Clive Chapter 0 & Section 1.1
A Little Light Concepts Pre-Reading

Susan Huang, Maxwell Jones, AJ Lim,
Reed Luttmer, Vianna Seifi, Maria Yampolsky

August 29, 2023

This is a heavily condensed/trimmed version of Chapter 0 and Section 1.1 of *An Infinite Descent into Pure Mathematics* by Clive Newstead. Typically, Chapters 0 and 1.1 are assigned as readings to students but this is a more accessible summary of most of the content. We provide important definitions/examples and reference some relevant examples from the textbook for extra reinforcement. If you are looking for a more in-depth version of this material, the complete version can be found at https://infinitedescent.xyz/dl/infdesc.pdf.

NOTE: This is a relatively condensed version of around 50 pages of material and we've only included things we've deemed very important, so please don't skim!

Contents

Chapter 0

0.1 Propositions, Theorems, Lemmas, Corollaries

Definition: Proposition
A proposition is a statement to which it is possible to assign a truth value ('true' or 'false').

The vast majority of your time in this class will be spent proving propositions. If a proposition is true, a *proof* of the proposition is a logically valid argument demonstrating that it is true, which is pitched at such a level that a member of the intended audience can verify its correctness. In this course, "the intended audience" comprises other students in this course. Thus when writing a proof, ensure that your level of detail makes it understandable to your classmates.

Some non-examples of propositions are *This sentence is false* and *The happiest donkey in the world* - it doesn't make sense to assign truth values to them, so we won't bother trying to prove them.

When specifying the role of certain propositions that we prove true, we sometimes label them as **theorems, lemmas, or corollaries**.

- A **theorem** is a key result which is particularly important.
- A **lemma** is a result which is proved for the purposes of being used in the proof of a theorem.
- A **corollary** is a result which follows from a theorem without much additional effort.

0.2 Number sets

Definition: Set
A set is a collection of objects. The objects in the set are called elements of the set. If X is a set and x is an object in X, then we write $x \in X$ (in LaTeX, `x \in X`) to denote the assertion that x is an element of X.

Number sets are sets whose elements are numbers. For instance, we could consider a set that contains 0, 1, 2, 3, 4, and so on forever. We call this set the natural numbers, or the naturals for short, and it is represented by the symbol $\mathbb{N}$.

Definition: Natural Numbers
The natural numbers $\mathbb{N}$ (in LaTeX, `\mathbb{N}`) is defined as the set containing 0, 1, 2, 3, and so on. It is an infinite set. In more familiar terms, they are the non-negative whole numbers. We write $\mathbb{N}$ for the set of all natural numbers; thus, the notation '$n \in \mathbb{N}$' is equivalent to saying n is a natural number.

0.3 Number bases

Definition: Base-b Expansion
Let $b > 1$, The base-b expansion of a natural number n is the string $d_r d_{r-1} \cdots d_0$ such that

- $n = d_r \cdot b^r + d_{r-1} \cdot b^{r-1} + \cdots + d_0 \cdot b^0$;
- $0 \leq d_i < b$ for each i; and
- If $n > 0$ then $d_r \neq 0$ - the base-b expansion of zero is 0 in all bases b.

Certain number bases have names; for instance, the base-2, 3, 8, 10 and 16 expansions are respectively called *binary, ternary, octal, decimal and hexadecimal.*

0.4 Integers ($\mathbb{Z}$)

Definition: Integers
Consider a set initially containing just the naturals. For each natural n, we also add $-n$ to the set. This set is known as the set of integers, or $\mathbb{Z}$ (in LaTeX, `\mathbb{Z}`).
Since $-n + n = 0$, we say that $-n$ is the *additive inverse* of n. Thus we can also define the integers as the naturals and their additive inverses.
We write $\mathbb{Z}$ for the set of all integers; thus, the notation '$x \in \mathbb{Z}$' means x is an integer.

0.4.1 Division of integers

Definition: Divides
Let $a, b \in \mathbb{Z}$. We say that b **divides** a if there is some integer k such that $a = bk$. We often write $b \mid a$ (in LaTeX, `b \mid a`) to mean that b divides a. We can also say that b is a *divisor* of a, b is a *factor* of a, or a is a *multiple* of b.

For example, 5 divides 15 because $15 = 5 \cdot 3$, and 3 is an integer. For any integer a, 1 divides a because $a = 1 \cdot a$ and a divides 0 because $0 = a \cdot 0$. Also for $a \in \mathbb{Z}$, 0 only divides a if $a = 0$ because if a is nonzero, then there does not exist any integer k such that $a = 0 \cdot k$.

Divisibility is an incredibly important topic in concepts. Make sure you're comfortable with the definition. We can use it to define even and odd integers. **For this class, you may argue that $a|b$ implies a is a factor of b**

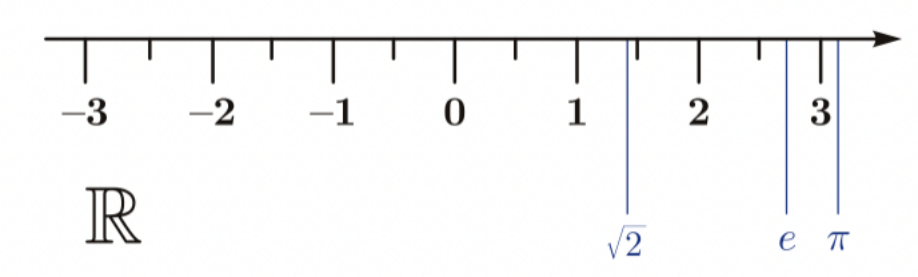
Definition: Even and Odd
An integer n is **even** if it is divisible by 2; otherwise, n is **odd**.
Applying the definition of divisible, we say n is even if there is an integer k such that $n = 2k$, and n is odd if there is an integer k such that $n = 2k + 1$.

