MATH 240 Fall 2024

notes by

Marcel Goh

A note on these notes. After each class, this document will be updated with the new material that was just covered. The datestamps in the left margin indicate when the notes from each day start. Subsections labelled with a $*$ are optional. This document is based on notes by Jeremy Macdonald, but any errors are likely my own. Please email me if you find any.

1. Set theory

1. A *set* is a collection of distinct objects, called its *elements* or its *members*. If x is a member of set A, then we write $x \in A$, and if x is not an element of A, then we write $x \notin A$. Sets can be written by listing out its elements. For example,

$$\{1, 4, 7, 10, \sqrt{782}\}$$

and

$$\big\{\{1, 2\}, \pi, \{4\}\big\}$$

are both sets (the second example shows that sets can themselves contain other sets). The order of the elements is not important, and duplicate elements are ignored (so $\{1, 2\} = \{2, 1\} = \{1, 1, 2\}$). The notation using { and } is useful for defining small, concrete examples, but expressing large sets can become very cumbersome. The first way one can describe larger sets is to use the ... symbol and the power of suggestion. For instance, anyone faced with the notation

$$A = \{1, 3, 5, 7, 9, \ldots\}$$

can quickly guess that this set is supposed to contain all the positive odd integers. We can also use ... to define finite sets. Most Canadians will be able to tell you that the set

$$\{\text{Alberta}, \text{British Columbia}, \ldots, \text{Yukon}\}$$

of provinces and territories contains 13 elements. But this notation inherently produces some ambiguity. For example, since the sequence of positive palindromic binary numbers starts $1, 3, 5, 7, 9, 15, 17, 21, 27, \ldots$, we are left with some doubt as to whether the set A above should be the set of odd numbers or the set of palindromic binary numbers.

But there is another, less ambiguous way to define large sets. It is called set-builder notation and it refers to any construction of the form

$$\big\{x \in U : P(x)\big\},$$

where x is a variable, U is a set, and P is a statement about x. The resulting set contains *all x such that $P(x)$ holds*. For example, letting $\mathbf{N}$ denote the set $\{0, 1, 2, 3, \ldots\}$ of counting numbers (more on this later), to define the set of all odd numbers, we can write

$$A = \{x \in \mathbf{N} : \text{there exists } k \in \mathbf{N} \text{ such that } x = 2k + 1\}.$$

Note that the statement $P(x)$ must contain x, but it may also contain other previously defined symbols, as well as new symbols defined within the statement (such as k in the example above).

Special sets of numbers. There are certain infinite sets of numbers that are used so often as to be given special bold notation. Back in elementary school, you learned to use the counting numbers $0, 1, 2, 3, \ldots$. We already saw this set in the previous paragraph; in the business, this set is known as the *natural numbers*, because if you go on a nature hike you can use them to count the number of bluebells, donkeys, etc. that you see. (Many mathematicians use the symbol $\mathbf{N}$ to denote this set without zero. When in doubt, clarify with the person you're talking to; in this class, $0 \in \mathbf{N}$.)

Sometime towards the start of junior high you were introduced to the concept of natural numbers. The set

$$\mathbf{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$$

is called the set of *integers* or *whole numbers*. (The word *integer* just means "whole" in Latin; cf. French *entier*. We use the letter $\mathbf{Z}$ because of the German word *Zahl* meaning "number.")

Even before you learned about negative numbers, you probably learned about fractions. They can be defined in set-builder notation as a collection of ratios of integers, where the denominator is not zero:

$$\mathbf{Q} = \{p/q : p, q \in \mathbf{Z}, q \neq 0\}.$$

(The nitpicky reader will notice that p/q is not stipulated to be a member of any set here. This is because a rigorous definition of $\mathbf{Q}$ involves quotienting out by an equivalence relation, which we don't know how to do yet.) This is the set of *rational numbers*. Remember that sets only contain distinct elements, so $2/3$, $4/6$, $6/9$, etc. are all considered the same rational number.

Lastly, we have the set $\mathbf{R}$ of real numbers. Constructing this set using only notions from set theory and logic is quite the byzantine task and well outside the scope of this course, but you can think of $\mathbf{R}$ as the set of decimal numbers with

a finite number of digits to the left of the decimal point, and a possibly infinite number of digits to the right of the decimal point.

