

Sheet 1: Basics

Definition 1 (Empty Set) The empty set is denoted by \emptyset ; it contains no elements

Definition 2 (Element) Instead of saying “ A contains a ,” we say that a is an element of A , and write this as $a \in A$. For the converse statement, that a is not an element of A , we write $a \notin A$.

Exercise 3 Is it true that every element of the empty set is a whistling, flying purple cow?

Yes. Since the empty set has no elements, it is vacuously true that all elements are whistling, flying purple cows.

Definition 4 (Subset) Let A and B be sets. If each element of A is also an element of B , we say that A is a subset of B . In symbols $A \subseteq B$.

Exercise 5 How many subsets does the empty set have?

Proof. The empty set has no elements and so the only set which could contain every element of \emptyset is \emptyset . So the empty set has only one subset, itself. \square

Exercise 6 Let $A_n = \{1, 2, \dots, n\}$. How many subsets does A_n have?

A_n has 2^n subsets.

Proof. We use induction on n . We see that the statement is true for $n = 1$ since $\{1\}$ has one element and its only subsets are $\{1\}$ and \emptyset and $2 = 2^1$. Let S_k be the set $\{1, 2, 3, \dots, k\}$. Then we assume S_k has 2^k subsets and show that S_{k+1} has 2^{k+1} subsets. Consider a set A such that $A \subseteq S_{k+1}$. Then we see that either $(k+1) \in A$ or $(k+1) \notin A$. Let $(k+1) \notin A$. Then $A \subseteq S_k$. But then there exists a set $A \cup \{k+1\} \subseteq S_{k+1}$ for every $A \subseteq S_k$. Therefore, for every subset A of S_k , A and $A \cup \{k+1\}$ are subsets of S_{k+1} . Thus, S_{k+1} has at least $2 \cdot 2^k = 2^{k+1}$ subsets since there are 2^k subsets of S_k .

But suppose there are more than 2^{k+1} subsets of S_{k+1} . Then there exists a subset B of S_{k+1} such that $B \not\subseteq S_k$ and $B \setminus \{k+1\} \not\subseteq S_k$. Then there exists a $b \in B$ such that $b \notin S_k$ and $b \neq k+1$. Since $B \subseteq S_{k+1}$, $b \in S_{k+1}$. But $S_k \cap S_{k+1} = S_k$ which means that S_{k+1} contains every element in S_k as well as $k+1$. Therefore, $b \in S_k$ or $b = k+1$. This is a contradiction. Therefore, S_{k+1} must have exactly 2^{k+1} subsets. \square

Exercise 7 What is the number of subsets of A_n that contain exactly 2 elements?

$\binom{n}{2} = \frac{n(n-1)}{2}$ subsets.

Proof. We note that in $A_1 = \{1\}$ there is only one element and so there are no subsets with 2 elements. So the theorem holds for $n = 1$ since $\frac{1(1-1)}{2} = 0$. We now assume that A_n has $\frac{n(n-1)}{2}$ subsets of size 2. The set A_{n+1} has $n+1$ elements and $A_{n+1} \setminus A_n = \{n+1\}$. So for every $k \in A_n$ there exists a subset $\{k, n+1\} \subseteq A_{n+1}$. Since there are n elements in A_n we have n more subsets of size 2 in A_{n+1} . So there are $\frac{n(n-1)}{2} + n = \frac{n^2 - n + 2n}{2} = \frac{n(n+1)}{2} = \frac{(n+1)(n+1-1)}{2}$ subsets of A_{n+1} of size 2. So the statement holds for $n = 1$ and $n+1$ when it holds for n so it must hold for all $n \in \mathbb{N}$. \square

Definition 8 (Union, Intersection, Difference and Direct Product) If A and B are sets then:

$$A \cup B = \{x \mid x \in A \text{ or } x \in B\}$$

the union of A and B ;

$$A \cap B = \{x \mid x \in A \text{ and } x \in B\}$$

the intersection of A and B and

$$A \setminus B = \{x \mid x \in A \text{ and } x \notin B\}$$

the difference of A and B . If $B = \{b\}$ is the set consisting of a single element b , we will write $A \setminus b$ rather than $A \setminus \{b\}$. Finally

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

the set of ordered pairs from A and B . The set $A \times B$ is called the direct product of A and B .

Definition 9 (Union and Intersection of Many Sets) Let S be a set consisting of sets. Then the intersection and union of S is defined as follows:

$$\bigcup_{A \in S} A = \{x \mid \text{there exists } A \in S \text{ such that } x \in A\}$$

and

$$\bigcap_{A \in S} A = \{x \mid \text{for all } A \in S \text{ we have } x \in A\}.$$

Theorem 10 Let X be a set and let S be a set consisting of subsets of X . Then

$$X \setminus \left(\bigcup_{A \in S} A \right) = \bigcap_{A \in S} (X \setminus A)$$

and

$$\bigcup_{A \in S} (X \setminus A) = X \setminus \left(\bigcap_{A \in S} A \right).$$

Proof. Let X be a set and let S be a set consisting of subsets of X .

Let $a \in X \setminus \left(\bigcup_{A \in S} A \right)$. Then $a \in X$ and $a \notin \left(\bigcup_{A \in S} A \right)$. That is, $a \notin A$ for all sets $A \in S$. Thus, for all sets $A \in S$, $a \in X \setminus A$. Since this is true for all sets $A \in S$ we may write $a \in \bigcap_{A \in S} (X \setminus A)$.

Let $a \in \bigcap_{A \in S} (X \setminus A)$. Thus, $a \in X$ and $a \notin A$ for every set $A \in S$. Since $a \notin A$ for all $A \in S$ we can state that $a \notin \bigcup_{A \in S} A$. But since $a \in X$, we can now write $a \in X \setminus \left(\bigcup_{A \in S} A \right)$.

Let $a \in \bigcup_{A \in S} (X \setminus A)$. Thus, $a \in X$ and $a \notin A$ for at least one $A \in S$. Since $a \notin A$ for at least one $A \in S$, then we can write $a \notin \bigcap_{A \in S} A$. But since $a \in X$, we can now write $a \in X \setminus \left(\bigcap_{A \in S} A \right)$.

Let $a \in X \setminus \left(\bigcap_{A \in S} A \right)$. Thus, $a \in X$, but $a \notin A$ for at least one $A \in S$. In other words, $a \in X \setminus A$ for at least one $A \in S$. Therefore we may write $a \in \bigcup_{A \in S} (X \setminus A)$.

Since we have shown both inclusions for both of De Morgan's Laws, we can conclude the result is true. \square

Definition 11 (Function) A function $f : A \rightarrow B$ is defined as a subset of $A \times B$ such that for all $a \in A$ there exists a unique $b \in B$ with $(a, b) \in f$. Instead of $(a, b) \in f$ we will use the notation $f(a) = b$.

Definition 12 (Domain and Range) The domain of f is A . The range of f (image under f) is

$$f(A) = \{f(a) \mid a \in A\}.$$

Definition 13 (Surjective, Injective and Bijective) A function $f : A \rightarrow B$ is surjective (onto) if $f(A) = B$. It is injective (1 to 1) if for all $a_1, a_2 \in A$, if $f(a_1) = f(a_2)$ then $a_1 = a_2$. It is bijective if it is surjective and injective.

Definition 14 (Inverse Function) Let $f : A \rightarrow B$ be a bijection. Then the inverse of f , $f^{-1} : B \rightarrow A$ is defined by

$$(b, a) \in f^{-1} \text{ if and only if } (a, b) \in f.$$

Definition 15 (Image and Preimage) Let $f : A \rightarrow B$ be a function. Let $X \subseteq A$. Then the image of X under f is

$$f(X) = \{f(x) \mid x \in X\}.$$

Let $Y \subseteq B$. Then the preimage of Y under f is

$$f^{-1}(Y) = \{x \in A \mid f(x) \in Y\}.$$

Exercise 16 $f^{-1}(f(X)) = X$ for all $X \subseteq A$.

False. Let $A = \{1, 2\}$ and $B = \{3\}$ such that $f(1) = f(2) = 3$. Then $f(\{1\}) = \{3\}$. But $f^{-1}(\{3\}) = \{1, 2\} \neq \{1\}$. We can prove the statement if we assume f is injective.

Proof. Let $f : A \rightarrow B$ be an injective function. Let $X \subseteq A$. Suppose $a \in f^{-1}(f(X))$. Then $a \in A$ and $f(a) \in f(X)$ which means there exists some $b \in X$ such that $f(b) = f(a)$. But f is injective and so $a = b$ and $a \in X$. Therefore $f^{-1}(f(X)) \subseteq X$. Now suppose $a \in X$. Then $f(a) \in f(X)$ and $a \in f^{-1}(f(X))$. Thus $X \subseteq f^{-1}(f(X))$. Since both sets are subsets of each other, they are equal. \square

Exercise 17 $f(f^{-1}(Y)) = Y$ for all $Y \subseteq B$.

