Saarland University
Faculty of Natural Sciences and Technology I
Department of Computer Science

Bachelor Thesis

Constructing Number Systems in Coq

submitted by

Carsten Hornung

submitted on
April 4, 2011

Supervisor
Prof. Dr. Gert Smolka

Advisor
Dr. Chad E. Brown

Reviewers
Prof. Dr. Gert Smolka
Dr. Chad E. Brown

Eidesstattliche Erklärung

Ich erkläre hiermit an Eides Statt, dass ich die vorliegende Arbeit selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel verwendet habe.

Statement in Lieu of an Oath

I hereby confirm that I have written this thesis on my own and that I have not used any other media or materials than the ones referred to in this thesis.

Einverständniserklärung

Ich bin damit einverstanden, dass meine (bestandene) Arbeit in beiden Versionen in die Bibliothek der Informatik aufgenommen und damit veröffentlicht wird.

Declaration of Consent

I agree to make both versions of my thesis (with a passing grade) accessible to the public by having them added to the library of the Computer Science Department.

Saarbrücken, _____ _____

Datum/Date Unterschrift/Signature

Abstract

The primary goal of this thesis is to give elegant constructions of the natural numbers, positive rational numbers and finally the real numbers in the proof assistant Coq. Coq is a widely used proof assistant implementing a program specification and mathematical higher-level language called Gallina. Gallina is based on an expressive formal language called the Calculus of Inductive Constructions that itself combines both a higher-order logic and a richly-typed functional programming language. Thus Coq provides a platform to define functions and predicates, to state mathematical theorems and to interactively develop formal proofs of them. To construct the number systems we use Landau's book *Grundlagen der Analysis* as a guide. It contains constructions of the (positive) rational numbers, the real numbers (based on Dedekind cuts) and the complex numbers starting from the natural numbers and the Peano axioms.

Acknowledgments

First of all I want to thank my advisor Dr. Chad E. Brown whose support during my work was invaluable. His experience in logic and mathematics always helped me getting to the heart of the matter.
A special thank goes to Prof. Dr. Gert Smolka for offering me such an interesting topic of investigation. His support essentially influenced my work and continually gave me different and more general views of considered problems. The work enormously improved my understanding of logic.
Furthermore I want to thank all my fellow students, family and girlfriend for their helpful support.

Contents

1 Introduction

1.1 Motivation

There are two different ways one can deal with number systems: Either giving axiomatizations of the properties of the numbers or constructing them from basic principles.
An axiomatization is a set of properties that specifies certain operations for a special structure. At the end of the 19th century the basic principles of the natural numbers were axiomatized by Peano [14] and Dedekind. According to Tarski, Hilbert was the first mathematician who axiomatized the real numbers in 1900 [16].
Instead of giving an axiomatization of a certain number system and assuming all of the properties one can assume a set of basic principles and prove the properties of the corresponding axiomatization.
A standard construction of the natural numbers in set theory is to define the natural numbers as follows:

$$\begin{aligned}
&\emptyset,\\
&\{\emptyset\},\\
&\{\emptyset, \{\emptyset\}\},\\
&\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\},\\
&\vdots
\end{aligned}$$

In a constructive type theory (including inductive types) one can define the natural numbers as a special inductive type. More precisely, constructive type theory has a generalization of $\mathbb{N}$ in the form of inductive types.
Among the possible ways to construct the real numbers one has

- Cauchy sequences
- Positional expansions
- Dedekind cuts

Landau's book *Grundlagen der Analysis* [13] contains constructions of the (positive) rational numbers, the real numbers (based on Dedekind cuts) and the complex numbers starting from the natural numbers and the Peano axioms. That

is, Landau combines both possibilities to deal with number systems. He uses an axiomatization of the natural numbers and constructs further number systems. In about 300 theorems and lemmas he proves the most common properties of numbers. He was very attentive in his work. However, the underlying set theory and logic he uses stay implicit. In this thesis we will construct the real numbers using Landau's book as a guide.

1.2 Constructions in this Thesis

In this thesis we construct different number systems in Coq and its underlying Calculus of Constructions based on constructive type theory. As it comes to the constructions, we will try to follow Landau's book as close as we can. If it makes sense to diverge from Landau's constructions due to additional assumptions or the underlying inductive structure in Coq, we will mention it explicitly and point out the reasons why we are doing so. Following Landau, we will mainly consider Dedekind cuts to construct the real numbers. We have the following sequence for the construction:

$$\mathbb{N}^+ \to \text{Fractions} \to \mathbb{Q}^+ \to \mathbb{R}^+ \to \mathbb{R}$$

From the natural numbers (without *0*) we define the set of all fractions as pairs of natural numbers. After that we define the positive rational numbers as a special subset of the fractions, namely the reduced fractions. Thereafter we construct Dedekind cuts representing the positive real numbers and finally we get the real numbers including zero and negative numbers.

1.2.1 Coq and the Calculus of Inductive Constructions

The Calculus of Inductive Constructions is an expressive formal language combining both a higher-order logic and a richly typed programming language. Coq is a widely used proof assistant implementing a program specification and mathematical higher-level language based on the Calculus of Inductive Constructions. Thus Coq provides a platform to define functions and predicates, to state mathematical theorems and to interactively develop formal proofs of them [1].

In Coq we consider propositions as types. To prove a proposition means to find a term with the corresponding type. That is, proofs are typed terms. Coq provides so called **tactics** that allow to construct a proof term step by step instead of giving it explicitly. In Coq *bool* is a finite inductive type with two constructors *true* and *false*. The set of propositions we are dealing with is *Prop*. The two corresponding values in *Prop* are *True* and *False*. *Prop* is not an inductive type like *bool*. There are a few typing rules for terms of type *Prop* such that we

can construct infinitely many closed terms of type *Prop*. If we deal with a certain x in *Prop* we have $\neg x$ as a special notation for $x \to \mathit{False}$. There are also infinitely many closed terms of type *bool* but all of them can be reduced to *true* or *false*. If we have a variable x of type *bool* we have different notations as follows:

$$\begin{aligned} \mathit{if}\ x\ \mathit{then}\ A\ \mathit{else}\ B &\rightsquigarrow \mathit{match}\ x\ \mathit{with}\ \mathit{true}\ \Rightarrow A \mid \mathit{false}\ \Rightarrow B\ \mathit{end} \\ \neg_b\, x &\rightsquigarrow \mathit{if}\ x\ \mathit{then}\ \mathit{false}\ \mathit{else}\ \mathit{true} \end{aligned}$$

If the context is clear or it is not relevant for the discussion we will also write $\neg$ instead of $\neg_b$. Obviously, we can map *bool* into *Prop* like already mentioned above:

$$\lambda\, x : \mathit{bool}.\ \mathit{if}\ x\ \mathit{then}\ \mathit{True}\ \mathit{else}\ \mathit{False}$$

In Coq we can define a hidden coercion that exactly does this job. These coercions make proofs more readable and could be replaced by the function itself at any time. It turns out that there is no obvious corresponding way to map *Prop* into *bool*. We are also able to prove $b \vee \neg b$ for any $b : \mathit{bool}$ with a simple case analysis because *bool* is a finite inductive type. We have two possibilities to deal with sets over a special type X. We either consider predicates of type $X \to \mathit{bool}$ or $X \to \mathit{Prop}$. Because of the defined coercion it is clear how to map sets of type $X \to \mathit{bool}$ into $X \to \mathit{Prop}$, but there is no way to go the other direction.

1.2.2 Classical Assumptions

For the natural numbers, fraction and positive rational numbers we do not need additional assumptions. For cuts, we need a special extensionality and excluded middle. As it comes to the construction of the real numbers, we need a stronger version of excluded middle to have case analyses within definitions.

Excluded Middle

A well known assumption is the following:

$$\mathit{XM} \quad := \quad \forall X : \mathit{Prop}.\ X \vee \neg X \qquad \textbf{Law of Excluded Middle}$$

If we are able to prove this theorem in a certain logic, we call it **classical**.