A set of numbers near and dear to many mathematicians' hearts is the set of *prime* numbers P, defined by

$$P = \big\{p \in \mathbf{N} : p \geq 2, \text{ and if } p = ab \text{ then } \{a, b\} = \{1, p\}\big\}.$$

(You may have met a different definition of prime numbers in the past. Pause a moment and convince yourself that the statement above defines the set of prime numbers as you know it.)

Set inclusion. When we use set builder notation $B = \big\{x \in A : P(x)\big\}$, every element of B is necessarily a member of the set A as well, since B is defined to be the set of all x in A satisfying $P(x)$. This is one way in which we can obtain a *subset* of another set. More generally, we write $B \subseteq A$ if every element of B is also an element of A, and $B \supseteq A$ if every element of A is an element of B. Sometimes, if $B \supseteq A$, we say that B *contains* A, or B *includes* A. For example, we have the chain

$$\mathbf{N} \subseteq \mathbf{Z} \subseteq \mathbf{Q} \subseteq \mathbf{R}$$

for the special sets of numbers defined earlier.

Symbols like $\subseteq$, $\supseteq$, and $=$ (that are used to produce statements) can be negated with a slash; for example, if there is some element of B that is not an element of A, then we write $B \not\subseteq A$.

The concept of set inclusion is important, because the most common way to prove that two sets A and B are equal is to show that A is a subset of B, then show that B is a subset of A. We illustrate this with the following example.

Proposition 1. *The sets*

$$A = \{x \in \mathbf{Z} : \textit{there exists } k \in \mathbf{Z} \textit{ such that } x = 2k + 1\}$$

and

$$A = \{x \in \mathbf{Z} : \textit{there exists } l \in \mathbf{Z} \textit{ such that } x = 2l + 5\}$$

are equal. (Both are different ways of expressing the set of all odd integers.)

Proof. Let $x \in A$. Then there exists $k \in \mathbf{Z}$ such that $x = 2k + 1$. Letting $l = k - 2$, we find that l is an integer (since k was). Furthermore,

$$x = 2k + 1 = 2k - 4 + 5 = 2(k - 2) + 5 = 2l + 5.$$

We have found l such that $x = 2l + 5$, so $x \in B$. This shows that $A \subseteq B$.

On the other hand, let $x \in B$, so that there exists $l \in \mathbf{Z}$ such that $x = 2l+5$. Now we let $k = l + 2$; $k \in \mathbf{Z}$ since $l \in \mathbf{Z}$. We have

$$x = 2l + 5 = 2l + 4 + 1 = 2(l + 2) + 1 = 2k + 1.$$

This shows that $x \in A$, and we have proved that $B \subseteq A$. This combined with the previous paragraph shows that $A = B$. ∎

The above result is not so important, but pay attention to the structure of this proof. It is called a "proof by double inclusion," since we have shown that A includes B and B includes A.

Set operations. Now we describe a number of operations that may be performed on sets to produce other sets. They can all be built up from the following two operations.

- The *union* $A \cup B$ of two sets A and B is the set of all elements that are either in A or in B (or both).
- The *intersection* $A \cap B$ of A and B is the set of all elements that are in both A and B.

As an example, if $A = \{1, 2, 4\}$ and $B = \{1, 3, 5\}$, then $A \cup B = \{1, 2, 3, 4, 5\}$ and $A \cap B = \{1\}$.

To avoid logical difficulties, we always assume that the sets we're working with are a subset of some larger ambient set U, often called the *universe*. Once we know what U is, we may define the *complement* of a set A to be the set $\overline{A}$ of all the elements in U except those that are in A. So if $U = \{1, 2, 3, 4, 5\}$ in the example above, then $\overline{A} = \{3, 5\}$ and $\overline{B} = \{2, 4\}$. What about $\overline{A \cup B}$? Well since $A \cup B$ is all of U, its complement must be empty, and we can denote it $\{\}$. This is one valid notation for the *empty set*. The other is $\emptyset$.