False. Let $A = \{1, 2\}$ and $B = \{3, 4\}$ such that $f(1) = f(2) = 3$. Then $f^{-1}(B) = \{1, 2\}$. But $f(\{1, 2\}) = \{3\} \neq B$. We can prove the statement if we assume f is surjective.

Proof. Let $f : A \rightarrow B$ be a surjective function. Let $Y \subseteq B$. Suppose $b \in f(f^{-1}(Y))$. Then there exists an $a \in f^{-1}(Y)$ such that $f(a) = b$ and so $f(a) \in f(f^{-1}(Y))$. Then $a \in f^{-1}(Y)$ and so $f(a) \in Y$. Thus $b \in Y$ and so $f(f^{-1}(Y)) \subseteq Y$. Now let $b \in Y$. Since f is surjective, $f(A) = B$ and so there exists an element $a \in A$ such that $f(a) = b$. Thus $f(a) \in Y$. Then $a \in f^{-1}(Y)$ and $f(a) \in f(f^{-1}(Y))$. Thus, $Y \subseteq f(f^{-1}(Y))$. Again, since both sets are subsets of each other, they must be equal. \square

Exercise 18 $f(X_1 \cap X_2) = f(X_1) \cap f(X_2)$ for all X_1 and $X_2 \subseteq A$.

False. Let $f : A \rightarrow B$ be a function such that $X_1 = \{1, 3\}$ and $X_2 = \{2, 3\}$ are subsets of A . Let $f(1) = f(2) = 10$ and $f(3) = 11$. Then we see that $f(X_1) = \{10, 11\}$ and $f(X_2) = \{10, 11\}$ and so $f(X_1) \cap f(X_2) = \{10, 11\}$. But $X_1 \cap X_2 = \{3\}$ and so $f(X_1 \cap X_2) = \{11\}$. We can prove the statement if we assume f is injective.

Proof. Let $f : A \rightarrow B$ be an injective function and let X_1 and X_2 be subsets of A . Suppose $b \in f(X_1 \cap X_2)$. Then there exists an $a \in X_1 \cap X_2$ such that $f(a) = b$. Thus, $a \in X_1 \cap X_2$ and so $a \in X_1$ and $a \in X_2$. Therefore $f(a) \in f(X_1)$ and $f(a) \in f(X_2)$ and so $f(a) \in f(X_1) \cap f(X_2)$ and $b \in f(X_1) \cap f(X_2)$. Thus, $f(X_1 \cap X_2) \subseteq f(X_1) \cap f(X_2)$.

Now suppose $a \in f(X_1) \cap f(X_2)$. Then $a \in f(X_1)$ and $a \in f(X_2)$. Then there exists a $b \in X_1$ such that $f(b) = a$ and a $c \in X_2$ such that $f(c) = a$. But since f is injective and $f(b) = f(c)$, then $b = c$ and so $b \in X_1$ and $b \in X_2$. Thus $b \in X_1 \cap X_2$ and so $f(b) \in f(X_1 \cap X_2)$ and $a \in f(X_1 \cap X_2)$. Therefore $f(X_1) \cap f(X_2) \subseteq f(X_1 \cap X_2)$. Since both sets are subsets of each other, they are equal. \square

Exercise 19 $f^{-1}(Y_1 \cap Y_2) = f^{-1}(Y_1) \cap f^{-1}(Y_2)$ for all Y_1 and $Y_2 \subseteq B$.

Proof. Let $f : A \rightarrow B$ be a function and let Y_1 and Y_2 be subsets of B . Let $b \in f^{-1}(Y_1 \cap Y_2)$. Then $f(b) \in Y_1 \cap Y_2$ and so $f(b) \in Y_1$ and $f(b) \in Y_2$. Thus $b \in f^{-1}(Y_1)$ and $b \in f^{-1}(Y_2)$ and so $b \in f^{-1}(Y_1) \cap f^{-1}(Y_2)$. Therefore $f^{-1}(Y_1 \cap Y_2) \subseteq f^{-1}(Y_1) \cap f^{-1}(Y_2)$.

Now let $b \in f^{-1}(Y_1) \cap f^{-1}(Y_2)$. Then $b \in f^{-1}(Y_1)$ and $b \in f^{-1}(Y_2)$. Thus $f(b) \in Y_1$ and $f(b) \in Y_2$ and so $f(b) \in Y_1 \cap Y_2$. Therefore $b \in f^{-1}(Y_1 \cap Y_2)$. Thus $f^{-1}(Y_1) \cap f^{-1}(Y_2) \subseteq f^{-1}(Y_1 \cap Y_2)$. Since both sets are subsets of each other, they are equal. \square

Exercise 20 $f(X_1 \cup X_2) = f(X_1) \cup f(X_2)$ for all $X_1, X_2 \subseteq A$.

Proof. Let $f : A \rightarrow B$ be a function and let X_1 and X_2 be subsets of A . Let $a \in f(X_1 \cup X_2)$. Then there exists a $b \in X_1 \cup X_2$ such that $f(b) = a$. Then $b \in X_1 \cup X_2$ which means $b \in X_1$ or $b \in X_2$. Thus $f(b) \in f(X_1)$ or $f(b) \in f(X_2)$ and so $f(b) \in f(X_1) \cup f(X_2)$ and $a \in f(X_1) \cup f(X_2)$. Therefore $f(X_1 \cup X_2) \subseteq f(X_1) \cup f(X_2)$.

Now let $a \in f(X_1) \cup f(X_2)$. Then $a \in f(X_1)$ or $a \in f(X_2)$. So there exists a $b \in X_1$ and $c \in X_2$ such that $a = f(b) = f(c)$ and $f(b) \in f(X_1)$ or $f(c) \in f(X_2)$. Thus $b \in X_1$ or $c \in X_2$. Therefore $b, c \in X_1 \cup X_2$ and so $f(b), f(c) \in f(X_1 \cup X_2)$ and $a \in f(X_1 \cup X_2)$. Thus $f(X_1) \cup f(X_2) \subseteq f(X_1 \cup X_2)$. Since both sets are subsets of each other, they are equivalent. \square

Exercise 21 $f^{-1}(Y_1 \cup Y_2) = f^{-1}(Y_1) \cup f^{-1}(Y_2)$ for all $Y_1, Y_2 \subseteq B$.

Proof. Let $f : A \rightarrow B$ be a function and let Y_1 and Y_2 be subsets of B . Let $a \in f^{-1}(Y_1 \cup Y_2)$. Then $f(a) \in Y_1 \cup Y_2$ which means $f(a) \in Y_1$ or $f(a) \in Y_2$. Thus $a \in f^{-1}(Y_1)$ or $a \in f^{-1}(Y_2)$ and so $a \in f^{-1}(Y_1) \cup f^{-1}(Y_2)$. Therefore $f^{-1}(Y_1 \cup Y_2) \subseteq f^{-1}(Y_1) \cup f^{-1}(Y_2)$.

Now let $a \in f^{-1}(Y_1) \cup f^{-1}(Y_2)$. Thus $a \in f^{-1}(Y_1)$ or $a \in f^{-1}(Y_2)$ which means $f(a) \in Y_1$ or $f(a) \in Y_2$. Therefore $f(a) \in Y_1 \cup Y_2$ and so $a \in f^{-1}(Y_1 \cup Y_2)$. Thus $f^{-1}(Y_1) \cup f^{-1}(Y_2) \subseteq f^{-1}(Y_1 \cup Y_2)$. Since both sets are subsets of each other, they are equivalent. \square

Theorem 22 $f(f^{-1}(f(X))) = f(X)$ for all $X \subseteq A$.

Proof. Let $f : A \rightarrow B$ be a function and let $X \subseteq A$. Let $a \in f(f^{-1}(f(X)))$. Then there exists some $b \in f^{-1}(f(X))$ such that $a = f(b)$. Since $b \in f^{-1}(f(X))$ we have $f(b) \in f(X)$ and so $a \in f(X)$. Thus $f(f^{-1}(f(X))) \subseteq f(X)$. Now let $a \in f(X)$. Then there exists a $b \in X$ such that $f(b) = a$. Since $f(b) \in f(X)$, $b \in f^{-1}(f(X))$. But then $f(b) \in f(f^{-1}(f(X)))$. Thus $f(X) \subseteq f(f^{-1}(f(X)))$. Since the sets are subsets of each other, they are equal. \square

Theorem 23 $f^{-1}(f(f^{-1}(Y))) = f^{-1}(Y)$ for all $Y \subseteq B$.

Proof. Let $f : A \rightarrow B$ be a function and let $Y \subseteq B$. Let $a \in f^{-1}(f(f^{-1}(Y)))$. Then $f(a) \in f(f^{-1}(Y))$ and so there exists a $b \in f^{-1}(Y)$ such that $f(a) = f(b)$. But then $f(b) \in Y$ and so $f(a) \in Y$ and $a \in f^{-1}(Y)$. Thus $f^{-1}(f(f^{-1}(Y))) \subseteq f^{-1}(Y)$. Now let $a \in f^{-1}(Y)$. Then $f(a) \in f(f^{-1}(Y))$ and $a \in f^{-1}(f(f^{-1}(Y)))$. Thus, $f^{-1}(Y) \subseteq f^{-1}(f(f^{-1}(Y)))$ and since the sets are subsets of each other, they must be equal. \square

Problem 24 Try to define the direct product of infinitely many sets.