Characterization of Equality

A popular assumption characterizing equality of functions is formulated as follows: Two functions are equal if they behave the same. That is, the two functions yield the same value for each argument of their domain. This assumption

is called **Functional Extensionality**.

$$FE \quad := \quad \forall X\ Y : Type\ \forall f\ g : X \to Y.(\forall x.\ f\ x = g\ x) \to f = g$$

We will also see another logical assumption called **Propositional Extensionality** characterizing equality for propositions.

$$PE \quad := \quad \forall X\ Y\ : Prop.\ (X \leftrightarrow Y) \to X = Y$$

We can prove neither *FE* nor *PE* in Coq. An assumption combining both *FE* and *PE* is called **Set Extensionality**.

$$SE \quad := \quad \forall X : Type\ \forall p\ q : X \to Prop.(\forall x.\ p\ x \leftrightarrow q\ x) \to p = q$$

Set Extensionality is provable from *FE* and *PE*. For cuts we need a special extensionality similar to *SE*, namely *CE* for **Cut Extensionality**.

Proof Irrelevance

The proposition that all proofs of an arbitrary proposition X are equal is called **proof irrelevance**.

$$PI \quad := \quad \forall X : Prop\ \forall x\ y : X.\ x = y$$

We cannot prove *PI* in Coq. We consider the same proposition for a value B of type *bool* instead of *Prop*. That is, B can be *true* or *false*. We assume we have two proofs b_1 and b_2 of B. In Coq we have no proof of *False* and exactly one proof for *True*, namely *I*. This fact allows us to say that b_1 and b_2 are equal. To be more explicit we can prove in Coq

$$BPI \quad := \quad \forall B : bool\ \forall b_1\ b_2 : B.\ b_1 = b_2$$

We can avoid dealing with *PI* until we come to Dedekind cuts. We know $PE \to PI$. We will also see that *CE* implies *PE*. That is, we only need *CE* and *XM* as assumptions for cuts.

1.2.3 Notations

In the next chapters we will consider different structures. To minimize and to avoid confusions we will use different characters for variables ranging over the elements of the considered structures.

Natural Numbers	$x, y, z \ldots$	(small latin letters)
Positive Rational Numbers	$X, Y, Z \ldots$	(capital latin letters)
Cuts	$\Theta, \Xi, \Phi \ldots$	(capital greek letters)
Real Numbers	$\epsilon, \eta, \zeta, \phi \ldots$	(small greek letters)

We will use calligraphic letters for constructors like $\mathcal{O}$, $\mathcal{S}$ and $\mathcal{P}$. We refer to subsets of the considered structures as P, Q and R if they are represented by predicates mapping into *Prop* and refer to them as p and q if the predicates map into *bool*. Since we consider sets to be predicates we sometimes write $P\ x$ instead of $x \in P$. If the context is clear we omit explicit quantification such that we consider all free variables as bound.

1.2.4 Proof Script

In the thesis we will refer to the detailed formalization of the different structures. The proof script can be found on the website of the thesis at `http://www.ps.uni-saarland.de/~hornung/bachelor.php`.

1.3 Related Work

There are already several formalizations of analysis in the literature: Chirimar and Howe [4] developed analysis in the Nuprl system [6] representing real numbers by Cauchy sequences. There is also a construction in Lego by Jones [11]. Harrison [9] presents classical analysis in the context of the Isabelle-HOL-system [8]. Ciaffaglione and Di Gianantonio [5] constructs the real numbers in Coq using infinite (lazy) streams. Furthermore Geuvers and Niqui [7] formalize the real numbers in the Coq system using Cauchy completion. Hence the main difference between the other two constructions in the Coq system is that we will use Dedekind cuts following Landau [13]. Lambert van Benthem Jutting [12], a Dutch mathematician, translates Landau's work to the Automath system in 1976. Brown again gives an automated translation from Automath to Coq [3].

1.4 Structure of this Thesis

In Chapter 2 we will construct the natural numbers $\mathbb{N}^+$ and present their basic properties. Chapter 3 outlines the construction of fractions which give us a base to construct the rational numbers $\mathbb{Q}^+$ in Chapter 4. In Chapter 5 we introduce Dedekind cuts which allow us to construct the real numbers $\mathbb{R}$ in Chapter 6. We will give both axiomatizations for every introduced structure and an outline of the constructions and proofs of interesting properties. The parts where we diverge from Landau and the necessary assumptions are summarized in Chapter 7.

2 Natural Numbers

In this chapter we introduce the natural numbers $\mathbb{N}^+$ and their basic properties.

2.1 Peano Axioms

At the end of the 19th century the basic principles of the natural numbers were determined. Two mathematicians involved in this development were Dedekind and Peano with the formulation of the **Peano axioms** also known as the **Dedekind-Peano axioms** [14]:

$$1 \in \mathbb{N}^+$$
$$\forall x \in \mathbb{N}^+.\ x + 1 \in \mathbb{N}^+$$
$$\forall x\ y \in \mathbb{N}^+.\ x = y \leftrightarrow x + 1 = y + 1$$
$$\forall x \in \mathbb{N}^+.\ x + 1 \neq 1$$
$$\forall P \subseteq \mathbb{N}^+.\ 1 \in P \rightarrow (\forall x \in P.\ x + 1 \in P) \rightarrow \forall x \in \mathbb{N}^+.\ x \in P$$

The first axiom says that *1* is a natural number. The second axiom says that for every natural number x there is a number $x + 1$ in $\mathbb{N}^+$. We refer to this natural number as the **successor** of x. The third axiom expresses that the successors of two numbers are equal if and only if the two numbers are equal. The fourth axiom says that there is no natural number having *1* as successor. The last axiom is the so called **induction axiom**: If *1* is in an arbitrary set P (**base case**) and $x \in P$ implies $x + 1 \in P$ for any x (**induction case**) we know that P contains every natural number.
To construct the different number systems, Landau assumes the Peano axioms above and defines the different operations like addition or multiplication. In Coq we can define an inductive type corresponding to the natural numbers. To be more explicit, in Coq we have

```
Inductive nat :=
| O : nat
| S : nat -> nat
```

We consider the elements of *nat* as the values we obtain from the constructors $\mathcal{O}$ and S:

$$\mathcal{O},\ S\ \mathcal{O},\ S(S\ \mathcal{O}),\ S(S(S\ \mathcal{O})),\ \ldots$$

We call $\mathcal{O}$ the **One** or the **O**rigin and say the constructor S yields the **successor** of a natural number. Hence we consider 1 to be $\mathcal{O}$ and $x + 1$ to be $S\ x$.
Corresponding to the successor function we can define a predecessor function yielding for a natural number different from $\mathcal{O}$ the predecessor. Because there is no predecessor of $\mathcal{O}$ and we cannot define partial functions we map $\mathcal{O}$ to itself.

```
Definition pred (x:nat) := match x with O => O | S y => y end.
```

We do not include 0 as a natural numbers. We consider the natural numbers starting from 1 because Landau does. Following Landau, we procrastinate the problem of dealing with 0 until we come to the real numbers.
Because of the underlying Calculus of Constructions we do not need to assume the Peano axioms. We can prove them rather easily. Since $\mathcal{O}$ is a natural number in our construction and the successor function S yields a natural number the first two Peano axioms do not have to be proven. Furthermore we just mention the injectivity of the successor function regarding the fourth Peano axiom since the other direction is trivial.

$$\forall x.\ \mathcal{O} \neq S\ x \tag{2.1}$$

$$\forall x\ y.\ S\ x = S\ y \rightarrow x = y \tag{2.2}$$

$$\forall P.\ P\ \mathcal{O} \rightarrow (\forall x.\ P\ x \rightarrow P\ (S\ x)) \rightarrow \forall x.\ P\ x \tag{2.3}$$

To be more explicit concerning the proofs we have in Coq:

```
Theorem S_neq_O (x:nat) : O <> S x.
intros x. discriminate.
Qed.

Theorem S_injective (x y: nat) : S x = S y -> x = y.
intros x y. apply (f_equal pred).
Qed.

Theorem ind_axiom (p:nat->Prop) : p O -> (forall x, p x -> p (S x)) -> forall x, p x.
intros p base step. fix IHx 1.
destruct x as [|x'].
exact base.
apply (step x' (IHx x')).
Qed.
```

The tactic *discriminate* applied to a subgoal of the form $A <> B$ checks whether the two values A and B are structural different from each other. In this case we have two values yielded by different constructors $\mathcal{O}$ and S. Hence the values are not equal. In Coq all constructors are injective and two terms are equal if they are structurally equal. The predefined

lemma *f_equal* : $\forall X\ Y : Type\ \forall x\ y \in X\ \forall f : X \to Y.\ x = y \to f\ x = f\ y$ where the first four arguments are hidden allows us to prove $x = y$ using the predecessor function *pred*. The same subgoal would be provable with the tactic *injection* that reduces the equality of two values yield by the same constructor to equality of their subterms. The tactic *fix* gives us **recursion**. Since induction is nothing but recursion we obtain induction. One can apply the fixed proposition to an arbitrary subterm. In this case we do a case analysis on x using the Coq tactic *destruct*. The case $x = \mathcal{O}$ is trivial since we have $p\ \mathcal{O}$ as an assumption. In the case that x consists of a subterm, here x', of the same type that is structural less than the initial one, one can apply the fixed proposition with this subterm. This corresponds to the application of the induction hypothesis.