Theorem: Division Theorem
Let $a, b \in \mathbb{Z}$, with $b \neq 0$. There is **exactly one** way to write $a = qb + r$ such that q and r are integers and $0 \leq r < |b|$. We call q the **quotient** and r the **remainder** of a when divided by b.

0.5 Rational ($\mathbb{Q}$) and irrational numbers

Definition: Rational Numbers
Rational numbers are numbers of the form $\frac{a}{b}$ where $a, b \in \mathbb{Z}$ and $b \neq 0$. The symbol $\mathbb{Q}$ (in LaTeX, `\mathbb{Q}`) represents the set of rational numbers; thus, $q \in \mathbb{Q}$ is equivalent to 'q is a rational number'.

Definition: Real Numbers
Real numbers are the points on the number line:



The symbol $\mathbb{R}$ (in LaTeX, `\mathbb{R}`) represents the set of all real numbers; thus $x \in \mathbb{R}$ is equivalent to x is a real number. You might have heard that this includes decimals that are infinite but don't repeat, such as π or e.
This isn't a super formal definition, but it will suffice for this course.

Definition: Irrational Numbers
An irrational number is a real number that is not rational. For instance, $\sqrt{2}$ is irrational.

Note that unlike the naturals, integers, rationals, and reals, there is no single letter representation of the set of irrational numbers. After we learn more about sets, we will be able to represent the irrational numbers as $\mathbb{R} \setminus \mathbb{Q}$ (in LaTeX, `\mathbb{R} \setminus \mathbb{Q}`).

0.6 Complex numbers ($\mathbb{C}$)

The square of any real number is always non-negative, but sometimes we may want to work with numbers whose squares are negative. For this, we must introduce imaginary numbers.

Definition: Imaginary Numbers
An imaginary number is a number whose square is negative. The [imaginary unit] i has the property that $i^2 = -1$.

Definition: Complex Numbers
A complex number is a combination of a real number and an imaginary number. Every complex number can be expressed as $a + bi$ where $a, b \in \mathbb{R}$. We call a the **real part**, and b is called the **imaginary part**. The symbol $\mathbb{C}$ represents the set of all complex numbers, thus, $z \in \mathbb{C}$ (in LaTeX, `z \in \mathbb{C}`) means that z is a complex number.

Remember a or b (or both) can be 0. So for example 3 and $5i$ are both complex numbers (even though you could also classify them as a real number and an imaginary number, respectively). Whereas the real numbers can be visualized on a number line, the complex numbers form a plane, namely the **complex plane**:

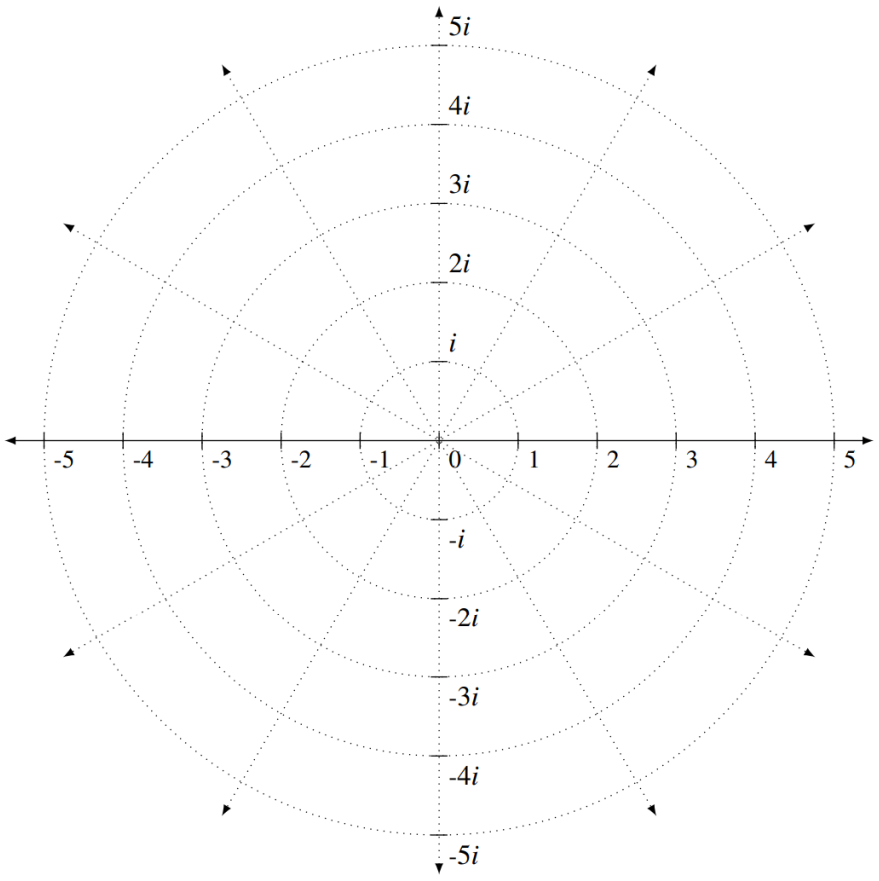


Figure 1: Illustration of the complex plane, with some points labelled.