Now is a good time to define the cardinality $|A|$ of a set A. This is the number of elements in it, so $|A| = |B| = 3$ in our example, and $|A \cup B| = 5$, etc. We have $|\emptyset| = 0$, and it is possible for the cardinality of a set to be infinity; for example, $|\mathbf{N}| = \infty$. We also have $|\mathbf{R}| = \infty$, but this infinity is, in some sense, larger than $|\mathbf{N}|$. (More on that later.)

Next, we define the *difference* $B \setminus A$ of two sets. This is the set of all elements in B that are *not* in A. So, using the complement notation we just learned about, we can express $B \setminus A = B \cap \overline{A}$. It is not necessary that A be a subset of B. In the small example above, we have $A \setminus B = \{2, 4\}$ and $B \setminus A = \{3, 5\}$.

Lastly, we define the *symmetric difference* $A \triangle B$ of two sets A and B to be the set of all elements that are either in A or in B *but not both*. Invoking the above example one last time, we have $A \triangle B = \{2, 3, 4, 5\}$. To practise using all the different operations we just learned, convince yourself that the following are all valid ways to express the symmetric difference:

$$A \triangle B = (A \cup B) \setminus (A \cap B) = (A \setminus B) \cup (B \setminus A) = \overline{\overline{A \cup B} \cup (A \cap B)}$$

2. More set identities abound. We state the following proposition without proof; you should try going though this list and convincing yourself that each identity holds, for all sets A, B, and C. (This is a great way of practising proofs by double inclusion.)

Proposition 2. *Let A, B, and C be subsets of a universe U. Then*

i) $A \cap U = A$ *and* $A \cup \emptyset = A$;
ii) $A \cup U = U$ *and* $A \cap \emptyset = \emptyset$;
iii) $A \cup A = A$ *and* $A \cap A = A$;
iv) $\overline{\overline{A}} = A$;
v) $A \cup B = B \cup A$ *and* $A \cap B = B \cap A$;
vi) $A \cup (B \cup C) = (A \cup B) \cup C$ *and* $A \cap (B \cap C) = (A \cap B) \cap C$;
vii) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ *and* $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$;
viii) $A \cup (A \cap B) = A$ *and* $A \cap (A \cup B) = A$; *and*
ix) $A \cup \overline{A} = U$ *and* $A \cap \overline{A} = \emptyset$. ∎

Some of these laws have names: (v) is called the commutative law, (vi) is called the associative law, (vii) is the distributive law, (viii) is called the absorption law, and (ix) is the complement law.

***Analogy with addition and multiplication.** Some of these laws bear some resemblance to laws about numbers that you already know. As an exercise, replace $\cup$ with $+$ (addition), $\cap$ with $\cdot$ (multiplication), $\overline{A}$ with $-A$ (negation), U with 1, and $\emptyset$ with 0 in all the formulas above, and now assume that A, B, and C are arbitrary real numbers. Which identities still hold in the number setting, and which ones don't? As a more advanced exercise, try replacing $\cup$ with $\triangle$ in the identities above (some statements will have to be tweaked a bit so that they're actually true, some won't). Now do the same replacement as before, except replace $\triangle$ with $+$. You will find that many more identities carry over.

De Morgan's laws. There are two important laws relating complements with union and intersection. We shall state them as a proposition, this time giving a proof (of one of them).

Proposition 2 (*De Morgan's laws*). *Let A and B be sets. Then*

i) $\overline{A \cup B} = \overline{A} \cap \overline{B}$; *and*
ii) $\overline{A \cap B} = \overline{A} \cup \overline{B}$.

Proof. Let $x \in \overline{A \cup B}$. This means that x does not belong to the union of A and B, x cannot be in A, nor can it be in B. Since $x \notin A$, $x \in \overline{A}$, and since $x \notin B$, $x \in \overline{B}$. Therefore, $x \in \overline{A} \cap \overline{B}$. This shows that $\overline{A \cup B} \subseteq \overline{A} \cap \overline{B}$.

Now assume that $x \in \overline{A} \cap \overline{B}$. So $x \in \overline{A}$ and $x \in \overline{B}$, meaning that $x \notin A$ and $x \notin B$. Since x is in neither A nor B, it is also not a member of the union $A \cup B$. We conclude that $x \in \overline{A \cup B}$. We have shown that $\overline{A} \cap \overline{B} \subseteq \overline{A \cup B}$, which fact, combined with the previous paragraph, completes the proof of (i).

