Introduction to mathematics

Radek Honzik

Charles University, Department of Logic

logika.ff.cuni.cz/radek

Preliminary version: October 8, 2022
(will be updated during semester)

Introduction

In this lecture, we will cover the following topics:

- Basics of set theory
- Construction of natural numbers $\mathbb{N}$
- Construction of integers $\mathbb{Z}$; algebraic notions: the group and ring structure of $(\mathbb{Z}, +, -, 0, \cdot, 1)$
- Construction of rationals $\mathbb{Q}$; the ordering on $\mathbb{Q}$, the field structure of $(\mathbb{Q}, +, -, 0, \cdot, 1)$
- Construction of reals $\mathbb{R}$; analytic notions: limits, suprema, infima, continuity.

There are lecture notes for this course (see Moodle).

Further reading:

Introduction to mathematics:

- J.K.Truss, Foundation of Mathematical Analysis. Clarendon Press, Oxford. 1997.
- Jiří Matoušek a Jaroslav Nešetřil, Kapitoly z diskrétní matematiky. Karolinum, Praha. 2002.
- Milan Mareš, Příběhy matematiky. Pistorius a Olšanská, Příbram 2008.
- Walter Rudin, Principles of Mathematical Analysis. McGraw-Hill, 3rd edition.

Mathematical Logic and Set theory:

- Antonín Sochor, Klasická matematická logika, Karolinum 2001.
- Vítězlav Švejdar, Logika: neúplnost, složitost a nutnost, Academia 2002.
- Bohuslav Balcar a Petr Štěpánek, Teorie množin, Academia 2000

We will focus on the on the mathematical way of thinking: from hypotheses and informal arguments to rigorous proofs. We will try to include one Theorem (a proved statement) in each section to give you the idea how the concepts which we introduce work.

Structure of arguments in mathematics:

- Starting with some *primitive notions*, which are implicitly defined by the theory we work in, all other notions are defined by means of *definitions* from earlier notions.
- Theorem, lemmas, claims are formulated for the defined notions and proved in the theory.
- Note: Some statements are considered "interesting" but no proof has been found for them or their negation. We will have more examples later, but the following is perhaps the easiest to formulate: (Goldbach's conjecture) *Every even number greater than 2 is the sum of two primes.*

Example (a bit informal). Suppose we know how to add and multiply reals $\mathbb{R}$.

Definition

We say that a real number is *rational* if it can be written as $\frac{p}{q}$ where $q \neq 0$, and p, q are from $\mathbb{Z}$. We say that a real number is *irrational* if it is not rational. We say that an integers x is *even* if it can be written as $2y$ for some integer y; it is *odd* if it can be written as $2y + 1$ for some y.

Theorem

There exist an irrational number. In fact if x is a real such that $x^2 = 2$, then x is irrational.

Proof.

Suppose for contradiction that x (we can denote it $\sqrt{2}$) is rational and let p, q be positive integers which have no common divisor greater than 1: $\sqrt{2} = \frac{p}{q}$. Equivalently, $2q^2 = p^2$. This means that p^2 is even, and also (check) that p is even, and can be written as $2r$ for some r. So we can write $2q^2 = (2r)^2$, equivalently $2q^2 = 4r^2$, and so $q^2 = 2r^2$. With the same argument as we argued for p, it follows that q must be even. But this is a contradiction because we assumed that p, q have no common divisor: but they do: 2. It means that our original starting assumption must be false, i.e. there are no such p, q and therefore $\sqrt{2}$ is irrational. □

Similar arguments can show that e is irrational (easy) and π is irrational (not that easy). But other theorems may mention more abstract structures, such as graphs, groups, trees, vector spaces, etc. This makes it essential learn all definitions and understand them. In fact how are e and π really defined? You may check for yourselves that their definition uses the notion of the limit of a sequence, which must itself be defined.

It is tempting to think that every "reasonable statement" can be proved or refuted in principle, only that we do not know how in this partical moment ($P = NP$? Riemann's hypothesis, Goldbach's conjecture, Twin-prime conjecture, and other). Unfortunately, by results of Gödel (here is where logic enters the picture), for every reasonable theory there are always infinitely many statements which the theory cannot prove or refute.

Natural numbers in set theory

Axioms of (naive) set theory: **(i) Structural properties.**

- We completely ignore the question *what* sets are, both in the metaphysical and physical sense.
- *Extensionality.* Two sets will be identical iff[1] they have the same elements; i.e. we disregard any intensional properties of the elements.
- *Infinity.* There is an infinite set.

[1] "Iff" is shorthand for "in and only if".

(ii) Algebraic properties.

- *Pairing.* For any two sets x, y there is another set $\{x, y\}$ that contains exactly the sets x, y.
- *Union.* For any set x there is another set $\bigcup x$ that contains all elements of all the elements of x (i.e. y is in $\bigcup x$ iff there is another set z in x, and y is in z).

  Comment. This operation has an obvious connection with the $\cup$ operation known from the basic (school-taught) set theory:

$$\bigcup\{x, y\} = x \cup y.$$

  $\bigcup$ is obviously more general – unlike the $\cup$ operation which joins elements from *two* sets, $\bigcup$ can join the elements of arbitrarily many sets (their number is determined by the size of x in $\bigcup x$).

- *Power set.* For any set x there is another set $\mathcal{P}(x)$ which contains exactly all the subsets of x.
- *Closure under arbitrary set-operations.* For any operation F from sets to sets, the image of F from a set x is also a set, i.e. $F''x = \{y \mid \exists q \in x \text{ such that } y = F(q)\}$ for a set x is a set.

  Comment. In formulating this property we have admittedly crossed the line of what is intuitively true. But a weakening of the above property is intuitive: if P is a property and x a set then there is a set y which contains exactly the elements of x satisfying property P. The stronger form is however necessary even for the most elementary proofs.

There may be other axioms such as Axiom of Foundation or Axiom of Choice but we will leave these aside for the moment.

The above axioms postulate what objects are sets. For instance if x is a set, then $\mathcal{P}(x)$ is a set. But what about $X = \{x \mid x \notin x\}$? Russell's paradox leads us to say that X must not be a set, or else our system is inconsistent.

*E*xercise: Show that that the assumption that $X = \{x \mid x \notin x\}$ is a set leads to a contradiction.

Basic properties of sets:

- $x \in y$, a binary relation of membership: if a set x is in the relation "to be an element of" with a set y, we write it symbolically as $x \in y$.
- $x \subseteq y \leftrightarrow (\forall q)\, q \in x \rightarrow q \in y$, we say that x is a *subset* of y. This relation is determined by the propositional connective "if, then", $\rightarrow$.

  Exercise: Show that for every x, y it holds that $x = y \leftrightarrow x \subseteq y \wedge y \subseteq x$.