Every complex number can be expressed as $a + bi$, but a number does not need to be written this way to be complex. For example (although the rest of this paragraph is beyond the scope of this course), you could also write a complex number as $ce^{i\theta}$ for $c, \theta \in \mathbb{R}$. If you read Infinite Descent, Clive will define complex numbers as a rotation of the real number line. In that case, the θ can be interpreted as what angle you are rotating the real number line by, and c can be interpreted as how far away from the origin you are moving.

0.7 Polynomials

Polynomials - you (probably) know them, you (possibly) love them, and it turns out that a more formal and general definition of them is quite intimidating. If you want the formal definition, refer to Infinite Descent, but the simpler definition below will suffice for this course:

Definition: Polynomials
A polynomial is an expression of the form

$$a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$$

where $n \in \mathbb{N}$. The numbers a_k are called the coefficients of the polynomial. When there is at least one non-zero coefficient, we say the degree of the polynomial is the largest value of k such that $a_k \neq 0$. By convention, the degree of the polynomial 0 is $-\infty$.

Polynomials of degree 1, 2, 3, 4 and 5 are respectively called linear, quadratic, cubic, quartic and quintic polynomials. Instead of writing out the coefficients of a polynomial each time, we may define $p(x) = x^2$ or $q(x) = 5x^4 - x^3 + 7$ and later write $p(1)$ to mean 1^2 or $q(1)$ to mean $5(1^4) - 1^3 + 7$.

Definition: Root(s) of a Polynomial
Let $p(x)$ be a polynomial. A root of $p(x)$ is a complex number α such that $p(\alpha) = 0$.

Strategy: Simon's Favorite Factoring Trick
The equation $xy + c_1x + c_2y = c_3$ such that $c_1, c_2, c_3 \in \mathbb{Z}$ can be factored into

$$(x + c_2)(y + c_1) = c_3 - c_1c_2$$

Here's a quick example. Consider the equation $2xy + 6x + 9y = 7$. In order to use Simon's Favorite Factoring Trick, we first divide the equation by 2 so the coefficient of xy is 1. Then, we can pattern match to find that

$$xy + 3x + \frac{9}{2}y = \frac{7}{2} \implies \left(x + \frac{9}{2}\right)(y + 3) = -10$$

0.8 Chapter 0 Exercises

Solutions to the following exercises can be found in the appendix, although you will learn the most if you attempt each problem to the best of your ability first.

0.4 What are the possible remainders of n^2 when divided by 3, where $n \in \mathbb{Z}$?

Closed questions

Definition: Closure
A set X is closed under an operation $\odot$ if, whenever a and b are elements of X, $a \odot b$ is also an element of X.

In the following questions, determine, with proof, which of the number sets $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$, and $\mathbb{R}$ are closed under the operation $\odot$ defined in the question. In other words, if a, b are from some set S, is $a \odot b$ always in S?

0.5 $a \odot b = a + b$

0.8 $a \odot b = (a-1)(b-1) + 2(a+b)$

0.9 $a \odot b = \frac{a}{b^2+1}$

0.10 (maybe make this suggested) $a \odot b = \frac{a}{\sqrt{b^2+1}}$

In this class, you may assume the following list of closure properties without proof. However, it is best practice to cite what closure property you are using.

- the naturals are closed under addition and multiplication
- the integers are closed under addition, subtraction, and multiplication
- the rationals are closed under addition, subtraction, multiplication, and nonzero division
- the reals are closed under addition, subtraction, multiplication, and nonzero division

Note: We expect you to show all intermediate steps in your proofs. For example, if you start with $a, b \in \mathbb{N}$, you must note that $a + b \in \mathbb{N}$ (and ideally cite that this is because the naturals are closed under addition) before using it in the rest of your proof.

Always-Sometimes-Never questions

In the following questions, determine, with proof, whether the conclusion is always, sometimes, or never true under the given hypotheses.

0.26 Let $a, b, c \in \mathbb{Z}$ and suppose that a divides c and b divides c. Then ab divides c.

0.27 Let $a, b, c \in \mathbb{Z}$ and suppose that a divides c and b divides c. Then ab divides c^2.

0.28 Let $x, y \in \mathbb{Q}$ and let $a, b, c, d \in \mathbb{Z}$ with $cy + d \neq 0$. Then $\frac{ax+b}{cy+d} \in \mathbb{Q}$.

Section 1.1: Propositional Logic

In mathematics, we write proofs by making **assumptions**, which are propositions that are known or assumed to be true. They include theorems that have already been proved, prior knowledge, and assumptions which are explicitly made using words like 'suppose' or 'assume'.

With these assumptions, we can achieve **goals**, which are propositions we are trying to prove.

0.9 Propositional formulae

Definition: Propositional Variable
A propositional variable is a symbol that represents a proposition. Propositional variables may be assigned truth values ('true' or 'false').

