alpha)$. Taking the sum over all $\beta \in \mathcal{A}$, we see that $\sum\limits_{\beta\in\mathcal{A}} c(I_\beta) \subseteq c(\sum\limits_{\alpha\in\mathcal{A}} I_\alpha)$. □

Some constructions of closure operations for numerical semigroup rings are as follows:

Construction 6.1 Let J be a relative ideal of S. For an ideal $I \subseteq S$, $I + J$ is the relative ideal $\{i + j \mid i \in I and j \in J\}$. Define $c(I) = (I + J) - J$. This gives a closure operation since clearly, $I \subseteq (I + J) - J$. Also if $I_1 \subseteq I_2$, then $(I_1 + J) \subseteq (I_2 + J)$ and $c(I_1) = (I_1 + J) - J \subseteq (I_2 + J) - J = c(I_2)$. Suppose $s \in c(c(I))$. Then $s + J \subseteq c(I) + J$. For any $t \in c(I)$, $t + J \subseteq I + J$ which implies that $s + J = t + J \subseteq I + J$ or $s \in (I + J) - J = c(I)$.

Construction 6.2 Let S and T be numerical semigroups and $\phi : S \to T$ be a numerical semigroup homomorphism. Also let $d : I(T) \to I(T)$ be a closure operation defined on T. For ideals I of S, define a closure c on $I(S)$ by $c(I) = \phi^{-1}(d(\phi(I)))$.

Exercise 6.2 Show that Construction 6.2 is a closure operation.

Construction 6.3 Let $\{c_\lambda\}_{\lambda\in\Lambda}$ be a collection of closure operations on $I(S)$. Define $c : I(S) \to I(S)$ by $c(I) = \bigcap\limits_{\lambda\in\Lambda} c_\lambda(I)$

Exercise 6.3 Show that Construction 6.3 is a closure operation.

Construction 6.4 Let d be an idempotent, extensive operation on $I(S)$. Let $\mathcal{S}$ be the set of all closure operations on $I(S)$ satisfying the property $c \in \mathcal{S}$ if and only if $d(I) \subseteq c(I)$ for all ideals in $I(S)$. Define $d^\infty : I(S) \to I(S)$ to be $d^\infty(I) = \bigcap\limits_{c \in \mathcal{S}} c(I)$.

Exercise 6.4 Show that Construction 6.4 is a closure operation.

6.2 Special types of closure operations on the set of ideals of numerical semigroups

These more specialized closure operations, will require not only a partially ordered set $(S, \leq)$ but S must also be at least a magma with binary operation under some binary operation $*$. We will call a partially ordered set which is also a magma an *ordered magma.* We will say that a closure operation $c : S \to S$ is a *nucleus* or is *semiprime* (depending on who you talk to) if $c(a) * c(b) \leq c(a * b)$ for all $a, b \in S$.

Exercise 6.5 For any ordered magma $(S, *)$ the following are equivalent:

(a) c is a nucleus.

(b) $c(c(a) * c(b)) = c(a * b)$ for all $a, b \in S$.

(c) $a * c(b) \leq c(a * b)$ for all $a, b \in S$.

Suppose now that S is a numerical semigroup. Then we say that a closure operation c defined on $I(S)$ is a nucleus if $c(I) + c(J) \subseteq c(I + J)$ for all $I, J \in I(S)$. For an element $s \in S$ and an ideal $I \subseteq S$, $s + I$ is also an ideal.

Exercise 6.6 Suppose that $c : I(S) \to I(S)$ is a closure operation on the ideals of S. Show that c is a nucleus if and only if $s + c(I) \subseteq c(s + I)$ for all $I \in I(S)$ and all $s \in S$.

For I and J ideals in a numerical semigroup S, we define $I -_S J = \{s \in S \mid s + J \subseteq I\}$

Exercise 6.7 Suppose c is a nucleus on $I(S)$ for a numerical semigroup S. If I and J are ideals in S, show that

1. $c(I -_S J) \subseteq c(I) -_S J$. Note this implies if I is c-closed then $I -_S J$ is c-closed.
2. $c(I) -_S J$ is c-closed.

