The curious world of constructive mathematics

Ingo Blechschmidt

Abstract. Constructive mathematics is a flavor of mathematics in which we use the axiom of choice and the technique of proof by contradiction only in certain special cases. The square root of two is constructively still irrational, but there might be vector spaces without a basis.

As a result, proofs are more informative (for instance regarding bounds), finer distinctions can be made (for instance between positive existence and mere impossibility of non-existence) and results apply more generally: Every constructive result also has a geometric interpretation, where it applies to continuous families, and an algorithmic interpretation, yielding computational witnesses such as procedures for computing the objects whose existence has been shown.

Relinquishing the axiom of choice and the principle of excluded middle also allows us to explore axioms and notions which are incompatible with these classical laws, such as mathematical settings in which all functions are continuous or in which the intuitive idea of a "generic ring" can be put on a firm basis.

Contents

LECTURE I

A first glimpse of constructive mathematics

This lecture provides a first glimpse of constructive mathematics with a focus on applications of constructive mathematics and on providing intuition for quickly discerning which techniques and results hold constructively.

This account is an update and translation of [13, Section 1] and references include [6, 7, 4, 46, 24, 44, 57] or more specifically [45, 41] for constructive algebra and [10] for constructive analysis.

Proposition I.1. *There are irrational numbers x and y such that x^y is rational.*

First proof. The number $\sqrt{2}^{\sqrt{2}}$ is rational or irrational. In the first case, set $x := \sqrt{2}$, $y := \sqrt{2}$. In the second case, set $x := \sqrt{2}^{\sqrt{2}}$, $y := \sqrt{2}$. □

Second proof. Set $x := \sqrt{2}$ and $y := \log_{\sqrt{2}} 3$. Then $x^y = 3$ is rational. The verification that y is irrational is even easier than that of $\sqrt{2}$.[1] □

The first proof is *unconstructive*: It does not actually give us an example for a pair (x, y) as desired. In contrast, the second proof is constructive – the existential claim is verified by an explicit construction of a suitable example.

Of the many axioms and inference rules of classical logic, exactly one is responsible for enabling unconstructive arguments, namely the *principle of excluded middle*:

$$\varphi \vee \neg\varphi.$$

The first proof above used this principle in its very first step. In constructive mathematics, we abstain from this principle; we build constructive mathematics on *intuitionistic logic*, which contains neither this principle nor the (equivalent) *principle of double negation elimination* stating $\neg\neg\varphi \Rightarrow \varphi$, and insofar as we layer a set theory on top of our logical foundation, we abstain from the axiom of choice (which in presence of other common set-theoretical axioms implies the principle of excluded middle, see Exercise I.8) and from Zorn's lemma. As a consequence, we cannot generally reason by contradiction in constructive mathematics, and to demonstrate the existence of an object it is not enough that its nonexistence would entail a contradiction.

Importantly, in constructive mathematicics we do *not* claim that the principle of excluded middle is false. Indeed, intuitionistic logic is downwardly compatible with classical logic (every intuitionistic proof is a fortiori also a classical proof), and some special instances of the principle of excluded middle and with it some special instances of proof by contradiction are intuitionistically verifiable (an example is given in Proposition I.10). Instead, in constructive mathematics we merely do not use the principle of excluded middle.

Also, deducing from a statement of the form "$\exists x \in X.\ \varphi(x)$" that there actually is an element $x \in X$ such that $\varphi(x)$, and then using this particular element in the rest of an

[1] Let $y = a/b$ with $a, b \in \mathbb{Z}$ and $b \neq 0$. Since $y > 0$, we may assume $a, b \in \mathbb{N}$. Then $3 = (\sqrt{2})^{a/b}$, hence $3^{2b} = 2^a$. This is in contradiction to the uniqueness of the prime factor decomposition, since the factor 3 occurs on the left but not on the right.

argument, is intuitionistically a valid logical inference, just as it is in classical logic. The axiom of choice is unrelated to this kind of proof step, even though they are sometimes mistaken.

1. Proof by contradiction vs. proof of a negation

A rumor about constructive mathematics states that constructively, the term "contradiction" would be generally forbidden. This rumor is false. In fact, we need to distinguish between two distinct figures of proof which are often conflated in classical informal mathematics:

1. "Assume $\neg\varphi$. Then . . ., a contradiction. Hence $\neg\varphi$ was false and thus φ holds."
2. "Assume ψ. Then . . ., a contradiction. Hence $\neg\psi$."

Arguments of the first form are proper proofs by contradiction and hence not generally accepted in constructive mathematics. What they establish is only $\neg(\neg\varphi)$, the impossibility of $\neg\varphi$; constructively, this is weaker than a positive affirmation of φ. Though there are situations in which $\neg\neg\varphi$ implies φ, generally it does not and hence intuitionistically arguments of the first form fail to estabilish φ.

In contrast, arguments of the second kind are fine from an intuitionistic point of view: They do not constitute proper proofs by contradiction, but instead are proofs of negated statements. That such proofs are valid follows directly from the definition of negation as a certain implication (which, incidentally, texts on classical logic often also adopt):

$$\neg\psi :\equiv (\psi \Rightarrow \bot),$$

where "$\bot$", pronounced "bottom", is *absurdity*, a canonical false statement. (Informally, absurdity is also written as "$\lightning$" or "$1 = 0$".) Hence, to establish $\neg\psi$, we may give a proof of $\bot$ under the assumption ψ, just as we may give a proof of β under the assumption α if we want to prove $\alpha \Rightarrow \beta$.

The two proofs below of the following fact from number theory demonstrate the difference:

Proposition I.2. *The number $\sqrt{2}$ is not rational.*

Proof (only valid classically). Assume that the claim is false, that is, that the number $\sqrt{2}$ is *not not* rational. Then $\sqrt{2}$ is rational. Hence there are integers a and b with $\sqrt{2} = a/b$. Thus $2b^2 = a^2$. This identity contradicts the uniqueness of the prime factor decomposition, since the factor 2 occurs an odd number of times on the left but an even number of times on the right. □

Proof (also valid intuitionistically). Assume that the number $\sqrt{2}$ is rational. Then there are integers a and b, . . ., a contradiction. [The requisite theorem on the uniqueness of the prime factor decomposition admits an intuitionistic proof.] □

Constructively stronger than the statement that $\sqrt{2}$ is merely *not rational* is the statement that for every rational number x the distance $|\sqrt{2} - x|$ is positive. This stronger claim admits an intuitionistic proof as well (Exercise I.4).

2. Constructive meaning of mathematical statements

By our training in classical mathematics, abstaining from the principle of excluded middle can feel peculiar, perhaps even outrageous: Isn't it obvious that every mathematical statement is true or false?

This sense of bewilderment is resolved by observing that *even though constructive mathematicians use the same logical symbols, they have a slightly different meaning in mind.* When a constructive mathematician argues for some statement φ, they mean that they have an *explicit witness* for φ. This shift in meaning from the classical interpretation is elaborated by the *Brouwer–Heyting–Kolmogorov interpretation* sketched below. It is

	classical logic	intuitionistic logic
statement φ	The statement φ holds.	We have a witness for φ.
$\bot$	A contradiction holds.	We have a witness for a contradiction.
$\varphi \wedge \psi$	φ and ψ hold.	We have a witness for φ and for ψ.
$\varphi \vee \psi$	φ or ψ hold.	We have a witness for φ or for ψ.
$\varphi \Rightarrow \psi$	If φ holds, then so does ψ.	We can (uniformly) construct witnesses for ψ from witnesses for φ.
$\neg\varphi$	φ does not hold.	There is no witness for φ.
$\forall x : X.\ \varphi(x)$	For all $x : X$ it holds that $\varphi(x)$.	We can (uniformly) construct, for all $x : X$, witnesses for $\varphi(x)$.
$\exists x : X.\ \varphi(x)$	There is at least one $x : X$ such that $\varphi(x)$ holds.	We have a $x : X$ together with a witness for $\varphi(x)$.

TABLE 1. Informal recursive definition of the notion of witnesses.

informal and philosophical in nature and not without issues [2, 18, 23], but still a useful guide to the constructive meaning of mathematical statements.

2.1. The Brouwer–Heyting–Kolmogorov interpretation. The notion of witnesses is compositional in nature and starts out with the notion of witnesses for *atomic statements*, those not built from substatements using the logical connectives $\wedge, \vee, \Rightarrow$ or the quantifiers $\forall, \exists$. For instance, in formal number theory, the atomic statements are of the form "$s = t$", where s and t are terms for natural numbers; statements of this form are so simple that we can check them directly so that witnesses don't need to supply particular additional information. We hence decree that true atomic statements have trivial witnesses and that false atomic statements have no witnesses at all.

Table 1 explains how compound statements should be witnessed. For instance, a witness of a statement of the form

$$\forall n : \mathbb{N}.\ \big(\varphi(n) \Rightarrow \psi(n)\big)$$

is a rule explaining how, for every natural number $n : \mathbb{N}$, witnesses for $\varphi(n)$ give rise to witnesses for $\psi(n)$.

Example I.3. According to the Brouwer–Heyting–Kolmogorov interpretation, the principle of excluded middle states that we can construct, for every φ, either a witness for φ or a witness for $\neg\varphi$. This claim is obviously false.

Example I.4. The BHK interpretation of a doubly negated statement $\neg\neg\varphi$ is that there is no witness for $\neg\varphi$. This state of affairs does not entail that we actually have a witness for φ; in a sense, the statement φ is only "potentially true".