For the sets A_1, A_2, A_3, \dots , we define the direct product of the sets as

$$A_1 \times A_2 \times A_3 \cdots = \{(a_1, a_2, a_3, \dots) \mid a_i \in A_i \text{ for every } i \in \mathbb{N}\}$$

Definition 25 (Equivalence Relation) Let A be a set. Then $\sim \subseteq A \times A$ is an equivalence relation if the following hold:

- 1) For all $a \in A$ we have $a \sim a$ (reflexivity);
- 2) For all $a, b \in A$, if $a \sim b$ then $b \sim a$ (reflexivity);
- 3) For all $a, b, c \in A$, if $a \sim b$ and $b \sim c$ then $a \sim c$ (transitivity).

Exercise 26 L is the set of lines on the plane. For $a, b \in L$ let $a \sim b$ if a and b are parallel.

Proof. We see that $a \sim b$ is reflexive because every line a has the same slope as itself and is therefore parallel to itself. We also see that it is symmetric as two lines which are parallel have the same slope and so $a \sim b$ implies $b \sim a$. Additionally, if we take three lines a, b and c such that a has the same slope as b and b has the same slope as c then a must have the same slope as c and so $a \sim b$ and $b \sim c$ implies $a \sim c$. Since all three conditions are met, the relation is an equivalence relation. \square

Exercise 27 For $a, b \in L$ let $a \sim b$ if a and b intersect each other.

This is not an equivalence relation since it fails the transitive property. If we take two lines a and c to be parallel, then a line b may intersect both of them, but it doesn't imply that a intersects c .

Exercise 28 For $a, b \in \mathbb{Z}$ let $a \sim b$ if $a - b$ is even.

Proof. We see that \sim is reflexive since for some $a \in \mathbb{Z}$ $a - a = 0$ which is even so $a \sim a$. Also, if $a \sim b$ for $a, b \in \mathbb{Z}$ then $a - b = 2k$ for some $k \in \mathbb{Z}$ and so $b - a = -2k = 2(-k)$. Since $-k \in \mathbb{Z}$, $b - a$ is even and so $b \sim a$. Finally, if $a \sim b$ and $b \sim c$, then $a - b = 2k$ and $b - c = 2l$ for some $k, l \in \mathbb{Z}$. Then adding the equations we have $a - c = 2k + 2l = 2(k + l)$. Since $k + l \in \mathbb{Z}$, $a - c$ is even and $a \sim c$. Since the relation satisfies all three properties, it is an equivalence relation. \square

Exercise 29 For $a, b \in \mathbb{Z}$ let $a \sim b$ if $a - b$ is odd.

This relation fails the reflexive test since for all $a \in \mathbb{Z}$, $a - a = 0$ which is not odd and so $a \not\sim a$.

Exercise 30 For $a, b \in \mathbb{Z}$ let $a \sim b$ if $a - b$ is divisible by 7.

Proof. We see that \sim is reflexive since for some $a \in \mathbb{Z}$ $a - a = 0$ which is divisible by 7 so $a \sim a$. Also, if $a \sim b$ for $a, b \in \mathbb{Z}$ then $a - b = 7k$ for some $k \in \mathbb{Z}$ and so $b - a = -7k = 7(-k)$. Since $-k \in \mathbb{Z}$, $b - a$ is divisible by 7 and so $b \sim a$. Finally, if $a \sim b$ and $b \sim c$, then $a - b = 7k$ and $b - c = 7l$ for some $k, l \in \mathbb{Z}$. Then adding the equations we have $a - c = 7k + 7l = 7(k + l)$. Since $k + l \in \mathbb{Z}$, $a - c$ is divisible by 7 and $a \sim c$. Since the relation satisfies all three properties, it is an equivalence relation. \square

Exercise 31 Do 2) and 3 imply 1)?

No. We can use a counterexample where L is the set of lines on the plane and for $a, b \in L$, $a \sim b$ if a and b never intersect. Then $a \sim a$ since a always intersects a . But if a never intersects b , then b never intersects a and so we have symmetry. And for $a, b, c \in L$ such that $a \neq c$, if $a \sim b$ and $b \sim c$, then $a \sim c$ so we have

transitivity.

Definition 32 (Equivalence Class) Let A be a set and let \sim be an equivalence relation on A . Then for $a \in A$, the \sim -equivalence class of a is defined as:

$$\bar{a} = \{x \in A \mid a \sim x\}.$$

Theorem 33 We have

$$\bigcup_{a \in A} \bar{a} = A$$

Furthermore, for all $a, b \in A$ we have

$$\bar{a} = \bar{b} \text{ or } \bar{a} \cap \bar{b} = \emptyset.$$

Proof. Let A be a set and let \sim be an equivalence relation on A . Let $x \in \bigcup_{a \in A} \bar{a}$. Then $x \in \bar{a}$ for some $a \in A$. By definition, $x \in \{m \in A \mid a \sim m\}$ and so $x \in A$. Therefore, $\bigcup_{a \in A} \bar{a} \subseteq A$. Now suppose $x \in A$. Since \sim is an equivalence relation on A , we know $x \sim x$ and so $x \in \bar{x}$. Thus $x \in \bigcup_{a \in A} \bar{a}$ and $A \subseteq \bigcup_{a \in A} \bar{a}$.

Suppose that there exist $a, b \in A$ such that $\bar{a} \neq \bar{b}$ and $\bar{a} \cap \bar{b} \neq \emptyset$. Then there exists an x such that $x \in \bar{a}$ and $x \in \bar{b}$ and so $a \sim x$ and $b \sim x$. But then $x \sim b$ and so $a \sim b$ and $b \sim a$. Now if we choose an element $c \in \bar{a}$ we see that $a \sim c$. But also $c \sim a$, $c \sim b$ and $b \sim c$. This implies that $c \in \bar{b}$ and so $\bar{a} \subseteq \bar{b}$. A similar argument is used to show that $\bar{b} \subseteq \bar{a}$. Thus, $\bar{a} = \bar{b}$ which is a contradiction. \square

Exercise 34 Try to write a formal definition of a partition.

We define a partition of a set A to be a set P consisting of n subsets of A such that

$$\bigcup_{S \in P} S = A,$$

where S is a subset of A , and $S_i \cap S_j = \emptyset$ for all $1 \leq i, j \leq n$.

Exercise 35 How does a partition naturally define an equivalence relation on a set A ?

A partition will divide a set into separate equivalence classes \bar{a}_i . If $x \in A$ and $x \in \bar{a}_i$ then $a_i \sim x$. Thus, the equivalence relation \sim is defined by which equivalence class x falls into.

Exercise 36 How many equivalence classes are there in Exercise 30?

There are 7 equivalence classes. For the proof, we first prove a lemma showing that every $x \in \mathbb{Z}$ can be written as $x = 7n + k$ where $k \in \{0, 1, 2, 3, 4, 5, 6\}$.

Proof. Let $x \in \mathbb{N} \cup \{0\}$ and let $S = \{0, 1, 2, 3, 4, 5, 6\}$. Then let $T = \{k \in \mathbb{N} \cup \{0\} \mid \text{there exists } n \in \mathbb{Z} \text{ such that } x = 7n + k\}$. Then we see that $T \neq \emptyset$ since $x = 7(0) + x$ and $x \in \mathbb{N} \cup \{0\}$ and $n \in \mathbb{Z}$. Then we see there exists a least element m of T and so $x = 7n + m$ for some $n \in \mathbb{Z}$. If $m \in S$ then we are done. If $m \notin S$ then $m > 7$ and so $m - 7 > 0$. Therefore we can write $x = 7(n + 1) + (m - 7)$ and so $(m - 7) \in T$. But $m - 7 < m$ and since m is the least element of T this is a contradiction so $m \in S$. Therefore every $x \in \mathbb{N} \cup \{0\}$ can be written as $7n + k$ for some $n \in \mathbb{Z}$ and $k \in S$. We now consider the case where $x \in \mathbb{Z} \setminus (\mathbb{N} \cup \{0\})$. We see that $-x = -7n - k = 7(-n - 1) + (-k + 7)$. But if $k \neq 0$ then $-k + 7 \in S$ and if $k = 0$ then $x = 7n$ and so $-x = 7(-n)$ and so we see that for $x \in \mathbb{Z}$ we can write $x = 7n + k$ for $n \in \mathbb{Z}$ and $k \in S$. \square

Now we prove the original result.