2.2 Order and Operations

Based on the inductive definition of the natural numbers we are able to define an order for them. We can even define $\leq$ to have type $nat \to nat \to bool$, i.e. mapping into *bool* instead of *Prop*. We will also see that this fact will give us more flexibility in defining other functions or predicates.

$$\mathcal{O} \leq y \quad := \quad true \tag{2.4}$$

$$S\ x \leq S\ y \quad := \quad x \leq y \tag{2.5}$$

$$S\ x \leq \mathcal{O} \quad := \quad false \tag{2.6}$$

$$x < y \quad := \quad S\ x \leq y \tag{2.7}$$

The definition of $\leq$ is realized in Coq by a *match* on x and y where the two cases $x = \mathcal{O}$ and $y = \mathcal{O}$ are directly defined to be *true* and *false*. In 2.5 we have a recursive call and in 2.7 we have a special notation. It actually suffices to have $\leq$ as a reflexive, antisymmetric and transitive order of the natural numbers such that we can define $\geq$ and the irreflexive orders $<$ and $>$ as special notations for $\leq$. It should be clear how to define $\geq$ and $>$ from this. Because it suffices and the number of proofs reduce to a minimum we exclusively consider $\leq$ and $<$. We can easily prove by induction on x **trichotomy** for $<$ on $\mathbb{N}^+$.

Lemma 2.2.1 (Trichotomy) For all natural numbers x and y we exactly have one of the cases

$$x < y, \quad x = y, \quad y < x$$

In this section we diverged from Landau's definitions the first time. His definitions of $<$ and $\leq$ are as follows (to prevent confusion we call them $<_L$ and $\leq_L$):

$$x <_L y \quad := \quad \exists z.\ y = x + z \tag{2.8}$$

$$x \leq_L y \quad := \quad x <_L y \vee x = y \tag{2.9}$$

It is easy to show the equivalence between our definitions and Landau's. But for now we do not have a definition for +. Hence diverging from Landau allows us here to define the order mapping into *bool* in a quite easier way before addition. We will sometimes use the equivalence to split $x \leq y$ in the two cases above.

We can also give definitions for **addition** and **multiplication** for the natural numbers just using the underlying inductive structure.

$$x + \mathcal{O} \quad := \quad S\, x \tag{2.10}$$

$$x + S\, y \quad := \quad S\, (x + y) \tag{2.11}$$

$$x \cdot \mathcal{O} \quad := \quad x \tag{2.12}$$

$$x \cdot S\, y \quad := \quad x \cdot y + x \tag{2.13}$$

We will now define **subtraction**. The first time Landau introduces subtraction is in his chapter about fractions. However, we will discuss the definition of subtraction in this section for two reasons: Landau does not give an explicit definition of the **difference** of two numbers. He merely calls the z from 2.8 the difference of y and x. We cannot globally define values the way Landau does because we have to give an explicit function. The second reason is the following: Since subtraction should map into *nat* it only makes sense to define $x - y$ for natural numbers $y < x$.

$$S\, x - \mathcal{O} \quad := \quad x \tag{2.14}$$

$$S\, x - S\, y \quad := \quad x - y \qquad \text{if } y < x \tag{2.15}$$

In Coq we do not have the opportunity to define partial functions. We have already encountered this issue in the definition of the predecessor function *pred*. We could define − like *pred* for every argument even if it makes no sense, i.e. mapping x and y where $x \leq y$ to $\mathcal{O}$. However, as it comes to subtraction for cuts, we need the proof that the second operand is less than the first operand within the definition of − for cuts. For this reason we already define − for natural numbers with an additional argument, a proof of $y < x$. To be more explicit, in Coq we have:

```
Fixpoint sub_nat (x y:nat) : y<x -> nat := match x,y with
| O , y => fun (l:y<O) => match l with end
| S x' , O => fun _ => x'
| S x' , S y' => fun (l:S y'<S x') => sub_nat x' y' l
end.
```

The case $x = \mathcal{O}$ is critical since $y < \mathcal{O}$ reduces to *False*. We do not have any proof of *False*. For that a *match* on the proof of $y < \mathcal{O}$ does not give us any case and we are done. The other two cases should be intuitively clear.

2.3 Properties of the Natural Numbers

We now state some (provable) properties of the natural numbers. We defined $<$, $+$ and $\cdot$ and we will see that we can use these operations to define similar operations on the other structures like the fractions.

$\forall x\ y.\ x + y = y + x$	Commutativity of $+$	(2.16)
$\forall x\ y\ z.\ (x + y) + z = x + (y + z)$	Associativity of $+$	(2.17)
$\forall x\ y.\ x \cdot y = y \cdot x$	Commutativity of $\cdot$	(2.18)
$\forall x\ y\ z.\ (x \cdot y) \cdot z = x \cdot (y \cdot z)$	Associativity of $\cdot$	(2.19)
$\forall x\ y\ z.\ x \cdot (y + z) = x \cdot y + x \cdot z$	Distributivity of $+$, $\cdot$	(2.20)
$\forall x.\ 1 \cdot x = x$	Identity of $\cdot$	(2.21)
$\forall x\ y\ z.\ x < y \to y < z \to x < z$	Transitivity of $<$	(2.22)
$\forall x.\ \neg\ x < x$	Irreflexivity of $<$	(2.23)
$\forall x\ y.\ x < y \vee x = y \vee y < x$	Trichotomy of $<$	(2.24)
$\forall x\ y\ z.\ x < y \to x + z < y + z$	Monotonicity of $+$	(2.25)
$\forall x\ y\ z.\ x < y \to x \cdot z < y \cdot z$	Monotonicity of $\cdot$	(2.26)
$\forall x\ y\ z.\ x + z = y + z \to x = y$	Injectivity of $+$	(2.27)
$\forall x\ y.\ x < y \to \exists z.\ x + z = y$		(2.28)
$\forall x\ y.\ x \neq y + x$		(2.29)
$\forall P.\ 1 \in P \to (\forall x.\ x \in P \to x + 1 \in P) \to \forall x.\ x \in P$	Induction axiom	(2.30)

Since we defined $\mathbb{N}^+$ without 0 there is no identity for $+$ as for $\cdot$.

2.4 Well-Ordering Principle

For the structure of the natural numbers and the order $\leq$ we can state an interesting property of sets of natural numbers known as the **Well-Ordering Principle**. Landau introduced this principle in his construction of the real numbers [13] in Theorem 27.

Theorem 2.4.1 (Well-Ordering Principle) Every nonempty set of natural numbers P contains a smallest element m. In other words:

$$WP \quad := \quad \forall P \subseteq \mathbb{N}^+ .\ P \neq \emptyset \to \exists m \in P.\ \forall x \in P.\ m \leq x$$

We will consider a non-constructive proof that uses sets of type $nat \to Prop$ and a second more computational version that uses $nat \to bool$. It will turn out that the first version yields a stronger proposition equivalent to XM. Recall that every time we use P for a set we mean P of type $nat \to Prop$ and every time we use p we mean p has type $nat \to bool$.

2.4.1 Non-constructive Proof

There are many standard proofs for this principle. We show here an abstract one very close to Landau's.

