Discrete Math: COMP 201

T. V. H. Prathamesh

July 2023

"*Logic takes care of itself; all we have to do is to look and see how it does it.*"
Ludwig Wittgenstein

1 Introduction

Let us assume that we are building mathematics from scratch. Assume that you have to teach mathematics to an alien ignorant of the ways of mathematics (or even numbers) but sound in logic, or worse you have to teach it to a machine made up of digital circuits. How would we do it?

We can assume that the alien has a conceptual understand of about 'sets'. To know what a set is, does not require us to know any mathematics apriori (meaning beforehand). But we need to verify, what the alien knows about sets is what we know about it too.

How would we start with it?

1.1 Logic

We begin with logic. We assume that we know if every statement (at least any statement of any interest to us) is either true or false. We further know that every logical statement can be written using a symbol. Let us assume the symbols can come from any alphabet such as P, Q, R...

We can also assume that we can put two of these statements together and create more (complex) statements. This act of putting together two or statements is achieved using the connectives: and, or, implies. We represent them symbolically by using $\wedge$ (and), $\vee$ (or), and $\rightarrow$ (implies) respectively. Thus if P and Q are statements, then $P \wedge Q$, $P \vee Q$, and $P \rightarrow Q$ are also statements. So are $P \wedge (Q \vee P)$ and on.

Truth of these compound statements can be determined by following laws:

Rules

1. $P \wedge Q$ is true, only when both P and Q are true.
2. $P \vee Q$ is true, when either P is true, or Q is true.
3. $P \to Q$ is true, if when P is true, Q is also true.

To elaborate on the above example, if P is false, the statement $P \to Q$ holds true regardless of whether Q is true or false. To illustrate this, consider the example: ”*if* sun rises in west, *then* Sri city is a hub of winter sports”, or ””*if* Krea is in Goa, *then* the president of India is Draupadi Murmu.” One can see that in the first instance cited above, the premise is false and the conclusion is false too. In the second instance, the premise is false and the conclusion is true. It is interesting to note that both these statements are true. This stems from the idea that if our assumptions are flawed ,it would be valid to conclude any statement (true or false) from . To elaborate on the above by means of examples:

Examples

1. If I am the king of France, then Ulaan Bator is the capital of Denmark.
2. If I am the king of France, Paris is the capital of France.
3. If 1+1=3, then earth revolves around the sun.
4. If 1+1=3, then sun revolves around the earth.
5. If there is smoke on the hill, there is fire.
6. If 2+2 = 4, then 2+2 = 4.
7. If the world is round, then the sky is blue.

As an exercise, let us figure out which of the following statements are valid:

Exercise

1. If 3 is a prime, then 6 is not a prime.
2. If 4 is a prime, then 6 is a prime.
3. If 4 is a prime, then 6 is not a prime.
4. If 3 is a prime, then 6 is a prime.

Another exercise to ensure that we understood the idea well enough. You are free to assume that the term capital here means the current capital of India:

Exercise

1. If Delhi is the capital of India, then the Parliament is in Delhi.
2. If Delhi is the capital of India, then Gateway of India is in Delhi.
3. If Chennai is the capital of India, then Parliament is in Chennai.
4. If Chennai is the capital of India, then India Gate is in Delhi.

Now that we clarify the meaning of our terms, we can now turn our attention to another logical operation. Associated to every statement (say P) is a statement, which is the **negation** of the statement, denoted by $\neg P$. The truth table for the negation can be understood in terms of the following statements:

P	$\neg P$
T	F
F	T

We now turn our attention to the semantics of the negation operation.

Semantics refers to meaning associated to terms. Given any language, two things are fundamental to it: syntax and semantics. Syntax specifies the grammatical rules for the language and semantics discusses how the terms of the language are associated with the objects and ideas they refer to.

In terms of the meaning of the operation, negation of a statement is true whenever the original statement is false and vice versa. For instance, given the statement ”cat is black”, it is negated by the sentence ”cat is not black”. Similarly one might want to negate the statement ”world is flat.” To show that this statement is false, it suffices to state that ”world is not flat.” It does not require us to state that word is not spherical. One must observe that negation is not the same as opposite. As an exercise, we attempt to negate the following sentences:

Exercise

1. I am not crying. There are two ways of stating this. One way is to state that you are indeed crying, and the other is to state that you are not not crying.
2. p is greater than 0. This statement is false, when p is not greater than 0. This is true whenever $p \leq 0$.
3. Square of the number n is divisible by a prime.
4. We are in the classroom and we are trying to stay awake.
5. We are not the classroom and we are trying to stay awake.
6. x is less than 4 and greater than or equal to 5.
7. We are in the classroom or we are trying to stay awake.
8. If I am in the classroom, then I am trying to stay awake.
9. I am trying to stay awake because I am in the classroom.
10. If p is an odd number, then 2 does not divide p.
11. 4 does not divide p, because p is a prime.

Consider some of the the statements above:

- We are in the classroom **and** we are trying to stay awake.
- x is less than 4 **and** greater than or equal to 5.

Both the statements above are in the form $P \wedge Q$. These statement holds true when both of them holds true, and is false when either of them is false. Thus it's negation should be true, when either of them is false, and false when both of them are true. One can notice that statements of the form $\neg P \vee \neg Q$ satisfy these conditions. We can see why this is the case, by the means of a truth table below:

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

One can see above that $\neg(P \wedge Q)$ is true if and only if $(\neg P \vee \neg Q)$ is true, and $\neg(P \wedge Q)$ is false if and only if $(\neg P \vee \neg Q)$ is false. Thus we can write $\neg(P \wedge Q) \longleftrightarrow (\neg P \vee \neg Q)$. Thus the negation of the two statements mentioned above can be written as:

- We are **not** in the classroom **or** we are **not** trying to stay awake.

- x is **not** less than 4 **or** x **is not greater than or equal to** 5.

If we observe closely at what we did above, we converted one formula into another, by looking at how they return the same value, for the same choice of evaluation of the variables involved. If a formula $F_1 \longleftrightarrow F_2$, then we can write $F_1 \equiv F_2$. A few examples cited below:

Rules

1. $\neg(P \wedge Q) \equiv (\neg P \vee \neg Q)$.
2. $\neg(P \vee Q) \equiv (\neg P \wedge \neg Q)$.

The above two are called **De Morgan's** laws for Boolean Algebra. We further add more statements to the list. We leave it to the reader to verify their correctness as exercises:

Exercises

- $\neg(\neg P) \equiv P$
- $(P \vee Q) \wedge R \equiv (P \wedge R) \vee (Q \wedge R)$.
- $(P \wedge Q) \vee R \equiv (P \vee R) \wedge (Q \vee R)$.
- $P \rightarrow Q \equiv (\neg P \vee Q)$
- $(P \rightarrow Q) \equiv (\neg Q \rightarrow \neg P)$

We now ask the reader to frame a few sentences corresponding to the above statements, to see how the symbols translate into the semantics. To cite the case of the second example: ”A student is in the classroom or in zoom, and the instructor is in classroom” is the same as ”A student is in the classroom and the instructor is in the classroom, or the student is in zoom and the instructor is in the classroom.” Note that there is a subtlety which distinguishes this from $P \vee (Q \wedge R)$. Can you convince yourself, which this is the case? The last of the statements above is particularly interesting, since it tells us that if P implies Q, then negation of Q implies the negation of P. Testing the same on a few examples:

Examples

- If India is a democracy, then there are elections in India.
- If there are no elections, then India is not a democracy.
- If sky is green, then earth is round.
- If the earth is not round, then the sky is not green.

While we are on statements, we take a brief detour to discuss statements which are always true. Such statements are called *Tautologies.* For instance, it will either today or it won't. Such a statement is always true because it encapsulates all the possibilities. Another example would be if that is the case, then it is the case. To write down these in terms of formal symbols, we obtain the following:

- $P \vee \neg P$
- $P \to P$
- $(P \to Q) \to (Q \to R) \to (P \to R)$
- $P \wedge Q \to P$
- $Q \wedge P \to P$
- $P \to (P \vee Q)$
- $(P \wedge (P \to Q)) \to Q$

One may note that the sentences listed above are illustrative, but by no means exhaustive of the list of tautologies.

Exercises

1. Check that the above statements always return the value True, regardless of the value of the variables involved.
2. Write two sentences corresponding to the last of the tautologies listed.

Since there exist statements, which are always true, regardless of the values that the variables assume, it follows that there are statements which are always false. One way to obtain them is by negating the statements which are always true. For instance, ”It will rain today or it will not rain today” negates to ”It will not rain today and it will rain today”. This is a logical impossibility. This is formally a contradiction. Contradiction formally means it is a compound statement, which is a conjunction of a statement and it's negation. For the case considered here, it is $P \wedge \neg P$.

1.1.1 Algebra of logic

In the section above, we deduced that to show logical equivalence between two formulae, we draw truth tables, and then show that for a given assignment of values to variables, the formulae return the same value. These are the building blocks of formulae. But it can also be derived from substituting appropriate terms in a previously proved equivalence (either by truth tables or by substitution). Consider the following equality:

$$\neg(P \to Q) \equiv (P \land \neg Q)$$

This can be proved along the following lines:

1. $(P \to Q) \equiv (\neg P \lor Q)$ [Derived Before]
2. $\neg(\neg P \lor Q) \equiv (\neg(\neg P) \land (\neg Q))$ [By substituting eq(1)]
3. $(\neg(\neg P) \equiv P$ [Derived before]
4. $(\neg(\neg P) \land (\neg Q)) \equiv P \land \neg Q$ [Substituting (3) in (2)]
5. Thus proved. [From 2 and 4]

1.2 Logic With Quantifiers

If one notices, the statements made earlier were possible to discuss simple declarations, which spoke about a specific object (”cat is black”, ”earth is spherical”,...), but logic also deals with statements which make claims about multiple objects at the same time. For instance : All swans are black, all chairs have four legs, ChatGPT is mostly wrong, maths can be fun at times, sun never rises in the east. Reasoning about such statements is a little more complicated. For instance consider the following statements:

- All swans are black.
- Some swans don’t like hilsa.

What can we infer about black objects from above? Maybe that all black creatures don’t like hilsa? Definitely not. Since there maybe black creatures other than swans which like hilsa. But can we infer that some black objects don’t like hilsa? Definitely! Because some of the black objects are swans, and some swans don’t like hilsa.

Nothing that we learnt so far in terms of logic, enables us to make inferences of this kind. We thus need to specify the inference that we make here. In order to make such inferences, we need to look a little deeper inside the sentences. We concern ourselves to two kinds of qualifiers about quantities of objects. First is ”For all”, and the other is ”There exists”. We claim that these two suffice, because the first considers statements which makes a universal claim about all objects under consideration, and the second assets existence of an objection and contains with it the qualifier some. Consider the following sentences:

Examples

1. All men are mortal.
2. All beedles are tweedledums.

3. All triangles have three edges.
4. There exists a planet which is not round.
5. There exists an odd number, which is not prime.
6. There exists a triangle in which all sides are not equal.

We can see that in the first three statements, we explicitly or implicity use the term ”for all”, in the latter, we use the term ”there exists”. We further introduce the notation In the cases, these terms are more or less explicitly used. We look at some examples, where such qualifies are more implicit. As an exercise, identify the quantifiers used in the following examples:

Examples

- Every chair in this class has at least four legs.
- I can find a bored student in this room.
- There is a prime number p, such that $p + 2$ is prime.
- This program does not work on a particular case.
- For all inputs, this program is correct.
- Not everyone in the class is keen to watch Oppenheimer.
- No one wants to skip their lunch break to attend a lecture.
- There is a person who wants to skip lunch break for a lecture.