Notice that $\subseteq$ is a *partial order, partial ordering, or just ordering*: it is a binary relation which is

- *reflexive*: $x \subseteq x$ for every set x.
- *transitive*: $x \subseteq y$ and $y \subseteq z$ implies $x \subseteq z$ for all sets x, y, z.
- *weakly anti-symmetrical*: $x \subseteq y$ and $y \subseteq x$ implies $x = y$ for all x, y.

Exercise. Verify that $\subseteq$ is indeed a partial ordering.

- $x \cap y = \{q \mid q \in x \wedge q \in y\}$, the operation of *intersection*. This operation is determined by the propositional connective *and*, $\wedge$.
- $x \cup y = \{q \mid q \in x \vee q \in y\}$, the operation of *union*. This operation is determined by the propositional connective *or*, $\vee$.
- $x - y = \{q \mid q \in x \wedge q \notin y\}$, the operation of *subtraction*. This operation is determined by the propositional connective *not*, $\neg$.
- $\mathcal{P}(x)$ is the powerset of x: $\mathcal{P}(x) = \{q \mid q \subseteq x\}$.
- $\{x, y\}$ is a set which contains exactly x, y as elements. Note that it works for a single set x as well: $\{x, x\} = \{x\}$; this set is called the *singleton* (singleton) of x.

- Comprehension. Given a property φ and a set y, there is a set x of all q which are in y and satisfy φ: $x = \{q \mid q \in y \wedge \varphi(q)\}$. I.e. for all q, $q \in x$ if and only if $q \in y \wedge \varphi(q)$.
  Notation. Sometimes we write $\{q \in y \mid \varphi(q)\}$ instead of $\{q \mid q \in y \wedge \varphi(q)\}$. This is just a matter of notation. In any case, these two expressions denote the same set. (We prefer the notation $\{q \in y \mid \varphi(q)\}$ because it is shorter.)

- Assume there is at least one set x. Then there is an *empty set*, denoted by $\emptyset$, where $\emptyset = \{q \mid q \in x \wedge q \neq q\}$.
  Exercise. Verify that there is only one empty set; i.e. the definition of the empty set does not depend on the initial set x: if x_1 and x_2 are two sets, then $\{q \mid q \in x_1 \wedge q \neq q\} = \{q \mid q \in x_2 \wedge q \neq q\}$.
  Exercise. Verify that the empty set $\emptyset$ is a subset of every set, i.e. if x is a set, then $\emptyset \subseteq x$. However, notice that it is *not* true that $\emptyset$ is an element of every set. Give an example of a set x such that $\emptyset \notin x$.
  Exercise. Use the previous exercise to conclude that $\mathcal{P}(x)$, the powerset of x, is always non-empty, even if $x = \emptyset$.

We say that a structure $\langle B, \wedge, \vee, -, 0, 1\rangle$ is a Boolean algebra if B is a set, $\wedge$ and $\vee$ are binary operations, $-$ is an unary operation and $0, 1$ are constants, and the following axioms hold:

- Associativity of $\wedge, \vee$:
  $a \wedge (b \wedge c) = (a \wedge b) \wedge c$ and $a \vee (b \vee c) = (a \vee b) \vee c$.
- Commutativity of $\wedge, \vee$:
  $a \wedge b = b \wedge a$ and $a \vee b = b \vee a$.
- Absorption:
  $a \wedge (a \vee b) = a$ and $a \vee (a \wedge b) = a$.
- Distributivity:
  $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$ and
  $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$.
- Axioms of constants:
  $a \vee -a = 1$ and $a \wedge -a = 0$.

Exercise: Verify that if x is a nonempty set, then

$$\langle \mathcal{P}(x), \cap, \cup, -, \emptyset, x \rangle$$

is a Bolean algebra, called the *powerset algebra*, when we identify $\wedge$ with intersection, $\vee$ with union, $-a$ with the operation of subtraction $x - a$, 0 with the empty set and 1 with the set x.

Show also that the de Morgan's law holds:

$$-(a \cup b) = -a \cap -b \text{ and } -(a \cap b) = -a \cup -b.$$

- Generalisation of $\cup$ and $\cap$ for any set x:

$$\bigcup x = \{q \mid (\exists y)(y \in x \wedge q \in y)\}$$

and

$$\bigcap x = \{q \mid (\forall y)(y \in x \to q \in y)\}.$$

Exercise. $\bigcup\{x, y\} = x \cup y$, $\bigcap\{x, y\} = x \cap y$. $\bigcap \emptyset = V$ (all sets), $\bigcup \emptyset = \emptyset$.

Definition of $\mathbb{N}$ in set theory:

Definition

A set x is called *inductive* if it contains $\emptyset$ and with every element y in x, x also contains the set $y \cup \{y\}$.

Definition

The *axiom of infinity* is the following startement: There exists an inductive set.

Definition (Natural numbers)

$\mathbb{N}$, the set of natural numbers, is defined as

$$\mathbb{N} = \bigcap \{x \mid x \text{ is an inductive set}\}, \tag{1}$$

in other words $\mathbb{N}$ is defined to be the intersection of all inductive sets.

Theorem (Induction)

Assume A is a subset of $\mathbb{N}$ such that $\emptyset \in A$ and for every $n \in A$ also $n \cup \{n\} \in A$. Then $A = \mathbb{N}$.

Proof.

Our assumption about A means that A is an inductive set. Since $\mathbb{N}$ is the least inductive set, we get $\mathbb{N} \subseteq A$. By the assumption of theorem, we also know that $A \subseteq \mathbb{N}$, which implies $\mathbb{N} = A$ as required. □

Comparing sizes of sets:

Definition

A set a has the same size as a set b if there is a bijection f from a onto b, and we denote this by $a \approx b$. We say that a is smaller than b if there is a 1-1 function f from a into b, and we denote this by $a \preceq b$. We say that a is strictly smaller if $a \preceq b$ but $a \not\approx b$, and we denote this by $a \prec b$.

If $a \approx \mathbb{N}$, then we say that a is *countable*. If $\mathbb{N} \prec a$, we say that a is *uncountable*.

Theorem (Cantor)

For every set X it holds

$$X \prec \mathcal{P}(X).$$

In particular, the set $\mathcal{P}(\mathbb{N})$ is uncountable.

Proof.

A function $h : X \to \mathcal{P}(X)$ defined by $h(x) = \{x\}$ for each $x \in X$ is clearly 1-1 from X to $\mathcal{P}(X)$. This means that X is smaller than $\mathcal{P}(X)$: $X \preceq \mathcal{P}(X)$.

Now we show that there is no bijection between X and $\mathcal{P}(X)$, which will imply $X \prec \mathcal{P}(X)$. In fact, we will show a stronger property, namely that there is no surjection from X onto $\mathcal{P}(X)$.

Suppose for contradiction that there exists a surjection f from X onto $\mathcal{P}(X)$. □

Continuation of proof.