Theorem 2.4.2 $XM \to WP$

Proof (Well-Ordering Principle) We assume XM. Given a nonempty set P we define the set $M = \{\, y \mid \forall x \in P.\ y \leq x \}$. Obviously we have

$$\mathcal{O} \in M \tag{2.31}$$

since $\forall x.\ \mathcal{O} \leq x$ (see Definition 2.4). However, M does not contain every natural number: Since P is nonempty we have an $x \in P$. By induction on x, Definition 2.5 and Definition 2.6 we have $\forall x.\ S\ x \leq x = false$. For that we have $\forall x \in P.\ S\ x \notin M$. Now we know that there must be an m such that

$$m \in M \wedge S\ m \notin M \tag{2.32}$$

If not, M would contain every natural number (because of 2.31 and the induction axiom 2.3). To follow the argumentation in the last sentence, we need XM. We now prove that this m is our desired m. That is, we will prove

$$m \in P \tag{2.33}$$

$$\forall x \in P.\ m \leq x \tag{2.34}$$

If $m \in M$ were not in P then $S\ m$ would also be in M because of the construction of M. Here we used again XM. That would contradict 2.32. Hence $m \in P$. 2.34 follows directly from $m \in M$ (2.32). ∎

Theorem 2.4.3 $WP \to XM$

Proof We assume the Well-Ordering Principle WP and consider an arbitrary X of type $Prop$. We consider the set $P = \{\, x \mid \mathcal{O} < x \vee X \}$. Since $\mathcal{O} < S\ \mathcal{O}$ we have that P is nonempty. From WP we now know that there exists an $m \in P$ with $\forall x \in P.\ m \leq x$. We have to prove $X \vee \neg X$. We do a case analysis for m. If $m = \mathcal{O}$ than we know that X holds since $m \in P$ and $\mathcal{O} < \mathcal{O} = false$ (Definitions 2.6 and 2.7). We now consider the successor case $m = S\ m'$ and prove $\neg X$. Since $\neg X$ means $X \to False$ we can assume X. That is, every natural number is in P. Hence $\mathcal{O} \in P$. We now have a contradiction since $\forall x \in P.\ m \leq x$ applied to $\mathcal{O}$ reduces to $False$ because m has the form $S\ m'$ and $S\ m' < \mathcal{O} = false$ (Definition 2.6). ∎

2.4.2 Constructive Proof

The proofs of 2.32 and 2.33 are proofs by contradiction where the logical assumptions *CP* and hence the equivalent *XM* are hidden. Because we want to avoid the use of these assumptions we try to find a more concrete way to prove the Well-Ordering Principle. Since we now consider $p : nat \to bool$ we can have a conditional as already mentioned in Section 1.2. In Coq we have the opportunity to define functions and it provides ways to compute values. Since the Calculus of Constructions only allows terminating functions we cannot define a function *first* as follows:

$$first\ p\ x \quad := \quad if\ p\ x\ then\ x\ else\ first\ p\ (S\ x)$$

We should be convinced that the application $first\ p\ \mathcal{O}$ would yield the value m discussed in Section 2.4.1 assuming that p is nonempty. To guarantee termination, if one defines a function, the Calculus of Inductive Constructions implemented in Coq always requires a decreasing argument. That is, if one considers a recursive call of a function there has to be at least one determined argument of an inductive type that is a structural subterm of the initial argument. To have a definition of a terminating function we can define *first* depending on an upper bound. Initializing this upper bound with an element in p guarantees that we find the least element in p. To be more explicit we define

$$first\ p\ \mathcal{O} \quad := \quad \mathcal{O} \tag{2.35}$$

$$first\ p\ (S\ x) \quad := \quad if\ p\ (first\ p\ x)\ then\ first\ p\ x\ else\ S\ x \tag{2.36}$$

Lemma 2.4.4 $\forall p \forall x.\ p\ x \to p(first\ p\ x)$

Proof Case analysis for x. The case $x = \mathcal{O}$ is obvious since $first\ p\ \mathcal{O} = \mathcal{O}$ because of Definition 2.35. Now we consider the successor case. We assume $p\ (S\ x)$. We must prove $p\ (first\ p\ (S\ x))$.

$first\ p\ (S\ x) = if\ p\ (first\ p\ x)\ then\ first\ p\ x\ else\ S\ x$ Def. 2.36

Case $p\ (first\ p\ x) = true$.

$first\ p\ (S\ x) = first\ p\ x$

Since $p\ (first\ p\ x)$ holds we know $p\ (first\ p\ (S\ x))$ holds.
Case $p\ (first\ p\ x) = false$.

$first\ p\ (S\ x) = S\ x$

Since $p\ (S\ x)$ holds we know $p\ (first\ p\ (S\ x))$ holds. ∎

Lemma 2.4.5 $\forall p \forall x.\ \mathit{first}\ p\ x \leq x$

Proof Let p be given. We argue by induction over x. The base case is obvious since $\mathit{first}\ p\ \mathcal{O} = \mathcal{O} \leq \mathcal{O}$ by Definition 2.4. We assume $\mathit{first}\ p\ x \leq x$ as induction hypothesis.
Case $p\ (\mathit{first}\ p\ x) = \mathit{true}$.

$$\begin{aligned} \mathit{first}\ p\ (S\ x) &= \mathit{if}\ p\ (\mathit{first}\ p\ x)\ \mathit{then}\ \mathit{first}\ p\ x\ \mathit{else}\ S\ x && \text{Def. 2.36} \\ &= \mathit{first}\ p\ x \\ &\leq x \leq S\ x && \text{IH} \end{aligned}$$

Case $p\ (\mathit{first}\ p\ x) = \mathit{false}$.

$$\begin{aligned} \mathit{first}\ p\ (S\ x) &= \mathit{if}\ p\ (\mathit{first}\ p\ x)\ \mathit{then}\ \mathit{first}\ p\ x\ \mathit{else}\ S\ x && \text{Def. 2.36} \\ &= S\ x \leq S\ x \end{aligned}$$

■

Lemma 2.4.6 $\forall p \forall x.\ p\ (\mathit{first}\ p\ x) \to \forall y.\ x < y \to \mathit{first}\ p\ x = \mathit{first}\ p\ y$

Proof Let p, x and y be given and assume $p\ (\mathit{first}\ p\ x)$. We argue by induction over y. The base case $y = \mathcal{O}$ is trivial since $x < y$ hence $S\ x \leq \mathcal{O}$ yields a contradiction because of the Definitions 2.7 and 2.6. We now have $x < y \to \mathit{first}\ p\ x = \mathit{first}\ p\ y$ as induction hypothesis and consider the inductive step for the successor case $S\ y$. We assume $x < S\ y$ and have $x \leq y$ because of Definition 2.7 and Definition 2.5.
Case $x = y$.

$$\begin{aligned} \mathit{first}\ p\ (S\ y) &= \mathit{if}\ p\ (\mathit{first}\ p\ y)\ \mathit{then}\ \mathit{first}\ p\ y\ \mathit{else}\ S\ y && \text{Def. 2.36} \\ &= \mathit{if}\ p\ (\mathit{first}\ p\ x)\ \mathit{then}\ \mathit{first}\ p\ x\ \mathit{else}\ S\ x && x = y \\ &= \mathit{first}\ p\ x && \text{assumption} \end{aligned}$$

Case $x < y$.

$$\begin{aligned} \mathit{first}\ p\ (S\ y) &= \mathit{if}\ p\ (\mathit{first}\ p\ y)\ \mathit{then}\ \mathit{first}\ p\ y\ \mathit{else}\ S\ y && \text{Def. 2.36} \\ &= \mathit{if}\ p\ (\mathit{first}\ p\ x)\ \mathit{then}\ \mathit{first}\ p\ x\ \mathit{else}\ S\ y && \text{IH} \\ &= \mathit{first}\ p\ x && \text{assumption} \end{aligned}$$

■

Lemma 2.4.7 $\forall p \forall x\ y.\ p\ y \to \mathit{first}\ p\ x \leq y$

Proof Let p, x and y be given and assume $p\ y$. We can split into two cases since trichotomy holds. Case $x \leq y$. We know $\mathit{first}\ p\ x \leq x \leq y$ by Lemma 2.4.5. Case $y < x$. From Lemma 2.4.4 and $p\ y$ we have $p\ (\mathit{first}\ p\ y)$. From that, Lemmas 2.4.6 and 2.4.5 we have $\mathit{first}\ p\ x = \mathit{first}\ p\ y \leq y$. ■

Proof (Well-Ordering Principle) Let p be a nonempty set and x be given such that $p\ x$ holds. Let m be our *first* $p\ x$. Both $m \in p$ and $\forall y \in p.\ m \leq y$ follow from Lemmas 2.4.4 and 2.4.7. ∎

2.5 Complete Induction

As it comes to the real numbers we want to prove the irrationality of the square root of two. There is a lot of work to do until we come to this. However, we can prove $x^2 \neq 2 \cdot y^2$ for arbitrary natural numbers x and y that gives us later the irrationality. Landau proves this property in his chapter about cuts using the Well-Ordering Principle from Section 2.4. It turns out that we can prove this proposition using **complete induction** without any additional assumptions.