For reasons of brevity and precision in logical arguments, it often makes sense to symbolically encode statements of this form and use formulae to talk about them. First thing we notice is that every state above is of either of the following forms:

”**For every** x, x has the property P”
”**There exists** an x, x has the property P”

We use the symbols ($\forall$) to denote **“for all”**, and ($\exists$) to denote **“there exists.”** They are also referred to as universal quantifier ($\forall$) and existential quantifier ($\exists$) respectively. Further we introduce the abstraction of a property. Using these symbols, we can rewrite statements in a more concise symbolic form, illustrated as below:

”All elements are greater than 0”,	$\forall x.\ x > 0$
”Not all elements are equal to each other”,	$\neg(\forall x.\forall y.\ x = y)$
”Everything is impermanent.”	$\forall x.\ impermanent(x)$
”Everything is not permanent.”	$\forall x.\ \neg permanent(x)$
”All things red are visible.”	”$\forall x.\ red(x) \to visible(x)$

We consider similar statements with respect to existential quantifiers:

”There exists an element, less than 0”,	$\exists x.\ x < 0$
”There exist elements, which are equal to each other”,	$(\exists x.\exists y.\ x = y)$
”Something is impermanent.”	$\exists x.\ impermanent(x)$
”Something is not permanent.”	$\exists x.\ \neg permanent(x)$
”Some things red are invisible.”	”$\forall x.\ red(x) \to invisible(x)$
”Nothing travels faster than speech of light.”	”$\neg\exists x.\ fasterthanlight(x)$

1.2.1 Negating Quantifiers

So far, we noticed that we negated statements which do not involve quantifiers. How do we negate statements which have quantifiers in them? Consider the following statements:

1. All swans are white.
2. There does exist a swan which is magenta.

Negating the first statement involves conjuring up the possible situations, when the first statement is false. The statement is precisely false, when there exists a swan which is not white. This can be summed up in the following rule:

Rules

$$\neg(\forall x.P(x)) \equiv \exists x.\neg(P(x))$$

On a similar note, the claim that there exists a swan which is magenta, is negated by the assertion that all swans are not magenta. In formal language, this idea is written as:

Rules

$$\neg(\exists x.P(x)) \equiv \forall x.\neg(P(x))$$

Exercises

Negate the following sentences:

1. $\forall x.\ (\not P(x))$
2. $\exists x.\ (\not P(x))$

3. $\forall x.\exists y.\ x < y.$

4. $\exists y.\ \forall x.\ x < y.$

5. $\forall \epsilon.\ \exists \delta.\ (x - y < \delta) \implies (f(x) - f(y)) < \epsilon$

1.2.2 More Rules and Common Mistakes

In order to reason with quantifiers, we begin by noting that quantifiers are very subtle objects and need to be carefully used. First and foremost, we can observe that we can use multiple quantifiers in a single statement. . Consider the following set of statements:

- For every student, there exists a seat such that student can sit on the seat.
- There exists a seat, such that every student sits on the seat.

First asserts that that each student gets a seat, second hints at the fact that there is a seat on which all the students sit on it. Consider this in context of mathematics.

- For every natural number n, there exists a natural number m, such that $n < m$.
- There exists a natural number m, such for every natural number n, $n < m$.

First tells you that every natural number is less than some other natural number. Second (erroneously) claims that some natural number is larger than all others. Thus the order of $\forall$ and $\exists$ **cannot** necessarily be interchanged. The order matters.

Another common misconception is in use of negation along with quantifiers.

1. For all things, they can never move as fast as light.
2. Not all things can move at the speed of light.
3. There exists a person, who does not enjoy this lecture.
4. There does not exist a person, who enjoys this lecture.

If we notice, the first statement and second statements are distinct. The first statement asserts that nothing can move as fast as light. Second tells us that, not all the things move at the speed of light, it admits the possibility that some things may move at the speed of the light as long as there are things that don't, while the first statement does not allow such a possibility since it explicitly makes a claim on all things. Similarly, the third statement claims that someone does enjoy this lecture. While the fourth asserts that no on enjoys this lecture by denying the existence of a person who enjoys the lecture. Thus the third and fourth are distinct statements. Thus negation of a quantifier, is not the same as negation of the property bound to the quantifier. Negation cannot be interchanged with a quantifier.

To cite it more formally:

Rules

- $\forall x.\ \neg P(x) \neq \neg(\forall x.\ P(x))$.
- $\exists x.\ \neg P(x) \neq \neg(\exists x.\ P(x))$.

Remark: One may infact notice the following set of equalities actually hold true:

- $\exists x.\ \neg P(x) = \neg(\forall x.\ P(x))$.
- $\forall x.\ \neg P(x) = \neg(\exists x.\ P(x))$.

We now look at another subtlety, which involves using quantifiers to argue about using quantifiers in conjunction with other operators:

1. It is true for all students, that a student are a classroom now and will have lunch later.
2. It is true for all students, that a student is in a classroom now, and it is true for all students that a student will have lunch later.
3. It is true for all students, a student will be in classroom, or a student will have lunch later.
4. It is true for all students, that a student will be in classroom now, it is true for all students that a student will lunch later.

The first statement asserts that every student is in a class, and will have lunch later. This is equivalent to the the second statement that all students are in classroom now and all students will have lunch later. This owes itself to the fact that all students have the property $PandQ$. Thus all students have property P and all students have property Q. But when we talk about all students either being in classroom now or having lunch later, is not equivalent to stating that all students are in classroom now or will have lunch later. Thus:

Rules

- $\forall x.\ (P(x) \wedge Q(x)) = ((\forall x. P(x)) \wedge (\forall x.\ Q(x)))$.
- $\forall x.\ (P(x) \vee Q(x)) \neq ((\forall x. P(x)) \vee (\forall x.\ Q(x)))$.

As an exercise, convince yourself of the following statements. Note that the order is reversed here:

Exercises

1. $\exists x.\ (P(x) \wedge Q(x)) \neq ((\exists x.\ P(x)) \wedge (\exists x.\ Q(x)))$.
2. $\exists x.\ (P(x) \vee Q(x)) = ((\exists x. P(x)) \vee (\exists x.\ Q(x)))$.

Last of them deal with quantifiers to be used in association with implication:

- It holds for everyone, that if the person is a vegan they may not be interested in cheeses.
- If everyone is a vegan, then everyone is not interested in cheese.

Note that these two are distinct statements. First of the two statements may imply the second (why?), but not the other way around.

Exercises

What happens to $\exists x. P(x) \rightarrow Q(x)$?

1.3 Sets

Having agreed upon a definition of logic, we are in a position to construct objects of mathematics. In this section, we will see how the most common objects that we know, can be constructed from sets.. We will not formally define, but consider the set to be an 'undefinable' object that we know intuitively to denote a collection of objects. For instance, a collection of students in a classroom is a set of students in a classroom. Equally we can write set of trees in a university campus, or a set of humans on planet, or set of cars in a country. One may note that a set cannot contain multiple copies of the same object. (For instance: $\{a, a\}$ is not a set.

Given an object and a set, either the object belongs to the set or does not. We use the following notation to denote it:

$$x \in S$$

We interpret this to mean,the object x belongs to the set S. Along with the above, we further introduce the following notations in our language of logic:

$$\forall x \in S. P(x)$$

This denotes the fact that for all elements of S, $P(x)$ holds. We can additionally write,

$$\exists x \in S. P(x)$$

This denotes the fact that there exists an element of S, for which $P(x)$ holds. Additionally. we use the notation:

$$x \notin S$$

To denote that x does not belong to S. One may note that:

$$(x \notin S) \equiv \neg(x \in S)$$

Now we may wish to know how to list out particular elements. We have two ways of doing so.

1. Extensional: We enumerate all the objects of the set.

$$C = \{COMP\ 201, COMP\ 203\}$$

$$S = \{Andhra\ Pradesh, Telangana, Tamil\ Nadu, Kerala, Karnataka\}$$

2. Intensional: We will specify a set by the common property that all the elements of the set share.

$$C = \{x \mid x\ is\ a\ CS\ compulsory\ course\ this\ trimester.\}$$

$$S = \{x \mid x\ is\ a\ province\ in\ south\ India\}$$

One may note that the extensional set as defined above by listing out all the elements, works only for finite sets. There are sets that are potentially infinite (assume the family tree of someone in a universe which never comes to an end). In such a case, the explicit way of specifying all the elements of a set is through the use of recursion. Consider the following cases:

- $Adam \in X$.
- $(x \in X) \rightarrow (ChildOf\ x) \in X)$.

This set will contain infinite elements, $Adam$, $ChildOf\ Adam$, $ChildOf\ ChildOf\ Adam$,...

- $Today \in S$
- $(x \in S) \rightarrow (Day_after_tomorrowx) \in S)$.

This set will contain again infinite elements (assuming that earth perpetually moves around the sun), Today, Day After Tomorrow, Day after day after tomorrow and on.

Give the above, we will now make explicit certain assumptions about sets.

Rules

1. Two sets are equal, if and only if they contain the same elements.
2. There exists a set with no elements that we call the empty set ($\emptyset$).
3. Given a set A and a property P, there exists a set B, such that
$$B = \{x \in A | \; P(x)\}$$
4. Given two sets A and B, there exists a set which contains both A and B as elements.
5. Given a set A, there exists a set of all subsets of A. We call this power set and denote it by $P(A)$.
6. Given a set of sets $X = \{A, B, ...\}$, where A, B and all other elements of X are sets, there exists a set Y, which consists of elements of each of the sets.
7. There exists an infinite set.

The rules are by no means exhaustive, infact we explicitly omit three, one for reasons of pedagogy, and the other will be introduced later. We may not strictly abide by the rules here, but will use them as a guiding map.

We are now in a position to formally introduce set theoretic constructions:

Definition

Definition 1. $A \cup B = \{x \mid x \in A \vee x \in B\}$

We refer to the above as the **union** of A and B.

Definition

Definition 2. $A \cap B = \{x \mid x \in A \wedge x \in B\}$

We refer to the above as the **intersection** of A and B.

Definition

Definition 3. $A^c = \{x \mid x \notin A\}$

We refer to the above as the **complement** of A.

Definition

Definition 4. $A \setminus B = \{x \in A \mid x \notin B\}$

We refer to the above as the difference of two sets A and B.

Definition

Definition 5. $A \subseteq B \equiv (\forall x \in A,\ x \in B)$

We refer to A as the subset of B. This relationship can be both strict if B is not a subset of A.

Definition

Definition 6. $A \subset B \equiv (A \subseteq B) \wedge (A \neq B)$

We refer to A as the subset of B. This relationship can be both strict if B is not a subset of A.

Given that we got definitions, out of the way, we are in a position to venture into the domain of mathematical proofs. We begin by stating a few results and proving them:

Theorem 1.

$$A \cup A = A$$

Proof

Proof. From the definition of union, we have the following:

$$A \cup A = \{x \mid x \in A \vee x \in A\}$$

Note that $x \in A \vee x \in A =\ x \in A$ follows from the logical assertion that $P \vee P = P$. Thus it follows that:

$$A \cup A = \{x \mid x \in A\}$$

But the R.H.S is the definition of A. Thus is follows that:

$$A \cup A = A$$

□

Exercises

Prove that $A \cap A = A$.

Theorem 2. $(A \subseteq B) \wedge (B \subseteq A) \longleftrightarrow (A = B)$

Proof

Proof. This statement is of the form: $P \longleftrightarrow Q$. In order to prove a statement of this form, it suffices to prove $P \to Q$ and $Q \to P$. Thus we prove the following statements:

1. $(A \subseteq B) \wedge (B \subseteq A) \longrightarrow (A = B)$: We assume $(A \subseteq B) \wedge (B \subseteq A)$ and prove $A = B$. In order to prove $A = B$, or in general to prove two sets are equal, we rely on the axiom (1) of sets stated above, which says that two sets are equal if and only if they contain the same elements. This is formally stated as follows:

   $$(\forall x \in A.\ x \in B) \wedge (\forall x \in B.\ x \in A)$$

   Now from the assumption that $A \subseteq B$ and the definition of a subset, it follows that:

   $$\forall x \in A.\ x \in B. \tag{1}$$

   Similarly from the assumption the assumption that $B \subseteq A$, and the definition of a subset, it follows that:

   $$\forall x \in B.\ x \in A. \tag{2}$$

   From 1 and 2, it follows that:

   $$(\forall x \in A.\ x \in B) \wedge (\forall x \in B.\ x \in A) \tag{3}$$

   From the definition of equality of sets, stated above, it follows that $A = B$.

2. $A = B \to (A \subseteq B) \wedge (B \subseteq A) \longrightarrow (A = B)$: It follows from the definition of equality of sets, that:

   $$(\forall x \in A.\ x \in B) \wedge (\forall x \in B.\ x \in A) \tag{4}$$

   Thus it follows that:

   $$(\forall x \in A.\ x \in B) \tag{5}$$

   $$(\forall x \in B.\ x \in A) \tag{6}$$

   Thus it follows from 5 and definition of a subset that $A \subseteq B$. Similarly it follows from the definition of 6 and the definition of a subset, that $B \subseteq A$. Thus we have

   $$(A \subseteq B) \wedge (B \subseteq A)$$

□

We now proceed to the proving the following theorem, which is a tad more complicated but instructive on how to proceed with proofs of statements.