Proof. Let $x \in \mathbb{Z}$ and let $S = \{0, 1, 2, 3, 4, 5, 6\}$. Then we see that $x = 7n + k$ and $x - k = 7n$ for some $n \in \mathbb{Z}$ and $k \in S$. But then $x \sim k$ and so $x \in \bar{k}$. Since there are only 7 possible values for k , we see that there are at most 7 equivalence classes. If we choose two elements $p, q \in S$ such that $p \neq q$ then without loss of generality we can assume $p > q$ and so $(p - q) \in S$. But then $p - q \neq 7n$ for some $n \in \mathbb{Z}$ and so $p \not\sim q$ and $\bar{p} \neq \bar{q}$. So no two equivalence classes are the same. Additionally, for every $p \in S$ we see that $p = 7(0) + p$ and since $0 \in \mathbb{Z}$ and $p \in S$, we see every element of p is in an equivalence class. So we see that there are at least 7 and at most 7 equivalence classes so there must be exactly 7 equivalence classes. \square

Problem 37 Try to find a way to multiply and add the equivalence classes from Exercise 30.

It seems that if $a \in \bar{a}$ and $b \in \bar{b}$ then $(a + b) \in \overline{a + b}$ and $ab \in \overline{ab}$. Also, for a scalar c , $ca \in \overline{ca}$ for all $a \in \bar{a}$.

Definition 38 (Ordering) Let A be a set. Then $< \subseteq A \times A$ is an ordering if the following hold:

- 1) For all $x, y \in A$ such that $x \neq y$ we have $x < y$ or $y < x$;
- 2) For all $x, y \in A$ if $x < y$ then $x \neq y$;
- 3) For all $x, y, z \in A$ if $x < y$ and $y < z$ then $x < z$.

Theorem 39 If $x, y \in A$, then it cannot be true that both $x < y$ and $y < x$.

Proof. Suppose that $x < y$ and $y < x$. Then $x < x$ and so $x \neq x$. This is a contradiction. \square

Sheet 2: The Continuum

Axiom 1 *There is at least one point in C .*

Axiom 2 *The relation $<$ is an ordering on C .*

Definition 1 (First and Last Point) *If $A \subseteq C$ is a subset, then a point $a \in A$ is called a first point of A if for all $x \in A$, either $x = a$ or $a < x$. The last point is defined analogously.*

Lemma 2 *Every nonempty finite set of points of C has a first and a last point*

Proof. A subset of C with one element, a , has a first point and a last point since for every element x in the set, $a = x$ or $a < x$ and for every element x in the set, $a = x$ or $a > x$. So a is the first point and the last point. We now consider a set $S \subseteq C$ which has n elements and since $n \in \mathbb{N}$ we can use induction on n . We assume every subset of C with n elements has a first point and a last point. Now let T be a set with $n + 1$ elements. Consider the set $T \setminus \{a\}$ for some $a \in T$. $T \setminus \{a\}$ has n elements so it has a first point x and a last point y . Since $a \notin T \setminus \{a\}$ we see that $a \neq x$ and $a \neq y$. Because $<$ is an ordering on C , we have four cases:

Case 1: Let $a < x$ and $a < y$. Then a is less than every point in T and y is greater than every point in T so the first and last points are a and y .

Case 2: Let $x < a$ and $a < y$. Then a is between x and y and so x is the first point of T and y is the last point.

Case 3: Let $x < a$ and $y < a$. Then x is less than every point in T and a is greater than every point in T so the first and last points are x and a .

Case 4: Let $a < x$ and $a > y$. Since we know that $x < y$ (because x is the first point of $T \setminus \{a\}$), then we have $a < x$ and $x < y$ so $a < y$. But this is a contradiction so this case is impossible.

We see that in all possible cases T has $n + 1$ elements and has a first point and a last point. Thus, by induction, every nonempty finite subset of C has a first and a last point. □

Theorem 3 *Let A be a nonempty finite set of points of C . If A contains n points, then we can label them as a_1, a_2, \dots, a_n in such a way that $a_1 < a_2, a_2 < a_3, \dots, a_{n-1} < a_n$. (In other words, $a_i < a_{i+1}$ for $i = 1, 2, \dots, n - 1$.)*

Proof. A subset of C with one element can be indexed by labeling it a_1 . Now let S be a subset of C with n elements. Since $n \in \mathbb{N}$ we can use induction on n . We assume that every subset of C with n elements can be indexed as a_1, a_2, \dots, a_n such that $a_i < a_{i+1}$ for $i = 1, 2, \dots, n - 1$. Now consider a set T with $n + 1$ elements. By Lemma 2 we know that T has a first point and a last point. Let x be the last point. We see that $T \setminus \{x\}$ has n elements and so it can be indexed a_1, a_2, \dots, a_n so that $a_i < a_{i+1}$ for $i = 1, 2, \dots, n - 1$. We now call x, a_{n+1} . We see that T can be indexed since $a_n < a_{n+1}$ and so $a_i < a_{i+1}$ for $i = 1, 2, \dots, n$. Since a set with one element can be indexed, and a set with $n + 1$ elements can be indexed whenever a set with n elements can be indexed, we see that all nonempty finite sets can be indexed. □

Definition 4 (Betweenness) *Let x, y, z be points of C . We say that y lies between x and z if $x < y$ and $y < z$.*

Corollary 5 *Of three distinct points, one always lies between the other two.*

Proof. By Theorem 3, we can label three distinct points in a set a_1, a_2 and a_3 such that $a_1 < a_2$ and $a_2 < a_3$. Thus a_2 will always be between a_1 and a_3 . □

Axiom 3 The continuum C has no first point and no last point.

Corollary 6 C is infinite.

Proof. Suppose, to the contrary, that C is finite. Then by Axiom 1 C has at least one point and by Lemma 2 C has a first and last point. But this defies Axiom 3. This is a contradiction. \square

Definition 7 (Region) Let a, b be points in C such that $a < b$. The set of all points that lie between a and b is called the region $(a; b)$.

Theorem 8 For every point $p \in C$, there exists a region containing p .

Proof. Since C has no first and last points then for every $p \in C$ there exist $a, b \in C$ such that $a < p$ and $p < b$. Therefore, since p is between a and b , p is contained in the region $(a; b)$. \square

Definition 9 (Limit Point) Let $A \subseteq C$ be a subset. A point p is called a limit point of A if for every region R that contains p , R contains at least one point in A other than p . In other words, for every region R such that $p \in R$ we have

$$R \cap (A \setminus p) \neq \emptyset.$$

Theorem 10 Let $A \subseteq B \subseteq C$ be subsets. If some point p is a limit point of A , then it is also a limit point of B .

Proof. Let $A \subseteq B \subseteq C$ be subsets. If p is a limit point of A , then for every region R containing p , it also contains at least one point in A . But since $A \subseteq B$, all points in A are also in B . Thus, if R contains at least one point in A , then it also contains at least one point in B . Therefore p must also be a limit point for B . \square

Definition 11 (Exterior) Let $(a; b)$ be a region. Then $C \setminus (a; b) \setminus a \setminus b$ is called the exterior of $(a; b)$; the symbol is $\text{ext}(a; b)$.

Lemma 12 For any region $(a; b)$, we have

$$C = \{x \mid x < a\} \cup \{a\} \cup (a; b) \cup \{b\} \cup \{x \mid b < x\}.$$

Proof. Let $(a; b)$ be a region in C . Suppose there is an element $k \in C$ such that $k \notin \{x \mid x < a\} \cup \{a\} \cup (a; b) \cup \{b\} \cup \{x \mid b < x\}$. Then $k \neq a$ and $k \neq b$. But also $k \notin (a; b)$ and so k is not between a and b . Thus $k \not> a$ or $k \not< b$ which means $k < a$ or $k > b$. But we see that $k \notin \{x \mid x < a\}$ and $k \notin \{x \mid b < x\}$. This is a contradiction. \square

Lemma 13 For any region $(a; b)$, we have

$$C = \text{ext}(a; b) \cup (a; b) \cup \{a\} \cup \{b\}$$

Proof. We see that $\text{ext}(a; b) = C \setminus (a; b) \setminus a \setminus b$. Thus $\text{ext}(a; b) \cup \{b\} = C \setminus (a; b) \setminus a$ and likewise $\text{ext}(a; b) \cup \{a\} \cup \{b\} = C \setminus (a; b)$. Thus $\text{ext}(a; b) \cup \{a\} \cup \{b\} \cup (a; b) = C$. \square

Lemma 14 No point of the exterior of a region is a limit point of the region. No point of a region is a limit point of the exterior of the region.

Proof. Let $A = (a; b)$ be a region and let $p \in \text{ext}(A)$. Suppose $p < a$. Then there exists a point $x \in \text{ext}(A)$ such that $x < p$. So we have $(x; a)$ is a region containing p , which contains no points in A . We can make a similar statement if $p > b$. Likewise, if $p \in A$, then A is a region containing p , but no points in A are in $\text{ext}(A)$ so p cannot be a limit point of $\text{ext}(A)$. \square

Theorem 15 *If two regions A and B have a point x in common, then $A \cap B$ is also a region containing x .*

Proof. Let $A = (a_1, a_2)$ and $B = (b_1, b_2)$ be regions such that $x \in A$ and $x \in B$. Then we see that $x \in A \cap B$. Without loss of generality, let $a_1 = b_1$ or $a_1 < b_1$. Then we see that $a_2 > b_1$, otherwise $A \cap B = \emptyset$. Thus there are six cases.