The proof of (ii) is similar and left to the reader as an exercise. ∎

Armed with all of these laws, we are able to perform lots of mechanical set manipulations to simplify expressions. For example, consider the expression

$$\big((A \setminus B) \cup A\big) \cap \overline{A \cap \overline{B}}.$$

Since $A \setminus B = A \cap \overline{B}$ and invoking the second De Morgan law on the right of the intersection yields

$$\big((A \cap \overline{B}) \cup A\big) \cap (\overline{A} \cup B).$$

Now, we can use absorption on the left-hand side to obtain

$$A \cap (\overline{A} \cup B),$$

and then distributing gives us

$$(A \cap \overline{A}) \cup (A \cap B) = \emptyset \cup (A \cap B) = A \cap B.$$

We thus see that the nasty expression $\big((A \setminus B) \cup A\big) \cap \overline{A \cap \overline{B}}$ is simply another way of writing $A \cap B$.

The Cartesian product and power set. From the real line $\mathbf{R}$, we can geometrically construct the Cartesian plane $\mathbf{R}^2$ by lining up parallel copies of $\mathbf{R}$, one for each element of the original line and all parallel to the original line. Notationally, $\mathbf{R}^2$ is the set of all ordered pairs (a, b), where $a, b \in \mathbf{R}$. Generalising this, for any sets A and B we can define the *Cartesian product* $A \times B$ to be the set

$$A \times B = \big\{(a, b) : a \in A, b \in B\big\}.$$

We sometimes write A^2 for $A \times A$, and more generally A^n for the n-fold Cartesian product of A with itself. (This explains the notation $\mathbf{R}^2$ for the Cartesian plane, and $\mathbf{R}^n$ for the n-dimensional vector space over $\mathbf{R}$.) Note that $A \times B$ is not equal to $B \times A$ in general.

Proposition 3. *If A and B are finite sets, then $|A \times B| = |A| \cdot |B|$.*

Proof. The set $A \times B$ consists of all ordered pairs (a, b) where $a \in A$ and $b \in B$. There are $|A|$ choices for a, and for a, there are $|B|$ ways to pair it with a b from B. So there are $|A| \cdot |B|$ pairs in total. ∎

Now we define the *power set*. For a set A, this is the set of all subsets of A, and is commonly denoted by $\mathcal{P}(A)$ or 2^A. (We will use the latter notation in these notes.) In set-builder notation, we have

$$2^A = \{X \subseteq U : X \subseteq A\}.$$

As an example, if $A = \{1, 2, 3\}$, then

$$2^A = \big\{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\big\}.$$

Note that even though, say, $1 \in A$, we do not have $1 \in 2^A$. We do, however, have $\{1\} \in 2^A$.

Another example is $2^{\mathbf{Z}}$, the set of all subsets of integers. If P is the set of primes, then $P \in 2^{\mathbf{Z}}$. Also in $2^{\mathbf{Z}}$ is the set $S = \{n^2 : n \in \mathbf{Z}\}$ of square numbers.

There is a way of encoding subsets with strings of 0s and 1s. Suppose we have a set

$$\{-3, 1, 7, 19, 23\}.$$

Fixing this order of the elements, for any arbitrary subset of this set, we can associate to it a binary string. Consider the subset $\{1, 19, 23\}$. This corresponds to the binary string 01011: since the first element, 3, is not in the subset, we write a 0. Then 1 is in the subset, so we write a 1, and so on. This is a reversible process. Given a binary string of length 5, say, 00101, we can reconstruct the subset that corresponds to it. The first two 0s mean that -3 and 1 do not belong to the set, but 7 does, 19 doesn't, and 23 does. So the subset is $\{7, 23\}$. In this way we see that there is a one-to-one correspondence between the elements of 2^A and binary strings of length $|A|$. We'll use this fact in the proof of the following proposition.