Example I.5. Assuming that we cannot find our apartment key, but know that it has to be somewhere (because we used it last night to unlock the door), constructively we can only defend the doubly negated statement

$$\neg\neg(\exists x.\ \text{the key is at position } x).$$

Example I.6. We are running errands and are remembering that we need to fetch certain ingredients. Unfortunately we don't recall any of them right now. Then we can constructively defend the statement that the set of ingredients to fetch is not empty, not however the stronger statement that this set is inhabited.

Example I.7 ([50, 48])**.** A video surfaced depicting Kate Moss taking drugs, more precisely either drugs of some type A or drugs of some type B. However from the video it wasn't

clear which type of drug it actually was. Hence there was no evidence for either type of consumption; Kate Moss wasn't prosecuted.

Remark I.8. The reference of an unspecified "we" in table 1 renders our account of the BHK interpretation not only informal, but is also somewhat misleading. As in classical mathematics, judgments of intuitionistic logic do not actually depend on you, me or other mathematicians. It's perfectly possible that statements which haven't yet been constructively verified admit (as yet unknown) witnesses. More details can be found in [37, pp. 42] and in [2, 18, 23]. The Brouwer–Heyting–Kolmogorov interpretation is made more formal and precise by *realizability theory* [9, 49].

2.2. The computability interpretation. A second interpretation of mathematical statements suited for constructive mathematics is given by the following motto: In a certain sense, *we accept a mathematical statement in constructive mathematics if and only if there is a computer program witnessing it in finite time.* For instance, that the statement

$$\forall n : \mathbb{N}.\ \exists p : \mathbb{N}.\ p \geq n \wedge p \text{ is prime}$$

is valid in constructive mathematics corresponds to the fact that there is a computer program which reads a number n as input and then, after some computation, produces a prime number $p \geq n$ as output (together with a witness that p is in fact greater or equal than n and that p is prime).

For the motto to be correct, the notion of "witnessed by a computer program" has to be interpreted in sufficiently generous manner, not least because uncountable and uncomputable structures have their place in constructive mathematics just as in classical mathematics. A more formal rendition is provided by the celebrated *Curry–Howard correspondence* and *propositions as (some) types*.

Remark I.9. Constructive mathematics is emphatically not the same as computable mathematics; in particular, there are statements which do admit a witness by a computer program but which are rejected in (most schools of) constructive mathematics (see Exercise I.6). The apparent tension with the motto presented above is resolved in its more formal treatment. In any case, the two subjects are closely related and their connection provides useful intuition.

2.3. The geometric interpretation. A third interpretation of mathematical statements suited for constructive mathematics, and of a substantially different kind than the BHK and the computability interpretation, is provided by geometry. In a certain sense, *we accept a mathematical statement in constructive mathematics if and only if it holds locally in continuous families*.

For instance, while it is a fact of classical mathematics that every complex number has a square root, a fundamental observation in complex analysis is that such roots cannot be picked in a locally continuous manner. Hence the standard formulation of the fundamental theorem of algebra fails in constructive mathematics.[2] This example will be discussed in more detail in Section **??**.

The geometric interpretation not only gives transparent explanations to the logical subtleties of constructive mathematics, but is in a more precise form also the workhorse of many modern applications of constructive mathematics to mathematics in general. We

[2]More precisely, the fundamental theorem of algebra fails for the complex numbers built from pairs of Dedekind reals. Constructively, the reals built using Dedekind cuts are not the same as the reals built using Cauchy sequences; in fact, the latter are a subset of the former and serve a different purpose. Such a bifurcation of classically equivalent notions is typical of constructive mathematics. The fundamental theorem of algebra is correct for the flavor of complex numbers built from Cauchy reals [52], and also for the algebraic numbers [45, Section VII.4] [XXX insert better references] and for complex polynomials (of either flavor) which are separable. Furthermore, the fundamental theorem of algebra holds in an approximate sense and in a multiset sense [51], and the standard version only requires mild choice principles [17].

will hence dedicate ample of space to the geometric interpretation by devoting Lecture III to it, and will discuss some of its more advanced applications in Lecture IV.

3. Finer distinctions supported by constructive mathematics

By relinquishing the blanket principle of excluded middle, constructive mathematics allows us to make finer distinctions – distinctions which are hidden in classical mathematics, but carry algorithmic and geometric significance. We have already seen one instance of this increased expressiveness in Example I.5: In classical mathematics, we are trained to cancel double negations as soon as they arise, but constructively there is a substantial difference between actually having a mathematical object and merely knowing that its nonexistence is impossible.

3.1. Decidability of equality. A further examples pertains to the basic notion of equality. In classical mathematics, any given elements a, b of a set X are either equal or not – trivially so, by the principle of excluded middle. Constructively, the situation is more nuanced.

Firstly, in a positive direction, we do have the following result.

Proposition I.10. *For every pair of natural numbers a and b, either $a = b$ or $a \neq b$.*

Proof (constructive). We spell out only the case $b = 0$, that is, we only spell out a proof that every natural number a is either zero or not. To this end, we do a induction on a.

The base step $a = 0$ is trivial, since if $a = 0$ then also $a = 0 \vee a \neq 0$ (we can always weaken statements by adding additional disjuncts).

In the inductive step $a \to a + 1$, we have $a + 1 \neq 0$ by one of the basic axioms of arithmetic (for a complete list, see Exercise II.2) and hence in particular $a+1 = 0 \vee a+1 \neq 0$ by weakening. (This proof is one of the rare instances of a correct induction proof where the inductive step does not refer to the induction hypothesis.) □

As from any constructive proof, a computer program witnessing the asserted fact can be extracted. It will (roughly) have type $\mathsf{Nat} \times \mathsf{Nat} \to \mathsf{Bool}$, computing true or false depending on whether its two inputs agree or are distinct. Because the presented proof proceeded by induction, the resulting program will proceed by recursion.

Sets like the set of natural numbers for which equality is decidable have a special name in constructive mathematics, hinting at a connection with topology:

Definition I.11. A set X is *discrete* if and only if for every elements $a, b \in X$, either $a = b$ or $a \neq b$.

In classical mathematics, all sets are discrete. Constructively, discreteness is a nontrivial property, and although $\mathbb{N}$ is discrete and with it also $\mathbb{Z}$ and $\mathbb{Q}$, there are many important sets which constructively cannot be shown to be discrete:

Proposition I.12. *Already in the case $X = \{\star\}$ it holds that if the powerset $P(X)$ is discrete, then the principle of excluded middle holds.*

Proof. Let φ be a statement and consider the element $K_\varphi := \{x \in X \mid \varphi\} \in P(X)$. If $K_\varphi = X$, then φ; and if $K_\varphi \neq X$, then $\neg\varphi$. □

Proposition I.13. *If the set of (any of the usual flavors of the) reals is discrete, then the principle of omniscience holds (XXX this has not been introduced).*

The failure of the discreteness of the set of real numbers can be explained in computational terms as follows. In computable mathematics, a real numbers is represented by a program computing better and better rational approximations. Given two such programs, we can simulate or execute them to obtain approximations to a desired precision, hoping to distinguish the two represented real numbers. However, in case that the two numbers actually agree, in finite time we will never verify this fact: Computably, we cannot rule

out the possibility that a difference between the two numbers will only be detected in the as yet unexplored range of rational approximations.[3]

Lest an impression that only topologically simple domains can be shown to be discrete in constructive mathematics emerges, here is a more sophisticated example of a discrete set.

Proposition I.14. *The set $\overline{\mathbb{Q}}$ of algebraic numbers is discrete.*

Proof. See [45, Section XXX]. □

3.2. Minima of sets of natural numbers. As an approximate rule of thumb, in the author's personal experience, every result of classical mathematics which has received constructive scrutiny turned out to either

(a) be manifestly and unsurprisingly unconstructive, or
(b) admit a constructive reformulation.

Of course, the jury is still out on the many results not yet studied from a constructive point of view.

The results "every vector space has a basis" and "there exist nonmeasurable subsets of the reals" are of the first kind. Such results often provide great abstract insight to the mathematical landscape – it is comforting to know that there cannot be vector spaces so bizarre that they don't have a basis or that the notion of measurable subsets is not trivial. On the other hand, such results also tend to not influence concrete situations too much: How could an infinite basis for which there is no hope that we ever learn any actual description of inform our computations? (Better uncover topological structure and look for a Schauder basis!)

Indeed, there are even metatheorems, reported on in Lecture II, to the effect that in sufficiently concrete and logically simple situations, the axiom of choice and the principle of excluded middle do not allow to prove results which couldn't be proven without them. And as further evidence, there is Friedman's *grand conjecture* [**XXX**] – informal but not yet challenged – that every result published in the Annals by a mathematician not self-identifying as a set theorist or logician can be (reformulated to be) provable even in EFA, a foundational system much weaker than ZFC, ZF or even Peano arithmetic.

An example of a result of type (b) uses the basic observation that every inhabited set of natural numbers contains a minimal element. This result is not available in constructive mathematics as stated, but there are two constructive substitutes.

Definition I.15. A set X is *inhabited* if and only if there exists an element of X.

Constructively, the condition that a set X is inhabited is stronger than X merely not being empty. The latter is equivalent to the statement that it is *not not* the case that X is inhabited.

Proposition I.16. *If every inhabited set of natural numbers contains a minimal element, then the principle of excluded middle holds.*

To salvage the classical result, we can strengthen its assumption or weaken its conclusion.

Definition I.17. A subset $U \subseteq X$ is *detachable* if and only if for every element $x \in X$, either $x \in U$ or $x \notin U$.

