Foundations of modern mathematics

Radek Honzik

Charles University, Department of Logic, version November 11, 2024

logika.ff.cuni.cz/radek

Lecture notes

Introduction

We will discuss the following topics:

- Development of mathematical analysis by Descartes, Fermat, Newton and Leibniz in 17th century. While some of the ideas of analysis have been mentioned earlier, they were not developed to their full potential. Differentiation, integration, measure theory and other belong here.
- Development of abstract algebra, in particular group theory, ring theory etc. in the 18th and 19th century (Lagrange, Galois).

- Development of set theory by Cantor in the 19th century. Set theory provides a unifying language and background and allows formal development of mathematical objects such as real numbers.
- Development of mathematical logic by Hilbert and Ackermann in the early 20th century. By applying mathematical methods to proofs in mathematics, it is possible to show that certain propositions can be proved or refuted in the given theory (Axiom of Choice, Continuum Hypothesis, Euclid's 5th postulate, etc). Clarification of the difference between *true* and *provable*.

There will be slides for the course.
Further reading:

- J.K.Truss, Foundation of Mathematical Analysis. Clarendon Press, Oxford. 1997.
- Walter Rudin, Principles of Mathematical Analysis. McGraw-Hill, 3rd edition.
- David S. Dummit and Richard M. Foote, Abstract algebra, John Wiley and Sons, 2004
- Bohuslav Balcar a Petr Štěpánek, Teorie množin, Academia 2000
- Tomáš Jech, Set theory, Springer, 2000.
- Kenneth Kunen, Set theory – An introduction to independence proofs. Elsevier.

- Antonín Sochor, Klasická matematická logika, Karolinum 2001.
- Vítězlav Švejdar, Logika: neúplnost, složitost a nutnost, Academia 2002.

We will focus on the on the mathematical way of thinking: from hypotheses and informal arguments to rigorous proofs.

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.

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. □

The method of proving theorems from given assumptions traces back to Euclid's Elements (3rd century BC) and his treatment of elementary number theory and geometry. It was made more rigorous in the modern times.

Let us start with set theory and mathematical logic because modern mathematics is formulated in the language of set theory and explicitly or implicitly uses results from mathematical logic.

In particular, our discussion of analysis and abstract algebra will be formulated in the set-theoretical language.

A simple application of set theory in mathematics was Cantor's argument that there are far more irrational numbers than rationals – but without producing any concrete set of examples! Compare with our earlier argument that $\sqrt{2}$ is irrational.

Theorem

Rational numbers $\mathbb{Q}$ are a countable set,[a] *whereas real numbers $\mathbb{R}$ are uncountable:*[b] *it follows that $\mathbb{R} \setminus \mathbb{Q}$ is an uncountable set.*

[a] There is a bijection onto $\mathbb{N}$.

[b] X is uncountable if it is infinite and there is no bijection onto $\mathbb{N}$.

Note: We say that a real number is *transcendental* if it not a root of any polynomial with rational coefficients. For instance $\sqrt{2}$ is a root of the quadratic polynomial $x^2 - 2 = 0$, and therefore is irrational but not transcendental. By non-trivial arguments, one can show that e, π are transcendental. It is simple to generalize the above theorem to claim that the set of all non-trascendental numbers is just countable.

We need the following three facts for prove our theorem:

Fact

1. $\mathbb{R}$ *is an uncountable set.*
2. *If X is an infinite set, then $|X^2| = |X|$, i.e. there is a bijection between X and its square X^2.*
3. *If X, Y are infinite sets, then $|X \cup Y| = |X \times Y| = max(|X|, |Y|)$.*

Do you have some idea how to prove this fact?

Proof.

Proof of theorem. The set of integers $\mathbb{Z}$ is countable: define $f(x) = -2x$, for $x \leq 0$, and $f(x) = 2x - 1$ for $x > 0$; then f is a bijection from $\mathbb{Z}$ onto $\mathbb{N}$. Every rational number can be identified with a pair (p, q) of integers; since $\mathbb{Z} \times \mathbb{Z}$ is again countable by Lemma (2), the set of such pairs is countable, and it follows $\mathbb{Q}$ is countable. Since $\mathbb{R} = \mathbb{Q} \cup (\mathbb{R} \setminus \mathbb{Q})$, by Lemma (3), the size irrationals $\mathbb{R} \setminus \mathbb{Q}$ must be the same as $\mathbb{R}$, in particular uncountable. □

The proof met with opposition because it argues that there are many irrational numbers, without producing any concrete example. The whole method of using infinite sets was questioned. Today, the argument has become universally accepted.

Reals, continuity and limits

Until the development of set theory in 19th and early 20th century, there was a gap between *numerical and algebraical* notions and the *analytical* notions. The former were related to numbers, the latter to geometry.

The basic analytic notion is that of *continuity* (of a line) which can be motivated by requiring that a continuous line which starts with negative values and continues to positive values must have a point which has value 0. It was unclear how this can be modelled by means of discrete objects such as numbers.

At the first glance, the rationals $(\mathbb{Q}, <)$ should be rich enough because they satisfy the density condition:

Definition

For all $x, y \in \mathbb{Q}$, if $x < y$, then there is $z \in \mathbb{Q}$ such that $x < z < y$.

However, $\mathbb{Q}$ has gaps: for instance the set $A = \{x \in \mathbb{Q} \,|\, 0 < x, x^2 < 2\}$ is bounded from above and does not have the greatest point. Similarly $B = \{x \in \mathbb{Q} \,|\, 0 < x, x^2 > 2\}$ is bounded and does not have the least point. It is easy to check that $A \cup B$ contains all positive rationals, but "misses" $\sqrt{2}$.

Using a set-theoretical construction it is possible to fill in the "gaps" and construct a continuous real line, thus unifying numbers and geometry.

Definition

Assume $(X, <)$ is a linearly ordered set which is dense and does not have the least or greatest element.[a] We say that $A \subseteq X$ is bounded from above if there is an upper bound for A: i.e., there is $x \in X$ such that for all $a \in A$, $a \leq x$. We say that y is a supremum of A, $\sup(A) = y$, if y is the least upper bound. The notions of lower bound and infimum are defined analogously.

[a] *Exercise:* Check it must be infinite.

Exercise: Check that A from the previous slides does not have the supremum in $\mathbb{Q}$, and B does not have the infimum in $\mathbb{Q}$. Also check that if a supremum or infimum exists, it must be unique.

We will extended $(\mathbb{Q}, <)$ to $(\mathbb{R}, <)$ by adding all missing suprema and infima, but will do in the minimal way possible to ensure that $\mathbb{Q}$ is dense in the extension $\mathbb{R}$: it will be the case that for all $x < y$ in $\mathbb{R}$ there will be $q \in \mathbb{Q}$ with $x < q < y$.

Definition

A linearly ordered $(X, <)$ which is dense and without the least and greatest elements is *order-complete* if every $A \subseteq X$ bounded from above has the supremum.[a]

[a] Equivalently, A bounded from below has the infimum, and equivalently bounded subsets have both the supremum and infimum.