Define

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

Note that $A \subseteq X$. Since $A \subseteq X$ (i.e. $A \in \mathcal{P}(X)$), there is $a \in X$ such that $f(a) = A$ because f is onto. It must be the case that either $a \in A$ or $a \notin A$: If $a \in A$, then $a \notin f(a) = A$, contradiction. If $a \notin A$, then $a \notin f(a)$ and so $a \in A$, contradiction. It follows that there cannot be a surjection from X onto $\mathcal{P}(X)$, and in particular no bijection. □

Some basic notions and their properties.

Definition

If x, y are sets, then the *Cartesian product* $x \times y$ of x, y is defined as follows: $x \times y = \{\langle a, b\rangle \mid a \in x \wedge b \in y\}$.

Definition

A *binary relation* r on sets x, y is a subset of $x \times y$, i.e. $r \subseteq x \times y$.

If r is a relation on x, y, we define the *domain* of r as

$$\mathrm{dom}(r) = \{q \mid (\exists q' \in y)\langle q, q'\rangle \in r\}. \tag{2}$$

and similarly we define *range* of r as

$$\mathrm{rng}(r) = \{q \mid (\exists q' \in x)\langle q', q\rangle \in r\}. \tag{3}$$

We also define the *inverse relation* $r^{-1} = \{\langle q, q' \rangle \mid \langle q', q \rangle \in r\}$, and if $a \subseteq x$ we define the *image of r on a*:

$$r''a = \{q \mid (\exists q' \in a)\langle q', q \rangle \in r\}.$$

If $a \subseteq x$ then we say that $r \restriction a$ is the *restriction* of r to a, where

$$r \restriction a = \{\langle q, q' \rangle \mid \langle q, q' \rangle \in r \wedge q \in a\}.$$

Exercise. Check the following for binary relations x, w and sets y, z:

1. $x \cup w, x \cap w, x - w$ are binary relations,
2. $x''(y \cup z) = x''y \cup x''z$,
3. $x''(y \cap z) \subseteq x''y \cap x''z$ and $x''y - x''z \subseteq x''(y - z)$.

Give an example where the converse inclusion $\supseteq$ does not hold in the previous line.

Definition

A binary relation r is called a *function* if it satisfies the following:

$$(\forall x, y_1, y_2)(\langle x, y_1\rangle \in r \wedge \langle x, y_2\rangle \in r \rightarrow y_1 = y_2).$$

Since every function f is a relation, we can use for f the notation defined above for relation. The following is specific for functions:

- If $x \in \mathrm{dom}(f)$ we write $f(x)$ for the unique y such that $\langle x, y\rangle \in f$.
- Let $f : x \rightarrow y$ and $g : y \rightarrow z$ be two functions. This notation means that $\mathrm{dom}(f) = x$, $\mathrm{dom}(g) = y$ and $\mathrm{rng}(f) \subseteq y$ and $\mathrm{rng}(g) \subseteq z$. We will denote as $g \circ f$ the function $h : x \rightarrow z$ defined by $h(q) = g(f(q))$ for every $q \in x$. Note that this deviates from the notation used for composition of relations. The reason is that if we write $(g \circ f)(q) = g(f(q))$, it suggests that f is the first function which we apply.

A function f is called *injective*, or 1-1, if it satisfies:

$$(\forall x_0, x_1 \in \mathrm{dom}(f))\ x_0 \neq x_1 \rightarrow f(x_0) \neq f(x_1).$$

Exercise. Verify that f is 1-1 if and only if f^{-1} is a function.
f is *onto* y if $\mathrm{rng}(f) = y$. f is a bijection if it is both injective and onto.

Exercise. Suppose n is a fixed element of $\mathbb{N}$. Consider function $f : \mathbb{N} \rightarrow \mathbb{N}$, $g : \mathbb{Z} \rightarrow \mathbb{Z}$, and $h : \mathbb{Q} \rightarrow \mathbb{Q}$ defined as follows: $f(m) = m + n, g(x) = x + n$, $h(q) = q + n$. Determine whether f, g, h are injective, onto, or bijections.

Exercise. Let x, y be any sets and f a function. Prove the following properties.

1. $(f^{-1})''(x \cap y) = (f^{-1})''x \cap (f^{-1})''y$.
2. $(f^{-1})''(x - y) = (f^{-1})''x - (f^{-1})''y$.
   If f is moreover 1-1, then it also holds:
3. $f''(x \cap y) = f''x \cap f''x$ and $f''(x - y) = f''x - f''y$.

Definition

For all sets x, y, let us define:

$$^{x}y = \{f \mid f : x \to y\}.$$

Sometimes we write y^x if there is no danger of confusion (however, sometimes y^x denotes the size of ^{x}y).

Exercise. Show by induction on $n \in \mathbb{N}$ that for all $m \in \mathbb{N}$, $|^{n}m| = m^n$.

Exercises.

- Let x be a non-empty set. Show there is a bijection between the Cartesian product $x^2 = x \times x$, and the set ${}^2x$.
- Let x be a set. There is a bijection between the set of all subsets of x, $\mathcal{P}(x) = \{y \mid y \subseteq x\}$ and the set ${}^x2$.

An axiomatic approach to $\mathbb{N}$. An axiomatic approach is useful if we wish to avoid the use of set theory in defining $\mathbb{N}$ and aritmetics. However, as we will see later on, the axiomatic approach is by necessity weaker than we would like to have it; in particular it is not possible to give a reasonable axiomatization of natural numbers and ensure that the resulting axiomatization will be strong enough to prove or refute every arithematical statement (Gödel's first incompleteness theorem).

What follows is the standard axiomatization of arithmetics in the first-order logic, called the *Peano arithmetics*, in the honor of G. Peano (1858–1932), an Italian mathematicians who first formulated a similar axiomatization.[2]

[2] Peano's axiomatization was in the second-order logic, see the lecture notes for more details.

First-order axiomatisation of arithmetics (Peano arithmetics, PA):
(Q1) $(\forall x, y)(S(x) = S(y) \to x = y)$,
(Q2) $(\forall x)(S(x) \neq 0)$,
(Q3) $(\forall x)(x \neq 0 \to (\exists y)x = S(y))$,
(Q4) $(\forall x)(x + 0 = x)$
(Q5) $(\forall x, y)(x + S(y) = S(x + y))$
(Q6) $(\forall x)(x \cdot 0 = 0)$
(Q7) $(\forall x, y)(x \cdot S(y) = x \cdot y + x)$
(Induction) For every formula $\varphi(x)$ in the language $\{0, S, +, \cdot\}$ (including parameters) the following is an axiom:

$$[\varphi(0) \wedge (\forall x)\,(\varphi(x) \to \varphi(S(x)))] \to (\forall x)\,\varphi(x).$$

Note that PA contains infinitely many axioms (because Induction is a collection of infinitely many instances of induction). It can be shown that no finite subtheory of PA is equally strong as PA, so the infinite number of axioms is necessary.

By Gödel's 2nd incompleteness theorem, a finite argument is not sufficient to argue that PA is consistent.[3] If it is consistent, Gödel's 1st incompleteness theorem shows that there are infinitely many φ such that PA does not prove either φ or $\neg\varphi$ (we say that φ is *independent* over PA). It may be that some of the open problems in arithmetics cannot be decided by the axioms of PA. An analogous coveat applies to axiomatization of set theory.