For example, consider the proposition

$$\text{If } c \text{ divides } b \text{ and } b \text{ divides } a, \text{ then } c \text{ divides } a.$$

The three statements 'c divides b', 'b divides a' and 'c divides a' are all propositions in their own right. We can replace these simpler propositions with propositional variables. Letting p represent 'c divides b', q represent 'b divides a' and r represent 'c divides a', we can rewrite our original proposition as:

$$\text{If } p \text{ and } q, \text{ then } r.$$

Breaking down the proposition in this way makes it clear that a feasible way to prove it is to assume p and q, and then derive r from these assumptions. But importantly, it suggests that the same proof strategy might work for other propositions which are also of the form 'if p and q, then r', such as the following proposition (for a given integer n):

$$\text{If } n > 2 \text{ and } n \text{ is prime, then } n \text{ is odd.}$$

Definition: Propositional Formula
A propositional formula is an expression that is either a propositional variable, or is built up from simpler propositional formulae ('subformulae') using a logical operator. In the latter case, the truth value of the propositional formula is determined by the truth values of the subformulae according to the rules of the logical operator.

If that doesn't make sense, don't worry! It will become clearer as we introduce you to the logical operators below.

0.10 Conjunction & Disjunction

Definition: Conjunction ($\wedge$)
The conjunction operator is written in math notation as $\wedge$ (in LaTeX, `\land`). The proposition '$p \wedge q$' is equivalent to 'p is true and q is true'.

Check your understanding: what is the truth value of 'I am above 5 feet tall and I am an MCS student'? What about the proposition 'Earth revolves around the Sun $\wedge$ birds exist'?

We present a truth table of $p \wedge q$ below, where T represents 'true', and F represents 'false':

p	q	$p \wedge q$
T	T	T
T	F	F
F	T	F
F	F	F

We can read the first row as 'if p is true and q is true, then $p \wedge q$ is true.' Note that this is the only case where $p \wedge q$ is true. This motivates the following proof strategy:

Strategy: Proofs with Conjunctions
To prove a proposition of the form $p \wedge q$ is true, it suffices to show that p is true and then also show that q is true. Conversely if we are assuming that $p \wedge q$ is true, then we are free to use the fact that p is true and the fact that q is true.

Definition: Disjunction ($\vee$)
The disjunction operator is the logical operator $\vee$ (in LaTeX, `\lor`). '$p \vee q$' is equivalent to 'p is true or q is true'.

We present a truth table of $p \vee q$ in the following:

p	q	$p \vee q$
T	T	T
T	F	T
F	T	T
F	F	F

You can see in the table above that the only time $p \vee q$ is false is when *both* p and q are false. This leads to the following proof strategy:

Strategy: Proving Disjunctions
To prove $p \vee q$ true, it suffices to show that just one of p or q is true. Another common technique is to assume p is false and show that q must then be true.

Strategy: Assuming Disjunctions - Proof By Cases
If we are assuming that $p \vee q$ is true, and our goal is to prove the proposition r, we almost always want to split into cases. To do so, temporarily assume that p is true and show that r being true follows. Then, assume separately that q is true and show that r being true also follows in that case.

As a concrete example of this casework strategy, we prove the following proposition:

Proposition 1.1.18
Let $n \in \mathbb{N}$. Then n^2 leaves a remainder of 0 or 1 when divided by 3.

Proof
Let $n \in \mathbb{Z}$. By the division theorem, one of the following must be true for some $k \in \mathbb{Z}$:

$$n = 3k \text{ or } n = 3k + 1 \text{ or } n = 3k + 2.$$

We now case on n in the following:

- Case 1: Suppose $n = 3k$. Then

  $$n^2 = (3k)^2 = 9k^2 = 3 \cdot (3k^2) + 0$$

  So n^2 leaves a remainder of 0 when divided by 3.
- Case 2: Suppose $n = 3k + 1$. Then

  $$n^2 = (3k + 1)^2 = 9k^2 + 6k + 1 = 3(3k^2 + 2k) + 1$$

  So n^2 leaves a remainder of 1 when divided by 3.
- Case 3: Suppose $n = 3k + 2$. Then

  $$n^2 = (3k + 2)^2 = 9k^2 + 12k + 4 = 3(3k^2 + 4k + 1) + 1$$

  So n^2 leaves a remainder of 1 when divided by 3.

In all possible (exhaustive) cases, n^2 leaves a remainder of 0 or 1 when divided by 3. □

0.11 Implications & Biconditionals

Definition: Implication
The implication operator is written in mathematical notation as $\implies$ (in LaTeX, `\implies`). The propositional formula $p \implies q$ is shorthand for 'if p is true, then q is true'.

Strategy: Proving Implications (Direct Proof)
In order to prove $p \implies q$, it suffices to assume that p is true, then show that q is true based on that assumption.

It may be helpful to think of an implication as a contract or a promise. The propositional formula $p \implies q$ is equivalent to saying when p happens, I promise that q will happen.

Note: this interpretation promises nothing about q when p isn't true. In the case that p is false, q could be anything - true or false - and we would still consider $p \implies q$ to be true.

As an example, consider the very true implication

$$\text{you come to recitation} \implies \text{Susan will be happy}$$

There are only two possible cases: either you come to recitation, or you don't.