Case 1: Let $a_1 < b_1$ and $a_2 < b_2$. Then we have $a_1 < b_1 < a_2 < b_2$ and so $A \cap B = (b_1, a_2)$.

Case 2: Let $a_1 < b_1$ and $a_2 > b_2$. Then we have $a_1 < b_1 < b_2 < a_2$ and so $A \cap B = (b_1, b_2)$.

Case 3: Let $a_1 < b_1$ and $a_2 = b_2$. Then we have $a_1 < b_1 < b_2 = a_2$ and so $A \cap B = (b_1, b_2)$.

Case 4: Let $a_1 = b_1$ and $a_2 < b_2$. Then we have $b_1 = a_1 < a_2 < b_2$ and so $A \cap B = (b_1, a_2)$.

Case 5: Let $a_1 = b_1$ and $a_2 > b_2$. Then we have $a_1 = b_1 < b_2 < a_2$ and so $A \cap B = (b_1, b_2)$.

Case 6: Let $a_1 = b_1$ and $a_2 = b_2$. Then we have $a_1 = b_1 < b_2 = a_2$ and so $A \cap B = (b_1, b_2)$.

We see that in all cases, $A \cap B$ is a region which contains x . □

Corollary 16 *If n regions R_1, R_2, \dots, R_n have a point x in common, then their intersection $R_1 \cap R_2 \cap \dots \cap R_n$ is also a region containing x .*

Proof. We use induction on n . Note that if $x \in R_1$ then R_1 is a region containing x . We now assume that for n regions R_1, R_2, \dots, R_n which all contain a point x , the intersection $R_1 \cap R_2 \cap \dots \cap R_n$ is a region containing x . Consider $n + 1$ regions R_1, R_2, \dots, R_{n+1} . Which all contain a point x . We know that the intersection $R_1 \cap R_2 \cap \dots \cap R_n$ is a region containing x by the inductive hypothesis. But then by Theorem 15 we know that $R_1 \cap R_2 \cap \dots \cap R_n \cap R_{n+1}$ is also a region containing x . Since this is true for $n = 1$ and for $n + 1$ when it's true for n , it must be true for all $n \in \mathbb{N}$. □

Theorem 17 *Let A and B be subsets of C . We have p is a limit point of $A \cup B$ if and only if p is a limit point of A or p is a limit point of B .*

Proof. Let p be a limit point of $A \cup B$. Then suppose to the contrary that p is not a limit point of A and p is not a limit point of B . Then there exist R_1 and R_2 such that $p \in R_1$, $p \in R_2$, $R_1 \cap (A \setminus p) = \emptyset$ and $R_2 \cap (B \setminus p) = \emptyset$. Then there exists an $R_3 = R_1 \cap R_2$ which also contains p . And since $R_3 \cap (A \setminus p) = \emptyset$ and $R_3 \cap (B \setminus p) = \emptyset$ we see that $R_3 \cap ((A \cup B) \setminus p) = \emptyset$ which means p is not a limit point of $A \cup B$. This is a contradiction. Conversely, if p is a limit point of A or p is a limit point of B then by Theorem 10, p must be a limit point of $A \cup B$ since $A \subseteq A \cup B$ and $B \subseteq A \cup B$. □

Corollary 18 *Let A_1, A_2, \dots, A_n be subsets of C . We have p is a limit point of the union $A_1 \cup A_2 \cup \dots \cup A_n$ if and only if p is also a limit point of at least one of the sets A_k .*

Proof. We use induction on n . Note that if p is a limit point of one set A_1 , then it is a limit point of A_1 . We now assume that if p is a limit point of the union of the n sets A_1, A_2, \dots, A_n , then it is a limit point of at least one of the sets A_k . Now consider the $n + 1$ sets $A_1, A_2, \dots, A_n, A_{n+1}$ and let p be a limit point of their union. We know that if p is a limit point the union $A_1 \cup A_2 \cup \dots \cup A_n$ then p is a limit point of at least one set A_k . And so using Theorem 17 we know that p is a limit point of at least one set A_k or p is a limit point of A_{n+1} . So we see that p is a limit point of at least one of the sets A_1, A_2, \dots, A_{n+1} . Since this is true for one set and for $n + 1$ sets when it's true for n sets, it must be true for every natural number of sets.

For the converse we use induction on n . Given that p is a limit point of A_1 , then p is a limit point of A_1 . We now assume that given n sets A_1, A_2, \dots, A_n and p is a limit point of at least one of the sets A_k , then it is a limit point of the union $A_1 \cup A_2 \cup \dots \cup A_n$. Consider $n + 1$ sets $A_1, A_2, \dots, A_n, A_{n+1}$ such that p is a

limit point of at least one of the sets A_k . Then we know p is a limit point of the union $A_1 \cup A_2 \cup \cdots \cup A_n$ or p is a limit point of A_{n+1} and so by Theorem 17 we see that p is a limit point of the union $A_1 \cup A_2 \cup \cdots \cup A_n \cup A_{n+1}$. Since this is true for one set and true for $n + 1$ sets when it's true for n sets, it must be true for all $n \in \mathbb{N}$. \square

Exercise 19 Find realizations of $(C, <)$, that is, concrete sets endowed with a relation $<$ that satisfies all the axioms so far. Are they the same? What does this question mean?

The sets \mathbb{Z} and \mathbb{Q} are two sets with an ordering $<$ which satisfy the axioms so far. There are other sets such as the set of odd integers or even integers which also satisfy the axioms and have an ordering. The set of even integers is essentially the same as \mathbb{Z} in this case though because there is a bijection between them which preserves the ordering.

Sheet 3: The Continuum Continued

Definition 1 (Disjoint) Two sets A and B are disjoint if $A \cap B = \emptyset$. A set of sets S is pairwise disjoint if for all sets $A, B \in S$ we have $A = B$ or $A \cap B = \emptyset$.

Theorem 2 If $p, q \in C$ and $p < q$, then there exist disjoint regions containing p and q .

Proof. Let $a, c, p, q \in C$ such that $a < p$, $p < q$ and $q < c$. Then there are two possibilities. There may be another point $b \in C$ which is between p and q . We see that this implies $p < b$ and $b < q$ and so the region $(a; b)$ contains p and the region $(b; c)$ contains q but $(a; b) \cap (b; c) = \emptyset$. There is also the possibility that there are no points between p and q . Then the region $(a; q)$ contains p but not q and the region $(p; c)$ contains q but not p and $(a; q) \cap (p; c) = (p; q) = \emptyset$. \square

Corollary 3 A set consisting of one point has no limit points.

Proof. Let $A \subset C$ be a set with one point x . If $p \in C$ is to be a limit point of A , then every region which contains p must also contain a point in A which is not p . So we see $p \neq x$. But then $p < x$ or $p > x$. In either case, Theorem 2 shows that there are disjoint regions containing p and x which means there exist regions containing p , but no points in A so p cannot be a limit point of A . \square

Theorem 4 A finite set of points has no limit points.

Proof. A finite set $S \subseteq C$ of n points can be indexed a_1, a_2, \dots, a_n . Now let $p \in C$ be a limit point of S . We have six cases.

Case 1: Let $p < a_1$. Then there exists a point $x \in C$ such that $x < p$ and so the region $(x; a_1)$ contains p , but no points of S .

Case 2: Let $p = a_1$. Then there exists an $x \in C$ such that $x < p$ and so the region $(x; a_2)$ contains p but no elements of S which are not equal to p .

Case 3: Let $p \in (a_1; a_n)$ such that $p = a_i$ for some $i = 2, 3, \dots, n-1$. But then the region $(a_{i-1}; a_{i+1})$ contains p , but no elements of S other than p .

Case 4: Let $p \in (a_1; a_n)$ such that $p \neq a_i$ for all $i = 2, 3, \dots, n-1$. Then there exists an a_i for $i = 1, 2, \dots, n-1$ such that $p \in (a_i; a_{i+1})$. But then the region $(a_i; a_{i+1})$ contains p and no points in S .

Case 5: Let $p = a_n$. Then there exists a $y \in C$ such that $p < y$ and so the region $(a_{n-1}; y)$ contains p , but no elements of S other than p .

Case 6: Let $a_n < p$. Then we see that there exists a $y \in C$ such that $p < y$ and so the region $(a_n; y)$ contains p , but no elements of S .

In each case we see that p is not a limit point of S and so we know that $p \notin \{x \mid x < a_1\} \cup \{a_1\} \cup (a_1; a_n) \cup \{a_n\} \cup \{x \mid x > a_n\} = C$. This is a contradiction. \square

Corollary 5 If $A \subseteq C$ is a finite set and $x \in A$, then there exists a region R such that $A \cap R = \{x\}$.

Proof. Let $A \subseteq C$ be a finite set of n elements such that $x \in A$. We know that x cannot be a limit point of A by Theorem 4 and so there exists a region R such that $x \in R$ and $R \cap (A \setminus x) = \emptyset$. But then we have $R \cap A = \{x\}$. \square

Theorem 6 If p is a limit point of a set A and R is a region containing p , then the set $R \cap A$ is infinite.