[3] Set theory can prove that PA is consistent; but this is may be viewed as cheating because set theory itself is more in danger of inconsistency than PA. Usually, the consistency of PA, and also of set theory, is taken on faith based on intuition and the past experience (no inconsistency has been discovered since the beginning of mathematics in the ancient Greece).

An example of finite combinatorics: Ramsey theorem for graphs.

Motivation. Suppose there are n people at the party. What is the biggest group of people such that either everyone knows everyone in that group, or nobody knows anybody in that group (we call such a group *homogeneous*)? In particular is there a number n such that in every party with n people one can find a homogeneous group with 5 people (or any other number you wish)?

Intuitively, the bigger the homogeneous set, the more *order* we have in the group of people (or equivalently, less chaos).

From popular mathematics, one perhaps knows that in any party with at least 6 people there is a homogeneous group with 3 people. In a party with at least 18 people, there is a homogeneous group with size 4. What about a homogeneous group of size 5? Currently, it is known that it suffices to have a party of 48, but it is currently unknown whether already 43 is not enough. How do we get these numbers? And how is it possible that we do not know the exact number for a homogeneous group of size 5? After all 43 is a very small number, so perhaps computers could help us here?

To formulate this problem in the mathematical language, first notice that it is irrelevant what the people in the party are – it is enough to know their number. Thus n people in a party can be represented by natural numbers $\{1, \ldots, n\}$. The fact that two people m, k know each other can be represented by considering the set $\{m, k\}$. Thus we can represent the situation by fixing a set E of two-element subsets of $\{1, \ldots, n\}$ such that for any pair of people k, m, k knows m if and only if $\{k, m\} \in E$.[4]

[4] Notice that we need to make some extra assumptions in formalising the problem: we have decided that the relation of knowing one another is symmetric: k knows m if and only if m knows k.

The pair $\langle \{1, \ldots, m\}, E \rangle$ is an example of a undirected graph:

Definition

Let V be a non-empty set and E a subset of $[V]^2$, where $[V]^2$ is the set of all two-element subsets of V, i.e.

$$[V]^2 = \{\{v_1, v_2\} \mid v_1 \neq v_2 \ \& \ v_1, v_2 \in V\}.$$

We call elements in V *vertices*, and elements in E *edges*. The pair $\langle V, E \rangle$ is called a *undirected graph*.

If we changed the definition by writing $E \subseteq V^2$, then we get the notion of a *directed* graph – in a directed graph, one considers also the order of the elements in the edges: $\langle v_1, v_2 \rangle$ may be in E, but $\langle v_2, v_1 \rangle$ not (and $v_1 = v_2$ is allowed).

What is the number of undirected graphs on n vertices?

Lemma

For $n > 1$, there are 2^l many undirected graphs on $V = \{1, \ldots, n\}$, where $l = \frac{1}{2}n(n-1)$. This means that the number of graphs grows exponentially with the number of vertices.

Proof.

Fist compute the size of $[V]^2$ which is $l = \frac{1}{2}n(n-1)$. Then realize that $E \subseteq [V]^2$, and so the number of graphs on V is the size of the powerset of $[V]^2$, which is 2^l. □

We have discussed above that it is currently unknown what is the least number n such that every undirected graph on n vertices has a homogeneous set of size 5 (we only know that n is in the set $\{43, 44, 45, 46, 47, 48\}$). To answer this question, it is enough to check all undirected graphs on 43 vertices (and possibly on 44–47). This seems feasible until we calculate the number of such graphs: $2^{\frac{1}{2}43 \cdot 42}$ which is extremely big.[5] Of course, finding the exact number for a homogeneous set of size 6, 7, 101, etc. is even more difficult. The crude force will not going to help us here.

[5] Technically speaking not all graphs need to be checked – some are isomorphic, i.e. behave the same way, but even with this limitation the number of graphs is too high (see below on slide 55 for a discussion of isomorphisms).

Definition

Let $\langle V, E \rangle$ be a undirected graph. We say that $H \subseteq V$ is a homogenous set of vertices if either all vertices in H are connected by edges with every other element in H (i.e. $[H]^2 \subseteq E$), or no elements in H are connected with edges (i.e. $[H]^2 \cap E = \emptyset$).

We now have everything set up to formulate a mathematical theorem corresponding to the above-mentioned problem.

Theorem (Finite Ramsey[a] theorem for graphs)

[a] Frank P. Ramsey (1903–1930) was a British mathematician and philosopher.

Let k be a natural number, $k > 1$. Then there exists a number n such that every undirected graph $\langle V, E \rangle$ on n vertices has a homogeneous subset of size at least k.

Note that the theorem claims the existence of *some* n which suffices. The proof we give actually gives an algorithm for computing some such n with respect to the size of $|V|$ (and for finding a homogeneous set). However, this n is far from being optimal in the cases which can be checked. No significantly better algorithm for finding n is known at the moment.

- Our strategy is to find in every graph on $n > 1$ vertices a homogenous set of size at least $\frac{1}{2}\log_2 n$. For a given k, it therefore suffices to take n equal to 2^{2k} because then $\frac{1}{2}\log_2 n = k$.
- Without the loss of generality $V = \{1, \ldots, n\}$. To simplify our exposition, note that we can represent unordered pairs in E by ordered pairs $\langle k, m\rangle$ with the condition that $k < m$.
- We say that a pair $\langle k, l\rangle$ has color c_1 if k and m are connected by an edge, and color c_0 otherwise.

- Denote $X_0 = V$. Fix the vertex 1, denote it v_0, and consider all pairs $\langle v_0, k \rangle$ for $1 < k \leq n$ and look at the color of the pairs. There must be one prevailing color: there are at least $\lceil \frac{1}{2}(n-1) \rceil$-many pairs $\langle v_0, k \rangle$ which have all either color c_1 or color c_0.
- Choose this prevailing color, and consider the set $X_1 = \{v_0, v_1, \ldots\}$ of the vertices such that for every element $x > 1$ in X_1, $\langle v_0, x \rangle$ has the prevailing color.
- Now start with v_1 and consider the prevailing color for pairs $\langle v_1, x \rangle$ for $x \in X_1$, $x > v_1$, and define the set $X_2 = \{v_0, v_1, v_2, \ldots\}$ similarly as X_1.

- Repeat this argument several times till you have no more vertices to consider (i.e. till $X_r = \{v_0, \ldots, v_r\}$).
- Denote the resulting set of vertices $A = \{v_0, v_1, \ldots, v_r\}$.
- For every $0 \leq i < r$, we do not lose more than one half of the elements in X_i when defining X_{i+1}. It follows that that we can carry out this construction at least $\log_2 n$-many times, and each time we repeat the step from X_i to X_{i+1} we fix one more element v_i which stays in A. Thus the size of A is therefore at least $\log_2 n$.