In the case that you come to recitation, the truth of the implication promises that Susan will be happy. It cannot be the case that Susan is not happy, because that would violate the promise, and the implication would be false.

In the case that you don't come to recitation, nothing is promised about Susan's emotions. Susan could very well be happy despite teaching to an empty classroom - maybe her co-TA gave her an origami hedgehog. It could also be the case that Susan is not happy.

Note that this means that $p \implies q$ is true even if p is false and q is true. The only thing that would violate the implication's promise is if p is true and q is false.

We now consider an alternate way of saying $p \implies q$. First let's look at truth table of $p \implies q$:

p	q	$p \implies q$
T	T	T
T	F	F
F	T	T
F	F	T

Again, we can see that the only case where $p \implies q$ is false is when p is true and q is false. Two propositions are **logically equivalent** if they have the same truth table, and it turns out that $p \implies q$ is **logically equivalent** to $\neg p \vee q$.

p	q	$\neg p$	$\neg p \vee q$
T	T	F	T
T	F	F	F
F	T	T	T
F	F	T	T

Observe that the truth value of $\neg p \vee q$ is the same as that of $p \implies q$ for every possible truth value combination of p and q. Intuitively, both $p \implies q$ and $\neg p \vee q$ are true in the case where p is false, and further, in the case where p is true, both statements only hold if q is true. **Thus when proving $p \implies q$, it suffices to prove $\neg p \vee q$.**

Definition: Converse
The converse of a proposition of the form $p \implies q$ is the proposition $q \implies p$.

Note that having an implication be true does not tell us whether the converse will be true. If you aren't sure about this, think about the truth tables for $p \implies q$ and $q \implies p$.

A quick remark on terminology is pertinent. The following table summarizes some common ways of referring to the propositions '$p \implies q$' and '$q \implies p$'.

$p \implies q$	$q \implies p$
if p, then q	if q, then p
p only if q	p if q
p is sufficient for q	p is necessary for q

We so often encounter the problem of proving both an implication and its converse that we introduce a new logical operator that represents the conjunction of both.

Definition: Biimplication
The biconditional operator is the logical operator $\iff$ (in LaTeX, `\iff`), defined by declaring $p \iff q$ to be logically equivalent to $(p \implies q) \wedge (q \implies p)$.
The expression $p \iff q$ is commonly said as 'p if and only if q' and sometimes written as 'p iff q'.

We will often use biimplication when solving equations. For example, let's say we are tasked with finding all real solutions x to the equation $\sqrt{x-1}+4 = x-3$. We have:

$$\begin{aligned}
\sqrt{x-1}+4 = x-3 &\implies \sqrt{x-1} = x-7 && \text{subtracting 4}\\
&\implies x-1 = (x-7)^2 && \text{squaring}\\
&\implies x-1 = x^2-14x+49 && \text{expanding}\\
&\implies x^2-15x+50 = 0 && \text{rearranging}\\
&\implies (x-5)(x-10) = 0 && \text{factoring}\\
&\implies x = 5 \text{ or } x = 10
\end{aligned}$$

We aren't done yet. Right now we have shown that *if* x solves the equation, *then* $x = 5$ or $x = 10$. In other words, we have shown that 5 and 10 are the only *possible* solutions, but we haven't yet shown that they *actually are* solutions. We need to check the converse, so we plug our potential solutions into the equation:

$$\begin{aligned}
x = 5: &\quad \sqrt{x-1}+4 = \sqrt{5-1}+4 = \sqrt{4}+4 = 6 \neq 2 = 5-3 = x-3\\
x = 10: &\quad \sqrt{x-1}+4 = \sqrt{10-1}+4 = 3+4 = 7 = 10-3 = x-3
\end{aligned}$$

We see that 10 is a solution, but 5 is not. Thus $\sqrt{x-1}+4 = x-3 \iff x = 10$.

0.12 Quadratic Formula

Theorem: Quadratic Formula
Let $a, b \in \mathbb{C}$. A complex number α is a root of the polynomial x^2+ax+b if and only if

$$\alpha = \frac{-a+\sqrt{a^2-4b}}{2} \text{ or } \frac{-a-\sqrt{a^2-4b}}{2}$$

In this course, you may use the quadratic formula without derivation. Next, we present an alternate method of solving (monic) quadratics, made famous by Po-Shen Loh:

Take a quadratic $x^2 + Bx + C$, where $B, C \in \mathbb{C}$. If it can be written $(x - r)(x - s)$ for $r, s \in \mathbb{C}$, it was discovered by Vieta (a math person) that $-B = r + s$ and $C = rs$.

We can then see that there is some $u \in \mathbb{C}$ such that r and s are $\frac{-B}{2} \pm u$ (depending on which one is bigger if r and s are real numbers). If you aren't convinced, try it out with some numbers of your own.

Then, we can plug these expressions for r and s into $C = rs$ to get

$$\begin{aligned} & C = \left(\frac{-B}{2} + u\right)\left(\frac{-B}{2} - u\right) \\ \iff & C = \frac{B^2}{4} - u^2 \\ \iff & u^2 = \frac{B^2}{4} - C \\ \iff & u = \pm\sqrt{\frac{B^2}{4} - C} \end{aligned}$$

For instance, take the quadratic $x^2 + 20x + 91$. Maybe you didn't know that $91 = 7 \times 13$. However, try solving this using the steps outlined above. You will find that you did not need to know about the factorization about 91 to do so.