Theorem 3. $((A \cap B) \cup C) = ((A \cup C) \cap (B \cup C))$

Proof

Proof. In this statetement we have to prove equality of two sets. From Theorem (2), that it suffices to prove the following:

1. $(A \cap B) \cup C \subseteq (A \cup C) \cap (B \cup C)$
2. $(A \cap B) \cup C \subseteq (A \cup C) \cap (A \cup C)$

Note that this is a fairly useful tactic and will be used extensively in all proofs of equality of sets here on, that is to show equality of two sets we will show that each of them are a subset of another. We will now attempt to prove the following:
To Prove: $(A \cap B) \cup C \subseteq (A \cup C) \cap (B \cup C)$ In order to show that one set (say X)is a subset of another (Y), the general strategy is to show that any arbitrary element of X belongs to Y. We will adopt the same here. Consder a fixed but arbitrary element a such that:

$$a \in ((A \cap B) \cup C) \tag{7}$$

. It follows from the definition of union of sets that:

$$(a \in (A \cap B)) \vee (a \in C) \tag{8}$$

It further follows from the definition of intersection of sets, that:

$$((a \in A) \wedge (a \in B)) \vee (a \in C) \tag{9}$$

Note that the equation here is of the following logical form:

$$(P \wedge Q) \vee R$$

From Boolean algebra, we know that:

$$((P \wedge Q) \vee R) \equiv (P \vee R) \wedge (Q \vee R)$$

Thus we can rewrite 9 as the following:

$$((a \in A) \vee (a \in C)) \wedge ((a \in B) \vee (a \in C)) \tag{10}$$

It thus follows from above and the definition of union that:

$$(a \in (A \cup C)) \wedge (a \in (B \cup C)) \tag{11}$$

It thus follows from above and the definition of intersection that:

$$(a \in ((A \cup C) \cap (B \cup C)) \tag{12}$$

Since a was a fixed but arbitrary element of $(A \cap B) \cup C$, it follows that:

$$\forall x \in (A \cap B) \cup C.\ x \in ((A \cup C) \cap (B \cup C))$$

From the definition of a subset, it follows that:

$$((A \cap B) \cup C) \subseteq ((A \cup C) \cap (B \cup C)) \tag{13}$$

It thus remains **to prove** the following subset relation:

$$((A \cup C) \cap (B \cup C)) \subseteq ((A \cap B) \cup C)) :$$

In a manner similar to the proof of the earlier statement, we show that any arbitrary element of $((A \cup C) \cap (B \cup C))$ belongs to $((A \cap B) \cup C))$. Consider a fixed but arbitrary element a such that:

$$a \in ((A \cup C) \cap (B \cup C)) \tag{14}$$

. It follows from the definition of intersection of sets that:

$$(a \in (A \cup B)) \wedge (a \in (C \cup B)) \tag{15}$$

It further follows from the definition of union of sets, that:

$$((a \in A) \vee (a \in C)) \wedge ((a \in B) \vee (a \in C)) \tag{16}$$

Note that the equation here is of the following logical form:

$$(P \vee Q) \wedge (Q \vee R)$$

From Boolean algebra, we know that:

$$(P \vee R) \wedge (Q \vee R) \equiv ((P \wedge Q) \vee R)$$

Thus we can rewrite 16 as the following:

$$((a \in A) \wedge (a \in B)) \vee (a \in C) \tag{17}$$

It thus follows from above and the definition of intersection that:

$$((a \in (A \cap B) \vee (a \in C)) \tag{18}$$

It thus follows from above and the definition of union that:

$$(a \in ((A \cap B) \cup C)) \tag{19}$$

Since a was a fixed but arbitrary element of $((A \cup C) \cap (B \cup C))$, it follows that:

$$\forall x \in ((A \cup C) \cap (B \cup C)).\ x \in ((A \cap B) \cup C)$$

From the definition of a subset, it follows that:

$$((A \cup C) \cap (B \cup C)) \subseteq ((A \cap B) \cup C)$$

Since we proved the subset containment both ways, it follows from the previous set and the 13 that:

$$((A \cap B) \cup C) \ = \ ((A \cup C) \cap (B \cup C))$$

□

A similar related theorem, which is fundamental to set theory happens to be the following:

Theorem 4. $((A \cup B) \cap C) = ((A \cap C) \cup (A \cap B))$

Proof

Proof. We leave the proof of this as an exercise for the reader. However, as a hint recall the following result:

$$(P \vee Q) \wedge R \equiv (P \wedge R) \vee (Q \wedge R) \tag{20}$$

□

Theorem 5.

$$(A \cup B)^c = (A^c \cap B^c)$$

Proof

Proof. From the definition of union, we have the following:

$$A \cup B = \{x \mid x \in A \vee x \in B\}$$

It follows from here that

$$x \notin (A \cup B) \equiv \neg(x \in A \vee x \in B)$$

From the logical assertion that $\neg(P \vee Q) = \neg P \wedge \neg Q$, it follows that: u

$$x \notin (A \cup B) \equiv \neg(x \in A) \wedge \neg(x \in B)$$

$$x \notin (A \cup B) \equiv (x \notin A) \wedge (x \notin B)$$

From the definition of complement, it follows that:

$$(A \cup B)^c = \{x \mid x \notin (A \cup B)\}$$

From the statement earlier, it follows that:

$$(A \cup B)^c = \{x \mid (x \notin A) \wedge (x \notin B)\}$$

By applying the definition of complement on the right hand side, it follows that:

$$(A \cup B)^c = \{x \mid (x \in A^c) \wedge (x \in B^c)\}$$

The R.H.S is equal to $A^c \cap B^c$. Thus it follows that:

$$(A \cup B)^c = A^c \cap B^c$$

□

Exercises

Prove that:

$$(A \cap B)^c = (A^c \cup B^c)$$

We end this with a proof involving subsets:

Theorem 6. *$A \subseteq B$ and $B \subseteq C$ implies $A \subseteq C$.*

Proof

Proof. To prove that $A \subseteq C$, it suffices to prove that given any element of A, it is a member of C. Let X be a fixed but arbitrary member of A. Now since $A \subseteq B$, it follows that $x \in B$. Since $B \subseteq C$ and $x \in B$, from the definition of subset, it follows that $x \in C$. Since x was an arbitary element, it follows that every element of A belongs to C. Thus it follows that $A \subseteq C$. □

Exercises

Prove that $A \subseteq C$ and $B \subseteq C$, implies $A \cup B \subseteq C$.

In the above examples, we looked at true claims. **How do we prove that a certain claim is not true? or rather disprove a claim?** We illustrate it using the following example: Consider the claim:

$$A \subset (B \cup C) \to (A \subset B) \vee (A \subset C)$$

To disprove this claim, it suffices to show a single example where this does not occur. This is called a counter example. Consider the following candidates for A, B and C:

$$A = \{a, c\}, B = \{a, b\}, C = \{c, d\}$$

One may notice that:

$$\{a, c\} \subseteq \{a, b, c, d\}$$

But A is not a subset of B or C. Thus it follows that:

$$\neg(A \subset (B \cup C) \to (A \subset B) \vee (A \subset C))$$

We end the section by writing a last definition, the definition of a power set of a set:

Definition

Definition 7. *Power set of a set A is the set of all subsets of A.*

$$P(A) = \{X | X \subseteq A\}$$

Exercises

1. Prove that for a set A:
$$(A^c)^c = A$$
2. Write the power set of the set $\{a, b, c, d, e\}$.
3. Write the power set of the set $\{a, b, \{a, b\}\}$.
4. Write the power set of the set $\{a, b, \{a, b\}, \{c\}\}$.

1.4 Constructing Natural Numbers

We are now ready to begin constructing natural numbers from the toolkit developed so far. Importance of this exercise, is not merely because it is an interesting foundational question, but also because it teaches us how to use a rather limited toolkit to encode more complex ideas, a challenge for any programmer or computer scientist . To revisit our toolkit, notice that our toolkit contains sets, axioms for sets, subsets, union of sets, complements of sets, and intersection of sets. In order to construct numbers, each number has to be encoded as a set. But the question arises, which set do we choose to represent each number as a set? The set used to define a number, cannot be made up of real world objects, since mathematics is used to make statements about the real world and not the other way around. It cannot refer to other number either. So the question is what sets do we have at our disposal to construct natural numbers?

Notice that while we discussed quote a few properties of sets and constructions from the sets, the only set whose precise existence can guaranteed from all that we stated far is the empty set, which follows from the second rule cited above. But a empty set by itself is not enough to construct all natural numbers. So let's try and see if we can construct another set. Note that we can try as a candidate, another set. That is $\{\emptyset\}$. Now this may sound paradoxical, since a set consisting of an empty set does not make sense. First and foremost, as an analogy notice that an empty box is different from a box containing containing an empty box. A box containing an empty box is not empty, since it contains an empty box. Further the following property holds in the empty set, but not in $\{\emptyset\}$.

$$P(S) \equiv \forall x.\ x \notin S$$

One can see that $P(\emptyset)$ is true, but $P(\{\emptyset\})$ is not, since $\emptyset \in \{\emptyset\}$. Now consider rule (4), given two sets, we construct a set which contains both the sets, thus we can construct $\{\emptyset, \{\emptyset\}\}$. We can now recursively construct $\{\emptyset, \{\emptyset, \{\emptyset\}\}\}$, and on . Now we are in a position to construct natural numbers:

Definition

Definition 8. ***Natural numbers***, *labelled* $\mathbf{N}$, *are defined by the following rules:*

- $\emptyset \in \mathbf{N}$. *(Note: This corresponds to 0).*
- *If* $n \in \mathbf{N}$, *then* $n \cup \{n\} \in \mathbf{N}$.

Thus we have the natural numbers, we associate a number as per our known convention to each of the numbers thus formed, to cite a few instances, as labelled by the common integers next to them:

0. $\emptyset$
1. $\{\emptyset\}$
2. $\{\emptyset, \{\emptyset\}\}$
3. $\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$
4. $\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}\}\}$
5. $\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}\}\ , \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}\}\}\}\}\}$.

Thus each natural number corresponds to the number of elements , which occur in its construction. It is easy to check that no natural number is equal to another, since each natural number has varying count of elements in the set.This definition was provided by the mathematician-computer scientist-physicist-economist, John Von Neumann.

Now that we have natural numbers, we can now proceed to define addition and multiplication of natural numbers. Now what kind of an object is addition, as we know it? consider a few examples.

- 2+ 1 = 3
- 101+7 = 4

In each of these examples, addition takes two elements and returns one. An object that we know which takes some input elements and returns an output is a function (in mathematics as well as programming). The alien may not know what we mean by functions. So we may need define functions in terms of sets. Additionally, we further want to explain the idea of one number being smaller than other. This is a kind of a relation between numbers. Thus we embark on constructing a series of seemingly abstract set theoretic concepts, which will enable us to define addition and inequality of natural numbers.

Thus we now proceed to define the following:

1. Ordered pair of elements. (also known as tuples)
2. Relations between elements of a set.
3. Functions

2 Relations and Functions

An ordered pair of elements is commonly known and used in informal mathematics especially in the context of co-ordinate geometry, where we write (a, b) to stand for two elements a and b, where a corresponds to first co-ordinate and b corresponds to second co-ordinate. While we define ordered pairs in terms of sets, we need to notice two points under consideration. To illustrate these points, we consider the following example of the graph of average students marks, where we write the batch of the students in x axis, and the average marks on the right axis. The batch number is usually a natural number like 2017, 2018 and on. The average marks can range to hold decimal values. This $(2017, 67.7)$ maybe a graph where the first digit is a natural and the second digit a real number. Further, we note that $(67.7, 2017)$ is not the same as $(2017, 67.7)$. Thus the order matters, unlike in a set, where order of the elements do not matter. To sum this up:

1. Thus ordered pair of elements, can consist of pairs of elements, where each element belongs to a different set.
2. Order of the occurence of elements in a set matters.

Definition

Definition 9. *Given two sets A and B, we define an ordered pair in A and B to be the following element:*

$$(a, b) = \{\{a\}, \{a, b\}\}$$

Note that in the definition above, both the first and the second element can be distinguished. This definition allows us to define the set of all ordered pairs, which we term as product of sets:

Definition

Definition 10. *Product of two sets A and B is defined as the set:*

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

We illustrate this with a few examples:

Examples

- $A = \{a, b\}$, $B = \{1, 2, 3\}$.

$$A \times B = \{(a, 1),\ (a, 2),\ (a, 3),\ (b, 1),\ (b, 2),\ (b, 3)\}$$

- $A = \{a, b, c\}$, $B = \{1, 2\}$.

$$A \times B = \{(a, 1),\ (a, 2),\ (b, 1),\ (b, 2),\ (c, 1),\ (c, 2)\}$$

- $A = \emptyset, B = \{a, b\}$

$$A \times B = \emptyset$$

We define a relation as the following:

Definition

Definition 11. *A relation R is a subset of $A \times A$. Further, we use the notation $a\ R\ b$ to denote that $(a, b) \in R$*

In each of the examples below, R is a relation on A:

Examples

- $A = \{1, 2, 3\}$, $R = \{(1, 1), (1, 2), (2, 3)\}$
- $A = \{1, 2, 3\}$, $R = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 3)\}$

- $A = \{a, b\}$, $R = \{(a, a), (b, b)\}$

Before we define functions, notice that in both mathematics and programming, function corresponds to the idea of an object, which for a given input, returns an output. Two things to observe:

- For every possible input value, functions has to define an output to be well-defined.

- For any given input value, the function has to return a a unique output value. Function cannot return two output values for the same input value.

This idea can be recast in terms of sets.