We say that $\alpha \subseteq \mathbb{Q}$ is a *Dedekind cut* if:

1. α is not empty and $\alpha \neq \mathbb{Q}$,
2. α is an initial segment in the sense that if $q \in \alpha$ and $p < q$, then also $p \in \alpha$,
3. α has no greatest element.

We define $\alpha < \beta$ if α is a proper subset of β. And finally we define

$$\mathbb{R} = \{\alpha \,|\, \alpha \text{ is a cut in } \mathbb{Q}\}.$$

Note that we can identify a rational number q with the cut $\alpha_q = \{q' \in \mathbb{Q} \,|\, q' < q\}$, and so rational numbers are included in $\mathbb{R}$ as the cuts α_q for $q \in \mathbb{Q}$. However, $\mathbb{R}$ contains much more cuts, for instance the set $A = \{q \in \mathbb{Q} \,|\, 0 \leq q, q^2 < 2\} \cup \{q \in \mathbb{Q} \,|\, q < 0\}$ is a cut, and not of the form α_q for some rational number q (because $\sqrt{2}$ is irrational).

Theorem

The following holds of $\langle \mathbb{R}, < \rangle$*:*

1. $<$ *is a linear ordering on* $\mathbb{R}$ *extending (up to isomorphism)* $\mathbb{Q}$*,*
2. $\langle \mathbb{R}, < \rangle$ *is oder-complete (has all the required suprema and infima),*
3. $\mathbb{Q}$ *is dense in* $\mathbb{R}$*.*

It is also the case (but we will not prove it) that any $(X, <)$ which satisfies (1)–(3) is isomorphic to $(\mathbb{R}, <)$. It means that reals are uniquely defined by these properties.

(1) *Exercise.*
(2) This follows because if A is a bounded collection of cuts, then $\bigcup A$ is the supremum of $\alpha \in A$ by the definition of $\bigcup$, and it is easy to check that $\bigcup A$ is also a cut.
(3) If $\alpha < \beta$ and $\alpha \neq \beta$, then there is $q \in \beta \setminus \alpha$, $q \in \mathbb{Q}$, such that $\alpha_q \neq \alpha$ (in fact, there must be infinitely many of these). It follows that α_q satisfies $\alpha < \alpha_q < \beta$.

We now show that $(\mathbb{R}, <)$ which we just constructed works for the motivating example which which we started. Let us first define the notion of continuity.

Definition (ϵ-δ-definition of continuity)

We say that a function $f : \mathbb{R} \to \mathbb{R}$ is *continuous* at r if for every $\epsilon > 0$ there exists $\delta > 0$ such that for all x, if $|x - r| < \delta$, then $|f(x) - f(r)| < \epsilon$.

We say that f is continuous on some set $A \subseteq \mathbb{R}$, $A \subseteq \text{dom}(f)$, if f is continuous on every $r \in A$.
All polynomials, sin, cos, e^x and many other are continuous on their domains (continuity is closed under composition of functions).

Lemma

Suppose f is a continuous function defined on some open interval X which contains the closed interval $[0, 1]$ such that $f(0) < 0$ and $f(1) > 0$. Then there is $x \in (0, 1)$ such that $f(x) = 0$.

Proof.

Set $A = \{y \in [0,1] \,|\, f(y) < 0\}$ and $r = \sup A$ (note that r must be in $[0,1]$ because 1 is an upper bound of A). We claim that $f(r) = 0$. Suppose this is not the case, and either $f(r) > 0$ or $f(r) < 0$. Suppose first $f(r) > 0$. Let $\epsilon > 0$ satisfy $\epsilon < f(r)$ so that $f(r) - \epsilon > 0$. By continuity of f at r, there is $\delta > 0$ such that for all $x \in (r - \delta, r + \delta)$, $f(x) \in (f(r) - \epsilon, f(r) + \epsilon)$, in particular $f(x) > 0$, and hence every such x must be an upper bound of A. It follows that r is not the least upper bound of A, a contradiction. Argue similarly that if $f(r) < 0$, then r cannot be an upper bound of A. In particular $r \in (0,1)$ because $f(1) > 0$ and $f(r) = 0$. □

Loose ends in the previous proof? Not really, but as an excercise, add details to the previous proof and clarify the argument.

Related, and perhaps more elementary, is the notion of a *limit of a sequence of numbers*, which can be also used to construct $\mathbb{R}$.

We say that $(a_n)_{n\in\mathbb{N}}$ is a sequence of rational numbers[1] if there is a function $f : \mathbb{N} \to \mathbb{Q}$ such that $f(n) = a_n$ for each $n \in \mathbb{N}$. We write just (a_n) instead of $(a_n)_{n\in\mathbb{N}}$.

Definition

We say that (a_n) *converges* to a rational number a, and we write this as $\lim_{n\to\infty} a_n = a$, or just $\lim(a_n) = a$, if for any rational number $\epsilon > 0$ there is $n_0 \in \mathbb{N}$ such that for every $n \geq n_0$, $|a_n - a| < \epsilon$.

If (a_n) does not converge, we say that it *diverges*.

Exercise. Show that there are sequence which have no limits in $\mathbb{Q}$. Show that if the limit exists it is unique. Finally show that the

We saw that there are sets of rationals which "should" have a supremum,[2] but their supremum does not exist in $\mathbb{Q}$. Similarly, there are sequences of rationals which "should" have a limit, but they don't have it in $\mathbb{Q}$. Which sequences should have a limit?

Definition

A sequence (a_n) of rational numbers is a *Cauchy*[a] *sequence* if for every $\epsilon > 0$ there exists n_0 such that for every $m, n \geq n_0$ it holds $|a_m - a_n| < \epsilon$.

[a] A French mathematician, 1789-1857.

[2] Precisely the sets which have an upper bound in $\mathbb{Q}$.

Exercise. Show that a convergent sequence is always a Cauchy sequence, and that all Cauchy sequences are bounded (i.e. have an upper bound in $\mathbb{Q}$).
Exercise.* Show that there is a Cauchy sequence of rationals which does not have a limit in $\mathbb{Q}$.

Cantor used Cauchy sequences to define $\mathbb{R}$: First we define that two Cauchy sequences (a_n) are (b_n) are equivalent, $(a_n) \equiv (b_n)$, if $(a_n - b_n)$ has the limit 0. Then we define

$$\mathbb{R} = \{[(a_n)]_{\equiv} \mid (a_n) \text{ is a Cauchy sequence of rationals}\}.$$

This definition also yields a linear order with the properties (1)–(3) mentioned in the Theorem above, and by the note below the theorem, the resulting structure is isomorphic to the one defined by means of Dedekind cuts.

The Cantor's definition of $\mathbb{R}$ immediately gives:

Theorem

A sequence (a_n) of real numbers is Cauchy if and only if it converges.

This is also true for the Dedekind's construction of $\mathbb{R}$ because, as we already mentioned, both constructions yield an isomorphic structure.

Note. More details about these concepts can be found in my lecture notes Introduction to mathematics I, II, or in any good book on mathematical analysis (such as J.K.Truss, Foundation of Mathematical Analysis. Clarendon Press, Oxford. 1997).