[3]This argument can be formalized using Turing machines and realizability theory; see [11, Section 4.2.1] for a review. The analysis dramatically changes (see [11, Section 4.2.2]) if we instead refer to the infinite-time Turing machines of Hamkins and Lewis [32] which can carry out an infinite amount of computation before halting. A philosophically intriguing (and, by necessity, informal) account referring to machines in the real world as opposed to idealized Turing machines has been put forward by Andrej Bauer [8].

For instance, the subset of $\mathbb{N}$ consisting of the prime numbers is detachable, while the subset of those numbers n such that the n-th Turing machine terminates cannot constructively be shown to be detachable.[4]

Proposition I.18. (a) *Every detachable inhabited subset of* $\mathbb{N}$ *contains a minimum.*
(b) *Every inhabited subst of* $\mathbb{N}$ *does* not not *contain a minimum.*

4. Exercises

Exercise I.1 (Constructive status of classical tautologies)**.** Which of the following classical tautologies can reasonably be expected to admit constructive proofs?

(a) $\neg(\alpha \vee \beta) \implies \neg\alpha \wedge \neg\beta$
(b) $\neg(\alpha \wedge \beta) \implies \neg\alpha \vee \neg\beta$
(c) $(\alpha \Rightarrow \beta) \implies (\neg\alpha \vee \beta)$
(d) $(\alpha \vee \beta) \wedge \neg\alpha \implies \beta$
(e) $\forall M : P(X).\ (\exists x : X.\ x \in M) \vee M = \emptyset$ (already interesting for $X = \{\star\}$)
(f) $\forall n : \mathbb{N}.\ (n = 0 \vee n \neq 0)$
(g) $\forall x : \mathbb{R}.\ (x = 0 \vee x \neq 0)$
(h) $\forall x : \mathbb{R}.\ (\neg(\exists y : \mathbb{R}.\ xy = 1) \Rightarrow x = 0)$
(i) $\forall z : \overline{\mathbb{Q}}.\ (z = 0 \vee z \neq 0)$
(j) $\forall f : \mathbb{N} \to \{0,1\}.\ (\neg\neg\exists n : \mathbb{N}.\ f(n) = 0) \Rightarrow (\exists n : \mathbb{N}.\ f(n) = 0)$ (Markov's principle)
(k) $\forall f : \mathbb{N} \to \{0,1\}.\ \exists n : \mathbb{N}.\ (f(n) = 1 \Rightarrow (\forall m : \mathbb{N}.\ f(m) = 1))$ (Drinker's paradox)
(l) $\forall f : \mathbb{N} \to \{0,1\}.\ (\exists n : \mathbb{N}.\ f(n) = 0) \vee (\forall n : \mathbb{N}.\ f(n) = 1)$
(m) $\forall f : \mathbb{N}_\infty \to \{0,1\}.\ (\exists n : \mathbb{N}_\infty.\ f(n) = 0) \vee (\forall n : \mathbb{N}_\infty.\ f(n) = 1)$
Remark. The set $\mathbb{N}_\infty$ is the *one-point compactification* of $\mathbb{N}$. A sensible definition of it in constructive mathematics is as the set of decreasing binary sequences $(x_0, x_1, x_2, \ldots)$. The naturals embed into $\mathbb{N}_\infty$ by mapping n to the sequence $1^n 0^\omega = (1, \ldots, 1, 0, \ldots, 0)$, and an element not in the image of this embedding is $\infty := 1^\omega = (1, 1, \ldots)$. Assuming the principle of excluded middle (or already weaker principles), every element of $\mathbb{N}_\infty$ is of one of these two forms. Martín Escardó has worked extensively on unexpected instances of the principle of omniscience for searchable sets like $\mathbb{N}_\infty$ [26, 28, 27].

Exercise I.2 (Basics on negation)**.** Recalling that negation is defined as implying absurdity, $\neg\varphi :\equiv (\varphi \Rightarrow \bot)$, verify intuitionistically without recourse to truth tables:

(a) $\varphi \Rightarrow \neg\neg\varphi$
(b) $\neg\neg\neg\varphi \Leftrightarrow \neg\varphi$
(c) $\neg\neg(\varphi \vee \neg\varphi)$
(d) $\neg\neg(\alpha \wedge \beta) \Leftrightarrow (\neg\neg\alpha \wedge \neg\neg\beta)$
(e) $\neg(\alpha \vee \beta) \iff (\neg\alpha \wedge \neg\beta)$
(f) $(\neg\neg\alpha \wedge (\alpha \Rightarrow \neg\neg\beta)) \implies \neg\neg\beta$
(g) $(\forall\psi.\ (\psi \vee \neg\psi)) \iff (\forall\psi.\ ((\neg\neg\psi) \Rightarrow \psi))$
Hint. Don't try to verify that double negation elimination for a specific statement ψ implies the principle of excluded middle for that same statement ψ – this cannot be shown. There are subtleties regarding the quantification over ψ (this is not expressible in pure first-order logic), however the exercise is still instructive if we gloss over this issue.

Exercise I.3 (An epistemic riddle on transcendental numbers)**.** Verify, using a proof by contradiction, that at least one of the numbers $e + \pi$ and $e - \pi$ is transcendental; and that at least one of the numbers $e + \pi$ and $e \cdot \pi$ is transcendental.
Note. At time of writing, for none of these numbers a (constructive or classical) proof of their transcendence is known.

Exercise I.4 (A stronger form of the irrationality of $\sqrt{2}$)**.** Mine the proof of Proposition I.2 to give an intuitionistic proof that for every rational number x, the distance $|\sqrt{2} - x|$ is positive.
Note. Strictly speaking, this exercise presupposes familiarity with an intuitionistic account of the basics of undergraduate real analysis. Without it, one cannot really be expected to precisely think about these matters. One such account (though assuming the axiom of dependent choice) is [10]. However, this exercise is insightful even when carried out slightly informally. Keep in mind that, to show that a real number is positive, constructively it is not enough to merely verify that it cannot be zero or negative. A safe way to verify that a real number a is positive is to exhibit a rational number b such that $a \geq b > 0$.

[4] A computable witness to detachability of this subset would be a *halting oracle*, but a basic fact of computability theory is that there no such oracles.

Exercise I.5 (Brouwerian counterexamples)**.** Show that each of the following statements implies the principle of excluded middle, hence is not available in constructive mathematics.

(a) Every ideal of $\mathbb{Z}$ is finitely generated.
Hint. Use that finitely generated ideals of $\mathbb{Z}$ are principal ideals and consider the ideal $\mathfrak{a} := \{x \in \mathbb{Z} \mid x = 0 \vee \varphi\}$.
Remark. The failure of every ideal of $\mathbb{Z}$ to be finitely generated should not be misconstrued to exclaim that in constructive mathematics, there suddenly would be ideals of $\mathbb{Z}$ of infinite rank. The failure is simply because, given an abstract ideal, we cannot pinpoint a finite system of generators.

(b) Over every field, the polynomial $X^2 + 1$ is either reducible or irreducible.
Hint. Consider the field $K := \{z \in \mathbb{Q}(i) \mid z \in \mathbb{Q} \vee \varphi\}$.

(c) Subsets of Kuratowski-finite sets are Kuratowski-finite.
Note. A set X is *Kuratowski-finite* if and only if, for some number $n \in \mathbb{N}$, there is a surjective map $[n] \to X$, where $[n] = \{0, 1, \ldots, n-1\}$. More briefly, a set X is Kuratowski-finite iff its elements can be enumerated: $X = \{x_1, \ldots, x_n\}$.

(d) Every subset of the (Cauchy or Dedekind) reals which is inhabited and bounded from above has a supremum.
Note. A *supremum* of a set M of reals is a number s such that $M \leq s$ (that is $x \leq s$ for all $x \in M$) and such that for every number s' with $M \leq s'$, $s \leq s'$. In constructive mathematics, we can make finer distinctions between the classically equivalent constructions of the real numbers: The reals constructed using Cauchy sequences inject into the reals constructed using Dedekind cuts which in turn inject into the MacNeille reals, and each serve a different purpose. The Cauchy and Dedekind reals cannot constructively be shown to be complete in the sense of this exercise, while the MacNeille reals can. Conversely, the rationals can be shown to be dense in the first two kinds of reals but not in the MacNeille reals [36, Section D4.7].

Show that the following statement implies Markov's principle (from Exercise I.1):

(e) Every real number which is not zero is invertible.

Brouwerian counterexamples abound in constructive mathematics; when developing a constructive account of a theory, they help to clearly demarcate its limits. As such additional Brouwerian counterexamples can be found in most texts on constructive mathematics, such as [45]; a compilation mainly from constructive analysis can be found in [43].

Exercise I.6 (Markov's principle)**.** Markov's principle is the statement that

$$\forall f : \mathbb{N} \to \{0,1\}.\ (\neg\neg\exists n : \mathbb{N}.\ f(n) = 0) \Rightarrow (\exists n : \mathbb{N}.\ f(n) = 0).$$

It is a simple instance of the classical principle of double-negation elimination, but not available in (most schools of) constructive mathematics.

(a) Why does Markov's principle imply that programs which do not run forever actually halt?
(b) Explain why Markov's principle is witnessed by a computer program (even though it does not admit a constructive proof). Which assumption on your metatheory does your argument require?

Exercise I.7 (Minima of sets of natural numbers, part one)**.**
(a) Give a constructive proof of Proposition I.18(b).
(b) What does the computational witness extracted from the proof of Proposition I.18(a) look like? Can you devise a different proof corresponding to a different algorithm?