Exercise 6.8

1. Show that any closure defined as in Construction 6.1 is a nucleus.
2. Show that any closure defined as in Construction 6.2 is a nucleus.
3. Show that any closure defined as in Construction 6.3 is a nucleus.
4. Show that as long as $I + d(J) \subseteq d(I + J)$ for all ideals I and J of $I(S)$, any closure defined as in Construction 6.1 is a nucleus.

We call a closure operation $c : I(S) \to I(S)$ on the set of ideals of a numerical semigroup a *star* operation if $s+c(I) = c(s+I)$ for all $I \in I(S)$ and all $s \in S$. Note that a star operation on $I(S)$ is a nucleus on $I(S)$ by the previous exercise. We will say a closure operation satisfies the difference property if for any $s \in S$ and any $I \in I(S)$, $c(s+I)_S - s = c(I)$.

Example 6.2 Let $S = \mathbb{N}_0$ and $c : I(\mathbb{N}_0) \to I(\mathbb{N}_0)$ be the closure operation defined by

$$c(< n >) = \begin{cases} < n > & \text{if } n < 5 \\ < 5 > & \text{if } n \geq 5. \end{cases}$$

Note that c is a nucleus since

$$c(< i >) + c(< j >) = \begin{cases} < i+j > & \text{if } i, j < 5 \\ < i+5 > & \text{if } i < 5 \text{ and } j \geq 5 \\ < j+5 > & \text{if } j < 5 \text{ and } i \geq 5 \\ < 10 > & \text{if } i, j \geq 5 \end{cases}$$

and

$$c(< i+j >) = \begin{cases} < i+j > & \text{if } i+j < 5 \\ < 5 > & \text{if } i+j \geq 5 \end{cases}$$

it is clear to see that $c(< i >) + c(< j >) \subseteq c(< i+j >)$. However, c doesn't satisfy the difference property as $c(3+ < 6 >)_{\mathbb{N}_0} - 3 =< 5 > -_{\mathbb{N}_0} 3 =< 2 > \neq c(< 6 >) =< 5 >$.

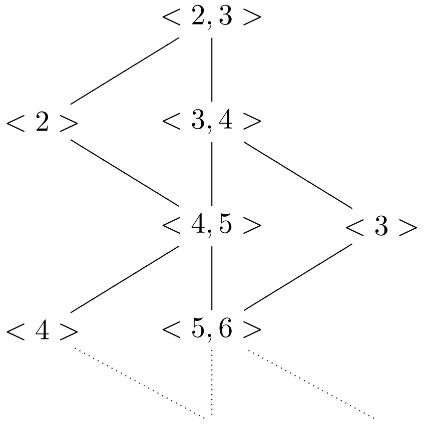
Exercise 6.9 Show that for any $r \in \mathbb{N}_0$, $c_r : I(\mathbb{N}_0) \to I(\mathbb{N}_0)$ defined by

$$c_r(< n >) = \begin{cases} < n > & \text{if } n < r \\ < r > & \text{if } n \geq r. \end{cases}$$

is a nucleus.

Exercise 6.10 Show that any nucleus on $I(\mathbb{N}_0)$ is either c_r or the identity.

The partially ordered set of the ideals in $S =< 2, 3 >$ is given by the (infinite) Hasse diagram:



Exercise 6.11 Describe two non-identity closure operations on $I(< 2, 3 >)$. Verify that each one is a closure operation.

Exercise 6.12 Come up with two distinct non-identity nuclei on $I(< 2, 3 >)$.

Theorem 6.3 *A closure operation c is a star operation on $I(S)$ if and only if satisfies the difference property and c also satisfies $c(< s >) =< s >$ for all $s \in S$,*

Proof: ($\Rightarrow$) Suppose c is a star operation. Then $c(< s >) = c(< s > +S) = s+c(S) =< s >$ and $c(s + I) - s = s + c(I)_S - s = c(I)$.