Metric spaces

Recall the definition of $f : \mathbb{R} \to \mathbb{R}$ being continuous at a point r:

Definition (ϵ-δ-definition of continuity)

We say that a function $f : \mathbb{R} \to \mathbb{R}$ is *continuous* at r if for every $\epsilon > 0$ there exists $\delta > 0$ such that for all x, if $|x - r| < \delta$, then $|f(x) - f(r)| < \epsilon$.

Suppose we would like to generalize the notion of continuity to other spaces such as $\mathbb{R}^n$, $n \in \mathbb{N}$, or $\mathbb{C}$. First, the notion of the absolute value $|x - r|$ must be formulated more generally.

Definition

We say that (X, d), $X \neq \emptyset$, is a *metric space* if $d : X^2 \to \mathbb{R}^+$ is a function which satisfies for all $x, y, z \in X$:

1. $d(x, y) = 0 \leftrightarrow x = y$,
2. $d(x, y) = d(y, x)$,
3. $d(x, z) \leq d(x, y) + d(y, z)$ (the triangle inequality).

Notice that the absolute value $|x - y|$ on $\mathbb{R}$ is a metric, which makes $(\mathbb{R}, |\cdot|)$ a metric space. Another example is $(\mathbb{R}^n, d)$ where $d(\vec{x}, \vec{y})$ is the distance of two vectors $\vec{x}$ and $\vec{y}$ in $\mathbb{R}^n$.[3]

[3] We will review the definition of a vector space later.

A more general – and hence more useful and applicable – definition of continuity reads as follows:

Definition (ϵ-δ-definition of continuity on metric spaces)

Suppose (X, d) is a metric space. We say that a function $f : X \to X$ is *continuous* at $r \in X$ if for every $\epsilon > 0$ there exists $\delta > 0$ such that for all x, if $d(r, x) < \delta$, then $d(f(r), f(x)) < \epsilon$.

Let us mention that the notion of metric can be used to define the notion of limit on an arbitrary metric space (X, d):

Definition

We say that a sequence (x_n) of points in X *converges* to a point $x \in X$, and we write this as $\lim_{n\to\infty} x_n = x$, or just $\lim(x_n) = x$, if for any real $\epsilon > 0$ there is $n_0 \in \mathbb{N}$ such that for every $n \geq n_0$, $d(x_n, x) < \epsilon$.

The notion of being Cauchy also generalizes:

Definition

A sequence (x_n) of points in X is a Cauchy sequence if for every real $\epsilon > 0$ there exists n_0 such that for every $m, n \geq n_0$ it holds $d(x_m, x_n) < \epsilon$.

We say that a metric space (X, d) is *complete* if every Cauchy sequence converges. We saw above that $(\mathbb{R}, |\cdot|)$ is complete. Also $(\mathbb{R}^n, d)$ are complete for $n > 1$. $(\mathbb{Q}, |\cdot|)$ is not complete.

General metric spaces are used in theoretical physics as generalizations of the Euclidian vector spaces $\mathbb{R}^n$, for instance to model behaviour of particles in quantum mechanics. We will show that a typical metric space used in physics[4] has always size 2^ω (so it has the same size as the real line).

[4] Hilbert spaces, which we will introduce later.

Definition

Let (X, d) be a metric space. We say that X is *separable* if there is a countable set $H \subseteq X$ such that for every $x \in X$ and every $\epsilon > 0$, there is some $h \in H$ with $d(x, h) < \epsilon$. We say that H is *dense* in X.

Separable metric spaces cannot be too large: we will show on the next slide that their size is at most 2^ω.

Theorem

Let (X, d) be a separable metric space, with $H \subseteq X$ countable and dense. Then $|X| \leq 2^{\omega}$.

Proof.

We will define a 1-1 function f from X to ${}^{\omega}H$ (the set of all countable sequences of elements in H); since $|{}^{\omega}H| = 2^{\omega}$, this suffices. For each x, let $f(x)$ be some sequence $\langle h_n^x \mid n < \omega \rangle$ such that for each n, $h_n^x \in H$ and $d(x, h_n^x) < \frac{1}{n}$ (this is possible because H is dense). If $x \neq y$, there is some n such that $d(x, y) > \frac{1}{n}$. It follows that for any $h \in H$, if $d(x, h) < \frac{1}{2}\frac{1}{n} = \frac{1}{2n}$, then $d(y, h) > \frac{1}{2n}$, and so $f(x) \neq f(y)$, because for all $m \geq 2n$, $h_m^x \neq h_m^y$. □

Let us denote by $\bar{B}(x, \epsilon)$ the set $\{y \in X \mid d(x, y) \leq \epsilon\}$. We say that $\bar{B}(x, \epsilon)$ is a closed ball with center x and radius ϵ.

Definition

Let (X, d) be a metric space. We say that $x \in X$ is an *isolated point* if there is some $\epsilon > 0$ such that x is the only element of $\bar{B}(x, \epsilon)$.

We will now state a converse to the previous Theorem: if X is a complete metric space without isolated points, then its size is at least 2^ω. As a corollary, if X is a complete separable metric space without isolated points, then its size is exactly 2^ω.

Theorem

if (X, d) is a complete metric space without isolated points, then its size is at least 2^ω.

Proof.

We will construct a 1-1 function f from ${}^{\omega}2$ into X. We will construct by induction on the length of $s \in {}^{<\omega}2$ a sequence $\langle B_s \,|\, s \in {}^{<\omega}2\rangle$ of closed balls in X. Set $B_\emptyset = X$. Choose $x \neq y$ arbitrarily in X. Let $d(x, y) = \epsilon$. Set $B_{\langle 0\rangle} = \bar{B}(x, 1/3\epsilon)$ and $B_{\langle 1\rangle} = \bar{B}(y, 1/3\epsilon)$. In the next step, pick any two points $x' \neq y'$ in $B_{\langle 0\rangle}$ (this is possible because x is not isolated). Let $d(x', y') = \epsilon'$. Set $B_{\langle 0,0\rangle} = \bar{B}(x', 1/3\epsilon')$ and $B_{\langle 0,1\rangle} = \bar{B}(y', 1/3\epsilon')$, etc. (continued on next slide). □

Proof.

For every $\varphi : \omega \to 2$, let $f(\varphi) = \bigcap\{B_{\varphi|n} \mid n < \omega\}$. By construction the diameters of $B_{\varphi|n}$ converge to 0, and so by completeness there is exactly one $x_\varphi \in X$ in the intersection, i.e. $\bigcap\{B_{\varphi|n} \mid n < \omega\} = \{x_\varphi\}$. If $\varphi \neq \varphi'$, then let n be the least $n < \omega$ with $\varphi(n) \neq \varphi'(n)$. By construction, $B_{\varphi|m} \cap B_{\varphi'|m} = \emptyset$ for every $m \geq n+1$, and so the convergence point cannot be the same for φ and φ', that is $f(\varphi) \neq f(\varphi')$. □

We will see later that a typical Hilbert space is in particular a complete separable metric space without isolated points, so its size is exactly 2^{ω}.

Examples. The real line $\mathbb{R}$ with the metric $d(x, y) = |x - y|$ is a complete separable metric space without isolated points, so has size 2^{ω}. In general the n-dimensional space $\mathbb{R}^n$ is a complete separable metric space without isolated points, and so has size 2^{ω}.