Exercise I.8 (Diaconescu's theorem)**.** The axiom of choice can be put as: "Every surjective map has a section." (A *section* s to a surjective map f is a map in the other direction such that $f \circ s = \mathrm{id}$.) A theorem of Diaconescu states that the axiom of choice implies the principle of excluded middle. To this end, let φ be a statement and consider the subsets

$$U = \{x \in X \mid (x = 0) \vee \varphi\}$$
$$V = \{x \in X \mid (x = 1) \vee \varphi\}$$

of the discrete set $X := \{0, 1\}$.

(a) Verify that $U = V$ if and only if φ.

(b) Using that $x = y \vee x \neq y$ for all elements $x, y \in X$, show that the existence of a section of the surjective map

$$\begin{array}{ccc} X & \longrightarrow & \{U, V\} \\ 0 & \longmapsto & U \\ 1 & \longmapsto & V \end{array}$$

implies $\varphi \vee \neg\varphi$.

LECTURE II

On the constructive content of classical proofs

Decades of experience in constructive mathematics show: *Most results in classical mathematics, even those whose proof rests on non-constructive principles like the axiom of choice or the principle of excluded middle, have a hidden constructive core.* With a mix of experience, seasoned tools and general metatheorems, this constructive content can be extracted from classical proofs. In this way we obtain constructive reformulations of classical results, especially if they are of a sufficiently concrete nature.

For instance, while the existence of maximal ideals in arbitrary rings is equivalent to the axiom of choice, every first-order consequence of their existence for linear algebra over rings also holds constructively.

This lecture illustrates the latent constructive nature of classical proofs with examples and presents two general metatheorems which elucidate proof mining for constructive content. The author learned this material mostly from diverse texts and slides of Thierry Coquand; the reference [20] is a good start.

Theorem II.1 (Dickson's lemma)**.** *Let $k \in \mathbb{N}$. Let $f : \mathbb{N} \to \mathbb{N}^k$ be an arbitrary map. Then there are indices $i < j$ such that $f(i) \leq f(j)$ (componentwise).*

Proof (classical). The case $k = 0$ is trivial and we omit demonstrations of the cases $k \geq 2$, hence let $k = 1$. In this case, the map f attains some minimal value. Set i to be (one of the) positions where this minimal value is attained. Set $j := i + 1$. Then, trivially, $f(i) \leq f(j)$. □

Theorem II.2. *Let M be a surjective matrix with more rows than columns over a commutative ring A with unit. Then $1 = 0$ in A.*

Proof (classical). Assume not. Then there is a maximal ideal $\mathfrak{m} \subseteq A$. The matrix M remains surjective when considered over the quotient ring $A/\mathfrak{m}$, and by maximality this quotient ring is a field. Hence we have a contradiction to basic linear algebra, namely to the basic fact that matrices over fields are not surjective if they have more rows than columns. □

What is the meaning of these non-effective proofs? Theorem II.1 claims the existence of a finite object with a decidable property (a pair (i, j) such that $f(i) \leq f(j)$), but the given proof employs transfinite methods and gives no indication how we could compute or otherwise find this object. Instead, the classical proof asks us to grasp the infinitude of all values of f and determine their minimum. The issue is even more pronounced with Theorem II.2, since the existence of maximal ideals in nontrivial rings requires the axiom of choice [54, 33, 5, 25, 34]. To add one more conundrum: Assume that we have a classical proof, using the principle of excluded middle and the axiom of choice, that some given Turing machine terminates. Can we then constructively accept that the machine will halt? Do we have an upper bound for the number of computational steps the machine carries out before halting?

Astoundingly, it is almost always the case that from classical proofs useful constructive content can be extracted. In fact, due to general metatheorems, in many cases there are

even explicit mechanical procedures for extracting this hidden content, while other cases require more creativity for determining suitable constructive reformulations. For instance:

(a) *Eliminating the axiom of choice by the L-translation.* Can the axiom of choice ever help in proving arithmetical statements, those first-order statements in which all quantifiers range over the natural numbers? Well, it surely might. But a result of Gödel states that ZFC (Zermelo–Fraenkel set theory with the axiom of choice) is conservative over ZF (ZF set theory without it) for such statements – hence all appeals to this axiom can be mechanically eliminated from a given proof. This is true even if the proof transcends the arithmetical realm and includes statements which are not arithmetical; only the asserted claim is required to be arithmetical. Hence we are free to use the axiom of choice, tranquil in knowing that we could always reformulate our proofs without it.[5]

(b) *Eliminating the principle of excluded middle by the double-negation translation and its variants.* At the price of slightly modifying the asserted claim, the principle of excluded middle can always be mechanically eliminated from a given proof. This elimination procedure is facilitated by the *double-negation translation* reviewed below. In some cases, a refined translation even allows us to preserve the asserted claim exactly; this technique is variously known as *Friedman's trick*, *nontrivial exit continuation* or (the baby version of) *Barr's theorem.* To cite a specific instance of this phenomenon, classical ZF set theory is conservative over its intuitionistic cousin IZF for Π^0_2-statements (statements of the form $\forall \ldots \forall.\ \exists \ldots \exists.\ \%$, where all quantifiers in the final "$\%$" are bounded).

(c) *Embracing generic models.* A useful companion to both of the aforementioned techniques is to switch from referencing all models of a certain kind to referencing only the *generic model*. For instance, Krull's lemma stating that a ring element is already nilpotent if it is contained in all prime ideals requires the Boolean Prime Ideal Theorem, a slightly weaker version of the axiom of choice but still ineffective and unconstructive. However, Krull's lemma is valid in the form that a ring element is nilpotent if it is contained in the *generic prime ideal*. This particular example has received lots of attention (see the references in [16]) and the general technique will be the object of the fourth lecture.

Noticeably missing in this list is any technique for eliminating uses of the *powerset axiom* stating that the collection of all subsets of a given set is again a set. While this axiom is uncontested by ordinary constructive mathematics and doesn't receive nearly as much philosophical attention as the axiom of choice or the principle of excluded middle, it is this axiom which actually and substantially increases logical strength. While ZFC, ZF and IZF are equiconsistent (and in fact verify the same arithmetical Π^0_2-statements), systems without the powerset axiom such as Kripke–Platek set theory (KP) or constructive Zermelo–Fraenkel set theory (CZF) are much weaker. We will not discuss this curious state of affairs and only note that rejecting the powerset axiom can be well-motivated and is the basis of *predicative mathematics*; references include [22, 1].

5. The double-negation embedding of classical into constructive mathematics

The premier difference between constructive and classical mathematics is in the existential quantifier "$\exists$" and disjunction "$\vee$". Constructively, to verify an existential statement, it is

[5] Zermelo–Fraenkel set theory with the axiom of choice is the go-to foundation of mathematics often cited as supporting "almost all" of current mathematics, one important exception being some (definitions and) results in category theory dealing with large structures [55, 29]. A fundamental result due to Gödel is that the axiom of choice "holds in L", the *constructible universe*, even if it might not hold in V, the true universe of all sets. More precisely, if ZFC shows some statement φ, then ZF shows its L-relativized version φ^L, where all quantifiers have been restricted to range over L instead of V. The conservation result follows because the natural numbers "are absolute between V and L" [30, 53].

not enough to verify the impossibility of nonexistence; and to verify a disjunction $\alpha \vee \beta$, it is not enough to verify the impossibility of $\neg\alpha \wedge \neg\beta$.

That is not to say, however, that the more informative versions of "$\exists$" and "$\vee$" of constructive mathematics would be in any senser "better" than their classical counterparts: There are many situations in which the classical semantics is exactly the appropriate one. Should we somehow combine classical and intuitionistic logic to form a joint logic supporting both the informative connectives from intuitionistic logic and the "platonic" connectives from classical mathematics?

Perhaps surprisingly, it turns out that no such combination is necessary, for the classical connectives are already definable in intuitionistic logic:

$$\begin{aligned} \exists^{\mathrm{cl}} x : X.\ \varphi(x) \quad &:\equiv \quad \neg\neg(\exists x : X.\ \varphi(x)) \qquad \text{(this is eqv. to } \neg(\forall x : X.\ \neg\varphi(x))) \\ \alpha \vee^{\mathrm{cl}} \beta \quad &:\equiv \quad \neg\neg(\alpha \vee \beta) \qquad \text{(this is eqv. to } \neg(\neg\alpha \wedge \neg\beta)) \end{aligned}$$

This observation is the starting point of the *double-negation embedding* of classical logic into intuitionistic logic. This embedding translates any statement φ into a related statement $\varphi^{\neg\neg}$, substituting all occurences of "$\exists$" and "$\vee$" by "$\exists^{\mathrm{cl}}$" and "$\vee^{\mathrm{cl}}$" (and prefixing all atomic statements by "$\neg\neg$") as detailed in Table **??**. Crucially, while the principle of excluded middle cannot be verified for "$\vee$", the principle of excluded middle for "$\vee^{\mathrm{cl}}$" is an intuitionistic tautology:

Theorem II.3. *For every statement φ, $\neg\neg(\varphi \vee \neg\varphi)$.*

Proof. By definition of negation, we are to prove

$$\underbrace{\big((\varphi \vee (\varphi \Rightarrow \bot)) \Longrightarrow \bot\big)}_{\equiv:\chi} \Longrightarrow \bot.$$

So assume χ; we are to show $\bot$.

Hypothetically, if φ, then in particular $\varphi \vee (\varphi \Rightarrow \bot)$ and hence, by χ, $\bot$. This argument establishes $\varphi \Rightarrow \bot$.

Thus in particular we have $\varphi \vee (\varphi \Rightarrow \bot)$ and hence, by χ again, $\bot$. □

The fundamental properties of the double-negation translation are summarized by the following theorem.