- A may not be homogenous but has the nice property that the color of any pair $\langle x, y \rangle$ in A, where $x < y$, depends only on the color of the first element.
- Choose a color which prevails in A and select those elements in A with this color. Denote the resulting set H. H is homogeneous and has size at least $\frac{1}{2}|A|$.
- It follows that $n = 2^{2k}$ satisfies the conditions of theorem, which finishes the proof.

Examples of graphs.

- Suppose $<$ is an ordering on some set X. Then $\langle X, < \rangle$ is a directed graph on X.
- A *finite tree* is a finite undirected graph (V, E) which does not contain any cycles, i.e. there is no sequence of distinct nodes $\{x_1, \ldots, x_n\}$ such that for all $1 \leq i < n$, $\{x_i, x_{i+1}\} \in E$ and $\{x_n, x_1\} \in E$. If $\langle V, E \rangle$ is moreover connected, i.e. every node is connected to some other node, then this is equivalent to saying that between any two nodes there is exactly one path.

Infinite graphs.

Note that we can define a graph on any set V, where V can be infinite. For instance if $E \subseteq [\mathbb{N}]^2$, then $\langle \mathbb{N}, E \rangle$ is an undirected graph of $\mathbb{N}$. Is there an analogue of Ramsey theorem for infinite graphs? Indeed, there is, and was also proved by Ramsey (more general versions are known).

Theorem (Infinite Ramsey theorem)

Every undirected graph on $\mathbb{N}$ has an infinite homogeneous set.

Note that both finite and infinite graphs are quite complicated strutures.

In fact graphs on $\mathbb{N}$ can be extremely complex: If ZFC (the standard set theory) is consistent, then there exists[6] $E \subseteq \mathbb{N}^2$ such that the directed graph $\langle \mathbb{N}, E \rangle$ models all axioms of set theory: the set $\mathbb{N}$ represents the domain of the set theory (i.e. all sets), and $\langle m, n \rangle \in E$ is interpreted as saying that m is an element of n. With this intepretation, any axiom φ of ZFC is true in $\langle \mathbb{N}, E \rangle$.

Hence all mathematics can be modelled as a directed graph on $\mathbb{N}$.[7]

[6] This follows from the Löwenheim-Skolem theorem for the 1st order predicate logic; you will learn more in Logic lectures.

[7] This may seem paradoxical. The philosophical discussion concerning the so called *Löwenheim-Skolem paradox* are extensive.

Graph isomorphisms.

If $V_1 = \{a, b, c\}$ and $V_2 = \{1, 2, 3\}$, then any graph on V_1 is different from any graph on V_2. However, they may be different only inessentially in the sense that if we "rename" the nodes, the graphs may become the same. As a simple example suppose $E_1 = [V_1]^2$ and $E_2 = [V_2]^2$: then $\langle V_1, E_1 \rangle$ and $\langle V_2, E_2 \rangle$ are different, but both have three nodes and every node is connected to every other node. If we are intersted only in the mathematical properties of graphs, then any result shown for the first graph applies to the second graph, and conversely, i.e. for mathematical purposes they are the same. $\langle V_1, E_1 \rangle$ is *isomorphic* to $\langle V_2, E_2 \rangle$ if we identify (for instance) a with 1, b with 2, and c with 3. See the definition on the next slide.

Definition

We say that undirected graphs $\langle V, E\rangle$ and $\langle U, F\rangle$ are *isomorphic* if there is a bijection $f : V \to U$ which satisfies for all $x \neq y \in V$:

$$\{x, y\} \in E \leftrightarrow \{f(x), f(y)\} \in F.$$

The notion of an isomorphism can be formulated for directed graphs, and more complicated structures. There weaker notions of *similarity* of structures, for instance *homomorphisms* or *embeddings*.

Integers $\mathbb{Z}$ as a group with respect to addition

Integers $\mathbb{Z}$ extend the natural numbers $\mathbb{N}$ and have the property that for every $n \in \mathbb{Z}$, there is an inverse element $-n \in \mathbb{Z}$ such that $n + (-n) = 0$. In particular, the operation of subtraction is total in $\mathbb{Z}$: $n - m = n + (-m)$. This extension $\mathbb{Z}$ is unique and the smallest such (every element of $\mathbb{Z}$ is either in $\mathbb{N}$ or is an inverse of an element in $\mathbb{N}$)

Integers $\mathbb{Z}$, together with the binary operation $+$, the unary operation $-$ and the constant 0, are an example of a *group*.

Groups

Definition

We say that a set G together with the constant $e \in G$, binary operation $\circ : G^2 \to G$ and unary operation $' : G \to G$ is a *group* if the following identities are true in G:

(G1) Associativity. For all $x, y, z \in G$, $(x \circ y) \circ z = x \circ (y \circ z)$,

(G2) Neutral element. For every $x \in G$, $x = x \circ e = e \circ x$,

(G3) Inverse element. For every $x \in G$, $x \circ x' = x' \circ x = e$.

If the operation $\circ$ is commutative, i.e.

(G4) For every $x, y \in G$, $x \circ y = y \circ x$,

we say that the group G is *abelian*, or commutative group.

Examples of groups

- The structure $\langle \mathbb{Z}, +, -, 0 \rangle$, i.e. integers with addition $+$, inverse element $-$, and the constant 0, is a commutative group.
- The structure $\langle \mathbb{Q} - \{0\}, \cdot, ^{-1}, 1 \rangle$, i.e. rational numbers without 0 with multiplication $\cdot$, inverse element $^{-1}$, and the constant 1, is a commutative group.
- The structure $\langle \{0, 1, 2\}, \circ, ', e \rangle$ where $\circ$ is defined by $n \circ m = n + m \bmod 3$, $n' = 3 - n \bmod 3$, and $e = 0$ is a finite commutative group. More generally, for any k there exists group of size k which has elements $\{0, \ldots, k-1\}$ and which has $+$ as the addition mod k.

- *Permutation groups.*
  Sym($\mathbb{N}$), the permutation group on $\mathbb{N}$ is defined as follows: a function $p : \mathbb{N} \to \mathbb{N}$ is in Sym($\mathbb{N}$) if it is a permutation, i.e. a bijection between $\mathbb{N}$ and $\mathbb{N}$. The neutral element is the identity function id defined by $\mathrm{id}(n) = n$ for every n. The inverse to p is p^{-1}, the inverse function. The binary operation is the composition of functions.

  Exercise. Show that Sym($\mathbb{N}$) is an example of a group which is not abelian.

A group of permutations on a set X is also called the *symmetric group on X*. *Cayley's Theorem* states that every group is isomorphic to a subgroup of some symmetric group, i.e. every group is included in some symmetric group. This means that symmetric groups of permutations are very general.

Basic properties of groups.