Topological spaces

For $r \in X$ and $0 < \epsilon$, we say that $B(r, \epsilon) = \{x \in X \mid d(r, x) < \epsilon\}$ is *an open ball (centered at r, with diameter ϵ)*.

What is "open" about $B(r, \epsilon)$? It is open in the sense that the "border", i.e. the points $\{x \in X \mid d(r, x) = \epsilon\}$, does not belong to the ball. This leads to a yet more general formulation of continuity which works even for spaces which do not have a (complete) metric.

From metric space to topological space

If (X, d) is a metric space, there is a natural way to define a certain *topology* on X. Topology is a more general notion than metric and it suffices to deal with continuity.

Definition

Let (X, d) be a metric space. A topology derived from d is the collection of all subsets $O \subseteq X$ such that for every $x \in O$ there is some $B(x, \epsilon)$ such that $B(x, \epsilon) \subseteq O$.

The collection of all such O satisfies the axioms of the *topological space*, see the next slide.

Definition

We say that the pair (X, τ) is a *topological space* if $\tau \subseteq \mathcal{P}(X)$ and:

1. $\emptyset$ and X in τ.
2. If O and O' are in τ, then so is $O \cap O'$.
3. If $\{O_j \,|\, j \in J\}$ is a set of elements of τ for some non-empty J, then $\bigcup_{j \in J} O_j$ is in τ.

Elements of τ are called *open sets*.

Example (The (standard) topology on $\mathbb{R}$.)

Suppose τ is the collection of all subsets O of the reals $\mathbb{R}$ such for every $x \in O$, there is some open interval $(x - \epsilon, x + \epsilon) = B(x, \epsilon)$ such that $B(x, \epsilon) \subseteq O$. Then $(\mathbb{R}, \tau)$ is a topological space.

Connecting this example with the definition of continuity, notice that the notion of an open set has the potential to express the ϵ-δ concept without the notion of a distance. Instead of making the values of ϵ (and δ) smaller and smaller, we can take smaller and smaller open sets.[5]

[5] Notice that the exact topology we choose will thus determine which functions are continuous.

Exercise. Typical sets which are not open are: finite sets, countable sets, sets of the form $[x, y]$ or $(x, y]$ for $x, y \in \mathbb{R}$. Are open sets closed under arbitrary intersections? Are they closed under inclusion?

Proof of the example.

(1) Clearly $\emptyset$ and $\mathbb{R}$ are in τ. (2) Suppose X, Y are in τ and $x \in X \cap Y$. Since X is open, there is some open interval I_X containing x with $I_X \subseteq X$, and similarly there is some I_Y containing x with $I_Y \subseteq Y$. It is easy to check that $I_X \cap I_Y$ is an open interval containing x and $I_X \cap I_Y \subseteq X \cap Y$. (3) If $x \in \bigcup_j O_j$, then for some $j \in J$, $x \in O_j$, and if I_j contains x and $I_j \subseteq O_j$, then clearly $I_j \subseteq \bigcup_j O_j$. □

Exercise. If we allowed in the definition of τ only open itervals I of the form (q, q') where $q, q' \in \mathbb{Q}$, we would get the same τ. The collection of such I with rationals endpoints q, q' forms a *countable base* of τ: every elementy $O \in \tau$ is obtained as a union of open itervals with rationals endpoints.

Example (The (standard) topology on $\mathbb{R}^n$.)

Let d be the usual metric on $\mathbb{R}^n$ given by $d((x_1,\dots,x_n),(y_1,\dots,y_n)) = \sqrt{(x_1-y_1)^2+\cdots+(x_n-y_n)^2}$. Let τ is the collection of all subsets O of the reals $\mathbb{R}^n$ such for every $x \in O$, there is an open ball $B(x,\epsilon)$ such that $B(x,\epsilon) \subseteq O$. Then $(\mathbb{R}^n,\tau)$ is a topological space.

Let us finish the discussion of topological concepts by giving the topological definition of continuity:[6]

Definition (Definition of continuity on topological spaces)

Suppose (X, τ) is a topological space. We say that a function $f : X \to X$ is *continuous* at $r \in X$ if for every open set $O_{f(r)}$ containing $f(r)$ there exists an open set O_r containing r such that $f[O_r] \subseteq O_{f(r)}$.

There are examples of non-metrizable topological spaces for example in functional analysis. However, even if a space is metrizable, it is illustrative, and useful in applications, to realize that some concepts such as continuity do not really depend on the notion of distance.

[6] Also the notion of a limit can be generalized in this way.

Metrizability: metric vs. topology

Let us review some important topological properties of metric space.

Definition

A topological space (X, τ) is *metrizable* if there is a metric d on X which generates τ (in the sense that every open set $O \in \tau$ is the union of some open balls $B(x, \epsilon)$).

Which topological spaces are metrizable? And in general, what are the topological properties of metric spaces?

Let (X, τ) be a topological space. If $x \in X$, we say that $O \in \tau$ is an (open) neighbourhood of x if $x \in O$.

Definition

We say that (X, τ) is *first-countable* if every $x \in X$ has a local countable base: i.e. for every x, there exists countably many open neighbourhoods O_i^x, $i < \omega$, of x such that every open neighbourhood of x contains some O_i^x.

Definition

We say that (X, τ) is *second-countable* if the whole X has a countable base: i.e. there exists countably many open sets O_i, $i < \omega$, such that for every $x \in X$ and every open neighbourhood O of x there is some $O_i \subseteq O$ which contains x.

Exercise. Assume X is uncountable and τ is the *discrete topology*, i.e. $\tau = \mathcal{P}(X)$. Then every singleton $\{x\}$ for $x \in X$ is an open set so (X, τ) is first-countable, but not second-countable.

Exercise. Let X be a non-empty set. Define $d : X^2 \to \{0, 1\}$ by setting $d(x, y) = 0$ if $x = y$, and $d(x, y) = 1$, if $x \neq y$. Show that (X, d) is a complete metric space, and infer that there is no upper limit on the size of complete metric spaces (contrast this with the Theorem which shows that a separable metric space has size at most 2^{ω}). Show further that the topology derived from d is the discrete topology.

Exercise. Show that if (X, d) is a metric space, then the derived topology is first-countable. [Hint. The open balls at x with rationals distances form a local basis.]

Theorem

Let (X, d) be a metric space and (X, τ) the topology derived from d. Then

1. *(X, d) is separable iff (X, τ) is second-countable.*
2. *(X, τ) is first-countable.*

As a corollary of (2) we get that if a topological space is metrizable, it must be first-countable.

Let us state as a fact that this for instance implies that the topological product of countably many metrizable places is metrizable, but an uncountable product of non-trivial (having more than 1 element) metrizable places is not-metrizable. For instance $2^\omega, \mathbb{R}^\omega$, or $\mathbb{I}^\omega$ (Hilbert cube) are metrizable, but 2^{ω_1} is not metrizable.

Proof.