Theorem II.4. *For every statement φ, …*

(a) *classical logic proves $\varphi \Leftrightarrow \varphi^{\neg\neg}$,*
(b) *intuitionistic logic proves $\neg\neg(\varphi^{\neg\neg}) \Rightarrow \varphi^{\neg\neg}$,*
(c) *(if φ is a geometric formula) intuitionistic logic proves $\varphi^{\neg\neg} \Leftrightarrow \neg\neg\varphi$, and*
(d) *classical logic proves φ from some set Γ of assumptions if and only if intuitionistic logic proves $\varphi^{\neg\neg}$ from the set $\Gamma^{\neg\neg}$ of translated assumptions.*

Proof. Instructive exercise. □

The double-negation embedding is not only conceptually pleasing, establishing that intuitionistic logic can serve as a common home for both classical and constructive mathematics, but also supplies us with a vast source of constructive results.

Example II.5. Classical linear algebra teaches us that every finite system of generators of a vector space over a residue field[6] can be thinned to a generating family in which

[6]Constructively, the notion of a field bifurcates into several nonequivalent notions: A nontrivial commutative ring with unit is a …

(a) a *geometric field* or *discrete field* iff every element is zero or invertible (as in $\mathbb{Q}$ or $\overline{\mathbb{Q}}$),
(b) a *residue field* iff every element which is not invertible is zero (as in the Cauchy or Dedekind reals), and
(c) a *field of fractions* iff every element which is not zero is invertible (as in the localization of the Cauchy or Dedekind reals at the set of non-zeros or in the *generic local ring* described in Lecture IV).

These each have their uses [35, 47].

no vector is redundant, hence to a basis. By slightly massaging the result obtained by the double-negation embedding, we obtain the constructive theorem that every finitely generated vector space over a residue field does *not not* possess a basis.

We will learn in Section **??** that this simple theorem immediately entails (a basic version of) *Grothendieck's generic freeness lemma*, a result in algebraic geometry fundamental to the theory of moduli spaces, if applied after localizing at the "generic prime filter" (this requires passing to a more adapted topos). It is marvelous how large the impact of this simple theorem from undergraduate linear algebra is, if made to apply in arbitrary toposes by the double-negation embedding and then specializing to a particularly well-adapted one.

6. Barr's theorem

Even though Barr's theorem has wide impact, there are definitive situations in which, provably so, no useful constructive content can be extracted. Exercise II.6 gives an example for this situation.

7. Examples from quadratic form theory

8. Exercises

Exercise II.1 (Drinker's paradox)**.** The Drinker's paradox is the tautology

$$\forall f : \mathbb{N} \to \{0,1\}.\ \exists n : \mathbb{N}.\ (f(n) = 1 \Rightarrow (\forall m : \mathbb{N}.\ f(m) = 1))$$

of classical logic. A proof proceeds as follows: By the principle of excluded middle, either there is a number n such that $f(n) = 0$ or not. In the first case, we can take such a number n as the desired n. In the second case, we can take $n := 0$.

(a) Determine the double-negation translation of the Drinker's paradox.
(b) Tell a classical logic fairy tale for Drinker's paradox similar to the story for Dickson's lemma. The protagonist of the story will change their mind regarding the correct value of n; what is their first choice?
(c) Connect the Drinker's paradox to the issue of minima of sets of natural numbers.

Exercise II.2 (Stability of the axioms)**.** Peano arithmetic (PA) is set in the language $(0, S, +, \cdot)$ and has the following axioms (where leading universal quantifiers are supressed for brevity):

(1) $Sx \neq 0$
(2) $Sx = Sy \Rightarrow x = y$
(3) $y = 0 \vee (\exists x.\ y = Sx)$
(4) $x + 0 = x$
(5) $x + Sy = S(x + y)$
(6) $x \cdot 0 = 0$
(7) $x \cdot Sy = (x \cdot y) + x$
(8) $P(0) \wedge (\forall n.\ P(n) \Rightarrow P(Sn)) \Longrightarrow (\forall n.\ P(n))$ (one axiom for each formula $P(n)$)

Heyting arithmetic (HA) has exactly the same axioms, but is based on intuitionistic logic instead of classical logic.

(a) Show that HA proves the double-negation translation of each axiom of PA.
(b) Convince yourself that IZF does not prove the double-negation translation of the axiom of choice. Hence the double-negation translation alone is insufficient to extract constructive content from proofs using the axiom of choice.

Exercise II.3 (Details on the double-negation translation)**.** Complete the verification of the fundamental properties of the double-negation translation stated as Theorem II.4.

Exercise II.4 (Minima of sets of natural numbers, part two)**.** In Proposition I.18(b) we showed that every inhabited set of natural numbers does *not not* contain a minimal element.

(a) Redo Exercise I.7(a) using the motto that in proofs of negated statements, we are allowed to use finitely many instances of the principle of excluded middle.
(b) Explain how Proposition I.18(b) follows from the double-negation embedding applied to the classical fact that every inhabited set of natural numbers directly contains a minimal element.
Hint. It is not enough to just cite the double-negation embedding. The resulting constructive theorem has to be massaged a bit to yield Proposition I.18(b).
(c) Explain in computational terms how your proof of Proposition I.18(b) runs its course.

Exercise II.5 (Grothendieck's generic freeness lemma, part one)**.** XXX

Exercise II.6 (No constructive content)**.** Let $\mathsf{Prf}(p)$ be a formula of arithmetic expressing that p is a correct encoding of a PA-proof of $\bot$. A consequence of Gödel's second incompleteness theorem is that there is no PA-proof of

$$G :\equiv (\forall p.\ \neg \mathsf{Prf}(p)),$$

even though for each number p_0 it is actually the case that (and PA can verify that) p_0 does not constitute a correct encoding of a PA-proof of $\bot$.

(a) Give a PA-proof, using the principle of excluded middle, of the statement

$$\exists q.\ (\mathsf{Prf}(q) \vee G).$$

(b) Show that for no number $q_0 \in \mathbb{N}$, the statement "$\mathsf{Prf}(\underline{q_0}) \vee G$" admits a PA-proof. In this sense no witness can be extracted from the classical proof in (a).

LECTURE III

Toposes and their internal language

Just as the easiest and shortest path between two truths of the real domain often passes through the complex domain, sometimes the easiest and most conceptual path to a result observes that the claim can also be formulated in the internal language of an alternate mathematical universe – an alternate topos – where the proof can be simple, direct and make use of the finer distinctions provided by intuitionistic logic.

As such, toposes are the workhorse of many modern applications of constructive mathematics to mathematics in general. Toposes originated in algebraic geometry, where they have been used as generalized spaces (allowing for a nontrivial category of opens instead of only a partially ordered set of opens), before category theorists observed that there is also a strong logical aspect to toposes: Toposes can be pictured as mathematical universes – universes in which we can do mathematics much in the same way as in the so-called standard topos of sets and maps, the single topos in which most mathematicians spend all their professional life in.

Besides the standard topos, in which mathematics unfolds exactly as known and classical logic reigns, there is a colorful host of alternate toposes – some intimately related and useful to the mathematics of the standard topos, some less so and important to computability theorists and logicians. In most alternate toposes, only intuitionistic logic is sound and it is a plain fact of the matter that the law of excluded middle and the axiom of choice fail.

In the lecture we will focus on precise definitions, examples of toposes, and logical applications to mathematics in general, laying the groundwork for the fourth lecture on generic models and carefully elucidating why it is that most toposes validate only intuitionistic logic. References include [11, 40, 56, 42, 31, 36] (and [14] for applications in algebraic geometry). These themes constitute just a tiny part of topos theory. Exposition on Olivia Caramello's grand topos-theoretic bridge-building program [19], on applications of toposes to the meta-analysis of logic [39] and how topos theory can be used to reconcile seemingly disparate positions in the philosophy of mathematics [38, 21] will take place in more informal settings than the lecture.

Analysis:

✓/✗ Every continuous function $f : [-1, 1] \to \mathbb{R}$ with $f(-1) < 0$ and $f(1) > 0$ has a zero.

✗/✗ Let X be a topological space and let $f : X \times [-1, 1] \to \mathbb{R}$ be a continuous function with $f(\cdot, -1) < 0$ and $f(\cdot, 1) > 0$. Then there is an open covering $X = \bigcup_i U_i$ such that for each index i, there is a continuous zero-picking function $z : U_i \to [-1, 1]$.

Linear algebra:

✓/✗ Every real symmetric matrix has an eigenvector.

✗/✗ Let X be a topological space and let $A : X \to M_n^{\text{sym}}(\mathbb{R})$ be a continuous map to the space of symmetric $(n \times n)$-matrices. Then there is an open covering $X = \bigcup_{i \in I} U_i$ such that or all indices $i \in I$, there is a continuous map $v : U_i \to \mathbb{R}^n$ such that for each $x \in U_i$, the vector $v(x)$ is an eigenvector of $A(x)$.

Commutative algebra:

✓/✓ Let M be a finitely generated projective module over a local ring A. Then M is finite free.

✓/✓ Let M be a finitely generated projective module over an arbitrary commutative ring A. Then there is a partition $1 = f_1 + \cdots + f_n \in A$ of unity such that, for each index i, the localized module $M[f_i^{-1}]$ is finite free over $A[f_i^{-1}]$.

✓/✗ Let M be a finitely generated module over a (residue) field k. Then M is finite free.

✗/✗ Let M be a finitely generated module over an arbitrary commutative ring A. Then there is a partition $1 = f_1 + \cdots + f_n \in A$ of unity such that, for each index i, the localized module $M[f_i^{-1}]$ is finite free over $A[f_i^{-1}]$.