0.13 Negation

Definition: Contradiction
A contradiction is a proposition that is known or assumed to be false. We will use the symbol $\perp$ (in LaTeX, `\bot`) to represent an arbitrary contradiction.

Some examples of contradictions include the propositions $0 = 1$, or '$\sqrt{2}$ is rational', or 'the equation $x^2 = -1$ has a solution $x \in \mathbb{R}$.'

Definition: Negation
The negation operator is the logical operator $\neg$ (in LaTeX, `\neg`), where $\neg p$ is equivalent to 'p is false'.

Note that if we can derive a contradiction from the assumption that p is true, then we can conclude that $\neg p$ is true. Conversely, if $\neg p$ is true and p is true, then we may derive a contradiction. We can apply this idea to use the following proof strategy:

Strategy: Proof by Contradiction
In order to prove a proposition p is false (that is, that $\neg p$ is true), it suffices to assume that p is true and show that this leads to a contradiction.

It may be helpful to think of this strategy as proving that it cannot be the case that a proposition is true, because in that case, we derive a contradiction, which is like breaking math and blowing up the world. There is only one other case for what the truth value of a proposition can be: false. Since we ruled out the true case, the proposition has to be false.

Note that this intuition relies on the fact that there are only two cases for what the truth value of a proposition can be: true and false. This is formalized in the following axiom:

Axiom: Law of Excluded Middle
Let p be a propositional formula. Then $p \vee (\neg p)$ is true.

Although this axiom may seem trivially true, it is not accepted in all mathematical contexts. In this class however, you can use it freely. The following proof strategy relies on the axiom:

Strategy: Using Law of Excluded Middle in Proofs
In order to prove a proposition q is true, it suffices to split into cases based on whether some other proposition p is true or false, and prove that q is true in each case.

This casing strategy is useful in many proofs, including the proof of the following proposition:

Proposition 1.1.46 Let $a, b \in \mathbb{Z}$. If ab is even, then a is even or b is even. (Note: by the logical definition of 'or' it is also acceptable for both a and b to be even.)

Proof Suppose $a, b \in \mathbb{Z}$ with ab even. By the division theorem, either a is even or a is odd.

- Case 1: Suppose a is even - then we're done.
- Case 2: Suppose a is odd. If b is also odd, then by the definition of odd, can write $a = 2k + 1$ and $b = 2l + 1$ for some integers k, l. This implies that

$$ab = (2k + 1)(2l + 1) = 4kl + 2k + 2l + 1 = 2(2kl + k + l) + 1$$

so that ab is odd since $2kl + k + l \in \mathbb{Z}$. This contradicts the given assumption that ab is even, and so b must in fact be even.

In both cases, either a or b is even. □

0.14 1.1 Exercises

(IMPORTANT) Exercise 1.1.48 in Clive's Infinite Descent may be useful for your future endeavors in this course :eyes:

1.1 For fixed $n \in \mathbb{N}$, let p represent the proposition 'n is even', let q represent the proposition 'n is prime' and let r represent the proposition '$n = 2$'. For each of the following propositional formulae, translate it into plain English and determine whether it is true for all $n \in \mathbb{N}$, true for some values of n and false for some values of n, or false for all $n \in \mathbb{N}$.

(a) $(p \wedge q) \implies r$

(b) $q \wedge (\neg r) \implies (\neg p)$

(c) $((\neg p) \vee (\neg q)) \vee (\neg r)$

(d) $(p \wedge q) \wedge (\neg r)$

1.3 Let p and q be propositions, and assume that $p \implies (\neg q)$ is true and that $(\neg q) \implies p$ is false. Which of the following are true, and which are false?

(a) q being false is necessary for p to be true.

(b) q being false is sufficient for p to be true.

(c) p being true is necessary for p to be false.

(d) p being true is sufficient for p to be false.

Appendix 1: Solutions to Exercises

Solutions to Chapter 0 Exercises

0.4 Solution The remainder can be 0 or 1. The proof of this is in Clive on page 37 and in these notes on page 10.

0.5 Solution The sets $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$, and $\mathbb{R}$ are all closed under $\odot$. The proofs are as followed:

- $\mathbb{N}$: Let $a, b \in \mathbb{N}$. The naturals are closed under addition, so $a \odot b = a + b \in \mathbb{N}$ as required.
- $\mathbb{Z}$: Let $a, b \in \mathbb{Z}$. The integers are closed under addition, so $a \odot b = a + b \in \mathbb{Z}$ as required.
- $\mathbb{Q}$: Fix $a, b \in \mathbb{Q}$. The rationals are closed under addition, so $a \odot b = a + b \in \mathbb{Q}$ as required.
- $\mathbb{R}$: Fix $a, b \in \mathbb{R}$. The real numbers are closed under addition, so $a \odot b = a + b \in \mathbb{R}$.