Theorem 2.5.1 $\forall P.\ (\forall y.\ (\forall z.\ z < y \to z \in P) \to y \in P) \to \forall x.\ x \in P$

The proof can be found in the script. This theorem allows us to prove the following lemma.

Lemma 2.5.2 $\forall y\ x.\ x^2 \neq 2 \cdot y^2$

Proof We consider the set $P = \lambda y. \forall x.\ x^2 \neq 2 \cdot y^2$ and want apply Theorem 2.5.1. To apply this, we have to prove

$$\forall y.\ (\forall z.\ z < y \to z \in P) \to y \in P$$

Let y be an arbitrary natural number and assume $\forall z.\ z < y \to z \in P$ as well as $x^2 = 2 \cdot y^2$ for an arbitrarily given x. We now want to have a contradiction. We only sketch the rest of the proof. The interested reader can find the whole proof in the script.
We can prove $y < x$ and $x - y < y$. We define $u = x - y$ and $t = y - u$. We now can prove $t^2 = 2 \cdot u^2$. This proof is a bit tedious. Since $u < y$ we can apply our assumption $\forall z.\ z < y \to \forall x.\ x^2 \neq 2 \cdot z^2$ with $z = u$ and $x = t$ and get a contradiction. ∎

2.6 Remarks

In this chapter we introduced the natural numbers and their basic theorems. We gave a collection of properties for the natural numbers and constructed them using an inductive type in Coq.

The first time we diverged from Landau's construction is the definition of $\leq$ or rather $<$. While he prefered to give the equivalent definition

$$x <_L y \quad := \quad \exists z. x + z = y$$

we have instead used the underlying structure of the Calculus of Constructions and used recursive definitions. For that we could already define the order for the natural numbers before addition. Like we have seen in Section 2.4 there was a way to prove the Well-Ordering Principle without the use of classical logic but using $nat \to bool$ for sets of natural numbers. The other representation of sets yields us a stronger proposition that is equivalent to *XM* and hence all classical assumptions.

3 Fractions

The next step towards the real numbers is to define fractions and prove theorems for them. We define the fractions F as all pairs over the natural numbers. This is exactly what Landau does.

$$F \quad := \quad \mathbb{N}^+ \times \mathbb{N}^+$$

In Coq this corresponds to an inductive definition.

```
Inductive frac :=
| over : nat -> nat -> frac
```

In the next chapters we will write

$$\frac{x_1}{x_2}$$

representing a fraction where $x_1, x_2 \in \mathbb{N}^+$. We call x_1 the **numerator** and x_2 the **denominator** of the fraction $\frac{x_1}{x_2}$ and refer to the fraction as x_1 **over** x_2.

3.1 Equivalence of Fractions

Since there are infinitely many fractions representing the same rational number we introduce a special equivalence relation $\sim$ for fractions that defines the equivalence of fractions using equality of natural numbers.

$$\frac{x_1}{x_2} \sim \frac{y_1}{y_2} \quad := \quad x_1 \cdot y_2 = y_2 \cdot x_2 \tag{3.1}$$

If $\frac{x_1}{x_2} \sim \frac{y_1}{y_2}$ holds we say $\frac{x_1}{x_2}$ **is equivalent to** $\frac{y_1}{y_2}$. Reflexivity, symmetry and transitivity follow directly from the fact that $=$ for the natural numbers is an equivalence relation. The equivalence between the fractions induces disjoint equivalence classes. In many books one sees $\left[\frac{x_1}{x_2}\right] = \left\{\frac{y_1}{y_2} | \frac{y_1}{y_2} \sim \frac{x_1}{x_2}\right\}$. These classes could be interpreted as the positive rational numbers. However, we will have a different representation.

3.2 Preorderings and Operations

Just as the defined equivalence of fraction reduces to equality of natural numbers we can also define a preordering of fractions in a similar way. We have

$$\frac{x_1}{x_2} \lesssim \frac{y_1}{y_2} \quad := \quad x_1 \cdot y_2 \leq y_1 \cdot x_2 \tag{3.2}$$

$$\frac{x_1}{x_2} < \frac{y_1}{y_2} \quad := \quad x_1 \cdot y_2 < y_1 \cdot x_2 \tag{3.3}$$

In Chapter 2 we stated trichotomy for natural numbers. This is also provable for fractions with the only difference that we consider $\sim$ instead of equality of fractions. We now define **addition** and **multiplication** for fractions.

$$\frac{x_1}{x_2} + \frac{y_1}{y_2} \quad := \quad \frac{x_1 \cdot y_2 + y_1 \cdot x_2}{x_2 \cdot y_2} \tag{3.4}$$

$$\frac{x_1}{x_2} \cdot \frac{y_1}{y_2} \quad := \quad \frac{x_1 \cdot y_1}{x_2 \cdot y_2} \tag{3.5}$$

In this section we also define **subtraction** for fractions. We remember that this operation expects an additional argument for the natural numbers. We can analogously define subtraction for fractions.

$$\frac{x_1}{x_2} - \frac{y_1}{y_2} \quad := \quad \frac{x_1 \cdot y_2 - y_1 \cdot x_2}{x_2 \cdot y_2} \qquad \text{if } \frac{y_1}{y_2} < \frac{x_1}{x_2} \tag{3.6}$$

Recall that the proof for $y_1 \cdot x_2 < x_1 \cdot y_2$ is directly given since $\frac{y_1}{y_2} < \frac{x_1}{x_2}$. We see now that all these definitions reduce to the definitions of the operations on the natural numbers.

3.3 Inverse of Multiplication

In contrast to the natural numbers, we have for every fraction $\frac{x_1}{x_2}$ a so called **inverse element** $\left(\frac{x_1}{x_2}\right)^{-1}$ **for multiplication**. For fractions we can directly define this value.

$$\left(\frac{x_1}{x_2}\right)^{-1} \quad := \quad \frac{x_2}{x_1} \tag{3.7}$$

The only property we expect from the inverse is stated in the following lemma.

Lemma 3.3.1 (Inverse of Multiplication) $\forall \frac{x_1}{x_2}.\ \left(\frac{x_1}{x_2}\right)^{-1} \cdot \frac{x_1}{x_2} \sim 1$

In our formalization 1 is a fraction corresponding to the natural number $\mathcal{O}$, i.e. $\frac{\mathcal{O}}{\mathcal{O}}$. Recall that $\mathcal{O}$ is not the zero 0. We will also write $\mathcal{O}$ instead of $\frac{\mathcal{O}}{\mathcal{O}}$ if the context is clear.

Proof We have

$$\left(\frac{x_1}{x_2}\right)^{-1} \cdot \frac{x_1}{x_2} \sim \frac{x_2}{x_1} \cdot \frac{x_1}{x_2} = \frac{x_2 \cdot x_1}{x_1 \cdot x_2} = \frac{x_1 \cdot x_2}{x_1 \cdot x_2} \sim \frac{\mathcal{O}}{\mathcal{O}}$$

The first equality is the definition of $\cdot$ for fractions. The second equality follows from the commutativity of $\cdot$ for natural numbers (see 2.18). The last equivalence is trivial (see Definition 3.1 and commutativity 2.18). ∎

3.4 Density

The relation $<$ for fractions is a **dense relation**. That is, there is always a fraction between two different fractions $\frac{x_1}{x_2}$ and $\frac{y_1}{y_2}$ if $\frac{x_1}{x_2} < \frac{y_1}{y_2}$.