✓/✓ Let M be a finitely generated module over a (residue) field k. Then M is *not not* finite free.

✓/✓ Let M be a finitely generated module over an arbitrary commutative ring A. If $f = 0$ is the only element of A such that $M[f^{-1}]$ is finite free over $A[f^{-1}]$, then $1 = 0$ in A.

✓/✓ If k is a (residue) field, there is no linear surjection $k^n \to k^m$ with $m > n$.

✓/✓ Let A be an arbitrary commutative ring. If there exists a linear surjection $A^n \to A^m$ with $m > n$, then $1 = 0$ in A.

9. Examples

10. Definition

11. The Kripke–Joyal semantics of sheaf toposes

12. Exercises

Exercise III.1 (The sheaf of real functions as a field [12, Exercise 28])**.** Let X be a topological space. Let $\mathcal{C}$ be the sheaf of continuous real-valued functions on X.

(a) Let U be an open of X. Let $f \in \mathcal{C}(U)$. Show that $U \models (\exists g : \mathcal{C}.\ fg =_{\mathcal{C}} 1)$ iff there is a function $g \in \mathcal{C}(U)$ such that $fg = 1$.
(b) Show that $\mathcal{C}$ is a *residue field* in that $X \models \forall f : \mathcal{C}.\ \big(\neg(\exists g : \mathcal{C}.\ fg = 1)\big) \Rightarrow f = 0$.
(c) Give an example of space X such that it is not the case that $\mathcal{C}$ is a field in the stronger sense that $\mathrm{Sh}(X) \models \forall f : \mathcal{C}.\ (\exists g : \mathcal{C}.\ fg = 1) \vee f = 0$.
(d) Let $X = \mathbb{C}$ and let $\mathcal{O}$ be the sheaf of holomorphic functions on X, that is $\mathcal{O}(U) = \{f : U \to \mathbb{C} \mid f \text{ holomorphic}\}$. Show that, in classical mathematics, the sheaf $\mathcal{O}$ is *discrete* in that

$$\mathrm{Sh}(\mathbb{C}) \models \forall f : \mathcal{O}.\ \forall g : \mathcal{O}.\ f = g \vee \neg(f = g).$$

Exercise III.2 (The geometric interpretation of double negation [12, Exercise 26])**.** Let φ be a formula over an open U of a topological space X.

(a) Show that there is a largest open, denoted "$[\![\varphi]\!]$", such that $[\![\varphi]\!] \models \varphi$.
Hint. Consider the union of all opens V such that $V \models \varphi$.
(b) Show that $X \models \neg\neg\varphi$ iff $[\![\varphi]\!]$ is dense.
Note. A subset $W \subseteq X$ is *dense* iff for every open $T \subseteq X$, if $W \cap T = \emptyset$ then $T = \emptyset$.
(c) Give a condition on the topological space X such that the principle of excluded middle (or equivalently the principle of double negation elimination) is valid in $\mathrm{Sh}(X)$.

Exercise III.3 (The fundamental properties of the sheaf semantics)**.** Complete the proof of Proposition **??**, so verify monotonicity and locality of the sheaf semantics.

Exercise III.4 (Unique local existence is global existence [12, Exercise 27])**.** Let F be a sheaf on a topological space X. Let φ be a formula over X. Assume that $\mathrm{Sh}(X) \models \exists! s : F.\ \varphi(s)$, that is

$$\mathrm{Sh}(X) \models \exists s : F.\ \varphi(s) \quad \text{and} \quad \mathrm{Sh}(X) \models \forall s : F.\ \forall t : F.\ (\varphi(s) \wedge \varphi(t) \Rightarrow s = t).$$

Show that for any open $U \subseteq X$, there is a unique section $s \in F(U)$ such that $U \models \varphi(s)$.
Note. If you do not know the general definition of a sheaf, then consider only the specific sheaf $\mathcal{C}$ of continuous real-valued functions.

LECTURE IV

Generic models and their applications

Commutative algebra progressed when the intuitive but informal notion of "the generic element of a given field k" was reified in the form of the specific element X of the polyomial ring $k[X]$. The caveat is, of course, that the expanded ring $k[X]$ is no longer a field.

A similar story unfolds one level up. *Topos theory provides us with "the generic ring", the ring we are implicitly picturing when someone utters the phrase "Let R be a ring".* The generic ring has exactly those properties (of the large class of "geometric implications") which all rings have. To have the generic ring in our ontology, we need to broaden our notion of existence—the generic ring is not a ring in the usual sense of the word, but a ring object in an enlarged topos, and still close enough to the familiar rings in that all constructive theorems about rings apply to it.

Bizarrely, the generic ring has the property (not formalizable as a geometric implication) that it is even a field. Hence, if we are to prove a geometric implication for all rings, we can just as well assume the field property.

The lecture introduces the notion of topos-theoretic generic models in general, focussing on the generic ring, the generic prime ideal and concrete applications.

The convergence radius of the Taylor series expansion of $1/(1-x)$ around the origin, that is the geometric series $1 + x + x^2 + \cdots$, is 1. That the convergence radius isn't larger doesn't come too surprising in view of the fact that the function $1/(1-x)$ has a non-removable discontinuity at $x = 1$. But why is also the convergence radius of the expansion of $1/(1+x^2)$,

$$1/(1+x^2) = 1 - x^2 + x^4 - x^6 + \cdots,$$

just 1? The function $1/(1+x^2)$ is perfectly well-defined at ± 1, infinitely derivable on all of $\mathbb{R}$, neatly decaying for $x \to \pm\infty$ and doesn't have any singularities.

A rewarding explanation of this phenomenon is nowadays relayed in any course on complex analysis: The function $1/(1+x^2)$ does have a singularity at distance 1 from the origin, namely at $\pm i$ in the complex plane, and the disk of convergence is and can only be so big that it just touches the nearest singularity.

This episode is one example of many how the "imaginary unit"—once an elusive *mathematical phantom*—affects the story of the real numbers even though it itself is not one of them. Like many mathematical phantoms before it, the imaginary unit obtruded its effects so convincingly that eventually we embraced it and broadened our notion of existence [58].

Toposes allow us to bring further entities into being, entities which do not exist in the standard topos but which nevertheless affect the story of the standard topos. We will focus on:

(a) The *generic ring* – which cryptically is also a field
(b) The *generic prime filter* of a given ring A – which XXX
(c) The *generic surjection* $\mathbb{N} \to X$ – which exists also when X is uncountable

The complex numbers can be compiled down to pairs of real numbers and hence exhibit already in their very construction an intimate connection with the real numbers; in a similar vein, these topos-theoretic generic models can be compiled away in that proofs employing them can be unrolled, in a mechanical fashion even, so as to not mention them.

13. Ring-theoretic prelude: the method of indeterminates

The Cayley–Hamilton theorem of linear algebra states that every square matrix over every commutative ring is a root of its characteristic polynomial. Among its many proofs, the following one is particularly interesting from a logical point of view: It is enough to verify the claim for the *ring-theoretic generic* $(n \times n)$*-matrix* $(A_{ij})_{ij}$ over the polynomial ring $\mathbb{Z}[A_{ij} \mid i, j \in \{1, \ldots, n\}]$, since this matrix can specialize to every specific matrix over every commutative ring and this kind of specialization preserves the n^2 polynomial identities expressing that the matrix is a root of its characteristic polynomial. Now to check this special case, it suffices to verify it for every choice of complex numbers $a_{ij} \in \mathbb{C}$ in place of the formal indeterminates A_{ij}. For complex matrices, the claim follows from the observation that the claim is immediate for the diagonalizable complex matrices and that these are dense in the space of all complex matrices.

This approach is known as the *method of indeterminates* and is amenable to many situations. For instance, there is the *ring-theoretic generic* n*-th root* (over $\mathbb{Z}[X]/(X^n - 1)$), the *ring-theoretic generic nilpotent element of index* $\leq n$ (over $\mathbb{Z}[X]/(X^n)$), the *ring-theoretic generic power series* (over $\mathbb{Z}[A_0, A_1, \ldots]$), and many others. The central features of the method of indeterminates are:

(1) We extend a certain base ring, often $\mathbb{Z}$, to a larger ring R_0 containing the *generic instance* of the problem at hand.
(2) For every specific instance in every ring R, there is a unique homomorphism $R_0 \to R$ mapping the generic instance to that one.
(3) Since homomorphisms of rings preserve polynomial identities, every polynomial identity (and in fact even every property which can be expressed as a geometric formula in the language of rings) satisfied by the generic instance passes down to every specific instance. In fact, the generic instance satisfies exactly those polynomial identities which are provable from the ring axioms.
(4) Crucially, the generic instance is applicable to special techniques (for instance involving complex numbers) and has special properties which themselves do not pass down to every specific instance, but which are useful in establishing those that do.

The generic models facilitated by topos theory generalize the ring-theoretic generic elements. The latter are restricted to those kinds of elements which can be described by polynomial identities (such as $X^n - 1$ for n-th roots). For example, there is no ring-theoretic generic non-nilpotent element or ring-theoretic generic regular element (a ring element $x \in A$ is *regular* if and only if for all $y \in A$, $xy = 0$ implies $y = 0$). The topos-theoretic generic models, in contrast, support arbitrary geometric implications as defining properties, and are not restricted to mere elements (or finite or infinite lists of elements): For instance, as elucidated in the next sections, there is the topos-theoretic *generic ring* or the topos-theoretic *generic prime filter* of any given ring.