(1) Hints. ($\Rightarrow$). Let H be a countable dense set. For every $x \in H$ consider the collection of open balls $B(x, 1/n)$, $0 < n < \omega$. Argue that $\{B(x, 1/n) \,|\, x \in H, 0 < n < \omega\}$ is a countable base of X. ($\Leftarrow$). Let $\{O_i \,|\, i < \omega\}$ be a countable base of X. Let $x_i \in O_i$ be arbitrary. Argue that $H = \{x_i \,|\, i < \omega\}$ is a dense set.

(2) Hints. Argue that for every x, the collection $\{B(x, 1/n) \,|\, 0 < n < \omega\}$ is an local countable base. □

Observe that for every topological space X (not necessarily metrizable) second countable implies separability. For the converse direction, it is essential that (X, d) is a metric space.

Definition

A topological space (X, τ) is *compact* if whenever $\{O_i \mid i \in I\}$ is a collection of open sets such that $\bigcup\{O_i \mid i \in I\} = X$, then there is a finite $J \subseteq I$ such that $\bigcup\{O_i \mid i \in J\} = X$.

We call $\{O_i \mid i \in I\}$ an open cover, and $\{O_i \mid i \in J\}$ its open subcover.

Compactness is an important notion connected to the compactness of propositional logic because of the connection between the compact product space 2^ω and evaluations of propositional atoms.

(Heine–Borel Theorem): $\mathbb{R}$ is not compact, but every closed bounded subset of $\mathbb{R}$ is compact (and every compact subset of $\mathbb{R}$ is of this form).

Compactness of metric spaces implies separability (and hence the existence of a countable base).

Lemma

Every compact metric space (X, d) is separable.

Proof.

For every n, consider the open cover

$$\mathcal{O}_n = \{B(x, 1/n) \mid x \in X\}.$$

By compactness there exist finite subcovers $\mathcal{O}_n^*$ for every n.
(Continues on next slide) □

Proof.

(Continuation of proof) Choose an arbitrary element from every set in $\mathcal{O}_n^*$ for every n. We claim that this countable collection of points is dense. To see this, let O be a non-empty open set. Fix any $x \in O$ and n so that $B(x, 1/n) \subseteq O$. Then for every $m \geq 2n$, $\mathcal{O}_m^*$ must contain some O' such that $O' \subseteq B(x, 1/n) \subseteq O$ because $\mathcal{O}_m^*$ must cover $B(x, 1/n)$, and in particular the center x of the ball. □

Algebra: groups and fields

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 $y = z$.*

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 illustrate the use of subgroups and the related notion of a partition to sketch a proof for 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.

Here is a summary of the key steps of the proof:

- 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*.[7] 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*[8] of the form $H \circ x = \{h \circ x \mid h \in H\}$:

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

[7] There is a natural correspondence between equivalences on G and partitions on G; see lecture notes Introduction to mathematics I.

[8] *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 equivalence 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.

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

A weaker notion than isomorphism is homomorphism:

Definition

Suppose $G = \langle G, +, -, 0\rangle$ and $F = \langle F, \cdot, ^{-1}, 1\rangle$ are two groups. We say they $f : G \to F$ is a *homomorphism* if for all $x, y \in G$:

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

It is easy to check that if $f : G \to F$ is an injective homomorphism, then G is isomorphic to the range of f viewed as a subgroup of F.

Theorem (Cayley)

Every finite[a] *group is isomorphic to a subgroup of a symmetric group.*

[a] It holds for infinite groups as well.

Proof.

(Sketch.) Suppose $G = \langle G, \cdot, ^{-1}, 1\rangle$ is group. We assign to each $g \in G$ a bijection f_g in $\mathrm{Sym}(G)$ as follows: $f_g : G \to G$ which assigns to $x \in G$ the element gx. This function is injective and since G is finite, it is a bijection, and hence a permutation. It is straightforward to check that the function $f : G \to \mathrm{Sym}(G)$, where $f(g) = f_g$ is an injective homomorphism and therefore the range of f is isomorphic to G. □

A *ring* 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

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

and

$$(1+1)(x+y) = (1+1)x + (1+1)y = x+x+y+y, \quad \text{using distributivity from the left.} \tag{2}$$

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.

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*.

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, $\mathrm{rng}(f) = R$. 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.[9]

[9] Up to isomorphism there is exactly one finite field of the given size (this is false for groups and rings).

Example 2.: Fields $\mathbb{Q}, \mathbb{R}, \mathbb{C}$. 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). Moreover, $\mathbb{Q}$ 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. Moreover, 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 $\mathbb{C}$.

Example 3. 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,[10] but some concepts cannot be developed completely (for instance differentiation can only be applied partially, with all but one coordinate being fixed).

Example 4. A combination of a group with a field is a *vector space*, which we will discuss in the next section.

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

Vector spaces

Recall we wish to introduce the notion of the Hilbert space. For this we need to introduce *vector spaces*, generalizations of the Euclidian spaces $\mathbb{R}^n$.

As the motivation, recall that elements of $\mathbb{R}^n$, n-tuples of real numbers $(x_1, \dots, x_n)$, can be "scaled" up and down by real numbers "acting on them": for instance $(1, 2)$ can be scaled up by factor of 2 by setting $2(1, 2) = (2, 4)$.

This is a rather special case because the *scalars*[11] are again real numbers; in general this does not have to be the case. Only the algebraic properties of scalars are important: they must form a *field*.

[11] The word derives from Latin "scala" = "ladder". However, the connection to "scaling" is also suggestive.

Definition

Let $V = (V, +, -, 0)$ be an abelian group and $F = (F, +, \cdot, 0_F, 1_F)$ a field.[a] We denote elements of V by symbols $x, y, \dots$ and elements of F by $\alpha, \beta, \dots$. V is a vector space over the field F, denoted by (V, F), if the following axioms hold:[b]

1. $\alpha(\beta x) = (\alpha\beta)x$.
2. $1_F x = x$.
3. $\alpha(x + y) = \alpha x + \alpha y$.
4. $(\alpha + \beta)x = \alpha x + \beta x$.

[a] The operation $+$ in V is typically different from $+$ in F, but we denote them by the same symbol because there is no danger of confusion.

[b] Elements of V are called "vectors". If $\alpha \in F$ and $x \in V$, you should think of αx as the vector in V which is the result of "α acting on x". This is no multiplication because α and x come from different structures.

Example

$\mathbb{R}^n$ is a vector space over the field $\mathbb{R}$ if we define the abelian group structure on $\mathbb{R}^n$ "coordinate-wise" by setting

- $(x_1, \dots, x_n) + (y_1, \dots, y_n) = (x_1 + y_1, \dots, x_n + y_n)$,
- $-(x_1, \dots, x_n) = (-x_1, \dots, -x_n)$ *and*
- $0 = (0, \dots, 0)$.

Acting of $\mathbb{R}$ on $\mathbb{R}^n$ is defined also "coordinate-wise" (using α to range over real numbers):

- $\alpha(x_1, \dots, x_n) = (\alpha x_1, \dots, \alpha x_n)$.

Check that $(\mathbb{R}^n, \mathbb{R})$ is a vector space.