Proof. Assume that p is a limit point of A and R is a region containing p . Assume to the contrary that $R \cap A$ is finite. Then p is not a limit point of $R \cap A$. But since $(A \setminus (R \cap A)) \cup (R \cap A) = A$, we see that p must be a limit point of $A \setminus (R \cap A)$. But we also have $R \cap (A \setminus (R \cap A)) = \emptyset$ and $p \in R$ so p is not a limit point of $A \setminus (R \cap A)$. This is a contradiction and so $R \cap A$ must be infinite. \square

Definition 7 (Closed Set) A set $A \subseteq C$ is closed if it contains all its limit points.

Corollary 8 Finite sets are closed.

Proof. Finite sets have no limit points and so they vacuously contain all of their limit points. \square

Definition 9 (Closure) Let $M \subseteq C$ be a set. Let \overline{M} , the closure of M , be the set consisting of M and all of its limit points:

$$\overline{M} = M \cup \{x \in C \mid x \text{ is a limit point of } M\}.$$

Theorem 10 A set $M \subseteq C$ is closed if and only if $M = \overline{M}$.

Proof. We see that if $M \subseteq C$ is closed, then it contains all its limit points. That is $\{x \in C \mid x \text{ is a limit point of } M\} \subseteq M$. So we have $M = M \cup \{x \in C \mid x \text{ is a limit point of } M\} = \overline{M}$. Conversely, if $M = \overline{M}$ then $M = M \cup \{x \in C \mid x \text{ is a limit point of } M\}$. Since $\{x \in C \mid x \text{ is a limit point of } M\} \subseteq M$, we see that M contains all its limit points and so it is closed. \square

Theorem 11 For all $M \subseteq C$ we have $\overline{\overline{M}} = \overline{M}$.

Proof. We wish to show that the set of limit points of \overline{M} is a subset of \overline{M} . Consider a limit point p of \overline{M} . Since $\overline{M} = M \cup \{x \mid x \text{ is a limit point of } M\}$ we see that p is a limit point of M or p is a limit point of the set of limit points of M . If p is a limit point of M , then $p \in \overline{M}$. If p is a limit point of the set of limit points of M , then every region containing p contains a limit point of M . But every region containing a limit point of M contains a point in M and so for all regions $R \subseteq C$ such that $p \in R$ we have $R \cap M \neq \emptyset$. But then either p is in M or p is a limit point of M and so $p \in \overline{M}$. Thus we see $\{x \mid x \text{ is a limit point of } \overline{M}\} \subseteq \overline{M}$ and so

$$\overline{\overline{M}} = \overline{M \cup \{x \mid x \text{ is a limit point of } M\} \cup \{x \mid x \text{ is a limit point of } \overline{M}\}} = \overline{M}.$$

\square

Corollary 12 If M is a set of points, then \overline{M} is closed.

Proof. By Theorem 11 we know $\overline{\overline{M}} = \overline{M}$ and so by Theorem 10, \overline{M} is closed. \square

Theorem 13 The sets C and \emptyset are closed.

Proof. All limit points are elements of C and so C must contain all its limit points and is closed. The empty set can have no limit points since there are no regions which contain a point in \emptyset . Therefore it vacuously contains all its limit points and is closed. \square

Definition 14 (Open Set) A set of points M is open if the complement $C \setminus M$ is closed.

Theorem 15 The sets C and \emptyset are open.

Proof. We see that the complement $C \setminus C = \emptyset$ and \emptyset is closed so C is open. Likewise $C \setminus \emptyset = C$ and C is closed so \emptyset is open. \square

Theorem 16 Every region is open and its complement is closed.

Proof. We wish to show that for all regions R , the complement $C \setminus R$ is closed. So we assume that for some region R there exists a limit point p of $C \setminus R$ such that $p \notin C \setminus R$. Thus, $p \in R$. But then, since $R \cap (C \setminus R) = \emptyset$, p is not a limit point of $C \setminus R$ and this is a contradiction. Thus, $C \setminus R$ contains all its limit points and so it is closed which means R is open for all $R \subseteq C$. \square

Theorem 17 (Open Condition) *A set $A \subseteq C$ is open if and only if for all $x \in A$, there exists a region $R \subseteq A$ such that $x \in R$.*

Proof. Let $A \subseteq C$ be open. Then $C \setminus A$ is closed. Assume there exists $x \in A$ such that for all regions R containing x , R is not a subset of A . Then for all regions R containing x , R contains at least one point in $C \setminus A$ and so x is a limit point of $C \setminus A$. But x is in A and $C \setminus A$ is closed and so we have a contradiction. Thus for all $x \in A$, there exists a region $R \subseteq A$ such that $x \in R$.

Conversely, let $A \subseteq C$ be a subset such that for all $x \in A$ there exists a region $R \subseteq A$ such that $x \in R$. Assume A is closed. Then $C \setminus A$ is not closed and so it doesn't include all its limit points. But then there exists a limit point p of $C \setminus A$ such that $p \in A$. And so there exists a region $R \subseteq A$ which contains p and so p is not a limit point of $C \setminus A$. This is a contradiction and so A must be open. \square

Corollary 18 *Every nonempty open set is the union of regions.*

Proof. We see by Theorem 17 that for every element x of a nonempty open set A , there exists a region $R \subseteq A$ such that $x \in R$. Since an R exists for every element of A , if we take the union of all such regions we will have a subset of A which contains every element of A . This must be equal to A . \square

Sheet 4: Construction of \mathbb{Q}

Let \mathbb{Z} denote the integers. Let

$$P = \{(a, b) \mid a, b \in \mathbb{Z}, b \neq 0\}$$

and let the relation \sim be defined on P by

$$(a_1, b_1) \sim (a_2, b_2) \text{ if } a_1 b_2 = a_2 b_1$$

Theorem 1 \sim is an equivalence relation on P .

Proof. Let $(a, b) \in P$. Then $ab = ab$ and so $(a, b) \sim (a, b)$. Hence, reflexivity applies to \sim . Now let $(a_1, b_1), (a_2, b_2) \in P$ such that $(a_1, b_1) \sim (a_2, b_2)$. Then $a_1 b_2 = a_2 b_1$ and so $a_2 b_1 = a_1 b_2$. Thus $(a_2, b_2) \sim (a_1, b_1)$ and so symmetry holds for \sim . Now suppose $(a_1, b_1), (a_2, b_2), (a_3, b_3) \in P$ such that $(a_1, b_1) \sim (a_2, b_2)$ and $(a_2, b_2) \sim (a_3, b_3)$. Then $a_1 b_2 = a_2 b_1$ and $a_2 b_3 = a_3 b_2$. Multiplying the first equation by b_3 we have $a_1 b_2 b_3 = a_2 b_1 b_3$. But then since $a_2 b_3 = a_3 b_2$ we have $a_1 b_2 b_3 = a_3 b_1 b_2$ and dividing by $b_2 \neq 0$ we have $a_1 b_3 = a_3 b_1$. Therefore $(a_1, b_1) \sim (a_3, b_3)$ implying transitivity and since all three conditions have been met, \sim is an equivalence relation on P . \square

Now let \mathbb{Q} denote the set of \sim -equivalence classes of P . We now define two operators, $+$ and \cdot as follows. For $X, Y \in \mathbb{Q}$ let $(a_1, b_1) \in X$ and $(a_2, b_2) \in Y$. Let

$$X + Y = \overline{(a_1 b_2 + a_2 b_1, b_1 b_2)}$$

and let

$$X \cdot Y = \overline{(a_1 a_2, b_1 b_2)}.$$

We now show that these definitions are well-defined.

Theorem 2 If $(a_1, b_1) \sim (c_1, d_1)$ and $(a_2, b_2) \sim (c_2, d_2)$ then

$$(a_1 b_2 + a_2 b_1, b_1 b_2) \sim (c_1 d_2 + c_2 d_1, d_1 d_2)$$

and

$$(a_1 a_2, b_1 b_2) \sim (c_1 c_2, d_1 d_2).$$

Proof. Let $(a_1, b_1) \sim (c_1, d_1)$ and $(a_2, b_2) \sim (c_2, d_2)$. Then we have $a_1 d_1 = b_1 c_1$ and $a_2 d_2 = b_2 c_2$. We multiply the first equation by $b_2 d_2$ so we have $a_1 b_2 d_1 d_2 = b_1 b_2 c_1 d_2$ and we multiply the second equation by $b_1 d_1$ so we have $a_2 b_1 d_1 d_2 = b_1 b_2 c_2 d_1$. Now we add the two new equations together so we have $a_1 b_2 d_1 d_2 + a_2 b_1 d_1 d_2 = b_1 b_2 c_1 d_2 + b_1 b_2 c_2 d_1$ and so $(a_1 b_2 + a_2 b_1) d_1 d_2 = (c_1 d_2 + c_2 d_1) b_1 b_2$ which implies $(a_1 b_2 + a_2 b_1, b_1 b_2) \sim (c_1 d_2 + c_2 d_1, d_1 d_2)$. Similarly, if we multiply $a_1 d_1 = b_1 c_1$ and $a_2 d_2 = b_2 c_2$ together we have $a_1 a_2 d_1 d_2 = b_1 b_2 c_1 c_2$ and so $(a_1 a_2, b_1 b_2) \sim (c_1 c_2, d_1 d_2)$. \square

Theorem 3 (Associativity of Addition) For all $p, q, r \in \mathbb{Q}$ we have $(p + q) + r = p + (q + r)$.