0.8 Solution The sets $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$, and $\mathbb{R}$ are all closed under $\odot$. We will do this in one proof:

Let $\mathbb{S} = \mathbb{N}, \mathbb{Z}, \mathbb{Q}$, or $\mathbb{R}$. Fix $a, b \in \mathbb{S}$. Note that we can write

$$a \odot b = (a-1)(b-1) + 2(a+b) = ab - a - b + 1 + 2a + 2b = ab + a + b + 1.$$

Since $\mathbb{S}$ is closed under multiplication, then $ab \in \mathbb{S}$. Now $a \odot b = ab + a + b + 1 \in \mathbb{S}$ since $ab, a, b, 1 \in \mathbb{S}$ and because $\mathbb{S}$ is closed under addition. So $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$, and $\mathbb{R}$ are all closed under $\odot$.

Note: In this case we used $\mathbb{S}$ as a stand in for the set in question because all 4 sets had the same two properties that we needed, namely being closed under addition and multiplication. If

this makes you uncomfortable, you can also replace $\mathbb{S}$ *with* $\mathbb{N}$ *then* $\mathbb{Z}$ *then* $\mathbb{Q}$ *and then* $\mathbb{R}$ *and do the proof four times as in the solution to 0.5.*

0.9 Solution The $\mathbb{Q}$ and $\mathbb{R}$ are closed under $\odot$ but $\mathbb{N}$ and $\mathbb{Z}$ are not. The proofs are as followed:

- $\mathbb{N}$ and $\mathbb{Z}$: Let $\mathbb{S} = \mathbb{N}$ or $\mathbb{Z}$. The operation $\odot$ is not closed under $\mathbb{S}$. In order to prove this, it suffices to find a counter example. Consider $a = b = 1$. Then $a \odot b = \frac{a}{b^2+1} = \frac{1}{1+1} = \frac{1}{2}$. Since $a, b \in \mathbb{S}$ but $a \odot b = \frac{1}{2} \notin \mathbb{S}$ then $\mathbb{S}$ isn't closed under $\odot$.

  Note: Other counter examples could work as well.

- $\mathbb{Q}$ and $\mathbb{R}$: Let $\mathbb{S} = \mathbb{Q}$ or $\mathbb{R}$. Take arbitrary $a, b \in \mathbb{S}$. Note that $b^2 \geq 0$ and $1 > 0$ so $b^2 + 1 > 0$. Furthermore, because $\mathbb{S}$ is closed under addition and multiplication, then $b^2 + 1 \in \mathbb{S}$. It follows that $\frac{a}{b^2+1} \in \mathbb{S}$ because $\mathbb{S}$ is closed under nonzero division. So $\mathbb{Q}$ and $\mathbb{R}$ are closed under $\odot$.

0.10 Solution Only $\mathbb{R}$ is closed under $\odot$, while $\mathbb{N}, \mathbb{Z}$, and $\mathbb{Q}$ are not.

- $\mathbb{N}$, $\mathbb{Z}$, and $\mathbb{Q}$. Let $\mathbb{S} = \mathbb{N}, \mathbb{Z}$, or $\mathbb{Q}$. Consider $a = 2$, $b = 1$. Clearly $a, b \in \mathbb{S}$. Furthermore, $a \odot b = \frac{a}{\sqrt{b^2+1}} = \frac{2}{\sqrt{1+1}} = \frac{2}{\sqrt{2}} = \sqrt{2}$. We observe that $\sqrt{2} \notin \mathbb{S}$ *(for* $\mathbb{N}, \mathbb{Z}$ *you can just state this, and for* $\mathbb{Q}$ *we explicitly said that* $\sqrt{2}$ *was irrational).* Hence $\mathbb{S}$ isn't closed under $\odot$.

- $\mathbb{R}$: Fix $a, b \in \mathbb{R}$. Then $b^2 + 1 \in \mathbb{R}$ since $\mathbb{R}$ is closed under multiplication and addition, and $b^2 + 1 > 0$ since $b^2 \geq 0$ and $1 > 0$. Thus $\sqrt{b^2 + 1} \in \mathbb{R}$ and $\sqrt{b^2 + 1} \neq 0$. It follows that $a \odot b = \frac{a}{\sqrt{b^2+1}} \in \mathbb{R}$ since the reals are closed under nonzero division.

0.26 Solution The conclusion is sometimes true. To prove this we will provide one example where it is true and another example where it is false.

First consider $a = 4$, $b = 6$, and $c = 12$. Clearly $a, b, c \in \mathbb{Z}$. Furthermore a divides c because $12 = 4 \cdot 3$ and $3 \in \mathbb{Z}$. Likewise b divides c because $12 = 6 \cdot 2$ and $2 \in \mathbb{Z}$. Note however that $ab = 24$ and 24 does not divide 12 because $12 = 24 \cdot \frac{1}{2}$ and $\frac{1}{2} \notin \mathbb{Z}$.

Now consider $a = 1$, $b = 2$, and $c = 8$. Then $a, b, c \in \mathbb{Z}$. Also a divides c and b divides c since $12 = 1 \cdot 12 = 2 \cdot 6$ and $12, 6 \in \mathbb{Z}$. Finally, $ab = 2$ and we already showed that 2 divides 12 since $12 = 2 \cdot 6$ where $6 \in \mathbb{Z}$.

Thus we have two examples of $a, b, c \in \mathbb{Z}$ where a divides c and b divides c. In one case we had ab divide c but in the other case ab did not divide c, which means the conclusion is sometimes true.