Lemma

Let G be a group, then:

1. *The neutral element is unique: if f is an element in G such that $x \circ f = f \circ x = x$ for every x, then $f = e$. Also $e = e'$.*
2. *The inverse element is unique: given y in G, if z is an element in G such that $z \circ y = y \circ z = e$, then $z = y'$.*
3. *For every x, y in G: $(x \circ y)' = y' \circ x'$.*
4. *For every x in G: $x'' = x$.*
5. *(The function $'$ is a 1-1 function.) For every $x, y \in G$: if $x \neq y$ then $x' \neq y'$.*
6. *(Cancelation). For every $x, y, z \in G$: if $x \circ y = x \circ z$, then $y = z$, and if $y \circ x = z \circ x$, then $y = z$.*

See the lecture notes for the proof.

Subgroups

Definition

Let G be a commutative group[a] with operations $\circ, ', e$ and H be a subset of G. We say that H is a *subgroup* of G, and write this as $H \leq G$, if:

- $e \in H$,
- For every $x \in H$, $x' \in H$,
- For every $x, y \in H$, $x \circ y \in H$.

We express the conditions (i)–(iii) by saying that H is *closed under the group operations*.

[a] For simplicity, we will consider only commutative groups.

Exercise. Convince yourself that every group G has at least two subgroups: one contains just the neutral element, and the second one is the whole group G (a group G is its own subgroup by the definition). There are groups, such as $\mathbb{Z}(p)$ for a prime number p (see below), which have just these two subgroups.

The conditions (i)–(iii) are equivalent to a single condition over any commutative group:

Lemma

Let $H \subseteq G$ and $H \neq \emptyset$. Then the following holds: H is a subgroup of G if and only if for every $x, y \in H$, $x \circ y' \in H$.

Exercise. Give a proof of this lemma.

We will use subgroups and the related notion of a partition to prove the following theorem for groups:

Theorem (Lagrange[a])

[a] Italian-French mathematician 1736–1813.

Let G be a finite group and H its subgroup. Then the size of H divides the size of G, i.e. $\frac{|G|}{|H|} = n$ for some $n \in \mathbb{N}$.

One of the consequences of this theorem is that a group of size p, where p is a prime number, does not have any proper subgroups. By a further argument it can be shown that this implies that up to isomorphism there is exactly one group of size p, p prime, and this group is commutative.

Proof of Lagrange's theorem

Please follow the proof in the lecture notes. Here is a summary of the key steps:

- System $A \subseteq \mathcal{P}(G)$ is called a *partition* of G if (i) $\emptyset \notin A$, (ii) $\bigcup A = G$, and (iii) For all $X, Y \in A$, if $X \neq Y$, then $X \cap Y = \emptyset$. Elements of A are called *equivalence classes*.[8] It follows that every element $g \in G$ is in exactly one of the equivalence classes.
- We show that the subgroup H of G generates a *partition* of H, denoted G/H, into *cosets*[9] of the form $H \circ x = \{h \circ x \mid h \in H\}$:

$$G/H = \{H \circ x \mid x \in G\}.$$

[8] There is a natural correspondence between equivalences on G and partitions on G; see lecture notes.

[9] *Coset* is another word for an *equivalence class* in the context of groups.

- Next we show that each coset $H \circ x$ has the same size as H.
- It follows that if n denotes the number of cosets, then $|G| = n|H|$, and this ends the proof.

Quotient groups.

Suppose $G = \langle G, +, -, 0 \rangle$ is a group, not necessarily commutative, and H its subgroup. We discussed how to define cosets $H + x$ for $x \in G$. If G is not commutative, then $H + x \neq x + H$ is possible. If this does not happen, it is possible to use H to define another group:

Definition

If for all x, $H + x = x + H$, then H is called *normal*, and we can form the *quotient group* G/H as follows:

- The domain of H/G is the set of equivalence classes $\{H + x \,|\, x \in G\}$.
- The operation $+_{G/H}$: $(H + x) +_{G/H} (H + y) = H + (x + y)$.
- The operation $-_{G/H}$: $-_{G/H}(H + x) = H + -x$.
- The neutral element: $0_{G/H} = H$.

Example.

Let $\mathbb{Z} = \langle \mathbb{Z}, +, -, 0 \rangle$ be the group of integers and for $k > 1$, let $\mathbb{Z}_k$ be the subgroup of $\mathbb{Z}$ of all multiples of k. Since $+$ is commutative, H is automatically normal, and therefore $\mathbb{Z}(k) = \mathbb{Z}/\mathbb{Z}_k$ is a well-defined quotient group. It is easy to see that there are k many equivalance classes: $\mathbb{Z}_k, \mathbb{Z}_k + 1, \ldots, \mathbb{Z}_k + (k-1)$. As it turns out, $\mathbb{Z}(k)$ is isomorphic to the group $\{0, \ldots, k-1\}$ where the operations are defined modulo k.

The description of $\mathbb{Z}(k)$ using the quotient group is preferable because it is an instance of a general method, whereas the "manual" definition of $\mathbb{Z}(k)$ with addition mod k only works for this specific case.

Rings and fields

A *ring* (okruh) is a structure which extends the notion of a group by adding one more binary operation called *multiplication*.

Definition

We say that a structure $\langle R, +, -, 0, \cdot, 1\rangle$ is a *ring* if $1 \neq 0$, and the following properties hold for all $x, y, z \in R$:

(R1) Associativity for $+, \cdot$.

(R2) Commutativity for $+$.

(R3) Neutral element for $+$. $0 + x = x + 0 = x$.

(R4) Inverse element for $+$. $x + (-x) = (-x) + x = 0$.

(R5) Neutral element for $\cdot$. $1x = x1 = x$.

(R6) Distributivity. $x(y + z) = xy + xz$, $(y + z)x = yx + zx$.

Note that if R is a ring, we require that $\langle R, +, -, 0\rangle$ is an abelian group. This is a natural condition; in fact in the presence of the distributivity axiom (R6), if $\langle R, +, -0, \rangle$ is a group it *must* be abelian (i.e. commutative): let x, y be elements of R, then

$$(1+1)(x+y) = 1(x+y) + 1(x+y) = x+y+x+y, \quad \text{using distributivity from the right} \tag{4}$$

and

$$(1+1)(x+y) = (1+1)x + (1+1)y = x+x+y+y, \quad \text{using distributivity from the left.} \tag{5}$$

It follows that $x+y+x+y = x+x+y+y$. By adding $-x$ from the left, and then $-y$ from the right, we obtain $y+x = x+y$.

If the operation of $\cdot$ is commutative, i.e.

Definition

(R7) Commutativity for '$\cdot$': $xy = yx$,

we call R a *commutative ring*.

If moreover a commutative ring R has no zero-divisor, i.e.

Definition

(R8) $xy = 0$ implies $x = 0$ or $y = 0$,

we call R an *integral domain*.[a]

[a] The existence of zero-divisors is not desirable if we want to have multiplicative inverses: assume $xy = 0$ and x and y are not 0, then neither x or y can have the inverse: assume x^{-1} is the inverse to x, then if we multiply $xy = 0$ by x^{-1}, we obtain $x^{-1}xy = x^{-1}0$, and so $y = 0$, which contradicts our initial assumption that both x and y are non-zero.