Proof. Let $p, q, r \in \mathbb{Q}$ such that $(p_1, p_2) \in p$, $(q_1, q_2) \in q$ and $(r_1, r_2) \in r$. Then we see that

$$\begin{aligned} (p + q) + r &= \overline{(\overline{(p_1, p_2)} + \overline{(q_1, q_2)})} + \overline{(r_1, r_2)} \\ &= \overline{(p_1 q_2 + p_2 q_1, p_2 q_2)} + \overline{(r_1, r_2)} \\ &= \overline{((p_1 q_2 + p_2 q_1) r_2 + p_2 q_2 r_1, p_2 q_2 r_2)} \\ &= \overline{(p_1 q_2 r_2 + p_2 q_1 r_2 + p_2 q_2 r_1, p_2 q_2 r_2)} \\ &= \overline{((q_1 r_2 + q_2 r_1) p_2 + p_1 q_2 r_2, p_2 q_2 r_2)} \\ &= p + \overline{(q_1 r_2 + q_2 r_1, q_2 r_2)} \\ &= p + (q + r). \end{aligned}$$

□

Theorem 4 (Commutativity of Addition) For all $p, q \in \mathbb{Q}$ we have $p + q = q + p$.

Proof. Let $p, q \in \mathbb{Q}$ such that $(p_1, p_2) \in p$ and $(q_1, q_2) \in q$. Then we have
 $p + q = (p_1, p_2) + (q_1, q_2) = (p_1q_2 + p_2q_1, p_2q_2) = (q_1p_2 + q_2p_1, q_2p_2) = (q_1, q_2) + (p_1, p_2) = q + p$. □

Theorem 5 (Additive Identity) There exists an $n \in \mathbb{Q}$ such that for all $p \in \mathbb{Q}$ we have $n + p = p$. Show that n is unique.

Proof. We see that if we let $n \in \mathbb{Q}$ such that $n = \overline{(0, 1)}$ and if we let $(p_1, p_2) \in p$ for some $p \in \mathbb{Q}$ then we have $n + p = \overline{(0, 1)} + (p_1, p_2) = \overline{((0)p_2 + (1)p_1, (1)p_2)} = \overline{(p_1, p_2)} = p$. Now suppose there exist two additive identities such that for all $p \in \mathbb{Q}$ we have $n_1 + p = p$ and $n_2 + p = p$. Then we have $n_2 = n_1 + n_2 = n_2 + n_1 = n_1$ and so $n_1 = n_2$. Thus, the additive identity is unique. □

From now on we will call the additive identity 0.

Theorem 6 (Additive Inverse) For all $p \in \mathbb{Q}$ there exists $q \in \mathbb{Q}$ such that $p + q = 0$. Show that q is unique.

Proof. Let $p \in \mathbb{Q}$ such that $(p_1, p_2) \in p$. Then we choose $q = \overline{(-p_1, p_2)}$ for $q \in \mathbb{Q}$. Then we have
 $p + q = (p_1, p_2) + \overline{(-p_1, p_2)} = \overline{(p_1p_2 + (-p_1)p_2, p_2p_2)} = \overline{(0, p_2p_2)} = \overline{(0, 1)} = 0$ since $(0)p_2p_2 = (0)(1)$. Now suppose there exist two additive inverses so that $p + n_1 = 0$ and $p + n_2 = 0$. Then we have $p + n_1 = p + n_2$ and adding $\overline{(-p_1, p_2)}$ to both sides we have

$$\overline{(-p_1, p_2)} + \overline{(p_1, p_2)} + n_1 = \overline{(-p_1p_2 + p_1p_2, p_2p_2)} + n_1 = 0 + n_1 = n_1$$

on the left and

$$\overline{(-p_1, p_2)} + \overline{(p_1, p_2)} + n_2 = \overline{(-p_1p_2 + p_1p_2, p_2p_2)} + n_2 = 0 + n_2 = n_2$$

on the right. So $n_1 = n_2$ and the additive inverse is unique. □

From now on we will call the additive inverse for p , $-p$.

Theorem 7 (Associativity of Multiplication) For all $p, q, r \in \mathbb{Q}$ we have $(p \cdot q) \cdot r = p \cdot (q \cdot r)$.

Proof. Let $p, q, r \in \mathbb{Q}$ such that $(p_1, p_2) \in p$, $(q_1, q_2) \in q$ and $(r_1, r_2) \in r$. Then we have
 $(p \cdot q) \cdot r = \overline{((p_1, p_2) \cdot (q_1, q_2))} \cdot (r_1, r_2) = \overline{(p_1q_1, p_2q_2)} \cdot (r_1, r_2) = \overline{(p_1q_1r_1, p_2q_2r_2)} = p \cdot \overline{(q_1r_1, q_2r_2)} = p \cdot (q \cdot r)$. □

Theorem 8 (Commutativity of Multiplication) For all $p, q \in \mathbb{Q}$ we have $p \cdot q = q \cdot p$.

Proof. Let $p, q \in \mathbb{Q}$ such that $(p_1, p_2) \in p$ and $(q_1, q_2) \in q$. Then
 $p \cdot q = \overline{(p_1, p_2) \cdot (q_1, q_2)} = \overline{(p_1q_1, p_2q_2)} = \overline{(q_1p_1, q_2p_2)} = \overline{(q_1, q_2) \cdot (p_1, p_2)} = q \cdot p$. □

Theorem 9 (Multiplicative Identity) There exists $e \in \mathbb{Q}$ such that for all $p \in \mathbb{Q}$ we have $e \cdot p = p$.

Proof. Let $p \in \mathbb{Q}$ such that $(p_1, p_2) \in p$ and let $e \in \mathbb{Q}$ such that $e = \overline{(1, 1)}$. Then we have
 $e \cdot p = \overline{(1, 1) \cdot (p_1, p_2)} = \overline{(p_1(1), p_2(1))} = p$. Suppose there exist two multiplicative identities e_1 and e_2 such that for all $p \in \mathbb{Q}$, $e_1 \cdot p = p$ and $e_2 \cdot p = p$. Then we have $e_1 = e_2 \cdot e_1$ and $e_2 = e_1 \cdot e_2 = e_2 \cdot e_1$. So we have $e_1 = e_2$ and so the multiplicative identity is unique. □

From now on we will call the multiplicative identity 1.

Theorem 10 (Multiplicative Inverse) For all $p \in \mathbb{Q}$ with $p \neq 0$ there exists $q \in \mathbb{Q}$ such that $p \cdot q = 1$.

Proof. Let $p \in \mathbb{Q}$ such that $(p_1, p_2) \in p$ and since $p_1 \neq 0$ let $q \in \mathbb{Q}$ such that $(p_2, p_1) \in q$. Then we see that $p \cdot q = \overline{(p_1, p_2)} \cdot \overline{(p_2, p_1)} = \overline{(p_1 p_2, p_1 p_2)} = \overline{(1, 1)} = 1$. Now suppose there are two multiplicative inverses for some $p \in \mathbb{Q}$ such that $p \cdot q_1 = 1$ and $p \cdot q_2 = 1$. Then, multiplying both equations by $\overline{(p_2, p_1)}$, we have $q_1 = \overline{(1, 1)} \cdot q_1 = \overline{(p_1 p_2, p_1 p_2)} \cdot q_1 = \overline{(p_2, p_1)} \cdot \overline{(p_1, p_2)} \cdot q_1 = \overline{(p_2, p_1)} \cdot \overline{(p_1, p_2)} \cdot q_2 = \overline{(p_1 p_2, p_1 p_2)} \cdot q_2 = \overline{(1, 1)} \cdot q_2 = q_2$. So the multiplicative inverse is unique. \square

From now on we will call the multiplicative inverse for p , p^{-1} .

Theorem 11 (Distributivity) For all $p, q, r \in \mathbb{Q}$ we have $p \cdot (q + r) = p \cdot q + p \cdot r$.