The distributivity axioms and the axiom $1_F x = x$ allows one to derive many other other useful properties, such as:

- $0_F x = 0$. Proof:
  $x = 1_F x = (0_F + 1_F)x = 0_F x + 1_F x = 0_F x + x$, and by adding $-x$ to both sides, this gives $0 = 0_F x$.
- $(-1_F)x = -x$. Proof. It suffices to show $(-1_F)x + x = 0$. This is equal to $(-1_F)x + 1_F x = (-1_F + 1_F)x = 0_F x = 0$.
- $(-\alpha)x = -(\alpha x) = \alpha(-x)$. Proof.
  $(-\alpha)x = (-1_F\alpha)x = -1_F(\alpha x) = -(\alpha x)$. And also
  $(-\alpha)x = (\alpha(-1_F))x = \alpha(-1_F x) = \alpha(-x)$.

Every vector space (V, F) has a *basis* which in a precise sense generates the whole space V. We need the notion of independence of vectors to define basis:

Definition

We say that distinct non-zero vectors $x_1, \dots, x_n$, $1 < n < \omega$, in V are *linearly independent* if whenever $\alpha_1 x_1 + \cdots + \alpha_n x_n = 0$, then for every $i \in \{1, \dots, n\}$, $\alpha_i = 0$.

If $x_1, \dots, x_n$ are not linearly independent, then at least on α_i is not equal to 0. Assume wlog we have $\alpha_1 \neq 0$; then $x_1 = (-\frac{\alpha_2}{\alpha_1})x_2 + \cdots + (-\frac{\alpha_n}{\alpha_1})x_n$; we say that x_1 is a linear combination of vectors $x_2, \dots, x_n$.

Definition

We say that $X \subseteq F$ is an *independent set* if for every $x_1, \dots, x_n$ in X, $x_1, \dots, x_n$ are linearly independent.

Equivalently, no non-zero vector in X is a linear combination of some finitely many vectors in X.

Definition

We say that $B \subseteq V$ is a *basis* of V over F if it is a maximal independent set in V, i.e. if C properly extends B,then C is no longer independent. We say that V over F has *dimension* κ (finite or infinite number) if there is a basis of size κ.

Example: In $\mathbb{R}^3$, any set of three vectors (x, y, z) of the form $x = (r, 0, 0), y = (0, s, 0), z = (0, 0, t)$ for $r, s, t \neq 0$ is a basis of $\mathbb{R}^3$. It follows that $\mathbb{R}^3$ has dimension 3.

We will not prove all results regarding bases, only that they exist – provided the Axiom of Choice (AC) holds.

Theorem

Suppose (V, F) is a vector space. Then the following hold:

- *If B is a basis of V, then every vector in V is a linear combination of some vectors in B.*
- *If there is a basis, then all bases have the same size (so the notion of dimension is well defined).*
- *(AC) Every vector space has a basis.*

Let us give some more complicated examples of vector spaces:

1. $\langle \mathbb{R}, +, -, 0\rangle$ as a vector space over $\mathbb{Q}$.
2. $\langle \mathbb{C}, +, -, 0\rangle$ as a vector space over $\mathbb{R}$ (and also over $\mathbb{Q}$).
3. Suppose $\mathbb{Q}(p(x))$ is the least field which extends $\mathbb{Q}$ and has all roots for the irreducible polynome $p(x)$ (with rational coefficients).[12] Then $\langle \mathbb{Q}(p(x)), +, -, 0\rangle$ is a vector space over $\mathbb{Q}$.

These the dimensions: (1) 2^ω, (2) 2 (over $\mathbb{R}$), 2^ω (over $\mathbb{Q}$), and (3) the (finite) degree of the polynome $p(x)$.
Let us note that a basis of $\mathbb{R}$ over $\mathbb{Q}$ is called *Hamel basis* and it may not exist without AC.

[12] $\mathbb{Q}(p(x))$ is called the *splitting field of* $p(x)$ *over* $\mathbb{Q}$. Note that $\mathbb{R}(x^2+1) = \mathbb{C}$.

What is missing to use these spaces in the analysis in physics, in particular in quantum mechanics? In short; the notion of an **angle**. In $\mathbb{R}^2$ and $\mathbb{R}^3$ it is natural to say that two vectors have a certain angle θ. Can this be defined abstractly?

Yes, it can, by means of the so called *inner product* of two vectors.[13] The inner product can be used to define a metric on the space.

Thus we get to the following definition, which we state a bit vaguely for the lack of time:

Definition

A vector space over $\mathbb{R}$ or $\mathbb{C}$ is called a **Hilbert space** if it has an inner product whose associated metric is Cauchy complete.

[13] The *scalar product* (also called the *dot product*) in $\mathbb{R}^2$ and $\mathbb{R}^3$ is an example of an inner product.

In the next section “Mathematical analysis”, we will return back to the simple setting of $\mathbb{R}$. However, bear in mind that the concepts of differentiation and integration can be to a large part developed in the more general setting of completely metrizable spaces such as the Hilbert space.

Mathematical analysis

Motivation. Let $f : \mathbb{R} \to \mathbb{R}$ be a continuous function. We would like to say how fast f grows at some x in its domain. We can call it the *rate of change of f* at x. We would like to define this rate of change globally in the sense that we would like to have a function $f' : \mathbb{R} \to \mathbb{R}$ such that

$$\text{the rate of change of } f \text{ at } x \text{ is } f'(x).$$

As we will see, this cannot be done for all continuous function, but it can be done for a large set of functions.

Motivation (continued). With f' being defined, we can compute points x where f does not go up or down, in other words it achieves its *local extreme*. If f has its local extreme at point x, it can mean that the point x is the optimal point for an application modelled by means of f.

Some examples. $f(x) = x^2$ has its extreme at 0. $\cos x$ has its extremes at points $k\pi$ for $k \in \mathbb{Z}$. $f(x) = 2x$ has no local extremes.

Motivation. A little reflection shows that for $f(x) = ax$, the rate of change is constantly a, i.e. $f'(x) = a$ for all x. Similarly, if $f(x) = a$, then the rate of change is constantly 0, i.e. $f'(x) = 0$ for all x. It is immediately obvious what the rate of change is for more complicated functions such as $f(x) = x^2$, or $f(x) = \sin x$. We will discuss this in a moment.

Connection with e. Consider the following question: Is there a function $f : \mathbb{R} \to \mathbb{R}$ such that:

1. $f(0) = 1$,
2. $f'(x) = f(x)$ for all x?

The value of $f(x)$ would thus be equal to its rate of change.

As we will see there is exactly one such function, and it is the function e^x. This function (being unique) can actually be used to *define* the number e.

The number e**.** We will define e in a standard way and then connect its definition with differentiation.

Definition

The *Euler number,* e is defined as the limit of the sequence

$$\sum_{n=0}^{\infty} \frac{1}{n!}.$$

Recall that for every $n \in \mathbb{N}$, $n! = 1 \cdot 2 \cdot n$ if $n \geq 1$, and $0! = 1$.

Lemma

The definition of e is correct, i.e. the sequence of partial sums of $(\frac{1}{n!})_n$ *is bounded, and therefore the sequence converges because* $\mathbb{R}$ *is closed under suprema of bounded subsets.*

Proof.