Definition

Definition 12. *A function f from a set A to a set B is a subset of $A \times B$, such that:*

1. $\forall a \in A.\ \exists b \in B.\ (a, b) \in f$. *(That is, for all elements a of A, there is an element b in B such that f maps a to b)*

2. $\forall a \in A.\ \exists b_1, b_2 \in B.\ (a, b_1) \in f(a, b_2) \in f \to (b_1 = b_2)$. *(For all elements a of A, if f maps a to elements b_1 and b_2, then $b_1 = b_2$. In other words, f maps an element to a single element).*

Notation: *We use $f : A \to B$, to denote the function $f \subseteq A \times B$. Further, we use notation $f(a) = b$, to denote $(a, b) \in f$.*

Consider a few examples of function:

Examples

1. $A = \{1, 2, 3\}$, $b = \{a, b\}$, $f = \{(1, a), (2, a), (3, a)\}$.

2. $A = \{1, 2, 3\}$, $b = \{a, b\}$, $f = \{(1, a), (2, a), (3, b)\}$.

3. $A = \{1, 2, 3\}$, $b = \{a, b\}$, $f = \{(1, a), (2, b), (3, a)\}$.

4. $A = \{1, 2, 3\}$, $b = \{a, b\}$, $f = \{(1, a), (2, b), (3, b)\}$.

5. $A = \{1, 2, 3\}$, $b = \{a, b\}$, $f = \{(1, b), (2, a), (3, a)\}$.

6. $A = \{1, 2, 3\}$, $b = \{a, b\}$, $f = \{(1, b), (2, a), (3, b)\}$.

7. $A = \{1, 2, 3\}$, $b = \{a, b\}$, $f = \{(1, b), (2, b), (3, a)\}$.

8. $A = \{1, 2, 3\}$, $b = \{a, b\}$, $f = \{(1, b), (2, b), (3, b)\}$.

Consider the following exercises:

Exercises

- Represent all the functions above using diagrams.
- Represent all the function in the above example, using the $f(x) = y$, notation.
- Write all the functions possible from the set $\{1, 2, 3\}$ to the set $\{a, b, c\}$.
- Write all the functions possible from the set $\{1, 2, 3\}$ to the set $\{1, 2, 3\}$.
- Write two functions from $f : \mathbf{N} \to \mathbf{N}$, without using addition, multiplication or any other yet to defined operation.
- Which of the following are valid functions. If any of them are invalid, please explain the reason:
  1. $A = \{a, b, c\}$, $b = \{x, y, z\}$, $f = \{(a, x), (a, y), (b, y, (c, z))\}$.
  2. $A = \{a, b, c\}$, $b = \{x, y, z\}$, $f = \{(a, x), (b, y)\}$.
  3. $A = \{a, b, c\}$, $b = \{x, b\}$, $f = \{(a, x), (b, y), (c, x)\}$.
  4. $A = \{a, b, c\}$, $b = \{x, y, z\}$, $f = \{(a, x), (b, y), (c, y)\}$.
  5. $A = \{a, b, c\}$, $b = \{x, y, z\}$, $f = \{(a, x), (b, y), (c, z)\}$.

We want to classify functions (not exhaustively) by observing how they behave on the ambient sets. In order to do so, we first use specific terms for the sets involved in a function definition.

Definition

Definition 13. *Given a function $f : A \to B$, the set A is called the domain and the set B is called the range.*

This provides us terminology to talk about classification of functions in terms of how they behave on the sets. We begin with the functions which do not map more than one element to another.

Definition

Definition 14. *A function $f : A \to B$ is defined to be* injective, *if $\forall x, y \in A.\ f(x) = f(y) \longleftarrow x = y$.*

Examples

Following functions are injective:

- $f : \{1, 2, 3\} \to \{a, b, c, d\}$, where
  - f(1) = a
  - f(2) = b
  - f(3) = c
- $f : \{1, 2, 3\} \to \{a, b, c\}$, where
  - f(1) = a
  - f(2) = b
  - f(3) = c
- $f : \{1, 2\} \to \{a, b, c\}$, where
  - f(1) = b
  - f(2) = a
- $f : \{1, 2\} \to \{1, 2, 3\}$, where
  - f(1) = 3
  - f(2) = 1

Examples

Following functions are **not injective**:

- $f : \{1, 2, 3\} \to \{a, b, c, d\}$, where
  - f(1) = a
  - f(2) = a
  - f(3) = c
- $f : \{1, 2, 3\} \to \{a, b, c\}$, where
  - f(1) = a
  - f(2) = b
  - f(3) = b
- $f : \{1, 2\} \to \{a, b, c\}$, where
  - f(1) = b
  - f(2) = b

- $f : \{1, 2\} \to \{1, 2, 3\}$, where
  - f(1) = 1
  - f(2) = 1

We now define a class of functions of functions, which make sure that every element in the range is mapped on to by some element of f.

Definition

Definition 15. *A function $f : A \to B$ is defined to be* surjective*, if $\forall y \in B.\ \exists x \in A.\ f(x) = y$.*

Examples

Following functions are surjective:

- $f : \{1, 2, 3\} \to \{a, b\}$, where
  - f(1) = a
  - f(2) = b
  - f(3) = b
- $f : \{1, 2, 3\} \to \{a, b, c\}$, where
  - f(1) = a
  - f(2) = b
  - f(3) = c
- $f : \{1, 2\} \to \{a\}$, where
  - f(1) = a
  - f(2) = a
- $f : \{1, 2, 3, 4\} \to \{1, 2, 3\}$, where
  - f(1) = 3
  - f(2) = 1
  - f(3) = 3
  - f(4) = 2

Examples

Following functions are **not surjective**:

- $f : \{1, 2, 3\} \to \{a, b, c\}$, where
  - f(1) = a
  - f(2) = a
  - f(3) = c
- $f : \{1, 2, 3\} \to \{a, b, c\}$, where
  - f(1) = a
  - f(2) = b
  - f(3) = b
- $f : \{1, 2\} \to \{a, b, c\}$, where
  - f(1) = a
  - f(2) = b
- $f : \{1, 2\} \to \{1, 2, 3\}$, where
  - f(1) = 2
  - f(2) = 1

Exercises

1. Given two examples of functions which are neither injective nor surjective.
2. Given an example of a function, which is injective but not surjective.
3. Given an example of a function, which is surjective but not injective.
4. Given two examples of a functions, which are both injective and surjective.

Definition

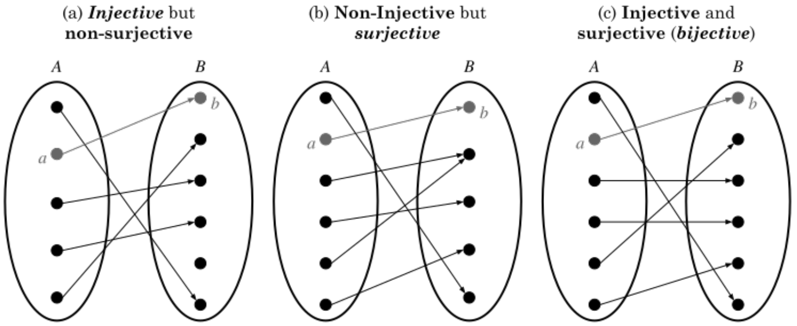
Definition 16. *A function $f : A \to B$, is said to be* bijective, *if it is* ***both*** *injective and surjective.*

Exercises

1. In terms of common sensical understanding of the term bijection, what does the existence of bijection between two A and B, tell us about the count of the number of elements in the set.

2. In the set of examples, given above, figure out which of the functions are bijective.

As a mnemonic, the following diagram may prove useful to visualise bijection. (Image source: Wikipedia commons by musical inquisit)


(a) *Injective* but **non-surjective**
(b) **Non-Injective** but ***surjective***
(c) **Injective** and **surjective** (***bijective***)
A
B
a
b
A
B
a
b
A
B
a
b

2.0.1 Successor, Addition and Multiplication

We are now equipped, to define addition, in order to define addition, we define the idea of a successor function on natural numbers, which takes a natural number, and returns the next natural number. In terms of intuition, it captures the idea of adding a natural number by 1.

Definition

Definition 17. *Successor S is a function $S : \mathbf{N} \to \mathbf{N}$, such that:*

- $S(0) = 1$
- $S(n) = (n \cup \{n\})$

Recall that $(n \cup \{n\})$ is the natural number succeeding n, as per the definition given before.

Even though successor function has this rigorous definition, in terms of working with natural numbers, it suffices to treat $S(n)$ as $n + 1$. Notice that every natural number is either 0 or $S(n)$ for some n. We assume the following statements about the successor function. Even though they can be proved, for reasons of sanity, we skip the proofs and assume these statements:

1. S is an injective function from $\mathbf{N}$ to $\mathbf{N}$.
2. Zero is not the successor of any element. That is, $\forall n \in \mathbf{N},\ S(n) \neq 0$.

This enables us to now define addition on natural numbers, through recursion. In order to define addition through recursion, we first observe the following:

- First observe that (as stated before), every natural number is either 0, or $S(n)$ for some $n \in \mathbf{N}$. For any definition, it suffices to define the function on these cases.

- adding 0 to any number m returns m.
- adding $S(n)$ (or $n + 1$, if you wish) to any number m, returns $S(n + m)$ (or $n + m + 1$.
- The points (2) and (3), enable us to define addition using recusion for all natural numbers.

The above set of observations are formally encoded in the following definition of addition.

Definition

Definition 18. *Addition (+) is defined as the function* $+ : \mathbf{N} \times \mathbf{N} \to \mathbf{N}$ *such that:*

1. $+(0,\ m) = m$, *for all natural numbers* m.
2. $+(S(n),\ m) = S(+(m, n))$, *for all natural numbers* n *and* m.

We use $n + m$, to denote $+(n, m)$. We can illustrate the working of the addition in the following examples:

Examples

- $0 + 1 = 1$ (from the condition (1) of definition of addition).
- However, $1 + 0$ is more subtle, since we do not yet know that $1 + 0 = 0 + 1$. Thus we take recourse to the definition:

$$1 + 0 = S(0) + 0$$

(from definition of 1)

$$= S(0 + 0)$$

(from definition of +)

$$= S(0)$$

(from definition of +)

$$= 1$$

(from definition of 1)

- We jump a few levels to evaluate $3 + 2$.

$$3 + 2 = S(2) + 2$$

(from definition of 3)

$$= S(2 + 2)$$

(from definition of +)

$$= S(S(1) + 2)$$

(from definition of 2)

$$= S(S(1 + 2))$$

(from definition of +)

$$= S(S(S(0) + 2))$$

(from definition of 1)

$$= S(S(S(0 + 2))$$

(from definition of +)

$$= S(S(S(2)))$$

(from definition of +)

$$= S(S(S(S(1)))$$

(from definition of 2)

$$= S(S(S(S(S(0))))$$

(from definition of 1)

$$= 5$$

We are now in a position to define multiplication. Like addition, multiplication can be seen as an operation. We observe the following about multiplication:

- Multiplication of any number by 0 is 0 itself.
- Multiplying $n + 1$ by a number m is $n * m + m$.

The above enable us to define multiplication recursively.

Definition

Definition 19. *Multiplication* ($* : \mathbf{N} \times \mathbf{N} \to \mathbf{N}$) *is defined as follows:*

1. $*(0, m) = 0$
2. $*(S(n), m) = (n * m) + m$

We use the term $n * m$ *to denote* $*(n, m)$

Analogous to above, we can produce a few evaluations of multiplication.

Examples

- $0 * 4 = 0$ (from the condition (1) of definition of addition).
- The case of $1 * 0$ is similar to $1 + 0$. It does not directly follow from the definition. It needs further application of the definition, or what we call proof by calculation.

$$\begin{aligned} 1 * 0 &= S(0) * 0 \\ &\text{(from definition of 1)} \\ &= S(0 * 0) \\ &\text{(from definition of *)} \\ &= S(0) \\ &\text{(from definition of *)} \\ &= 1 \\ &\text{(from definition of 1)} \end{aligned}$$

- We try to prove that $3 * 2$

$$3 * 2 = S(2) * 2$$

(from definition of 1)

$$= (2 * 2) + 2$$

(from definition of *)

$$= (S(1) * 2) + 2$$

(from definition of *)

$$= ((1 * 2) + 2) + 2$$

(from definition of *)

$$= ((S(0) * 2) + 2) + 2$$

(from definition of 1)

$$= (((0 * 2) + 2) + 2) + 2$$

(from definition of *)

$$= ((0 + 2) + 2) + 2$$

(from definition of *)

$$= (2 + 2) + 2$$

(from definition of +)

We leave it to the reader to verify $(2 + 2) + 2$

Exercises

In the manner described above:

1. Evaluate 4+5.
2. Evaluate 1+5
3. Evaluate 5 + 1;
4. Evaluate 4*4.
5. Evaluate 1*3.

We want to make certain general claims about addition and multiplication over natural numbers. For instance, it is not obvious that for all the natural numbers, the following hold:

- $a + 0 = 0 + a$, for all natural numbers a
- $(a+b)+c = a+(b+c)$, for all natural numbers a, b and c. This means that the order of addition is irrelevant, when adding more than two numbers. This property is called associativity. (Can you think of an operation,

which is not associate?)