Briefly, for every geometric theory $\mathbb{T}$ (set of geometric implications as axioms) over any signature, there exists a topos-theoretic generic model of $\mathbb{T}$. The analogy with the generic elements of ring theory is as follows:

(1) We extend the base universe, often the standard topos Set, to a larger topos $\mathrm{Set}[\mathbb{T}]$ containing the *generic model* $U_{\mathbb{T}}$ of $\mathbb{T}$.

(2) For every specific $\mathbb{T}$-model M in any topos $\mathcal{E}$, there is a unique map $\mathrm{Set}[\mathbb{T}] \to \mathcal{E}$ mapping $U_{\mathbb{T}}$ to M.[7]
(3) Since such maps preserve geometric implications, every property which can be expressed as a geometric implication passes from $U_{\mathbb{T}}$ to every specific model. In fact, the generic model satisfies exactly those geometric implications which are provable from the axioms of $\mathbb{T}$.
(4) Crucially, the generic model is applicable to special techniques and has special properties which themselves do not pass down to every specific model, but which are useful in establishing those that do.

14. A fantastical ring

[7]To be more precise, the category of maps $\mathrm{Hom}(\mathrm{Set}[\mathbb{T}], \mathcal{E})$ is equivalent to the category of $\mathbb{T}$-models in $\mathcal{E}$, naturally in $\mathcal{E}$. By "map", we mean what is called the "inverse image part of geometric morphisms" in topos theory.

15. The generic prime filter

A commutative ring A is often studied by its *stalks* $A_{\mathfrak{p}}$ at prime filters $\mathfrak{p} \subseteq A$, those subsets of A which validate the conditions on the right:

$$\begin{aligned} \top &\implies 0 \in \mathfrak{p} & 0 \in \mathfrak{p} &\implies \bot \\ x \in \mathfrak{p} \wedge y \in \mathfrak{p} &\implies x + y \in \mathfrak{p} & x + y \in \mathfrak{p} &\implies x \in \mathfrak{p} \vee y \in \mathfrak{p} \\ 1 \in \mathfrak{p} &\implies \bot & \top &\implies 1 \in \mathfrak{p} \\ x \in \mathfrak{p} \vee y \in \mathfrak{p} &\iff xy \in \mathfrak{p} & xy \in \mathfrak{p} &\iff x \in \mathfrak{p} \wedge y \in \mathfrak{p} \end{aligned}$$

The stalk $A_{\mathfrak{p}}$ is then the localization $A[\mathfrak{p}^{-1}]$, that is the ring of formal fractions x/s with $x \in A$ and $s \in \mathfrak{p}$, where $x/s = y/t$ iff there exists an element $u \in \mathfrak{p}$ such that $utx = usy$. The set $\mathfrak{p}$ is multiplicatively closed (and saturated) by the last two conditions.[8] Similarly, an A-module M is often studied by its stalks $M_{\mathfrak{p}} = M[\mathfrak{p}^{-1}]$.

Stalks are interesting because they allow us to zoom in on "local" situations—they tend to be simpler than the original ring or module, while still being intimately connected to the originals. For instance:

(a) The stalks $A_{\mathfrak{p}}$ are always *local rings*, rings such that a finite sum is invertible only if one of its summands also is. (This amounts to $1 \neq 0$ and that whenever $x + y$ is invertible, x is invertible or y is invertible; see Exercise IV.3.)
(b) Classically, if A is reduced, the stalks $A_{\mathfrak{p}}$ at *maximal* prime filters (equivalently minimal prime ideals) are even fields.
(c) Classically, an A-module M is flat if and only if all of its stalks $M_{\mathfrak{p}}$ are.

16. Explicit construction

[8] Textbooks on classical commutative algebra usually use *prime ideals* instead of *prime filters*, those subsets which validate the dual conditions on the left. In classical commutative algebra, we can freely pass between these two notions by taking complements, as the complement of a prime ideal is a prime filter and conversely. Constructivly, prime filters are more useful, and even classically they are slightly more convenient to work with.

17. Exercises

Exercise IV.1 (Verifying polynomial identities)**.**

Exercise IV.2 (Limitations of ring-theoretic generics)**.** Show that each of the following hypothetical ring-theoretic generics do not exist:

(a) the generic nilpotent element (of arbitrary index)
(b) the generic regular element
(c) the generic prime element

That is, show that there is no ring R_0 containing an element x_0 of the desired kind such that for every such element x of every ring R, there is a unique homomorphism $R_0 \to R$ mapping x_0 to x.

Exercise IV.3 (Local rings)**.** (a) Using the definition of local ring given on page 30, verify that every geometric field in the sense of Footnote 6 is a local ring; that the (Cauchy or Dedekind) reals form a local ring; that for each prime number p the subring of $\mathbb{Q}$ consisting of those fractions whose denominator is not divisible by p is a local ring; and that $\mathbb{Z}$ and $\mathbb{Q}[X]$ are not local rings.
Note. If $a < b$ are real numbers, then for every real number x, $x > a$ or $x < b$.

(b) Show that the stalk $A_{\mathfrak{p}}$ of a commutative ring A at a prime filter $\mathfrak{p}$ is a local ring. What goes wrong in case that $\mathfrak{p}$ is instead a prime ideal and one considers the localization $A[(A \setminus \mathfrak{p})^{-1}]$?

(c) Verify in classical mathematics that a ring is local if and only if it has exactly one maximal ideal.
Hint. Use that, in classical mathematics, every nonunit is contained in some maximal ideal.

Exercise IV.4 (Abstract existence of bounds from the method of indeterminates)**.** (a) Using Krull's lemma in its unconstructive form, verify for every commutative ring A that if a polynomial $f \in A[X]$ is nilpotent in $A[X]$, all its coefficients are nilpotent in A.

(b) Let $f \in A[X]$ be a polynomial of degree d such that $f^n = 0$. By the proof in (a), there exists a number m such that the m-th power of each of the coefficients of f vanishes. However, it is conceivable that m depends not only on d and n, but also on the ring A and the specific values of the coefficients. Explain how the method of indeterminates reviewed in Section 13 can be used to establish that there exists some bound on m depending only on d and n.

Exercise IV.5 (Anonymously Noetherian rings)**.** A commutative ring A is *anonymously Noetherian* iff for every ideal $\mathfrak{a} \subseteq A$ it is *not not* the case that $\mathfrak{a}$ is finitely generated.

(a) Show that residue fields in the sense of Footnote 6 are anonymously Noetherian.
(b) Verify that $\mathbb{Z}$ is anonymously Noetherian.
Note. Either run a direct proof or use the anonymous least number principle of Proposition I.18(a).
(c) Look up a proof of Hilbert's basis theorem, for instance the proof in [3, Theorem 7.5], and check that it can be massaged into a constructive proof of the statement that polynomial rings over anonymously Noetherian rings are anonymously Noetherian.

Exercise IV.6 (Prüfer domains as valuation domains [12, Exercise 43])**.** An *integral domain* is a commutative ring such that $1 \neq 0$ and such that $xy = 0$ implies $x = 0$ or $y = 0$. A *valuation domain* is an integral domain such that for any two elements, one divides the other. A *Prüfer domain* is an integral domain such that every finitely generated ideal $\mathfrak{a}$ is locally a principal ideal (in the sense that there exists a partition $1 = f_1 + \cdots + f_n$ such that, for each index i, the ideal $\mathfrak{a}[f_i^{-1}]$ is a principal ideal in $A[f_i^{-1}]$).

(a) Let A be a ring. Show that $A^\sim$ is an integral domain if A is. Does the converse hold?

(b) Let A be a valuation domain. Show that any matrix over A can be put into diagonal form by elementary row and column operations.
(c) Let A be an integral domain. Show that A is a Prüfer domain if and only if $A^\sim$ is a valuation domain.
(d) Let A be a Prüfer domain. Show that any matrix over A can locally be put into diagonal form by elementary row and column operations, by applying the result of part (b) to $A^\sim$.

Exercise IV.7 (A basic version of Kaplansky's theorem [12, Exercise 44])**.** (a) Let A be a local ring. Let $\mathfrak{a} \subseteq A$ be a finitely generated ideal such that $\mathfrak{a}^2 = \mathfrak{a}$. Show that $\mathfrak{a} = (0)$ or $\mathfrak{a} = (1)$.

Hint. Nakayama's lemma.

(b) Let A be a local ring. Let $M \in A^{n\times n}$ be an idempotent matrix. Verify that M is similar to a diagonal matrix with entries 0 and 1 by applying part (a) to the ideals of k-minors of M. Deduce that the cokernel of M is finite free.
(c) Let A be an arbitrary ring. Let $M \in A^{n\times n}$ be an idempotent matrix. Show that the cokernel of M is finite locally free, by applying the result of part (b) to $A^\sim$.
(d) Verify, without using the law of excluded middle or that A is Noetherian, that an A-module M is finitely generated and projective if and only if it is finite locally free.

Note. A self-contained solution is given in Ref. [15].

Bibliography

[1] P. Aczel and M. Rathjen. *Constructive set theory (book draft)*. 2010. URL: https://www1.maths.leeds.ac.uk/~rathjen/book.pdf.

[2] S. Artemov. *On Brouwer–Heyting–Kolmogorov provability semantics*. Slides for the *Mal'tsev Meeting*. 2013. URL: http://www.math.nsc.ru/conference/malmeet/13/Artemov.pdf.

[3] M. Atiyah and I. Macdonald. *Introduction to Commutative Algebra*. Addison–Wesley, 1969.

[4] J. Avigad. *Classical and constructive logic*. 2000. URL: https://www.andrew.cmu.edu/user/avigad/Teaching/classical.pdf.

[5] B. Banaschewski. "A new proof that 'Krull implies Zorn'". In: *Math. Log. Quart.* 40.4 (1994), pp. 478–480.