Lemma 3.4.1 $\forall \frac{x_1}{x_2}\ \frac{y_1}{y_2}.\ \frac{x_1}{x_2} < \frac{y_1}{y_2} \rightarrow \exists \frac{z_1}{z_2}.\ \frac{x_1}{x_2} < \frac{z_1}{z_2} < \frac{y_1}{y_2}$.

Proof We have that $x_1 y_2 < y_1 x_2$. From

$$x_1(x_2 + y_2) = x_1x_2 + x_1y_2 < x_1x_2 + y_1x_2 = x_2(x_1 + y_1) = (x_1 + y_1)$$

we have

$$\frac{x_1}{x_2} < \frac{x_1 + y_1}{x_2 + y_2}$$

and from

$$(x_1 + y_1)y_2 = x_1y_2 + y_1y_2 < y_1x_2 + y_1y_2 = y_1(x_2 + y_2)$$

we have

$$\frac{x_1 + y_1}{x_2 + y_2} < \frac{y_1}{y_2}$$

such that $\frac{x_1+y_1}{x_2+y_2}$ does the job. ∎

While there is a smallest natural number $\mathcal{O}$ because of Definition 2.4 and no greatest natural number because $\forall x.\ x < S\ x$, there is neither a smallest fraction nor a greatest fraction. We just prove that there is no smallest fraction. The prove that there is no greatest fraction is similar.

Lemma 3.4.2 $\forall \frac{x_1}{x_2}\ \exists \frac{y_1}{y_2}.\ \frac{y_1}{y_2} < \frac{x_1}{x_2}$.

Proof Since $x_1x_2 < x_1x_2 + x_1x_2 = x_1(x_2 + x_2)$ the fraction $\frac{x_1}{x_2+x_2}$ does the job. ∎

3.5 Remarks

In this chapter we constructed fractions as pairs of natural numbers. We defined a special equivalence relation for them, namely $\sim$. With respect to this equivalence relation we have infinitely many different fractions being equivalent to each other. Furthermore we stated an interesting property expressing the density of $<$. Recall that there is no natural number between an arbitrary x and $S\ x$ even though $x < S\ x$. Hence $<$ for natural numbers is not dense. In the structures we consider in the next chapters, density of $<$ is always required.

4 Positive Rational Numbers

In this chapter we consider the positive rational numbers $\mathbb{Q}^+$. Every time we say rational numbers we mean positive rational numbers.

4.1 Properties of the Positive Rational Numbers

Our second step to construct the real numbers is the construction of a structure for the rational numbers satisfying a certain set of properties. In addition to the properties of the natural numbers we have an inverse for multiplication and density of $<$. We want to construct a type *prat* that represents the positive rational numbers, give definitions for

$$\begin{aligned} 1 &: \mathit{prat} \\ < &: \mathit{prat} \to \mathit{prat} \to \mathit{bool} \\ + &: \mathit{prat} \to \mathit{prat} \to \mathit{prat} \\ \cdot &: \mathit{prat} \to \mathit{prat} \to \mathit{prat} \\ ()^{-1} &: \mathit{prat} \to \mathit{prat} \end{aligned}$$

and want to prove the following important properties.

$\forall X\ Y.\ X + Y = Y + X$	Commutativity of $+$	(4.1)
$\forall X\ Y\ Z.\ (X + Y) + Z = X + (Y + Z)$	Associativity of $+$	(4.2)
$\forall X\ Y.\ X \cdot Y = Y \cdot X$	Commutativity of $\cdot$	(4.3)
$\forall X\ Y\ Z.\ (X \cdot Y) \cdot Z = X \cdot (Y \cdot Z)$	Associativity of $\cdot$	(4.4)
$\forall X.\ 1 \cdot X = X$	Identity of $\cdot$	(4.5)
$\forall X.\ X^{-1} \cdot X = 1$	Inverse of $\cdot$	(4.6)
$\forall X\ Y\ Z.\ X \cdot (Y + Z) = X \cdot Y + X \cdot Z$	Distributivity of $+$ and $\cdot$	(4.7)
$\forall X\ Y.\ X < Y \vee X = Y \vee Y < X$	Trichotomy for $<$	(4.8)
$\forall X\ Y\ Z.\ X < Y \to Y < Z \to X < Z$	Transitivity of $<$	(4.9)
$\forall X.\ \neg\ X < X$	Irreflexivity of $<$	(4.10)
$\forall X\ Y\ Z.\ X < Y \to X + Z < Y + Z$	Monotonicity of $<$ and $+$	(4.11)
$\forall X\ Y\ Z.\ X < Y \to X \cdot Z < Y \cdot Z$	Monotonicity of $<$ and $\cdot$	(4.12)

$$\forall X\ Y.\ X < Y \to \exists Z.\ X < Z \wedge Z < Y \qquad \text{Density of } < \tag{4.13}$$

$$\forall X\ \exists Y.\ Y < X \tag{4.14}$$

$$\forall X\ \exists Y.\ X < Y \tag{4.15}$$

Furthermore we want an additional property fulfilled that we call the **minimality** of the rational numbers. Given a subset of the rational numbers it says that if this set includes *1* and is closed under addition, multiplication and the inverses we have all rational numbers in this set. That is, every rational number can be constructed with the given operations and there are no undesired numbers.

$$\begin{aligned}
&\forall P.\ P\ 1 \to \\
&\quad (\forall X\ Y.\ P\ X \to P\ Y \to P\ (X + Y)) \to \\
&\quad (\forall X\ Y.\ P\ X \to P\ Y \to P\ (X \cdot Y)) \to \\
&\quad (\forall X.\ P\ X \to P\ (X^{-1})) \to \\
&\quad \forall X.\ P\ X
\end{aligned}$$

This property is some kind of induction principle for the rational numbers.
The properties 4.14 and 4.15 expresses the fact that $\mathbb{Q}^+$ has no endpoints. Recall that density of $<$ for rational numbers in 4.13 as well as 4.14 do not hold for the natural numbers. Furthermore we do not have a multiplicative inverse for natural numbers.

4.2 Representation of the Rational Numbers

The problem already mentioned in the last chapter that there are many different fractions representing the same value with respect to the corresponding equivalence relation suggests the idea of a quotient type. In this case this is a type where each value represents a set of all fractions equivalent to a certain representative such that we can define the set of all positive rational numbers as follows.

$$\mathbb{Q}^+ \quad := \quad F/\sim$$

The resulting problem is obvious. To decide whether two rational numbers are the same or represent the same set of fractions we have to compare two infinite sets. Representing these sets as functions with type *frac* → *Prop* or *frac* → *bool* that would reduce to equality of functions. That is, this is the first time we would need the additional assumption *FE*. We can represent a value of this quotient type by a unique representative. This motivates to avoid the use of *FE* or other additional assumptions. We will represent a set of all equivalent fractions by

this unique representative. Equality of these sets of fractions would reduce to equality of fractions. Landau himself introduces the rational numbers in the chapter of the fractions, he explicitly represents them as sets of fraction. Hence, due to our desire to avoid additional assumptions, we diverge from Landau once again.

The most common candidate for this representative is the reduced fraction. It is equivalent to each other fraction in the set and is explicitly determined. There are different ways to compute the reduced fraction using the Euclidean algorithm or prime representation of natural numbers. We would like to minimize additional work and try to use structures already defined. In Chapter 2.4 we saw *first* yielding the minimum of a nonempty set represented by a predicate mapping into *bool*. This minimum is indeed unique. We will see that we can use this concept for fractions. For reasons of readability we write $x_1 \cdot y_2 = y_1 \cdot x_2$ instead of $\frac{x_1}{x_2} \sim \frac{y_1}{y_2}$.

Let $x = \frac{x_1}{x_2}$ be implicitly given. Intuitively we consider the set of all candidates for the numerator of the reduced fraction that is equivalent to a given fraction.

$$\begin{aligned} N_x &:= \{\, y_1 \mid \exists y_2.\ x_1 \cdot y_2 = y_1 \cdot x_2 \,\} \\ \mathit{rednum}_x &:= \min\ N_x \\ D_x &:= \{\, y_2 \mid x_1 \cdot y_2 = \mathit{rednum}_x \cdot x_2 \} \\ \mathit{redden}_x &:= \min\ D_x \end{aligned}$$

To apply *first* to compute the minimum we need both sets N_x and D_x represented by a set of type $\mathit{nat} \to \mathit{bool}$. For reasons of termination *first* needs an upper bound for at least one element in the set. Hence we also need two upper bounds.