- $a + b = b + c$, for all natural numbers a and b.
- $a * 0 = 0 * a$, for all natural numbers a
- $a * 1 = 1 * a = a$, for all natural numbers a
- $(a * b) * c = a * (b * c)$, for all natural numbers a, b and c. This means that the order of addition is irrelevant, when adding more than two numbers.
- $a * b = b * c$, for all natural numbers a and b.

Before we prove these properties, we will try to define order ($\leq$) on natural numbers. Along with defining order, it would serve as an ideal starting point to introduce certain kinds of proofs, which we extend to addition and multiplication soon. How would we define order on natural numbers using the available tools? First, what kind of an object is an order? Notice that an order exists between pairs of elements of a set. Thus one may be used think of it a set consisting of all pairs of elements from the same set, which are related by the order. This is precisely captured in the definition of a relation. Second, when are two elements related by the order on natural numbers? We say a number n is less than m, when $m - n$ is positive. Since we have not yet introduced subtraction. We can reframe it in terms of addition as n is less than m if there exists a k such that $n + k = m$.

Definition

Definition 20. *Order $\leq$ is a relation on $\mathbf{N}$, such that:*

$$n \leq m \longleftrightarrow \exists k.\ n + k = m$$

We use the term n is less than or equal to m to say this.

We illustrate the workings of this definition with a few examples:

Examples

- $0 < 1$, since $0 + 1 = 1$.
- $4 < 7$, since $4 + 3 = 7$.
- $100 < 1000$, since $100 + 900 = 1000$.
- $\neg(3 < 1)$, since $\forall n \in \mathbf{N}, 3 + n \neq 1$.

In above examples, the prove consists of computation with specific examples such as proving $3 + 2 = 4$, or showing $2 < 4$, can be done along similar lines. But in order to prove a general result such as $\forall n \in \mathbf{N}.0 < n$, we may need a more general technique. We introduce proof by induction, which is a useful technique to show results on all natural numbers.

Principles of Mathematical Induction: Assume that for a given property P, the following hold:

- $P(0)$
- For every $n \in \mathbf{N}$, $P(n) \to P(n+1)$.

Then we can assert that $\forall m \in \mathbf{N}, P(m)$ holds.

Note the subtlety that we assume that $P(n) \to P(n+1)$, which is not the same as assuming that $P(n)$ for all $n \in \mathbf{N}$. Since $A \to B$, does not imply that A is true.

Question: Why does this technique work? We provide some heuristic reasoning (not a proof), regarding why mathematical induction ought to work. Consider a property P, which satisfies the conditions of mathematical induction. Then the following hold:

- $P(0)$ is true, since it satisfies the condition that $P(0)$ is true.
- $P(1)$ is true, since $P(0)$ holds and $P(n) \to P(n+1)$, (remember that if A is true and $A \to B$, B has to be true.)
- $P(2)$ is true, since $P(1)$ holds from above and $P(n) \to P(n+1)$,
- $P(3)$ is true, since $P(2)$ holds from above and $P(n) \to P(n+1)$,

Thus by extending as above, for any natural number m, one should be able to say that $P(m)$ holds.

Question: How do we use this technique to prove a results?

Assume that you have to prove a result of the following type:

$$\forall\ n \in \mathbf{N}.\ P(n)$$

Where P denotes a property on natural numbers. We prove the following statements:

- Prove that $P(0)$ holds. That is, prove that 0 satisfies the property P in question.
- We need to further prove that $P(n) \to P(n+1)$, for every n. We prove it along following lines:
  - Assume that for some fixed but arbitrary n, $P(n)$ is true. We called this assumption, **Induction Hypothesis**.
  - Using the above as a hypothesis, prove that $P(n+1)$ is true.

Proving the set of statements above suffice to show that $\forall m.\ P(m)$ holds.

To illustrate the workings in a non-mathematical setting, consider the following example:

Consider that you are living on a planet, which has the following law of genetics:
Fact 1: If a parent has blue eyes, then all the children have blue eyes. **Fact 2:** Alta has blue eyes.

To Prove: All descendents of Alta have blue eyes. *Proof:* We prove the claim by using the induction on number of generations that separate a descendant from Alta. The property P here is the property of having blue eyes. The proof runs as follows:

- The property $P(0)$ would mean that the 0th descendant of Alta has blue eyes. Zero-th generation of Alta is Alta itself. Thus, Since Alta has blue eyes, $P(0)$ holds.
- We need to further prove that $P(n) \to P(n+1)$, for every n. We prove it along following lines:
    - Assume that for some fixed but arbitrary n, $P(n)$ is true. This implies that all the $n-$th generation descendants of Alta have blue eyes.
    - We need to prove that all the $(n+1)$-th generation of Alta have blue eyes. We know from above that all the n-th generation descendants of Alta have blue eyes. From Fact 1, we know that if either of the parents have blue eyes, all the children do. Everyone in $(n+1)$-th generation of Alta, has a parents in n-th generation. Thus it follows that everyone in the $n+1$-th generation of Alta has blue eyes.

Proving the set of statements above suffice to show that all descendants of Alta have blue eyes.

We show the following result using induction as a case in point:

$$\forall\, n \in \mathbf{N}.\ 0 \leq n$$

The property P here stands for the property on natural numbers of being greater than or equal to 0 ($P(n) \equiv (0 \leq n)$. We prove the following statements:

- Prove that $0 \leq 0$ holds. Proof:
    - $0 = 0 + 0$ (from definition of addition).
    - $0 \leq 0$. (from definition of $\leq$),
- We need to further prove that $0 \leq n \to 0 \leq (n+1)$, for every n. We prove it along following lines:
    - Assume that for some fixed but arbitrary n, $0 \leq n$ is true.
    - Using the above as a hypothesis, prove that $0 \leq (n+1)$ is true. Proof:
        - $0 + (n+1) = n+1$ (from definition of addition).
        - Thus $0 \leq (n+1)$

Proving the set of statements above suffice to show that $\forall m.\ 0 \leq m$ holds.

Note that in the proof above, we do not actually use the induction hypothesis, that is $0 \leq n$. This is an exception and not a norm. The above proof could be written without using induction. But we employ induction as a case in point.

Now we proceed to prove the statements on addition and multiplications:

2.1 Addition and Multiplication Theorems

In this section, we will prove a few results about addition, which we often take for granted, but would involve some deduction if we are to employ a rigorous definition of addition, as stated in the text. We begin by summarising the definition of addition stated earlier:

- $\forall m.\ 0 + m = m.$
- $\forall n,\ m.\ \ S(n) + m = S(n + m).$

Some of the properties of addition, which we conventionally assume, are not that straightforward from the definition. For instance $n + 0 = n$, for every natural number n. Since it does not follow from above $a + b = b + a$. Similarly it is not that obvious that $(a + b) + c = a + (b + c)$. This property refers to the fact that if we add a and b first and c later, it is the same as adding b and c first and a later. (For a computer scientist, order in which things are added can make a big difference). We list a few theorems below, which we prove later.

- $\forall n \in \mathbf{N}.\ n + 0 = n.$
- $\forall a,\ b \in nn.\ (a + b) + c = (a + b) + c.$
- $\forall a,\ b \in \mathbf{N}.\ a + b = b + a.$

Similarly, in the case of multiplication:

- $\forall n \in \mathbf{N}.\ n * 0 = 0.$
- $\forall n \in \mathbf{N}.\ 1 * n = n.$
- $\forall n \in \mathbf{N}.\ n * 1 = n.$
- $\forall a,\ b \in nn.\ (a * b) * c = (a * b) * c.$
- $\forall a,\ b \in \mathbf{N}.\ a * b = b * a.$

Theorem 7. $\forall n \in \mathbf{N}.\ n + 0 = n.$

Proof

Proof. We prove by induction on n. The proof proceeds as follows:

Base Case: To prove that $0+0=0$.

Proof of Base Case: The statement follows from the first condition in definition of addition, which states that $0+n=0$. By substituting n for 0, we get the statement.

Induction Hypothesis: *Assume* that $n+0=0$.

Induction Case: To prove that $S(n)+0=S(n)$.
Proof of Induction Case:

1. $S(n)+0=S(n+0)$ (from the condition II in definition of addition).
2. $(n+0)=n$ (from the Induction hypothesis)
3. $S(n+0)=S(n)$ (from the above statement)
4. $S(n)+0=S(n)$ (from statement I above and statement III).

It thus follows that: $\forall n \in \mathbf{N}.\ n+0=n$. □

Theorem 8. $\forall a,b,c \in \mathbf{N}.\ (a+b)+c=a+(b+c)$.

Proof

Proof. We prove by induction on a. The proof proceeds as follows:

Base Case: To prove that $(0+b)+c=o+(b+0)$.

Proof of Base Case: It follows from definition of addition that $(o+b)+c=(b+c)$. It further follows that $0+(b+c)=b+c$. T Thus it follows that $(0+b)+c=0+(b+c)$

Induction Hypothesis: *Assume* that $(a+b)+c=a+(b+c)$.

Induction Case: To prove that $(S(a)+b)+c)=a+(b+c)$
Proof of Induction Case:

1. $(S(a)+b)+c=S(a+b)+c$ (from the definition of addition)
2. $S(a+b)+c=S((a+b)+c)$ (from the definition of addition)
3. $((a+b)+c)=(a+(b+c))$ (from the induction hypothesis)

4. $S((a+b)+c) = S(a+(b+c))$ (from above)
5. $S((a+(b+c)) = S(a)+(b+c)$ (from definition of addition)
6. $S(a)+(b+c) = S(a)+(b+c)$ (from the previous steps)

Thus it follows from principle of induction that:

$$\forall a, b, c \in \mathbf{N}.\ (a+b)+c = a+(b+c)$$

□

It remains to be shows that addition is commutative ($a+b=b+a$), but inorder to show that using induction, it maybe useful to have an identity which allows us to know what happens to $a+S(b)$. since the definition of addition only describes $S(a)+b$. This lemma will be useful in proving commutativity, since we can anticipate that in proving commutativity of addition in the inductive case, we will need to show $S(a)+b = b+S(a)$, and we will need to reduce the right hand side to a nice enough form.

Theorem 9. *$\forall n, m \in \mathbf{N}.\ n+S(m) = S(n+m)$.*

Proof

Proof. We prove by induction on n. The proof proceeds as follows:

Base Case: To prove that $0+S(m) = S(0+m)$.

Proof of Base Case: It follows from definition of addition that $0+S(m) = S(m)$. It further follows that $S(0+m) = S(m)$, as $0+m = m$ from definition of addition. Thus it follows that $(0+S(m) = S(0+m)$

Induction Hypothesis: *Assume* that $n+S(m) = S(n+m)$.

Induction Case: To prove that $S(n)+S(m) = S(S(n)+m)$
Proof of Induction Case:

1. $S(n)+S(m) = S(S(n)+m)$ (from the definition of addition, the second case).

Thus it follows from principle of induction that:

$$\forall n, m \in \mathbf{N}.\ n+S(m) = S(n+m)$$

□

Theorem 10. $\forall a, b \in \mathbf{N}.\ a + b = b + a.$

Proof

Proof. We prove by induction on a. The proof proceeds as follows **Base Case:** To prove that $0 + b = b + 0$.
Proof of Base Case: $0 + b = b$ (from the definition of addition), and we further have that $b + 0 = b$, from the theorem above (n+ 0 = n). Thus it follows that $0 + b = b + 0$.

Induction Hypothesis: *Assume* that $a + b = b + a$.

Induction Case: To prove that $S(a) + b = b + S(a)$
Proof of Induction Case:

1. $S(a) + b = S(a + b)$ (from the definition of addition, the second case).
2. $b + S(a) = S(b + a)$ (from the previous theorem).
3. $a + b = b + a$ (from induction hypothesis)
4. $S(a + b) = S(b + a)$ (from previous statement).
5. $S(a) + b = a + S(b)$ (from the previous statements).

□

We leave the proofs by multiplications as an exercise, but we briefly sum up the exercises:

Exercises

1. $\forall n \in \mathbf{N}.\ n * 0 = 0.$
2. $\forall n \in \mathbf{N}.\ 1 * n = n.$
3. $\forall n \in \mathbf{N}.\ n * 1 = n.$
4. $\forall a,\ b \in nn.\ (a * b) * c = (a * b) * c.$
5. $\forall a,\ b \in \mathbf{N}.\ a * b = b * a.$

3 Equivalence Relations, Partitions and Construction of Integers

We will now proceed to construct integers. In order to do so, we will first define a useful tool called equivalence relations, which has far reaching applications including in terms of defining integers.