Definition

If moreover R carries a binary relation $\leq$ such that:

(R9) $\leq$ is a linear ordering,

(R10) Monotonicity with respect to $+$.
$x \leq y$ implies $x + z \leq y + z$,

(R11) Monotonicity with respect to $\cdot$.
$x \leq y$ and $0 \leq z$ implies $xz \leq yz$,

we call R an *ordered ring*.

Fact

The integers $\mathbb{Z} = \langle \mathbb{Z}, +, -, 0, \cdot, 1, \leq \rangle$ *are an ordered commutative ring which is an integral domain.*

Another widely used example of an integral domain is the ring of polynomials in the variable x over rationals or reals, denoted $\mathbb{Q}[x]$ or $\mathbb{R}[x]$, respectively: a polynomial is of the form

$$q_0 + q_1 x + q_2 x^2 + \cdots + q_n x^n,$$

for some $n < \omega$, and $q_0, \ldots, q_n$ either rationals or reals. It is possible to define additions and multiplication on polynomials so that the resulting structure is an integral domain. However, it is not a field (see below for the definition of field).

Here are some basic properties of rings:

Lemma

If R is a ring, then for all $x, y \in R$:

- $0x = x0 = 0$.
- $x(-y) = (-x)y = -(xy)$,
- $-x(-y) = xy$,
- $-x = (-1)x$

  If R is moreover an integral domain, then:
- *If $xy = xz$ and $x \neq 0$, then $y = z$ (Cancellation law).*

Proof: Exercise, or lecture notes.

Definition

A ring R is called a *division ring* if every non-zero element x has a multiplicative inverse, i.e. there exists y such that $xy = yx = 1$. A commutative division ring is called a *field*.

A field, possibly even an ordered field, is the strongest algebraic structure with binary operations $+, \cdot$, but it is is some sense very scarce. Examples:

- $\mathbb{Q}$ and $\mathbb{R}$ are *ordered fields*.
- $\mathbb{C}$ is a field, which cannot be ordered.[10]
- No other space $\mathbb{R}^n$ for $n > 2$ can be a field. $\mathbb{R}^4$, *quaternions*, can be equipped with multiplication but it fails to be commutative. $\mathbb{R}^8$, *octonions*, can be equipped with multiplication but it fails to be even associative.

[10] We may view $\mathbb{C}$ as the space $\mathbb{R}^2$ with suitably defined multiplaction for the "vectors" (x, y) in $\mathbb{R}^2$.

To anticipate some future topics, let us mention what is difference between the fields $\mathbb{Q}, \mathbb{R}, \mathbb{C}$:

- $\mathbb{Q}$ is not *complete* in an analytic sense: there are bounded subsets of $\mathbb{Q}$ which don't have a supremum or infimum. This is not an algebraic notion, but it is important for the development of mathematical analysis (the study of continuity, differentiation and integration). Morever, $\mathbb{Q}$ is not closed under *roots of polynomials*: there are polynomials with rational coefficients which do not have roots in $\mathbb{Q}$. Note that the existence of multiplicative inverses means that *linear equations* have roots: $q_0 + q_1 x = 0$, with $q_1 \neq 0$, has the root $-\frac{q_0}{q_1}$. However for all $n > 1$ there is a polynomial of degree n which does not have a root.

- $\mathbb{R}$ is complete in the analytic sense. It is has roots for more polynomials: $\mathbb{R}$ is a *real-closed field* which means that every polynomial of *odd* degree has roots.
- $\mathbb{C}$ is complete in the analytic sense. Morever, it is also *algebraically closed*: every polynomial with complex coefficients has roots. In fact, it is enough to add one special root i, which is the root for $x^2 + 1 = 0$, to $\mathbb{R}$ to obtain $\mathbb{C}$.

There are many uses of fields in mathematics. Before we mention a few, let us show that for finite rings, the notions of integral domain and field coincide:

Lemma

Any finite integral domain R is already a field.

Proof.

Consider a map $x \mapsto ax$ where a is some fixed $a \in R$ not equal to 0. Then this map is 1-1 from R to R by the cancellation law, and since R if finite, $\text{rng}(f) = R$. It follows that there is some x such that $ax = 1$, and this x is the inverse of a. Since a is arbitrary non-zero, this shows that every element has a multiplicative inverse. □

Example 1. Recall the quotient group $\mathbb{Z}(k)$ of addition modulo k. This structure can be also equipped with 1 and multiplication, and we obtain the ring $\mathbb{Z}(k)$: the multiplication is also defined as the usual multiplication mod k.

- If k is not prime, then $\mathbb{Z}(k)$ is a ring which is not an integral domain: if $k = mn$ for $m, n \neq 0$, $m, n < k$, then $mn = 0$ in $\mathbb{Z}(k)$.
- If k is prime, then $\mathbb{Z}(k)$ is an integral domain because if $mn = k = 0$ for $m, n < k$, then either m or n must be zero, otherwise m, n witness that k is not prime (note that $m, n < k$ so neither m or n can be 1 because then the other number would need to be k). It follows by the previous lemma that $\mathbb{Z}(k)$ is already a field.

Remark. Unlike groups, fields cannot have an arbitrary finite size. It can be shown that if F is a finite field, then $|F| = p^n$ for some prime number p.[11]

[11] Morever, every two finite fields of the same size are isomorphic, so up to isomorphism there is exactly one field of size p^n for every prime p and $1 \leq n \in \mathbb{N}$.

Example 2. Complete fields are used development of mathematical analysis. For instance, the notion of *differentiation* involves division, i.e. multiplicative inverses, and therefore in general a ring structure is not enough, and a field is required.

This is the reason whey real analysis and complex analysis are powerful tools. Analysis for vector spaces for $\mathbb{R}^n$ for $n > 2$ is possible,[12] but some concepts cannot be developed completely (for instance differentiation can only be applied partially, with all but one coordinate being fixed).

[12] Recall that $\mathbb{R}^n$ for $n > 2$ cannot be equipped by a field structure which extends $\mathbb{C}$.

Example 3. Vector space is an algebraical structure which combines an abelian group with a field.

Definition

We say that V is a *vector space* over a field F if the following hold:

- V is an abelian group.
- F is a field. We denote elements of F by Greek letters $\alpha, \beta, \ldots$, and write $\alpha\beta$ for their multiplication.
- Elements of F, called *scalars*, act on V: for every vector $x \in V$ and scalar α, αx is a vector. This acting has following properties:
  - $\alpha(\beta x) = (\alpha\beta)x$.
  - $1_F x = x$.
  - $\alpha(x + y) = \alpha x + \alpha y$.
  - $(\alpha + \beta)x = \alpha x + \beta x$.

A simple, but an important example, of a vector space is the n-dimensional vector space $\mathbb{R}^n$. The vectors are identified with n-tuples of reals, i.e. with elements of $\mathbb{R}^n$, and the the field F is the reals $\mathbb{R}$.