For reasons of termination it is impossible in general to represent a proposition including an existential quantifier over *nat* by a term of type *bool* since the witnessing value could be arbitrary large. In N_x the candidate for y_2 is unique and could be computed as $(y_2 \cdot x_2)\ \mathit{div}\ x_1$. However, defining *div* and proving its properties is more complicated than the method using the function *first*. To compute y_2 for a given y_1 we do the following. We consider the set of all y_2 such that $x_1 \cdot y_2 = y_1 \cdot x_2$ holds. Since

$$y_2 \leq x_1 \cdot y_2 = y_1 \cdot x_2$$

we can choose the upper bound for the application of *first* to be $y_1 \cdot x_2$ such that we find y_2 in every case. To be more precise, in Coq we define

$$\begin{aligned} \mathit{equiv}_x &:= \lambda y_1\ y_2.\ x_1 \cdot y_2 = y_1 \cdot x_2 \\ \mathit{getden}_x &:= \lambda y_1.\ \mathit{first}\ (\mathit{equiv}_x\ y_1)\ (y_1 \cdot x_2) \end{aligned}$$

$$n_x \quad := \quad \lambda y_1.\ x_1 \cdot (getden_x\ y_1) = y_1 \cdot x_2$$

where n_x represents N_x with the difference that n_x maps into *bool*. The cascaded function $equiv_x$ yields exactly the same as $\sim$. Given y_1, $getden_x$ computes the denominator y_2 such that $x_1 \cdot y_2 = y_1 \cdot x_2$. If there is no fitting y_2 (if y_1 is no candidate for the numerator) it does not matter what the function yields. We already illustrated above that we will find the candidate if there is one since $y_2 \leq y_1 \cdot x_2$. The set n_x should be equivalent to N_x introduced at the beginning of this section. Deciding whether a given y_1 is in this set means verifying that the denominator yielded by $getden_x$ satisfies the equivalence.
Since x_1 is in N_x we can choose x_1 to be the upper bound for the application of *first* to get the numerator. Notice that D_x can easily be represented by a predicate mapping into *bool* and that the upper bound for the minimum is analogously chosen like above.
Finally, in Coq we have

$$\begin{aligned} rednum_x &:= first\ n_x\ x_1 \\ redden_x &:= getden_x\ rednum_x \\ red_x &:= rednum_x\ /\ redden_x \end{aligned}$$

The denominator is now computed like above as the corresponding denominator $redden_x$ to the numerator $rednum_x$ of the reduced fraction. We are now able to prove the following proposition.

Lemma 4.2.1 $\forall y_1.\ N_x\ y_1 \leftrightarrow n_x\ y_1$

We use this fact in the following proofs. Furthermore we give up subscripts and write $red\ \frac{x_1}{x_2}$ instead of red_x. We now state and prove the two main properties of the function $red : frac \to frac$.

Lemma 4.2.2 $\forall x_1\ x_2.\ \frac{x_1}{x_2} \sim red\ \frac{x_1}{x_2}$

Proof Let x_1 and x_2 be given. Since

$$\frac{x_1}{x_2} \sim \frac{x_1}{x_2}$$

we know $N_x\ x_1$ and hence we have $n_x\ x_1$. By Lemma 2.4.4 we have $n_x\ (first\ n_x\ x_1)$ and we are done. The unconvinced reader is free to fill in the definitions of *red*, $rednum_x$, $redden_x$, n_x and $equiv_x$ to assure oneself. ∎

Lemma 4.2.3 $\forall x_1\ x_2\ y_1\ y_2.\ \frac{x_1}{x_2} \sim \frac{y_1}{y_2} \to red\ \frac{x_1}{x_2} = red\ \frac{y_1}{y_2}$

Proof Because $x = \frac{x_1}{x_2}$ was the implicitly given argument in the definition of *red* we now write $y = \frac{y_1}{y_2}$ as index for the corresponding functions in $red\ \frac{y_1}{y_2}$. From Lemma 4.2.2 and from the transitivity and symmetry of $\sim$ we have

$$red\ \frac{x_1}{x_2} \sim red\ \frac{y_1}{y_2}$$

If we know two fractions are equivalent and want to prove their equality, it suffices to prove the equality of the numerators. That is, we just have to prove

$$first\ n_x\ x_1 = first\ n_y\ y_1$$

Because x and y are equivalent the functions n_x and n_y behave the same. It is intuitively clear that *first* also behaves the same if the two given functions behave the same. This fact can be shown by induction on the second argument of *first*. (We assume this as proven; the interested reader can find this in the proof script) We now have to prove

$$first\ n_x\ x_1 = first\ n_x\ y_1$$

The case $x_1 = y_1$ should be trivial. Without loss of generality we can assume $x_1 < y_1$ (see also 2.2.1). We can now apply Lemma 2.4.6 since $n_x\ x_1$. ∎

We call a fraction $\frac{x_1}{x_2}$ **reduced** if $\frac{x_1}{x_2} = red\ \frac{x_1}{x_2}$. Since we can decide easily the equality of two fractions that induces a predicate $fred : frac \to bool$.
There are different ways to define predicate types that are all equivalent in Coq. We decide to have a record type including a fraction and a proof that it is reduced:

```
Record prat : Type :=
Prat { rep : frac
       redp : fred rep }
```

A record type gives us projection functions *rep* and *redp* in addition. Given a value X of type *prat* we call $rep\ X$ its **representative** and $redp\ X$ its corresponding proof. It should be clear how to implement this structure with a primitive inductive definition.

We can prove that the fraction yielded by *red* is always reduced.

Lemma 4.2.4 $\forall x_1\ x_2.\ fred\ (red\ \frac{x_1}{x_2})$

Proof Applying Lemma 4.2.3 to Lemma 4.2.2 gives us

$$red\ \frac{x_1}{x_2} = red\ (red\ \frac{x_1}{x_2})$$

and we are done. ∎

For that we will also write $red\ \frac{x_1}{x_2}$ representing the rational number we get from a certain fraction $\frac{x_1}{x_2}$ without mentioning the corresponding proof.

Now that we have each rational number represented by a fraction and a proof that this is reduced we have to say something about equality of rational numbers.

4.3 Equality of Rational Numbers

To prove the equality of two rational numbers we have to prove the equality of both the representatives and the corresponding proofs. The first thing is easily decidable. If the representatives are equal, then the equality of the corresponding proofs is trivial: Since we can prove *BPI* as discussed in Section 1.2.2 we have the equality of the two proofs. We can now state and prove the following lemma.

Lemma 4.3.1 $\forall X\ Y.\ rep\ X = rep\ Y \leftrightarrow X = Y$

Because of this fact we will often merely consider the representatives instead of the rational number including its corresponding proof.

4.4 Order and Operations

Since equality of rational numbers reduces to equality of fractions we can define the orders $\leq$ and $<$ for rational numbers using the preordering for fractions.

$$X \leq Y \quad := \quad rep\ X \lesssim rep\ Y \tag{4.16}$$

$$X < Y \quad := \quad rep\ X < rep\ Y \tag{4.17}$$

We can state and prove **trichotomy** for $<$ on $\mathbb{Q}^+$.

Lemma 4.4.1 (Trichotomy) For all rational numbers X and Y we exactly have one of the cases

$$X < Y, \quad X = Y, \quad Y < X$$

In the following we define **addition** and **multiplication** of rational numbers.

$$X + Y \quad := \quad red\ (rep\ X + rep\ Y) \tag{4.18}$$

$$X \cdot Y \quad := \quad red\ (rep\ X \cdot rep\ Y) \tag{4.19}$$

For the sake of completeness we also define **subtraction** for rational numbers.

$$X - Y \quad := \quad red\ (rep\ X - rep\ Y) \qquad \text{if } Y < X \tag{4.20}$$

The proof of $rep\ Y < rep\ X$ follows directly from $Y < X$.