Quite often in computing and mathematics, given a set, we are not always interested in the elements of the set itself, but in partitioning the set into multiple sets and then making inferences based on the set an element is contained in. This is an idea that we quite intuitively use very often. In terms of how we partition set of all species into plants and animals. Or set of all animals into arthopoda, fish, mamals, avian, amphibia, reptiles. We may partition students of the class depending on the location in the class (left, right or centre). This task is of enormous interest in computing, for instance, since a large number of digital recommendation systems partition the set of users (using their previously collected data) into sets of people with similar tastes and then accordingly make suggestions. We abstractly capture this idea in terms of sets as follows:

Recollect that a relation $R \subseteq A \times A$, for any set A. In addition, $(a, b) \in R$ is depicted using the notation $a\ R\ b$.

Definition

Definition 21. *An equivalence relation $\sim$ on a set A is any relation which satisfies the following properties:*

1. ***Reflexivity:*** $\forall a \in A.\ a \sim a$. *This refers to the fact that every element is related to itself by $\sim$.*

2. ***Symmetry:*** $\forall a, b \in A.\ (a \sim b) \longrightarrow (b \sim a)$. *This refers to the fact that if a is related to b by $\sim$, then b is also related to a by $\sim$.*

3. ***Transitivity:*** $\forall a, b, c \in A.\ ((a \sim b) \wedge (b \sim c)) \longrightarrow a \sim c$. *This refers to the fact that if a is related to b by $\sim$, and b is related to c by $\sim$, then a is related to c.*

Examples

Consider the following examples of equivlence relations on the set $A = \{a, b, c\}$:

1. $\sim = \{(a, a), (b, b), (c, c)\}$. It is straightforward to see that it is reflexive. Further the fact that it is symmetric and transitive follows from the fact that all elements are related only to themselves.

2. $\sim = \{(a, a), (b, b), (c, c), (a, b), (b, a)\}$. It is again obvious that these are reflexive relations. It further follows that it is symmetric as for each $x \sim y$, one can see that $y \sim x$. Similarly for each $x \sim y$

and $y \sim z$, it follows that $x \sim z$. Note that transitivity here is a little more tricky. For instance, one may observe that $\neg(a \sim c)$, that is a is not equivalent to c. This is not needed as the only two distinct elements which are related to each other are a and b. By using transitivity on both of them, we can get $a \sim a$ and $b \sim b$ (if we take $b \sim a$ and $a \sim b$). Since no intermediate related elements are present between a and c, it is not necessary for the relation to be equivalent, that $a \sim c$.

3. $\sim = \{(a,a),(b,b),(c,c),(a,b),(b,c),(a,c),(b,a),(c,b),(c,a)\}$ is an equivalence relation, as it obeys reflexivity, symmetry and transitivity.

More examples of equivalence relations:

Examples

1. Consider the set of all places. We define a relation 'connectedness' as follows: X is connected to Y if there is a way to go from X to Y via a two-way motorable road. It is easy to see that this relation is an equivalent relation. Every place is connected to itself. Given any two places, if there it a motorable road from one to another, there is one back as well (we mentioned that the road has to be two way). If one can get from a place X to Y via a motorable road, and from place Y to place Z. One can get from place X to place Z too.

2. We say two people are related to each other, if they are either directly related as parents, childrens, siblings, or through marriage or they have common relatives (note the recursion in definition here). This is an equivalence relation. Since every one is related to themselves, if X is related to Y, then Y is related to X, and if X is related to Y, and Y is related to Z, then X is related to Z.

3. Two words are said to be related if they have the same alphabets in the same order (even if one has lowercase alphabets and the other substitutes them for upper case alphabets). For instance, $Hello$ is equivalent to *hello* and $hELLo$. It is an easy exercise to check that this is an equivalence relation.

Some examples of non-equivalent relations:

Examples

Consider the following examples of equivalence relations on the set $A = \{a, b, c\}$:

1. $R = \{(a, a), (b, b)\}$. It is not an equivalence relation since c is not related to c in here.

2. $R = \{(a, a), (b, b), (c, c), (a, b)\}$. It is obvious that these are reflexive relations. But this relation is not symmetric, so it is not an equivalence relation as $a \sim b$ but $\neg(b \sim c)$

3. $R = \{(a, a), (b, b), (c, c), (a, b), (b, c), (b, a), (c, b), (c, a)\}$ is not an equivalence relation, as $a \sim b$ and $b \sim c$, but not $a \sim c$. Thus it violates transitivity.

Some additional examples of non-equivalence relations:

Examples

1. Twitter following is not an equivalence relation, since one person may follow another, but the vice versa might not hold true.

2. The relation of being a parent is not an equivalence relation on set of humans , since X is a parent of Y, does not mean Y is a parent of X , thus violates symmetric.

3. Relation of having a direct flight is not an equivalence relation on the set of places, since a place X may have a direct flight to Y, and Y may have a direct flight to Z, but X may not have a direct flight to Z. Thus it violates transitivity.

4. Consider the relation on set of people, where any two people are related to each other, if their annual income is within 11 Rs. margin of each other. This is not an equivalence relation, since consider a situation where X earns $Rs.$ 100, Y earns $Rs.$ 110, and Z earns $Rs.$ 120. X and Y are within 11 Rs. margin of each others income, and Y and Z are within 11 Rs margin of each others income, but X and Z are not.

One question that arises iis whether any relation R can be converted into an equivalence relations? As a matter of fact, it infact can be, by adding extra elements to the relation to ensure that it is reflexive, symmetric and transitive. This is captured by the following theorem.

Theorem 11. *Given any relation R (need not be equivalent) on A, there exists an equivalence R^* such that:*

$$R \subseteq R^*$$

and if E is any other equivalence relation containing R as a subset, it follows that:

$$R^* \subseteq E$$

Proof

Proof. Consider the equivalence relation R^* as follows:

- $(x, y) \in R \Rightarrow (x, y) \in R^*$.
- For every x in R such that $(x, y) \in R^*$ or (x, y) in R^* for some y, add $(x, x) \in R^*$. This ensures that R^* is reflexive.
- For every $(x, y) \in R^*$, add $(y, x) \in R^*$. This ensures that R^* is symmetric.
- For every $(x, y) \in R^*$ and $(y, z) \in R^*$, add $(x, z) \in R^*$. This ensures that R^* is transitive.

E is any other equivalence relation containing R as a subset. We leave the proof of the fact that $R^* \subseteq E$ as an exercise. □

To illustrate these relations, consider the case of examples listed above:

Examples

$A = \{a, b, c\}$

1. $R = \{(a, a), (b, b)\}$. $R^* = \{(a, a), (b, b,), (c, c)\}$.
2. $R = \{(a, a), (b, b), (c, c), (a, b)\}$. $R^* = \{(a, a), (b, b), (c, c), (a, b), (b, a)\}$
3. $R = \{(a, a), (b, b), (c, c), (a, b), (b, c), (b, a), (c, b), (c, a)\}$ To convert this to an equivalence relation, we need to (a, c) . Thus $R^* = \{(a, a), (b, b), (c, c), (a, b), (b, c), (b, a), (c, b), (c, a), (a, c)$.

Given an equivalence relation on a set, and an element belonging to the set, we are interested in finding out what are the elements related to the given elements by the equivalence relation. This brings us to the idea of an equivalence class, which is defined as follows:

Definition

Definition 22. *Given an equivalence relation $\sim$ on a set A, and an element $a \in A$, the* ***equivalence class of*** *a, denoted by $[a]$ is defined as :*

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

Consider the following relations and the equivalence classes that result in:

Examples

Consider the following examples of equivalence relations on the set $A = \{a, b, c\}$:

1. $\sim = \{(a, a), (b, b), (c, c)\}$.
   - $[a] = \{a\}$
   - $[b] = \{b\}$
   - $[c] = \{c\}$
2. $\sim = \{(a, a), (b, b), (c, c), (a, b), (b, a)\}$.
   - $[a] = \{a,\ b\}$
   - $[b] = \{a,\ b\}$
   - $[c] = \{c\}$
3. $\sim = \{(a, a), (b, b), (c, c), (a, b), (b, c), (a, c), (b, a), (c, b), (c, a)\}$
   - $[a] = \{a,\ b,\ c\}$
   - $[b] = \{a,\ b,\ c\}$
   - $[c] = \{a,\ b,\ c\}$

Consider the set $\mathbf{N}$ and the equivalence relation $\sim$ on $\mathbf{N}$ such that $m \sim n$, if and only if $m = n + 2 * k$ for some $k \in \mathbf{N}$ or $n = m + 2 * k$ for some k. We are merely formally stating that the difference between m and n is an even number. We leave it as an exercise to the reader to check that this is indeed an equivalence relation. We list its equivalence classes as follows:

1. $[0] = \{2 * n \mid n \in \mathbf{N}\}$. We are merely stating that the equivalence class of 0 is the set of even numbers.
2. $[1] = \{2 * n + 1 \mid n \in \mathbf{N}\}$. We are merely stating that the set of equivalence class is the set of odd numbers.
3. $[n]$ is equal to $[0]$ if n is even and equals $[1]$ if n is odd. (Why?)

If one observes then we may observe that:

- Equivalence classes of any two elements are the same or they are completely disjoint from each other.

- Union of equivalence classes of all the elements in a set is equal the set.

We formally state these observations in the following therem:

Theorem 12. *Given an equivalence class $\sim$ on a set A, the following theorems hold true:*

1. $a \in [a]$
2. $a \sim b \iff [a] = [b]$
3. $\neg(a \sim b) \iff [a] \cap [b] = \emptyset$
4. $\bigcup_{a \in A}[a] = A$.

Proof

Proof.

1. Given that $a \sim a$, it follows from the definition of $[a]$ that $a \in [a]$.

2. We begin by assuming that $a \sim b$, and show that $[a] = [b]$. To show that $[a] = [b]$, we begin by proving that $[a] \subseteq [b]$ and $[b] \subseteq [a]$. To show that $[a] \subseteq [b]$, consider a fixed but arbitrary $x \in [a]$. Thus $a \sim x$. From our assumption it follows that $a \sim b$. Since $\sim$ is equivalent and thus symmetric, it follows that $b \sim a$. Thus from transitivity of $\sim$ it follows that $b \sim x$. From the definition of equivalence classes, it follows that $x \in [b]$. Since x was an arbitrary element of $[a]$, it follows that $[a] \subseteq [b]$. The proof that $[b] \subseteq [a]$ is on similar lines. Thus it follows that $[a] = [b]$. We now assume that $[a] = [b]$, and show that $a \sim b$. From the proof of (1), it follows that $a \in [a]$ and $b \in [b]$. Since $[a] = [b]$, it follows that $b \in [a]$. Thus, by definition of an equivalence class, it follows that $a \sim b$.

3. We first assume $\neg(a \sim b)$ and show that $[a] \cap [b] = \emptyset$. We prove this by contradiction. Assume that $[a] \cap [b] \neq \emptyset$. Then it follows that there exists $x \in A$, such that $x \in [a] \cap [b]$. Thus, $x \in [a]$ and $x \in [b]$. Thus $a \sim x$ and $b \sim x$, from definition of an equivalence class. Given that $\sim$ is an equivalence relation and thus symmetric, it follows that $a \sim x$ and $x \sim b$ (observe that we use symmetric only on $b \sim x$ here). Since $\sim$ is an equivalence relation and thus transitive, it further follows that $a \sim b$. This contradicts the hypothesis that $\neg(a \sim b)$. Thus our assumption that $[a] \cap [b] \neq \emptyset$ was false and $[a] \cap [b] = \emptyset$. We now assume that $[a] \cap [b] = \emptyset$ and

show that $\neg(a \sim b)$. We prove this by contradiction too. Assume that $\neg(\neg(a \sim b)$. This is the same as $(a \sim b)$. From the definition of equivalence class, it follows that $b \in [a]$. From (1), it follows that $b \in [b]$. Thus $[a] \cap [b] \neq \emptyset$. This is a contradiction. Thus our assumption that $a \sim b$, was wrong and $\neg(a \sim b)$.

4. This is quite straightforward, to see since each $[a] \subseteq A$, for $a \in A$. Thus $\bigcup_{a \in A} [a] \subseteq A$ (as union of subsets of a set is a subset). Similarly for any $x \in A$, $x \in [x]$. Thus $x \in \bigcup_{a \in A} [a]$. Thus it follows that $A \subseteq \bigcup_{a \in A} [a]$. From the two subset relations established here, it follows that $\bigcup_{a \in A} [a] = A$.

□

One may note that in the context of the last result, one need not take a union over equivalence classes of all elements to obtain the set A, since multiple elements may have the same equivalence class. One can pick a representative element from each equivalence class and take a union over the set of representative elements. For instance in the context of equivalence relation mentioned in the example cited earlier over $\mathbf{N}$, it suffices to consider $[0]$ and $[1]$, and $\mathbf{N} = [0] \cup [1]$.