Clearly, the following holds for each n, $1 + 1 + \frac{1}{2} + \frac{1}{2 \cdot 3} + \cdots \frac{1}{2 \cdot 3 \cdots n} < 1 + 1 + \frac{1}{2} + \frac{1}{2^2} + \cdots + \frac{1}{2^{n-1}}$. The sum of geometrical sequence $(\frac{1}{2^n})_n$ on the right can be computed easily (it is equal to 2), and so $1 + \sum_{n=0} \frac{1}{2^n}$ is equal to 3. It follows that the limit e lies strictly between 2 and 3. □

We now show that e is irrational.[14] In order to show the irrationality of e, we first state without a proof an inequality which shows that the partial sums $s_n = \sum_{i=0}^{n} \frac{1}{i!}$ converge very fast to the limit value e.

Fact

It holds that

$$0 < e - s_n < \frac{1}{n!n}, \text{ for each } n. \tag{3}$$

Thus for instance s_{10} approximates e with error less than 10^{-7}.

[14] By a harder proof, one can also show that e is transcendental.

Theorem

e is irrational.

Proof.

Assume for contradiction that e is rational. Then $e = \frac{p}{q}$, where p, q are natural numbers > 0. By the previous Fact, we have

$$(*) \;\; 0 < q!(e - s_q) < \frac{1}{q}.$$

By our assumption, $q!e$ is a natural number. Since

$$q!s_q = q!\Big(1 + 1 + \frac{1}{2!} + \cdots + \frac{1}{q!}\Big) = q! + q! + \frac{q!}{2} + \cdots + \frac{q!}{q!}$$

is also a natural number, we see that $q!(e - s_q) = q!e - q!s_q$ is also a natural number > 0 (by $(*)$).

Since $q \geq 1$, $(*)$ implies that there exists a natural number strictly between 0 and 1, and this is a contradiction. □

Remark. The convergence of the progression $\sum_{n=0}^{\infty} \frac{1}{n!}$ was known before Euler (1707–1783), but Euler proved many new theorems concerning e, most notably the following so called Euler's identity:

$$e^{i\pi} + 1 = 0,$$

featuring the five important constants in mathematics: $e, i, \pi, 0, 1$, using exactly once the operation of multiplication and addition. Also note that the equation shows that the exponentiation of a transcendental number e with a complex exponent with a transcendental component π can equal an integer: $e^{i\pi} = -1$.

Differentiation. Let us first define the notion of a limit of a function.

Definition

Let $f : \mathbb{R} \to \mathbb{R}$ be a function. We write

$$\lim_{x \to p} f(x) = q$$

to denote the fact that f converges at p to q as x tends to p, more precisely: $\lim_{x \to p} f(x) = q$ if and only if for every $\epsilon > 0$ there is some $\delta > 0$ such that for every x such that

$$0 < |x - p| < \delta$$

it holds that

$$|f(x) - q| < \epsilon.$$

Definition

Let f be defined on some interval $[a, b]$. For each $x \in [a, b]$ form the quotient:

$$\phi(t) = \frac{f(t) - f(x)}{t - x}, \text{ for } a < t < b, t \neq x$$

and define

$$f'(x) = \lim_{t \to x} \phi(t),$$

provided that such a limit exits. We thus associate with each f another function f' defined at every x where the limit $\lim_{t \to x} \phi(x)$ exists. The domain $\mathrm{dom}(f')$ is thus a subset of $[a, b]$ and we call f' *the derivative* of f. If $x \in \mathrm{dom}(f')$ we say that f is *differentiable* at the point x.

Before we discuss the properties of differentiation, note that unlike the definition of continuity – which refers just to the *additive* structure of $\mathbb{R}$, or the space X –, differentiation uses also the *multiplicative* structure of $\mathbb{R}$: we need to be able to consider the division x/y for $y \neq 0$.

Thus the differentiation for a space X requires that X is a *field* – an important algebraic notion which has the operations $+$ and $\cdot$. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are examples fields (but $\mathbb{Q}$ is not complete, so it is not suitable for differentiation). There are many spaces X with just the additive structure $+$, but there are far fewer spaces X which have multiplication as well.

We will discuss this distinction later on.

Some context: Bolzano-Weierstrass and Heine-Borel theorems: We have defined differentiation in the previous lecture. Let us now discuss historical development which concerns both the notion of completeness of $\mathbb{R}$ and the notions of differentiation and integration (which we will define later on formally). This will put these notions into a larger picture.

According to Newton (1671), his motivations for the development of differential and integration calculus were the following:

1. If v is a constant speed, then $s = vt$ calculates the distance over time t. Suppose v is not constant, but instead is given by some function $v(x)$. How do we compute the distance s over a time t?
2. If we now distance s and time t, we can calculate the *average* speed v as $\frac{s}{t}$. Suppose s is given by a function $s(x)$: can we compute the speed v at any given moment?

Let us briefly comment both points. First note that by a "function" is meant a description of a motion which by definition was supposed to be "smooth". The definition of "continuity" is supposed to formalize this notion. However, as we will see, while *continuous* works for the first point, it does not entirely work for the second point.

Regarding (1) – this is the motivation for *integration* (the main operation behind it is multiplication). We will see that every continuous function on a closed interval $[a, b]$ is Riemann integrable.
Regarding (2) – this is the motivation for *differentiation* (the main operation behind it is division). We mentioned already that not every continuous function is differentiable. We can say that from this aspect, the correct formalization of being "smooth" is differentiable and not just continuous.

Notice that division is the inverse of multiplication. Incredibly, this algebraic property carries over to the analytical concept: the *Fundamental theorem of analysis* (properly developed by Newton and Leibniz) says that the derivative is the inverse of the integration (the exact version of the theorem will be stated below).

Now we prove two theorems: Bolzano-Weierstrass theorem which illustrates how the notion of continuity of $\mathbb{R}$ appeared in practice, and Heine-Borel theorem which provides a topological information for closed intervals and implies that every continuous function on $[a, b]$ is Riemann-integrable.[15]

[15] The more straightforward way to define integration; compare to Lebesgue integration developed later on.

Theorem (Bolzano-Weierstrass)

Every countable set $S \subseteq [a, b]$ *has a limit point, i.e. there is some* $x \in [a, b]$ *such that for every* $\epsilon > 0$*, there is some point in* $S \setminus \{x\}$ *which lies in the interval* $(x - \epsilon, x + \epsilon)$*.*

Proof.

Assume for simplicity of notation that $a = 0, b = 1$. Define a sequence of closed intervals I_n, $n \in \mathbb{N}$, such that $I_0 = [a, b]$, I_1 is either $[0, 1/2]$ or $[1/2, 1]$, depending on in which half there are infinitely many elements of S. Define I_2 to be the half of I_1 which contains infinitely many points in S from the points contained in I_1, etc. We would like to argue that $\bigcap_n I_n$ is non-empty, in fact it is equal to some singleton $\{x\}$. If this is the case, then it is easy to see that x is the limit. However, how do we know that $\bigcap_n I_n$ is not empty? This requires that $\mathbb{R}$ is complete, as we will se in the next lemma. □

Historical note: Balzano (1817) attempted to prove the theorem, but lacking the definition of $\mathbb{R}$, he could not prove the following lemma. Weierstrass (1874) provided the proof, after the properties of $\mathbb{R}$ were developed.