[6] A. Bauer. *Five Stages of Accepting Constructive Mathematics*. Lecture at the Institute for Advanced Study. 2013. URL: https://video.ias.edu/members/1213/0318-AndrejBauer.

[7] A. Bauer. "Five Stages of Accepting Constructive Mathematics". In: *Bull. Amer. Math. Soc.* 54.3 (2017), pp. 481–498.

[8] A. Bauer. "Intuitionistic Mathematics and Realizability in the Physical World". In: *A Computable Universe*. Ed. by H. Zenil. World Scientific Pub Co, 2012.

[9] A. Bauer. *Realizability as the connection between computable and constructive mathematics*. 2005. URL: http://math.andrej.com/data/c2c.pdf.

[10] E. Bishop and D. Bridges. *Constructive Analysis*. Springer, 1985.

[11] I. Blechschmidt. "Exploring mathematical objects from custom-tailored mathematical universes". In: *Objects, structures, and logics: FilMat studies in the philosophy of mathematics*. Ed. by G. Oliveri, C. Ternullo, and S. Boscolo. Springer, 2022.

[12] I. Blechschmidt. "Generalized spaces for constructive algebra". In: *Proof and Computation II. From Proof Theory and Univalent Mathematics to Program Extraction and Verification*. Ed. by K. Mainzer, P. Schuster, and H. Schwichtenberg. World Scientific, 2021, pp. 99–187.

[13] I. Blechschmidt. *Pizzaseminar zu konstruktiver Mathematik*. 2018. URL: https://pizzaseminar.speicherleck.de/skript2/konstruktive-mathematik.pdf.

[14] I. Blechschmidt. "Using the internal language of toposes in algebraic geometry". https://arxiv.org/abs/2111.03685. PhD thesis. University of Augsburg, 2017.

[15] I. Blechschmidt. *Vector bundles on affine schemes (short note)*. 2015. URL: https://www.ingo-blechschmidt.eu/kaplansky-en.pdf.

[16] I. Blechschmidt and P. Schuster. "Maximal ideals in countable rings, constructively". In: *Revolutions and Revelations in Computability. 18th Conference on Computability in Europe*. Ed. by U. Berger and J. Franklin. Lect. Notes Comput. Sci. Proceedings, CiE 2022, Swansea, Wales, July 11–15, 2022. Springer.

[17] D. Bridges, F. Richman, and P. Schuster. "A Weak Countable Choice Principle". In: *Proc. Amer. Math. Soc.* 128.9 (2000), pp. 2749–2752.

[18] W. de Campos Sanz and T. Piecha. "A critical remark on the BHK interpretation of implication". In: *Philosophia Scientiæ* 18 (2014), pp. 13–22.

[19] O. Caramello. *Theories, Sites, Toposes: Relating and studying mathematical theories through topos-theoretic 'bridges'*. Oxford University Press, 2018.
[20] T. Coquand. "Computational content of classical logic". In: *Semantics and Logics of Computation*. Ed. by A. Pitts and P. Dybjer. Cambridge University Press, 1997, pp. 33–78. URL: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.49.3492&rep=rep1&type=pdf.
[21] J. Couture and J. Lambek. "Philosophical reflections on the foundations of mathematics". In: *Erkenntnis* 34 (1991), pp. 187–209.
[22] L. Crosilla. "Exploring predicativity". In: *Proof and Computation*. Ed. by K. Mainzer, P. Schuster, and H. Schwichtenberg. World Scientific, 2018, pp. 83–108.
[23] D. van Dalen. "Kolmogorov and Brouwer on constructive implication and the Ex Falso rule". In: *Russian Math. Surveys* 59.2 (2004), pp. 247–257.
[24] M. Dummett. "The Philosophical Basis of Intuitionistic Logic". In: *Truth and Other Enigmas*. Duckworth, 1973, pp. 215–247.
[25] M. Erné. "A primrose path from Krull to Zorn". In: *Comment. Math. Univ. Carolin.* 36.1 (1995), pp. 123–126.
[26] M. Escardó. *Infinite sets that satisfy the principle of omniscience in all varieties of constructive mathematics*. Slides for Dagstuhl 2011, available online. 2011.
[27] M. Escardó. "Infinite sets that satisfy the principle of omniscience in any variety of constructive mathematics". In: *J. Symbolic Logic* 78.3 (2013), pp. 764–784.
[28] M. Escardó. *Infinite sets that satisfy the principle of omniscience in constructive type theory*. Slides for Tallinn 2017, available online. 2017.
[29] S. Feferman. "Set-theoretical foundations of category theory". In: *Reports of the Midwest Category Seminar III*. Vol. 106. Lecture Notes in Math. Springer, 1969, pp. 201–247.
[30] K. Gödel. "The consistency of the axiom of choice and of the generalized continuum-hypothesis". In: *Proc. Natl. Acad. Sci. USA* 24.12 (1938), pp. 556–557.
[31] R. Goldblatt. *Topoi: The Categorical Analysis of Logic*. Vol. 98. Stud. Logic Found. Math. Elsevier, 1984.
[32] J. Hamkins and A. Lewis. "Infinite time Turing machines". In: *J. Symbolic Logic* 65.2 (2000), pp. 567–604.
[33] W. Hodges. "Krull implies Zorn". In: *J. Lond. Math. Soc.* 19.2 (1979), pp. 285–287.
[34] P. Howard and J. Rubin. *Consequences of the Axiom of Choice*. Math. Surveys Monogr. AMS, 1998.
[35] P. T. Johnstone. "Rings, fields, and spectra". In: *J. Algebra* 49.1 (1977), pp. 238–260.
[36] P. T. Johnstone. *Sketches of an Elephant: A Topos Theory Compendium*. Oxford University Press, 2002.
[37] U. Kohlenbach. *Applied Proof Theory: Proof Interpretations and their Use in Mathematics*. Springer-Verlag, 2008.
[38] J. Lambek. "Are the traditional philosophies of mathematics really incompatible?" In: *Math. Intelligencer* 16.1 (1994), pp. 56–62.
[39] J. Lambek and P. Scott. *Introduction to higher-order categorical logic*. Vol. 7. Cambridges Stud. Adv. Math. Cambridge University Press, 1988.
[40] T. Leinster. "An informal introduction to topos theory". In: *Publications of the nLab* 1.1 (2011).
[41] H. Lombardi and C. Quitté. *Commutative Algebra: Constructive Methods*. Springer, 2015.
[42] S. Mac Lane and I. Moerdijk. *Sheaves in Geometry and Logic: a First Introduction to Topos Theory*. Universitext. Springer, 1992.
[43] M. Mandelkern. "Brouwerian counterexamples". In: *Math. Mag.* 62.1 (1989), pp. 3–27.
[44] S. Melikhov. "Mathematical semantics of intuitionistic logic". 2015. URL: https://arxiv.org/abs/1504.03380.

[45] R. Mines, F. Richman, and W. Ruitenburg. *A Course in Constructive Algebra*. Universitext. Springer, 1988.

[46] J. Moschovakis. "Intuitionistic logic". In: *The Stanford Encyclopedia of Philosophy*. Ed. by E. Zalta. 2021. URL: https://plato.stanford.edu/entries/logic-intuitionistic/.

[47] C. Mulvey. "Intuitionistic algebra and representations of rings". In: *Recent Advances in the Representation Theory of Rings and C^*-algebras by Continuous Sections*. Ed. by K. H. Hofmann and J. R. Liukkonen. Vol. 148. Mem. Amer. Math. Soc. American Mathematical Society, 1974, pp. 3–57.

[48] BBC NEWS. *Blair 'misunderstands drug laws'*. 2008. URL: https://news.bbc.co.uk/2/hi/uk.news/england/london/7440111.stm.

[49] J. van Oosten. *Realizability: An Introduction to its Categorical Side*. Vol. 152. Stud. Logic Found. Math. Elsevier, 2008.

[50] D. Piponi. *Drugs, Kate Moss, and Intuitionistic Logic*. 2008. URL: http://blog.sigfpe.com/2008/06/drugs-kate-moss-and-intuitionistic.html.

[51] F. Richman. "The fundamental theorem of algebra: a constructive development without choice". In: *Pac. J. Math.* 196.1 (2000), pp. 213–230.

[52] W. Ruitenburg. "Constructing roots of polynomials over the complex numbers". In: *Computational Aspects of Lie Group Representations and Related Topics, Proc. of the 1990 Computer Algebra Seminar held in Amsterdam*. Ed. by A. Cohen. Vol. 84. CWI Tract. Centrum voor Wiskunde en Informatica, Amsterdam, 1991, pp. 107–128.

[53] J. Schoenfield. "The problem of predicativity". In: *Essays on the Foundations of Mathematics*. Ed. by Y. Bar-Hillel, E. Poznanski, M. Rabin, and A. Robinson. Magnes, 1961, pp. 132–139.

[54] D. Scott. "Prime ideal theorems for rings, lattices and Boolean algebras". In: *Bull. AMS* 60 (1954), p. 390.

[55] M. Shulman. "Set theory for category theory". 2008. URL: https://arxiv.org/abs/0810.1279.

[56] T. Streicher. *Introduction to category theory and categorical logic*. https://www.mathematik.tu-darmstadt.de/~streicher/CTCL.pdf. 2004.

[57] T. Streicher. *Introduction to constructive logic and mathematics*. 2001. URL: https://www2.mathematik.tu-darmstadt.de/~streicher/CLM/clm.pdf.

[58] G. Wraith. *Mathematical phantoms*. 2007 or earlier. URL: http://www.wra1th.plus.com/gcw/math/MathPhant.html.