We will mathematically formulate the idea that equivalence classes *divide* the set into multiple distinct by introducing the notion of partition, which captures this phenomenon with precision. Before we introduce partition, we introduce the notation of union over an indexed set as follows:

Consider a set Λ, and consider a set of sets $\{X_{\$alpha} | \alpha \in \Lambda\}$, where each X_α is a set (indexed by α). We define:

$$\bigcup_{\alpha \in \Lambda} X_\alpha = \{x \mid x \in X_\alpha, \text{for some } \alpha \in \Lambda\}$$

.

This simply means that we take the union of all X_α's, for $\alpha \in \Lambda$. We illustrate it in the following examples:

- Let $\Lambda = \{1, 2, 3\}$. Let $X_1 = \{a,\ b\}$,$X_2 = \{c,\ d,\ e\}$, and $X_3 = \{f,\ g\}$.

$$\bigcup_{\alpha \in \Lambda} X_\alpha = \{a,\ b,\ c,\ d,\ e,\ f,\ g\}$$

.

- Let $\Lambda = \{1, 2\}$. Let $X_1 = \{a,\ b,\ c\}$,$X_2 = \{b,\ c,\ d\}$.

$$\bigcup_{\alpha \in \Lambda} X_\alpha = \{a,\ b,\ c,\ d\}$$

.

- Let $\Lambda = \mathbf{N}$. Let $X_n = \{2 * n,\ 2 * n + 1\}$. In this example, the n-th set X_n merely consists of the n-th odd and n-th even number.

$$\bigcup_{\alpha \in \Lambda} X_\alpha = \{0,\ 1,\ 2,\ ,3,\ ..\}(= \mathbf{N})$$

.

- Let $\Lambda = \{0,\ 1\}$. Let $X_0 = \{2 * n \mid n \in \mathbf{N}\}$ and $X_1 = \{2 * n \mid n \in \mathbf{N}\}$. In this example, the set X_0 merely consists of all the even numbers, and the set X_1 consists of all the odd numbers.

  $$\bigcup_{\alpha \in \Lambda} X_\alpha = \{0,\ 1,\ 2,\ ,3,\ ..\}(= \mathbf{N})$$

  .

We now define partition of a set A as follows:

Definition

Definition 23. *A partition P of a set A is a set of sets $\{X_\alpha \mid \alpha \in \Lambda\}$, where Λ is the indexing set, such that:*

1. *Any two sets in the partition have an empty intersection. To formally state, for $\beta, \gamma \in \Lambda$, $\beta \neq \gamma$:*

$$X_\alpha \cap X_\beta = \emptyset$$

2. *The union of all sets in the partition equals the set A. Formally put,*

$$\bigcup_{\alpha \in \Lambda} X_\alpha = A$$

Examples of partition:

Examples

1. Let $\Lambda = \{1, 2, 3\}$ and $P = \{X_1, X_2, X_3\}$. Let $X_1 = \{a,\ b\}$,$X_2 = \{c,\ d,\ e\}$, and $X_3 = \{f,\ g\}$. P partitions the set $\{a,\ b,\ c,\ d,\ e,\ f,\ g\}$

2. Let $\Lambda = \{1, 2, 3\}$ and $P = \{X_1, X_2, X_3\}$. Let $X_1 = \{a,\ b\}$,$X_2 = \{c,\ d,\ e\}$, and $X_3 = \{f,\ g\}$. P partitions the set $\{a,\ b,\ c,\ d,\ e,\ f,\ g\}$

3. Let $\Lambda = \mathbf{N}$ and $P = \{X_n \mid n \in \mathbf{N}\}$. Let $X_n = \{2*n,\ 2*n+1 \mid n \in \mathbf{N}\}$. P partitions the set $\mathbf{N}$.

4. Let $\Lambda = \{0,\ 1\}$. Let $P = \{X_0,\ X_1\}$, where $X_0 = \{2*n \mid n \in \mathbf{N}\}$ and $X_1 = \{2*n \mid n \in \mathbf{N}\}$. P partitions $\mathbf{N}$.

As stated earlier, equivalence classes seem to perform a task similar to partition. The set of equivalence classes of any equivalence relation, partition the set. One could similarly ask if whether given an partition, we can define an equivalence relation on the set whose equivalence classes are exactly the sets of the partition. Answer to this is yes. In order to show these results, we begin by defining the idea of representative elements of an equivalence, which enable us to avoid double counting equivalence classes.

Definition

Definition 24. *Given a set A and an equivalence relation $\sim$, the representative elements of equivalence classes of A under $\sim$ is a set S of elements of A such that:*

- *No two elements of S are equivalent to each other.*

$$\forall x, y \in S.\ \neg(x \sim y)$$

- *Every element of A is equivalent to some element of S.*

$$\forall x \in X.\ \exists y \in S.\ x \sim y$$

.

The following result follows as a direct consequence of the definition of the representative set, and the theorem 12. We omit the proof, since it is a direct consequence of the aforementioned results:

Theorem 13. *Let S be the set of representative elements of A under the equivalence relation $\sim$, the following hold:*

1. *$[a] \cap [b] = \emptyset$, if $a,\ b \in S$, and $a \neq b$.*
2. *$\bigcup_{a \in S}[a] = A$.*

To formally state the relationship between equivalence classes and partitions of a set:

Theorem 14.

1. *Given a set A, an equivalence relation $\sim$ on A and set of corresponding representation elements of the equivalence relation S, the set:*

$$\{[a] \mid a \in S\}$$

partitions the set A

2. *Given a partition P of A, there exists an $\sim$, such that that equivalence classes of $\sim$ are precisely the elements of the partition P.*

Proof

Proof. Proof of the statement (1) in the theorem is a direct consequence of the previous theorem and the definition of partition.
For proof of the statement (2), consider the relation $\sim$ on A such that $x\ y$ if and only if x and y belong to the same element of the partition

(That is, $\exists X \in P.\ x,\ y \in X$). We need to prove that this relation $\sim$ is an equivalence relation. Note that it is **reflexive** and any element $x \in X \to x \in X$. Similarly if both $x \sim y$, then $x, y \in X$ for some $X \in P$, then $y, x \in X$, therefore $y \sim x$ and thus the relation is **symmetric**. Consider $x \sim y$ and $y \sim z$. This implies that there exists $X \in P$ such that $x, y \in X$, similarly there exists $Y \in P$, such that $y, z \in Y$ (note that from the definition, it is not immediately straightforward that these sets X and Y have to be the same). Since $X \cap Y = \emptyset$ if $X \neq Y$, and $y \in X$ and $y \in Y$, it follows that $X = Y$. Thus $x,\ z \in X$. Thus $x \sim z$. It follows that the relation is **transitive**. Thus it follows from above that relations above is an equivalence relation. □

Thus, as implied by the previous theorem, every partition leads to an equivalence relation and vice versa.

4 Construction of Integers

We need to construct integers in order for subtraction to be a well defined function on natural numbers, as well as for negative numbers to exist. One of the roles played by subtraction lies is in cancellation of terms, for instance if we have $a + c = b + c$, by subtracting c from both sides we get $a = b$. But as it turns out, such a result for the restricted case of natural numbers (where a, b and c are all natural numbers), can be proved without subtraction. We show the theorem below, which additionally enables us to construct integers.

Theorem 15.

$$\forall a, b, k \in \mathbf{N}.\ (a + k) = (b + k) \Rightarrow (a = b)$$

Proof

Proof. We prove by induction on k.
Base Case: $k = 0$. Thus $a + 0 = b + 0 \Rightarrow a = b$ from the definition of addition by 0. **Induction Hypothesis:** Assume that for $k \in \mathbf{N}$, the following holds:

$$(a + k) = (b + k) \Rightarrow a = b$$

Induction Statement: We need to prove that:

$$a + S(k) = b + S(k) \Rightarrow a = b$$

Proof of the Induction Statement: Assume that:

$$a + S(k) = b + S(k)$$

It follows from the definition of addition that:

$$S(a+k) = S(b+k)$$

It follows from Peano's axioms that no two distinct elements have the same successor, thus it follows that:

$$a + k = b + k$$

From the induction hypothesis, it follows that:

$$a = b$$

□

In order to construct the integers, we first introduce an equivalence relation on $\mathbf{N} \times \mathbf{N}$ as follows: Consider the relation $\sim$ on $\mathbf{N} \times \mathbf{N}$, where:

$$(m_1, n_1) \sim (m_2, n_2) \iff (m_1 + n_2 = m_2 + n_2)$$

It is relatively straightforward to check that this relation is reflexive and symmetric. To see that this relation is transitive, consider:

- $(m_1, n_1) \sim (m_2, n_2)$
- $(m_2, n_2) \sim (m_3, n_3)$

Thus:

- $(m_1 + n_2) \sim (m_2 + n_1)$
- $(m_2 + n_3) \sim (m_3 + n_2)$

By adding n_3 to the first equality above, we get:

$$(m_1 + n_2) + n_3 = (m_2 + n_1) + n_3$$

By associativity of addition:

$$m_1 + (n_2 + n_3) = m_2 + (n_1 + n_3)$$

By commutativity of addition:

$$m_1 + (n_3 + n_2) = m_2 + (n_3 + n_1\text{‘})$$

By associativity of addition:

$$(m_1 + n_3) + n_2 = (m_2 + n_3) + n_1)$$

From the second equality above:

$$(m_1 + n_3) + n_2 = (m_3 + n_2) + n_1)$$

By associativity of addition:

$$(m_1 + n_3) + n_2 = m_3 + (n_2 + n_1)$$

By commutativity of addition:

$$(m_1 + n_3) + n_2 = m_3 + (n_1 + n_2)$$

By associativity of addition:

$$(m_1 + n_3) + n_2 = (m_3 + n_1) + n_2$$

From the previous theorem:

$$(m_1 + n_3) = (m_3 + n_1)$$

Thus it follows that $(m_1, n_1) \sim (m_3, n_3)$ When are two elements equivalent to each other under this relation? Even though, we have not formally defined subtraction, from what we intuitively know about subtraction from before, if follows that

$$(m_1, n_2) \sim (m_2, n_2) \iff m_1 - n_1 = m_2 - n_2$$

From this it follows that for any $(m, n) \in \mathbf{N} \times \mathbf{N}$, under this equivalence relation, if $m \geq n$, then $(m, n) \sim (k, 0)$ for some k since the difference is positive, else it equals $(0, k)$, for some k since the difference is negative.

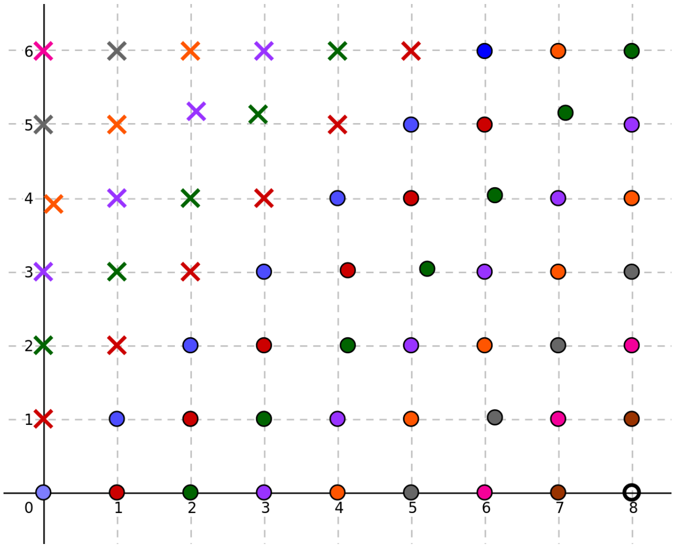
Definition

Definition 25. *Integers* $\mathbf{Z}$ *are defined as the equivalence classes of* $\mathbf{N} \times \mathbf{N}$*, under the relation* $\sim$ *given by:*

$$(m_1,\ n_1) \sim (m_2,\ n_2) \iff m_1 + n_2 = m_2 + n_1$$

Further we resort to abuse of notation and refer to the equivalence class containing $(n, 0)$ *as the integer* n*, and refer to the equivalence class containing* $(0, n)$ *as the integer* $-n$*.*

One can notice that when pairs of natural numbers are arranged on a grid, the equivalence class of any positive integer n, is precisely the set of points diagonally to the right of the points $(n, 0)$. Similarly, the equivalence class of any negative integer $-n$ is the set of points diagonally to the right of points $(0, n)$. It is illustrated in the figure below.