Proposition 4. *If A is finite, then $|2^A| = 2^{|A|}$.*

Proof. We just saw that there is a one-to-one correspondence between elements of 2^A and binary strings of length $|A|$. So it suffices to count the number of binary strings of length $|A|$. Well, each digit can be either 0 or 1, and there are $|A|$ digits, so the number of strings is

$$\underbrace{2 \cdot 2 \cdot \cdots \cdot 2}_{|A| \text{ times}} = 2^{|A|}. \quad \blacksquare$$

Counterexamples in proofs. We finish this subsection with a little example problem. *Is it true that $2^A \cup 2^B = 2^{A \cup B}$ for all sets A and B?*

Let's start by trying to prove the statement is true. As usual, we will attempt a double-inclusion proof. Let $2^A \cup 2^B$. This means X is either a subset of A or it is a subset of B. Either way, X is a subset of $A \cup B$, so $X \in 2^{A \cup B}$. So far so good; we have proved that $2^A \cup 2^B \subseteq 2^{A \cup B}$.

Now we try the other direction. Let $X \in 2^{A \cup B}$. So X is a subset of $A \cup B$. From here we want to say that X must be a subset of A or it must be a subset of B, but is that necessarily true? It is possible that X is contained slightly in A and slightly in B. So we have failed to prove that $2^{A \cup B} \subseteq 2^A \cup 2^B$ in general. But just because we have failed to prove that something is true doesn't mean we have proved it is false!

To actually prove that $2^{A \cup B} \subseteq 2^A \cup 2^B$ doesn't hold in general, we need to find a *counterexample*. That is, we need to construct sets A and B such that the statement is false. In this case, we can let $A = \{1, 2\}$, $B = \{3, 4\}$, so that $A \cup B = \{1, 2, 3, 4\}$. Then the set $\{1, 3\}$ is a subset of $A \cup B$ but is not a subset of A and it is not a subset of B. In other words, $\{1, 3\} \in 2^{A \cup B}$ but $\{1, 3\} \notin 2^A \cup 2^B$, proving that $2^{A \cup B} \not\subseteq 2^A \cup 2^B$.

3. **Russell's paradox.** Earlier, we said that the sets we are working with need to be a subset of a universe U, which has already been proven to be a set. We gave lots of ways to make sets out of new sets, such as the union and intersection

operations, etc. Starting with the empty set $\emptyset$ is a set, it is possible to define the set of natural numbers as follows. We can define $0 = \emptyset$, $1 = \{0\}$, and $2 = \{0, 1\}$, and so on. Now we take the set of all of these, and call this $\mathbf{N}$. (We can also define addition and multiplication on these set-theoretic "numbers" so that they behave like addition and multiplication do on $\mathbf{N}$.) From here we can do more funky stuff to define $\mathbf{Z}$, $\mathbf{Q}$, and $\mathbf{R}$, and prove that these are all sets (you can see this in a higher-level course on set theory, if you're interested). So there isn't much of a problem with all the sets we have played with so far; they are all subsets of things that are already known to be sets.

Ungodly things can happen if we don't stick by these rules. An example, due to Bertrand Russell, is the "set"

$$R = \{\text{sets } X : X \notin X\}.$$

In plain English, R is defined to be the set of all sets that contain themselves. This is not a subset of any known thing, so by our criterion above we would not consider it a set. But supposing it is, let us ask ourselves the following question. Does R contain itself? If it does not, then $R \notin R$, so R would be a set that satisfied the condition of R, so $R \in R$. But on the other hand, if $R \in R$, then R violates the condition defining R, so $R \notin R$. Round and round we go in a circle of contradiction.

Such is the price of meddling with "sets" that aren't subsets of known sets.

2. Propositional logic

A *proposition* is a statement that is true or false. For example "8 is even" is a statement we know to be true, and "8 is prime" is a statement we know to be false. The statement "n is prime" is not a proposition because its truth or falsity depends on what n is. (But if n is previously fixed to stand for some value, then this would be a proposition.) The statement "$2^{2^{2^{40}}} - 1$ is prime" is a proposition, because it is either true or false (even though you or I might not know which one it is).

A *propositional variable* or a *boolean variable* is a variable which can take either the value 0 or 1, where 0 means "false" and 1 means "true." Usually we use letters p, q, and r to denote propositional variables.