Proof. Let $p, q, r \in \mathbb{Q}$ such that $(p_1, p_2) \in p$, $(q_1, q_2) \in q$ and $(r_1, r_2) \in r$. Then we have

$$\begin{aligned} p \cdot (q + r) &= \overline{(p_1, p_2)} \cdot \left(\overline{(q_1, q_2)} + \overline{(r_1, r_2)} \right) \\ &= \overline{(p_1, p_2)} \cdot \overline{(q_1 r_2 + q_2 r_1, q_2 r_2)} \\ &= \overline{(p_1 q_1 r_2 + p_1 q_2 r_1, p_2 q_2 r_2)} \\ &= \overline{(p_1 q_1 r_2 + p_1 q_2 r_1, p_2 q_2 r_2)} \cdot \overline{(p_2, p_2)} \\ &= \overline{(p_1 p_2 q_1 r_2 + p_1 p_2 q_2 r_1, p_2 p_2 q_2 r_2)} \\ &= \overline{(p_1 q_1, p_2 q_2)} + \overline{(p_1 r_1, p_2 r_2)} \\ &= \overline{(p_1, p_2)} \cdot \overline{(q_1, q_2)} + \overline{(p_1, p_2)} \cdot \overline{(r_1, r_2)} \\ &= p \cdot q + p \cdot r. \end{aligned}$$

\square

Theorem 12 The function $f : \mathbb{Z} \rightarrow \mathbb{Q}$ where $f(n) = \overline{(n, 1)}$ is injective.

Proof. Let $a, b \in \mathbb{Z}$ such that $f(a) = f(b)$. Then we have $\overline{(a, 1)} = \overline{(b, 1)}$ and so $(a, 1) \sim (b, 1)$ which implies $a = b$. \square

Theorem 13 For all $m, n \in \mathbb{Z}$ we have

$$f(m + n) = f(m) + f(n) \text{ and } f(mn) = f(m) \cdot f(n).$$

Proof. Let $m, n \in \mathbb{Z}$. Then we have

$$\begin{aligned} f(m + n) &= \overline{(m + n, 1)} = \overline{(m(1) + n(1), (1)(1))} = \overline{(m, 1)} + \overline{(n, 1)} = f(m) + f(n). \\ f(mn) &= \overline{(mn, (1)(1))} = \overline{(m, 1)} \cdot \overline{(n, 1)} = f(m) \cdot f(n). \end{aligned}$$

\square

Theorem 14 For every rational number $r \in \mathbb{Q}$ there exist $m, n \in \mathbb{Z}$ such that $n \neq 0$ and $r = mn^{-1}$.

Proof. Let $r \in \mathbb{Q}$ such that $(m, n) \in r$ (since r is nonempty). Then we see $m, n \in \mathbb{Z}$. Thus we can write $m = \overline{(m, 1)}$ and $n = \overline{(n, 1)}$. And so $n^{-1} = \overline{(1, n)}$ since $n \neq 0$ and we have $m \cdot n^{-1} = \overline{(m, 1)} \cdot \overline{(1, n)} = \overline{(m, n)} = r$. \square

Lemma 15 Any element in \mathbb{Q} can be written as $\overline{(a, b)}$ with $b > 0$.

Proof. Let $\overline{(a, b)} \in \mathbb{Q}$. There are two cases:

Case 1: If $b > 0$ then we are done.

Case 2: If $b < 0$ then we have $a(-b) = -ab = (-a)b$ and so $(a, b) \sim (-a, -b)$. Thus $\overline{(a, b)} = \overline{(-a, -b)}$ and $-b > 0$. \square

We now define a relation $<$ on \mathbb{Q} . For $p, q \in \mathbb{Q}$ let $(a_1, b_1) \in p$ such that $b_1 > 0$ and let $(a_2, b_2) \in q$ such that $b_2 > 0$. Then we define

$$p < q \text{ if } a_1 b_2 < a_2 b_1$$

Theorem 16 *Show that $<$ is a well-defined relation on \mathbb{Q} .*

Proof. Let $(a_1, b_1), (a_2, b_2), (c_1, d_1), (c_2, d_2) \in \mathbb{Q}$ such that $(a_1, b_1) < (a_2, b_2)$ and $(a_1, b_1) \sim (c_1, d_1)$ and $(a_2, b_2) \sim (c_2, d_2)$. We take b_1, b_2, d_1 and d_2 to all be greater than 0 by Lemma 15. Then we have $a_1 b_2 < a_2 b_1$ and so $a_1 b_2 d_1 d_2 < a_2 b_1 d_1 d_2$. But we also know that $a_1 d_1 = b_1 c_1$ and $a_2 d_2 = b_2 c_2$. Making the appropriate substitutions we see $b_1 b_2 c_1 d_2 < b_1 b_2 c_2 d_1$. Since $b_1 b_2 > 0$ we have $c_1 d_2 < c_2 d_1$ and so $(c_1, c_2) < (d_1, d_2)$. This shows that $<$ is well-defined. \square

Theorem 17 *The relation $<$ is an ordering on \mathbb{Q} .*

Proof. Let $p, q, r \in \mathbb{Q}$ such that $(p_1, p_2) \in p, (q_1, q_2) \in q$ and $(r_1, r_2) \in r$. By Lemma 15 we let p_2, q_2 and r_2 all be greater than 0. If $p \neq q$ then we see that $(p_1, p_2) \sim (q_1, q_2)$ and so $p_1 q_2 \neq p_2 q_1$. Then we have either $p_1 q_2 < p_2 q_1$ and so $p < q$ or $p_2 q_1 < p_1 q_2$ and so $q < p$. Secondly if $p < q$ then we have $p_1 q_2 < p_2 q_1$ and so $p_1 q_2 \neq p_2 q_1$. Therefore $(p_1, p_2) \sim (q_1, q_2)$. Thus $p \neq q$. Finally, if $p < q$ and $q < r$ then $p_1 q_2 < p_2 q_1$ and $q_1 r_2 < q_2 r_1$. Multiplying the first inequality by r_2 and the second by p_2 we have $p_1 q_2 r_2 < p_2 q_1 r_2$ and $p_2 q_1 r_2 < p_2 q_2 r_1$ since $p_2 > 0$ and $r_2 > 0$. This implies $p_1 q_2 r_2 < p_2 q_2 r_1$ and since $q_2 > 0$ we have $p_1 r_2 < p_2 r_1$ and so $p < r$. Since all three conditions are satisfied, we see that $<$ is an ordering on \mathbb{Q} . \square

Exercise 18 *Is $(\mathbb{Q}, <)$ a model of C ? That is, which axioms does it satisfy?*

Proof. Since the integers are a subset of \mathbb{Q} and there exists at least one integer and since we showed that $<$ was an ordering on \mathbb{Q} , we see that axioms 1 and 2 are satisfied. Theorem 20 shows that there is no last point of \mathbb{Q} . To show that there is no first point we use a similar argument. Let $(a, b) \in \mathbb{Q}$ such that $b > 0$. We consider three cases:

Case 1: Let $a > 0$. Then $a(1) > (0)b$ and so $(a, b) > (0, 1) = 0$.

Case 2: Let $a < 0$. Then since $b > 0$, $a > ab - b$ which means $(a, b) > (a - 1, 1) = a - 1$.

Case 3: Let $a = 0$ then $(a, b) = (0, b) = 0$ and since $-1 < 0$ we see $(a, b) > (-1, 1) = -1$.

So we see that for any element of \mathbb{Q} there is always an element greater than it and an element less than it which means it can have no first or last point and so it satisfies axiom 3. \square

Theorem 19 *For every $p, q \in \mathbb{Q}$ such that $p < q$ there exists $r \in \mathbb{Q}$ such that $p < r < q$.*

Proof. Let $p, q, r \in \mathbb{Q}$ such that $(p_1, p_2) \in p, (q_1, q_2) \in q$ and $r = \overline{(p_1 q_2 + p_2 q_1, 2p_2 q_2)}$. Let $p < q$ and by Lemma 15 let $p_2 > 0$ and $q_2 > 0$. Then we have $p_1 q_2 < p_2 q_1$ and so $p_1 p_2 q_2 < p_2 p_2 q_1$ which implies $2p_1 p_2 q_2 < p_1 p_2 q_2 + p_2 p_2 q_1$. We see that this implies $(p_1, p_2) < \overline{(p_1 q_2 + p_2 q_1, 2p_2 q_2)}$ which means $p < r$. Similarly, we have $p_1 q_2 < p_2 q_1$ which means $p_1 q_2 q_2 < p_2 q_1 q_2$ and $p_1 q_2 q_2 + p_2 q_1 q_2 < 2p_2 q_1 q_2$. This implies $\overline{(p_1 q_2 + p_2 q_1, 2p_2 q_2)} < (q_1, q_2)$ which means $r < q$. Thus $p < r < q$. \square

Theorem 20 (Archimedean Property) *For every $p \in \mathbb{Q}$ there exists $n \in \mathbb{Z}$ such that $p < n$.*

Proof. Let $p \in \mathbb{Q}$ such that $(a, b) \in p$. Let $b > 0$ by Lemma 15. We have to consider three cases:

Case 1: Let $a > 0$. Then $a < ab + b$ and so $(a, b) < (a + 1, 1) = a + 1$.

Case 2: Let $a < 0$. Then $a(1) < b(0)$ and so $(a, b) < (0, 1) = 0$.

Case 3: Let $a = 0$. Then $(a, b) = (0, b) = (0, 1) = 0$ and since $0 < 1$ we see $(a, b) < (1, 1) = 1$. \square