Elements of an equivalence class corresponding to any positive number is denoted by the filled dots of the same color. Elements of the equivalence class corresponding to any negative number are denoted here by crosses of the same color. (Question: What do equivalence classes here have to do with lines of the form $x - y = c$) One may recollect that traditionally, we dealt with natural numbers as subsets of integers, while given our construction here, natural numbers cannot possibly be subset of integers, since integers are constructed in terms of equivalence classes of tuples of natural numbers. Note that there exists an injective map from natural number $\mathbf{N} \to \mathbf{Z}$, where $n \mapsto [(n, 0)]$. When we now refer to a natural $n \in \mathbf{Z}$, we are infact talking about the equivalence class $[(n, 0)]$. Once integers are constructed in this fashion and all the relevant operations are proved, we can forget all the we know about natural numbers from earlier, and work with their images in integers. This process gets repeated when we construct rationals, reals and on.

In order to define addition of two integers, we need to define a function on equivalence classes (more precisely on a tuple of two equivalence classes). The question then arises : how do we define functions on equivalence classes? Given a set A with an equivalence relation $\sim$, we outline the construction of a function from equivalence classes of A under $\sim$ to a set B (which can be any set) as follows:

- First define a function $f : A \to B$.
- If the function f satisfies the condition:

$$x \sim y \Rightarrow f(x) = f(y)$$

then we define a function $\bar{f}$ from equivalence classes of A to B as follows:

$$\bar{f}([x]) = f(y), \text{for some representative } y \text{ in [x]}$$

In order to show that $\bar{f}$ indeed defines a well-defined function, we need to ensure that it does not occur that $\bar{f}([x])$ maps to two distinct elements b_1 and b_2 in B. In our particular case, it is indeed important to show this since as there is a possibility that the answer may vary if we choose a different representative z in $[x]$, since $[x]$ can contain more than one element. We should that this possibility does not arise, as assume $y, z \in [x]$. Since $\sim$ is equivalent, it follows from transitivity that $y \sim z$. Given our assumption on f that $y \sim z$ implies that $f(y) = f(z)$. It follow that $f(y) = f(z)$. Thus $b_1 = b_2$, and $\bar{f}$ is a well defined function from the set of equivalence classes on A (denoted usually by $A/\sim$) to B.

It follows from the explanation above, that in order to define a function from a $\mathbf{Z} \times \mathbf{Z} \to \mathbf{Z}$, we need to first define a $(\mathbf{N} \times \mathbf{N}) \times (\mathbf{N} \times \mathbf{N}) \to \mathbf{Z}$ and show that it maps equivalent elements to the same elements. We begin by defining the $\oplus$ operation on $(\mathbf{N} \times \mathbf{N}) \times (\mathbf{N} \times \mathbf{N}) \to \mathbf{Z}$ as follows:

Definition

Definition 26.

$$(m,\ n) \oplus (p, q) = [(m + p,\ n + q)]$$

where $m, n, p, q \in \mathbf{N}$ and $+$ is the standard addition on $\mathbf{N}$ as defined earlier.

We prove that $\oplus$ maps equivalent pairs of natural numbers to the same element.

Theorem 16. *If $(m_1, n_1) \sim (m_2,\ n_2)$ and $(p_1,\ q_1) \sim (p_2,\ q_2)$, then:*

$$(m_1,\ n_1) \oplus (p_1,\ q_1) = (m_2,\ n_2) \oplus (p_2,\ q_2)$$

Proof

Proof. From the definition of $\oplus$ it follows that:

- $(m_1,\ n_1) \oplus (p_1,\ q_1) = [(m_1 + p_1,\ n_1 + q_1)]$
- $(m_2,\ n_2) \oplus (p_2,\ q_2) = [(m_2 + p_2,\ n_2 + q_2)]$

From the definition of $\sim$, it follows that:

- $m_1 + n_2 = m_2 + n_1$
- $p_1 + q_2 = p_2 + q_1$

By additing the LHS and RHS of the two sides above, we get:

$$m_1 + n_2 + p_1 + q_2 = m_2 + n_1 + p_2 + q_1$$

By applying associativity and commutativity, it follows that:

$$(m_1 + p_1) + (n_2 + q_2) = (m_2 + p_2) + (n_1 + q_1)$$

Thus it follows that from the definition of $\sim$ that:

$$(m_1 + p_1,\ n_1 + q_1) \sim (m_2 + p_2,\ n_2 + q_2)$$

From the results on equivlance classes, it follows that:

$$[(m_1 + p_1,\ n_1 + q_1)] = [(m_2 + p_2,\ n_2 + q_2)]$$

Thus the result follows as a consequence of definition of $\oplus$ □

We can now define addition on **Z** using the $\oplus$ operation on $\mathbf{N} \times \mathbf{N}$, as it preserves equivalence relation $\sim$ (i.e. maps equivalent elements to the same element), and the addition as a consequence becomes a well defined function.

Definition

Definition 27. *Addition on integers (+) is a function* $+ : \mathbf{Z} \times \mathbf{Z} \to \mathbf{Z}$ *such that:*

$$[(m, n)] + [(p, q)] = (m, n) \oplus (p, q)$$

Where $[(m, n)]$ *and* $[(p, q)]$ *are elements of* **Z** *and* (m, n) *and* (p, q) *are any elements of the the respective equivalence classes.*

We now state the following properties of addition without proof, and they can be assumed to be axiomatic for the rest of the text. We briefly sketch the method by which they can be proved.

Theorem 17. *The following properties hold true for addition on integers:*

1. *Addition is associative:*

$$\forall x, y, z \in \mathbf{Z}.\ (x + y) + z = x + (y + z)$$

2. *Addition is commutative:*

$$\forall x, y \in \mathbf{Z}.\ x + y = y + x$$

3. *There exists an identity element:*

$$\exists e \in \mathbf{Z}.\forall x \in \mathbf{Z}.\ x + e = x = e + x$$

4. *For every integer, there exists an inverse:*

$$\forall x \in \mathbf{Z}.\exists \bar{x} \in \mathbf{Z}.\ x + \bar{x} = e = \bar{x} + x$$

Proof

Proof. We do not mathematically prove the result here but outline the proof method. Students inclined to the method of rigour may attempt to prove the results on their own. For results (1) and (2), we can prove the result by showing that $\oplus$ is associative and commutative on $(\mathbf{N} \times \mathbf{N}) \times (\mathbf{N} \times \mathbf{N})$. This is fairly straightforward since $\oplus$ is directly defined in terms of addition on natural numbers. Then one has to show that this translates into associativity and commutativity of $+$. For the existence of identity element, it is fairly clear that the e that is stated in the theorem corresponds to the number 0 as an integer. We consider the equivalence class of $(0, 0)$. By first proving that it equals identity for $\oplus$, one can prove that addition by $[(0, 0)]$ takes every equivalence class to itself.
For the existence of inverse, note that the order of quantifiers is different for inverse from identity, which stems from the fact that there is a unique identity element for every integer, while for each element in $\mathbf{Z}$, there exists an inverse element. We begin by showing that $(m, n) \oplus (n, m) \sim (0, 0)$ and then obtaining the corresponding result in terms of $+$.

□

Similarly, we can now define multiplication on integers. However, in this case pairwise multiplication does not give us the multiplication we seek on integers. Since $(n, 0) * (0, m) = (0, 0)$ which amounts to saying $n * (-m) = 0$, even when both n and m are non-zero. Inorder to define it recollect that the numbers $[(m, n)]$ and $[(p, q)]$ correspond to traditionally known integers $m - n$ and $p - q$ and $(m - n) * (p - q) = (mp + nq - (np + mq)$ which would equal the elements

$(mq+np, np+mq)$. For the sake of readability, in the case of multiplication we will skip defining the intermediate function on $(\mathbf{N} \times \mathbf{N}) \times (\mathbf{N} \times \mathbf{N})$ and directly define it on $\mathbf{Z}$. We will assume without proof that it is well-defined. Interested students may attempt to prove it as an exercise.

Definition

Definition 28. *Multiplication of integers* ($*$) *is a function* $* : \mathbf{Z} \times \mathbf{Z} \to \mathbf{Z}$ *such that:*

$$[(m,n)] * [(p,q)] = [(mp+nq, mq+np)$$

We will state the following results without proof. They can be treated as axiomatic hereon:

Theorem 18. *Following properties hold true for multiplication on integers:*

1. *Multiplication is associative:*

$$\forall x, y, z \in \mathbf{Z}.\ (x * y) * z = x * (y * z)$$

2. *Multiplication is commutative:*

$$\forall x, y \in \mathbf{Z}.\ x * y = y * x$$

3. *There exists an identity element for multiplication:*

$$\exists i \in \mathbf{Z}. \forall x \in \mathbf{Z}.\ x * i = x = i * x$$

4. *Multiplication of any integer with* 0 *results in* 0.

$$\forall z \in \mathbf{Z}.\ z * 0 = 0 = 0 * z$$

5. *Addition and multiplication are distributive:*

$$\forall a, b, c.\ (a+b) * c = a * c + b * c$$

$$\forall a, c, d.\ a * (c+d) = a * c + a * d$$

One may observe that multiplication does not allow for existence of inverse, unlike addition. This is on account of the fact that:

- 1 is the multiplicative identity of integers.
- Inverse of an integer does not exist (it can be proved). This holds true in what we conventionally know as well, that is multiplicative inverse of

2 is 1/2, which is not an integer but what we traditionally call a 'rational number'.

Thus we further define rational numbers to extend the integers to contain multiplicative inverses. In order to construct rationals, note that every rational number is of the form $\frac{p}{q}$, where p and q are integers such that $q \neq 0$. This can easily by encoded as a tuple or an element of the set $\mathbf{Z} \times (\mathbf{Z} \setminus \{0\})$. Further, two distinct rational numbers $\frac{p}{q}$ and $\frac{r}{s}$ are the same if and only if $ps = rq$. This can easily be described as a relation on $\mathbf{Z} \times (\mathbf{Z} \setminus \{0\})$, which infact turns out to be an equivalence relation (and which can be proved with some effort). Addition of two rational numbers $\frac{p}{q}$ and $\frac{r}{s}$ is equal to the rational number $\frac{ps+rq}{qs}$. This is used to define addition on rational numbers.

Theorem 19. *The relation $\sim$ on $\mathbf{Z} \times (\mathbf{Z} \setminus \{0\})$ given by:*

$$(p, q) \sim (r, s) \iff (ps = rq)$$

is an equivalence relation on $\mathbf{Z} \times (\mathbf{Z} \setminus \{0\})$

Proof

Proof. We leave the proof to the reader as an exercise. □

Definition

Definition 29. *Rational number $\mathbf{Q}$ is defined as the set of equivalence classes of $\mathbf{Z} \times (\mathbf{Z} \setminus \{0\})$ under the relation $\sim$ described in the previous theorem. We denote the equivalence class $[(p, q)]$ using $\frac{p}{q}$. Where (p, q) is an element of the equivalence class.*

Definition

Definition 30. *Addition of two rational number $+ : \mathbf{Q} \times \mathbf{Q} \to \mathbf{Q}$ is the function*

$$[(p, q)] + [(r, s)] = [(ps+rq, qs)]$$

$+$ refers to addition of the integers.

Definition

Definition 31. *Multiplication of two rational number $* : \mathbf{Q} \times \mathbf{Q} \to \mathbf{Q}$ is the function*

$$[(p, q)] * [(r, s)] = [(pr, qs)]$$

Theorem 20. *Addition and multiplication are well defined functions on* **Q***. Further they satisfy the following properties.*

1. *Addition is associative.*
2. *Addition is commutative.*
3. *There exists an additive identity.*
4. *For every rational number, there exists an additive inverse.*
5. *Multiplication is associative.*
6. *Multiplication is commutative.*
7. *There exists an multiplicative identity.*
8. *For every non-zero rational number, there exists a multiplicative inverse.*
9. *Addition and multiplication are distributive:*

$$\forall a, b, c.\ (a + b) * c = a * c + b * c$$

$$\forall a, c, d.\ a * (c + d) = a * c + a * d$$

Now rational numbers may not still contain elements such as roots, transcadental numbers and other exotic numbers that we are familiar with, and useful for mathematics (we leave out imaginary numbers for now). These traditionally belong to the domain of real numbers. We will not construct real numbers, since it is rather elaborate, but we will rather describe real numbers through a series of axioms such that a set satisfying those conditions can be assumed to be real:

Definition

Definition 32. *Real number* $\mathbf{R}$ *is a set with addition, multiplication and order defined such that:*

- *Addition is associative, commutative, has additive identity and every element of reals has an additive inverse.*
- *Multiplication is associative, commutative, has multiplicative identity and every non-zero element of reals has a multiplicative inverse.*
- *Addition and multiplication obey distribution properties.*
- *Given and* $x \in \mathbf{R}$, *either* $x < 0$, $x > 0$ *or* $x = 0$.
- *Given any set* $S \subseteq R$ *such that* $\exists p \in \mathbf{R}$ *such that* $\forall x \in S.\ x < p$, *there exists an element* $r \in \mathbf{R}$ *such that* $\forall x \in S.\ x \leq r$ *and* $(y < x) \implies (\exists s \in S.\ y < s)$.