($\Leftarrow$) Now suppose that c satisfies the difference property and $c(< s >) =< s >$ for all $s \in S$. Now $s + c(I) = s + c(s + I)_S - s = c(s + I)$.

Exercise 6.13 Show that the only star operation on $I(\mathbb{N}_0)$ is the identity.

Exercise 6.14 Are there any non-identity star operations on $I(< 2, 3 >)$? Justify your answer.

Exercise 6.15 Draw an infinite Hasse diagram for the ideals of $< 3, 4, 5 >$.

Exercise 6.16 Are there any non-identity star operations on $I(< 3, 4, 5 >)$? Justify your answer.

Since closure operations are functions and the set of functions under composition forms a monoid (with identity the identity function), we would like to determine if the set of special types of closure operations also have an algebraic structure. For example consider the numerical semigroup $\mathbb{N}_0$.

Exercise 6.17 Find two examples of closure operations on $I(\mathbb{N}_0)$ so that when you compose the two, the composition is not a closure operation.

Exercise 6.18 Determine if the set of semiprime operations on $I(\mathbb{N}_0)$ is a monoid.

Exercise 6.19 Determine if the set of semiprime operations on $I(< 2, 3 >)$ is a monoid.

Suppose now that R is a commutative ring. Then we say that a closure operation c defined on $I(R)$, the ideals of R, is a nucleus if $c(I)c(J) \subseteq c(IJ)$ for all $I, J \in I(R)$. For an element $r \in R$ and an ideal $I \subseteq R$, rI is also an ideal. We say that a closure operation c is a star operation if $c(rI) = rc(I)$.

Exercise 6.20 Generalize all of the ideas presented above for semigroup rings.

Bibliography

[BF] Barucci, V., Froberg, R., *One dimensional almost Gorenstein rings*, J. of Alg.,**188**, (1997), 418-442.

[CCH] Calloway, L., Casher, J., Hoehn, S., *From Guessing Games to Compact Discs: Some Applications of Coding Theory*, SUMSRI, (2002).

[DM] Davis, B., Maclagan, D., *The card game SET*, Math. Intel., **25**, (2003), 33-40.

[El] Elliott, J., *Prequantales and Applications to semistar operations and module systems*, arXiv:1101.2462v1, January 12, 2011.

[Ep] Epstein, N., A guide to closure operations in commutative algebra, *Progress in Commutative Algebra 2: Closures, Finiteness and Factorization*, Edited by Christopher Francisco, Lee Klingler, Sean Sather-Wagstaff, Janet C. Vassilev, DeGruyter, Berlin, 2011.

[Fi] Fiedler, J., *Hamming Codes*, preprint, 2004.

[Fr] Fraleigh, J., *A first course in Abstract Algebra*, Seventh Edition, Addison Wesley, Boston, 2003.

[GP] Goodaire, E., Parmenter, M., *Discrete Mathematics with Graph Theory*, Third Edition, Pearson Prentice Hall, Upper Saddle River, New Jersey, 2006.

[Ho] Holdener, J., *Product Free Sets in the Card Game Set*, Primus, **15**, (2005), 289-297.

[Jo] Johnsonbaugh, R., *Discrete Mathematics*, Seventh Edition, Pearson Prentice Hall, Upper Saddle River, New Jersey, 2009.

[Na] Nari, H., *Symmetries on almost symmetric numerical semigroups*, arXiv:1111.6211v1, November 27, 2011.

[Ro] Robinson, S., *Why Mathematicians care about their hat color*, New York Times, April 10, 2001.

[Va] Vassilev, J., *Structure on the set of closure operations of a commutative ring*, J. of Alg., **321**, 2009, 2737-2353.

[Ve] Velleman, D., *How to Prove it*, Second Edition, Cambridge University Press, New York, New York, 2006.