Lemma

A nested sequence of closed intervals contains exactly one point in common.

Proof.

Let $[a_n, b_n]$ be the sequence of nested intervals: for every n, $[a_{n+1}, b_{n+1}]$ is included in $[a_n, b_n]$ and the distance $|a_n - b_n|$ decreases to 0 (i.e. for every $\epsilon > 0$, there is some n such that $|a_n - b_n| < \epsilon$). Let us denote $A = \{a_n \,|\, n \in \mathbb{N}\}$ and $B = \{b_n \,|\, n \in \mathbb{N}\}$ and let $a = \sup A$ and $b = \inf B$. It is easy to check that $a = b$ is the unique point contained in all the intervals. □

Let (X, τ) be a topological space. We say that $W = \{O_i \,|\, i \in I\}$ is an *open cover* of X if $\bigcup\{O_i \,|\, i \in I\} = X$ and each O_i is open. $\{O_j \,|\, j \in J\}, J \subseteq I$, is a *finite subcover of W* if $\bigcup\{O_j \,|\, j \in J\} = X$ and J is finite.

Definition

We say that a topological space (X, τ) is *compact* if every open cover of X has a finite subcover.

If a space is compact, then in some situations, an argument related to an infinite set can be proved by considering only its finite approximations.

$\mathbb{R}$ is not compact, but every closed interval $[a, b]$ is compact, which the Heine-Borel theorem. We will formulate it for the interval $[0, 1]$ for simplicity.

Theorem (Heine (1872) - Borel (1895))

Suppose $W = \{O_i \mid i \in I\}$ *are open sets in* $\mathbb{R}$ *such that their union covers* $[0,1]$. *Then there is a finite* $J \subseteq I$ *such that the union* $\bigcup\{O_i \mid i \in J\}$ *covers* $[0,1]$.

Proof.

Suppose for contradiction that there is some open cover W which does not have a finite subcover. Define a sequence of closed nested intervals I_n whose length converges to 0 such that for all n, I_n cannot be covered by finitely many open sets from W. Let x be the unique point in all of the I_n's. Since W is an open cover, there exists some O_i from the cover such that $x \in O_i$. By openness of O_i there is some $\epsilon > 0$ such that $(x - \epsilon, x + \epsilon) \subseteq O_i$. Since the lengths of the I_n's converge to 0, there is some n such that for all $m \geq n$, $I_m \subseteq (x - \epsilon, x + \epsilon) \subseteq O_i$. But this is a contradiction since we assumed that no I_m can be covered by finitely many sets from W (but $O_i \in W$ covers them). □

We will not prove how to calculate differentiation of the common functions, but state it as a fact:

- $c' = 0$, where c is a constant,
- $(x^{\alpha})' = \alpha x^{\alpha-1}$, where $\alpha \in \mathbb{R}$ if $x > 0$, or $x \in \mathbb{R}$ if $\alpha \in \mathbb{N}$,
- $(e^x)' = e^x$,
- $(a^x)' = a^x \text{ln} a$, for $x \in \mathbb{R}, a > 0, a \neq 1$,
- $(\text{ln}|x|)' = \frac{1}{x}$, for $x \in \mathbb{R} \setminus \{0\}$,
- $\text{log}_a|x| = \frac{1}{x \text{ln} a}$, for $x \in \mathbb{R} \setminus \{0\}, a > 0, a \neq 1$
- $(\text{sin} x)' = \text{cos} x$,
- $(\text{cos} x)' = -\text{sin} x$,
- $(\text{tan} x)' = \frac{1}{\text{cos}^2 x}$, for $x \neq \frac{\pi}{2} + \pi k, k \in \mathbb{Z}$,
- $(\text{cot} x)' = \frac{1}{\text{sin}^2 x}$, for $x \neq \pi k, k \in \mathbb{Z}$.

The method of proof is to first showing how to find the differentiation of $f+g$, fg, etc. and of $f \circ g$, provided we know how to compute f' and g'. For instance (with some obvious assumptions satisfied) $(fg)'(x) = f'(x)g(x) + f(x)g'(x)$ and if $h(t) = g(f(t))$ for $t \in [a,b]$, then $h'(x) = g'(f(x))f'(x)$ for $x \in [a,b]$. Proofs of these results can be found in any introductory book to analysis.

Recalling the two motivating questions of Newton, we know turn to the problem of *integration*.

We sketch the proof that differentiation and integration are in some sense dual notions (Fundamental theorem of calculus).

Theorem (The fundamental theorem of calculus)

Let f be Riemann-integrable on $[a, b]$ and assume that F is a differentiable function on $[a, b]$ and $F' = f$, then

$$\int_a^b f dx = F(b) - F(a).$$

We will not prove the theorem (any standard textbook contains it if you are interested). We will just define the notion of Riemann integral.

Two easy examples in Newton's motivation:

- Suppose $f(x) = 2$ for all $x \in [a, b]$. Then with the usual argument the area under the curve is $2(b - a)$. In the integral language, $F = 2x$ because $(2x)' = 2$. It follows that $\int_a^b f dx = 2b - 2a = 2(b - a)$.

- Suppose $f(x) = 2x$ for all $x \in [a, b]$ (i.e. velocity increases linearly with coefficient 2). Then the area under the curve is given by the formula for the area of a triangle. Suppose for simplicity $a = 0$, then the area is $\frac{1}{2}b(2b) = b^2$. If $a \neq 0$, then we need to add the area of the rectangle with sides $2a$ and $b - a$, and we have the area $2a(b - a) + \frac{1}{2}(b - a)2(b - a) = 2ab - 2a^2 + b^2 - 2ab + a^2 = b^2 - a^2$.

  In the integral language the computation is straightforward: $F = x^2$ because $(x^2)' = 2x$. It follows $\int_a^b f dx = b^2 - a^2$.

Let us now define the Riemann integral:

Definition

Let $[a, b]$ be an interval. A set $P = \{x_0, \dots, x_n\}$ is called a *partition* of $[a, b]$, if it holds that $a = x_0 < x_1 \cdots < x_n = b$. If P is a partition, we set $\Delta x_i = x_i - x_{i-1}$.

Definition

Let f be bounded on $[a, b]$, i.e. there are m, M such that $m \leq f(x) \leq M$ for all $x \in [a, b]$. Set $M_i = \sup\{f(x) \,|\, x_{i-1} \leq x \leq x_i\}$, and $m_i = \inf\{f(x) \,|\, x_{i-1} \leq x \leq x_i\}$.

$$U(P, f) = \sum_{i=1}^{n} M_i \Delta x_i, \text{ and } L(P, f) = \sum_{i=1}^{n} m_i \Delta x_i.$$

And finally:

$$\int_a^{*b} f dx = \inf\{U(P, f) \,|\, P \text{ partition}\},$$

$$\int_{*a}^{b} f dx = \sup\{L(P, f) \,|\, P \text{ partition}\}.$$

Definition

We say that f is *Riemann-integrable*, or shortly R-integrable, if the upper and lower integrals coincide:

$$\int_a^{*b} f dx = \int_{*a}^b f dx,$$

and we write the common value as

$$\int_a^b f dx.$$