0.27 Solution The conclusion is always true. The proof is as follows:

Fix $a, b, c \in \mathbb{Z}$ and assume a divides c and b divides c. Since a divides c then there is some $k \in \mathbb{Z}$ such that $c = ak$. Likewise since b divides c then there is some $j \in \mathbb{Z}$ such that $c = bj$. Hence $c^2 = (ak)(bj) = (ab)(kj)$. Since the integers are closed under multiplication, we know $kj \in \mathbb{Z}$. It follows that ab divides c^2 by the definition of division.

0.28 Solution The conclusion is always true. The proof is as follows:

Fix $x, y \in \mathbb{Q}$ and $a, b, c, d \in \mathbb{Z}$ such that $cy + d \neq 0$. Since $x, y \in \mathbb{Q}$ then we can write $x = \frac{j}{k}$ and $y = \frac{\ell}{m}$ for $j, k, \ell, m \in \mathbb{Z}$ with $k, m \neq 0$. Hence

$$ax + b = \frac{aj}{k} + \frac{bk}{k} = \frac{aj + bk}{k}$$
$$cy + d = \frac{c\ell}{m} + \frac{dm}{m} = \frac{c\ell + dm}{m} \neq 0$$

In order for $cy + d = \frac{c\ell + dm}{m} \neq 0$ to hold, we must have that $c\ell + dm \neq 0$. Furthermore, we have that $k \neq 0$, so $(c\ell + dm)k \neq 0$. Now observe that:

$$\frac{ax + b}{cy + d} = \frac{\frac{aj+bk}{k}}{\frac{c\ell+dm}{m}} = \frac{(aj + bk)m}{(c\ell + dm)k}$$

We know $(aj + bk)m \in \mathbb{Z}$ and $(c\ell + dm)k \in \mathbb{Z}$ because integers are closed under addition and multiplication. We already established that $(c\ell + dm)k \neq 0$. Thus by the definition of rational numbers, we can indeed conclude that $\frac{ax+b}{cy+d} = \frac{(aj+bk)m}{(c\ell+dm)k} \in \mathbb{Q}$.

Solutions to Chapter 1.1 Exercises

1.1 Solution

(a) 'if n is even and n is prime then $n = 2$.' This is true for all values of $n \in \mathbb{N}$. Fix $n \in N$ and suppose n is even and prime. Since n is even then $n = 2k$ for some $k \in \mathbb{Z}$. Assume for the sake of contradiction that $n \neq 2$. Then $k \neq 1$ hence either $k \leq 0$ or $k \geq 2$. If $k \leq 0$ then $n \leq 0$ so n can't be prime, which is a contradiction. If $k \geq 2$ then since $n = 2k$, we know that n has a factor (namely k) other than 1 and itself, so n isn't prime. We have arrived at a contradiction, thus we can conclude that $n = 2$.

(b) 'n is prime and doesn't equal 2 only if n isn't even.' This is true for all values $n \in \mathbb{N}$. Let $n \in \mathbb{N}$ and assume n is prime and $n \neq 2$. Now suppose for the sake of contradiction that n is even. Well now we have that n is prime and that n is even, so from part (a) we get that $n = 2$. This is a contradiction since we assume $n \neq 2$, thus we can conclude that n is even as desired.

Note: You can also prove this without relying on part (a), the proof would likely involve casing on values of n (or of k where $n = 2k$) as was done in the solution to (a).

(c) 'n isn't even or n isn't prime or $n \neq 2$'. This is true for some values of n and false for other values of n. Specifically, it is true for $n \in \mathbb{N}$ where $n \neq 2$ because then '$n \neq 2$' is true so the entire statement becomes true. However when $n = 2$ then 'n isn't even' is false (because $2 = 2 \cdot 1$ where $1 \in \mathbb{Z}$), and 'n isn't prime' is false, and '$n \neq 2$' is false, so the statement as a whole is false.

(d) 'n is even and n is prime and $n \neq 2$'. This statement is false for all $n \in \mathbb{N}$. Suppose for the sake of contradiction that there is some $n \in \mathbb{N}$ such the statement was true. It follows that n is prime and that n is even. The only even prime number is 2 (as shown in part a), so this would imply $n = 2$. However, we know from our assumption that $n \neq 2$. This is a contradiction. Thus the statement is always false.

1.3 Solution

(a) True: We can rewrite 'q being false is necessary for p to be true' as '$(\neg q)$ is necessary for p' which (looking at the table in the implications section if necessary) becomes $p \implies (\neg q)$. We were given that this is true.

(b) False: We can rewrite 'q being false is sufficient for p to be true' as '$(\neg q)$ is sufficient for p' which is equivalent to $(\neg q) \implies p$. We were given that this was false.

(c) False: We can rewrite 'p being true is necessary for p to be false' as 'p is necessary for $(\neg p)$', which is equivalent to $(\neg p) \implies p$. Finally, recall that in general an implication $a \implies b$ will only be false when a is true and b is false. So the fact that $(\neg q) \implies p$ is false implies that p is false. This means $(\neg p)$ is true so that $(\neg p) \implies p$ is false.

(d) True: 'p being true is sufficient for p to be false' can be rewritten as 'p is sufficient for $(\neg p)$' which is equivalent to $p \implies (\neg p)$. As established in part c, we know p is false, so then the implication $p \implies (\neg p)$ is true.