$\mathbb{R}$ with $+, -, 0$ can be viewed as a vector space over the field $\mathbb{Q}$, similarly $\mathbb{C}$ is a vector space over $\mathbb{Q}$ or $\mathbb{R}$.
See more details on the whiteboard.

Construction and uniqueness of $\mathbb{Z}$

Recall that $\mathbb{N}$ is defined as the unique set which is the intersection of all *inductive* sets.[13]

$$\mathbb{N} = \bigcap \{X \mid X \text{ is inductive}\}.$$

The uniqueness of $\mathbb{N}$ ensures that up to isomorphism, all other number domains $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are unique. This uniqueness extends to number domains considered as groups or rings.

[13] X is inductive if (i) $\emptyset \in X$, and (ii) for $x \in X$, $x \cup \{x\} \in X$.

Theorem

Up to isomorphism, the group $\langle \mathbb{Z}, +, -, 0 \rangle$ is unique.

To prove the theorem, we need to show two things:

- Existence: we need to construct $\mathbb{Z}$ (using $\mathbb{N}$ and constructions available by axioms of set theory).
- Uniqueness: we need to show that up to isomorphism, what we constructed is unique.

See the whiteboard for a sketch of the proof.

The notion of an isomorphism. The notion of isomorphism is defined with respect to the operations and relations which are present in the structures in question. We give just examples which are most important for us:

Definition

Suppose $G = \langle G, +, -, 0\rangle$ and $F = \langle F, \cdot, ^{-1}, 1\rangle$ are two groups. We say they are *isomorphic*, and we write $G \cong F$, if there is a bijection $f : G \to F$ which has the following properties for all $x, y \in G$:

- $f(x + y) = f(x)f(y)$,
- $f(-x) = f(x)^{-1}$,
- $f(0) = 1$.

It is in this sense that $\mathbb{Z}(k)$ is isomorphic to the addition on $\{0, \ldots, k-1\}$ mod k.

Definition

Suppose $(A, <)$ and $(B, \prec)$ are two partial orders. Then they are isomorphic if there is a bijection $f : A \to B$ which satisfies the following for all $x, y \in A$:

- $x < y \leftrightarrow f(x) \prec f(y)$.

For instance $(\mathbb{Z}, <)$ is isomorphic to $(\mathbb{Z}_k, <)$ for all $k > 1$. We will see in a future lecture that in this sense $(\mathbb{Q}, <)$ is isomorphic to each of its subintervals $((q_0, q_1), <)$, for $q_0 < q_1$.

But first let us say something about the size of number domains:

Comparing sizes of infinite sets: $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$

Suppose X, Y are sets (finite or infinite). Recall that X has a size smaller or equal than Y, $|X| \leq |Y|$, if there is an injective function from X into Y. X and Y have the same size, $|X| = |Y|$, if there is a bijection between them. X is strictly smaller than Y, $|X| < |Y|$, if there is an injective function from X into Y but no bijection.[14]

Definition

An infinite set X is called *countable* it there is a bijection between X and $\mathbb{N}$. Otherwise it is called uncountable.

Theorem

$\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ are all countable. $\mathbb{R}$, $\mathbb{C}$, $\mathbb{R}^n$, $n \in \mathbb{N}, n \geq 1$ are all uncountable and have the same size.

[14] Another notation for these notions is $X \preceq Y, X \approx Y, X \prec Y$.

With the Axiom of Choice, all reasonable definitions of *finite* are equivalent, and in particular X is finite if there is no injective function $f : X \to X$ which is not onto (in other words, X is finite iff every injective function $f : X \to X$ is already a bijection). For infinite sets this fails, so the following theorem (which we will prove in Set theory class) is useful when dealing with infinite sets:

Theorem (Cantor-Bernstein)

For all sets X, Y, if $|X| \leq |Y|$ and $|Y| \leq |X|$, then $|X| = |Y|$.

As we mentioned above, this theorem is trivial for finite sets: if X, Y are finite that and $f : X \to Y$, $g|Y \to X$ are injective, then both f, g are actually bijections.

For a set X, let $X^{<\omega}$ be the set of all finite sequences of elements in X.

Theorem

$|\mathbb{N}| \leq |\mathbb{Z}| \leq |\mathbb{Q}| \leq |\mathbb{N}^{<\omega}| \leq |\mathbb{N}|$. *Hence* $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ *are countable.*

Proof.

Hint: Let $P = \{p_0, p_1, \ldots\}$ be the set of all prime numbers. For each finite sequence $s = \langle n_0, \ldots, n_k \rangle$ of natural numbers, let $f(s)$ be the number $p_0^{n_0} \cdots p_k^{n_k}$. By the factorization theorem in arithmetics if $s \neq s'$ then $f(s) \neq f(s')$ and so f is injective function from $\mathbb{N}^{<\omega}$ into $\mathbb{N}$, and so $|\mathbb{N}^{<\omega}| \leq |\mathbb{N}|$. The rest follows by the Cantor-Bernstein theorm and the fact that $\mathbb{Z}$ and $\mathbb{Q}$ can be indentified with pairs of natural numbers. □

Theorem

$|\mathbb{N}| < |\mathbb{R}| = |\mathbb{C}| = |\mathbb{R}^n|$ *for all* $n \geq 1$.

Proof.

(Hint) It is a fact (which we will prove in Set theory class) that $|\mathbb{R}| = |\mathcal{P}(\mathbb{N})|$, in fact $(*)$ for any interval (r_0, r_1), $r_0 < r_1$, $|(r_0, r_1)| = |\mathcal{P}(\mathbb{N})|$. Racall that Cantor's theorem implies $|\mathbb{N}| < |\mathcal{P}(\mathbb{N})|$, and so $|R|$ is uncountable. Regarding the rest of the theorem, we will sketch that there is a injection from $(0,1) \times (0,1) \to (0,1)$, and so by Cantor-Bernstein and $(*)$ it follows $|\mathbb{R}| = |\mathbb{R}^2| = |\mathbb{C}|$. If $x = 0.x_0x_1\ldots$ and $y = 0.y_0y_1\ldots$ are two decimal representations of reals in $(0,1)$[a], set $f(x,y) = 0.x_0y_0x_1y_1\ldots$. Exercise: Check that this is an injective function. Exercise: Generalize this idea to argue that $(0,1)^n$ has the same size as $(0,1)$ for $n \geq 1$. □

[a] Use some unique representation: for instance avoid a tail of 9's, eg. use $0.1000\ldots$ and not $0.099999\ldots$ to represent $1/10$.

We will see in Set theory class that these results do not apply just to number domains: if X is an infinite set, the $|X^2| = |X|$ and by induction $|X^{<\omega}| = |X|$. This in general requires the Axiom of Choice.

The field $\mathbb{Q}$, and the uniqueness of the ordering on $\mathbb{Q}$

[The slides will be added as we approach this topic]