4.5 Natural Numbers as Rational Numbers

We intuitively know about the fact that the natural numbers can be considered as a subset of the rational numbers. We can also explicitly give a fraction $\frac{x_1}{x_2}$ that corresponds to an arbitrary natural number x. We can embed the natural

numbers into the rational number by giving an injective function mapping a natural number to a unique rational number

$$nat\_to\_prat : nat \to prat$$

satisfying certain properties summarized below for all natural numbers x and y. Recall that the operators $+$, $\cdot$ and $<$ are overloaded.

$$\begin{aligned} nat\_to\_prat(x + y) &= nat\_to\_prat\ x + nat\_to\_prat\ y \\ nat\_to\_prat(x \cdot y) &= nat\_to\_prat\ x \cdot nat\_to\_prat\ y \\ nat\_to\_prat(x < y) &\leftrightarrow nat\_to\_prat\ x < nat\_to\_prat\ y \end{aligned}$$

That is, *nat_to_prat* **respects** the operations $+$, $\cdot$ and the relation $<$. We can define this function as follows:

$$\begin{aligned} &nat\_to\_prat : nat \to prat \\ &nat\_to\_prat\ x \quad := \quad red\ \frac{x}{\mathcal{O}} \end{aligned}$$

It turns out that this definition fulfills the properties mentioned above. That is, we can say that every natural number can be considered as a rational number. In Coq we define *nat_to_prat* as a coercion. We will also omit the name *nat_to_prat* if the context is clear. The fraction $\frac{x}{\mathcal{O}}$ is already reduced. However, it turns out that it is easier to work with the definition if it includes *red*. Furthermore, including *red* gives us a more general result since the representative could be any other fraction in the set of the rational number as long as it is unique. Recall that $red\ \frac{x}{\mathcal{O}}$ represents the resulting rational number including its corresponding proof.
Landau goes the other direction. He explicitly redefines the natural numbers to be a subset of the rational numbers. To be more explicit, he defines a rational number to be a natural number if there is a fraction of the form $\frac{x}{\mathcal{O}}$ in the set of all equivalent fraction corresponding to this rational number.

4.6 Inverse of Multiplication

Similar to the fractions we have for every rational number X a so called **inverse element X^{-1} for multiplication**. We can also directly define this value.

$$X^{-1} \quad := \quad red\ (rep\ X)^{-1} \tag{4.21}$$

Recall that $()^{-1}$ is overloaded. In contrast to fractions we can state the lemma about the correctness of this operation with an equality $=$ instead of an equivalence $\sim$.

Lemma 4.6.1 (Inverse of Multiplication) $\forall X.\ X^{-1} \cdot X = 1$

In our formalization 1 is a rational number corresponding to the natural number $\mathcal{O}$. We do not explicitly write *nat_to_prat* from Section 4.5.

Proof Let X be given and $\frac{x_1}{x_2} = rep\ X$. We have

$$red\ \left(\frac{x_1}{x_2}\right)^{-1} \cdot \frac{x_1}{x_2} \sim \left(\frac{x_1}{x_2}\right)^{-1} \cdot \frac{x_1}{x_2} \sim \frac{\mathcal{O}}{\mathcal{O}} \tag{4.22}$$

The first equivalence follows from a lemma about fractions, Lemma 4.2.2 and the symmetry of $\sim$. The second equivalence follows from Lemma 3.3.1. Now we have

$$X^{-1} \cdot X = red\left(rep\ X^{-1} \cdot rep\ X\right) = red\left(red\ \left(\frac{x_1}{x_2}\right)^{-1} \cdot \frac{x_1}{x_2}\right) = red\left(\frac{\mathcal{O}}{\mathcal{O}}\right) = \mathcal{O}$$

The third equality follows from 4.22 and Lemma 4.2.3. The fourth equality follows from the definition of *nat_to_prat* in Section 4.5. ∎

Using the definition of $()^{-1}$ we can define an additional operations for two rational numbers X and Y called the **quotient of X and Y**.

$$\frac{X}{Y} \quad := \quad X \cdot Y^{-1} \tag{4.23}$$

Here we use the notation of a fraction representing the quotient of two rational numbers. We can state the property of the quotient in the following lemma.

Lemma 4.6.2 (Correctness of Quotient) $\forall X\ Y.\ X = \frac{X}{Y} \cdot Y$

Proof By the definition of the quotient, associativity of $\cdot$, Lemma 4.6.1 and the identity of $\cdot$ we have

$$\frac{X}{Y} \cdot Y = (X \cdot Y^{-1}) \cdot Y = X \cdot (Y^{-1} \cdot Y) = X \cdot \mathcal{O} = X$$ ∎

4.7 Special Properties of Rational Numbers

Density of $<$ for rational numbers directly follow from density of $<$ for fractions.

Lemma 4.7.1 $\forall X\ Y.\ X < Y \to \exists Z.\ X < Z \wedge Z < Y$

Proof Follows from Lemma 3.4.1. ∎

Lemma 4.7.2 $\forall X\ \exists Y.\ Y < X$.

Proof Follows from Lemma 3.4.2. ∎

We now consider another property of the rational numbers that gives us later the existence of a so called irrational number.

Lemma 4.7.3 ($\sqrt{2}$ does not exist) $\forall X.\ X \cdot X \neq S\ \mathcal{O}$

Proof Let X be given, $X = \frac{x_1}{x_2}$ be its representative and assume $X \cdot X = S\ \mathcal{O}$. We want to have a contradiction. The equality of the rational numbers $X \cdot X$ and $S\ \mathcal{O}$ gives us the equality of their representatives. That is, using the definition of $\cdot$ for rational numbers and fractions,

$$red\ \left(\frac{x_1 \cdot x_1}{x_2 \cdot x_2}\right) = red\ \frac{S\ \mathcal{O}}{\mathcal{O}}$$

This equality gives us the equivalence of the arguments of *red* because of Lemma 4.2.2 and the transitivity of $\sim$. That means, by the definition of $\sim$ and the identity of $\cdot$ for natural numbers

$$x_1 \cdot x_1 = S\ \mathcal{O} \cdot (x_2 \cdot x_2)$$

what gives us a contradiction by Lemma 2.5. ∎

4.8 Minimality

As mentioned at the beginning of this chapter we do not want to have additional numbers that cannot be constructed from *1* and the operations $+$, $\cdot$ and $()^{-1}$. In this section we will prove that this property is fulfilled. Landau does not mention the minimality of the rational numbers. We formulate this lemma with a set P of rational numbers: If P is closed under all operations and P contains *1*, then this set contains every rational number.

Lemma 4.8.1 (Minimality of *prat*)

$$\begin{aligned}
&\forall P.\ P\ \mathcal{O} \rightarrow \\
&\quad (\forall X\ Y.\ P\ X \rightarrow P\ Y \rightarrow P\ (X + Y)) \rightarrow \\
&\quad (\forall X\ Y.\ P\ X \rightarrow P\ Y \rightarrow P\ (X \cdot Y)) \rightarrow \\
&\quad (\forall X.\ P\ X \rightarrow P\ (X^{-1})) \rightarrow \\
&\quad \forall X.\ P\ X
\end{aligned}$$

Proof By induction on x we can prove $\forall x.\ P\ x$. The base case is trivial since $\mathcal{O}$ is in P. We now consider the successor case $S\ x$. Since x and $\mathcal{O}$ are in P by

assumption we have $S\ x = x + \mathcal{O}$ in P.
Every rational number is represented by a reduced fraction $\frac{x_1}{x_2}$. We know

$$\frac{x_1}{x_2} = \frac{x_1}{\mathcal{O}} \cdot \frac{\mathcal{O}}{x_2} = x_1 \cdot x_2^{-1}$$

Since x_1 and x_2 are in P and hence x_2^{-1} is in P we have $\frac{x_1}{x_2}$ in P. ∎

4.9 Remarks

In this chapter we introduced the rational numbers. To avoid the use of the additional assumption *FE* we defined a unique reduced fraction representing the set of all equivalent fractions to this representative. Most of the properties of the rational numbers can be proven with the properties of the fraction introduced in Chapter 3. Until now we could avoid classical assumptions like *XM* for the reason that we can explicitly compute the operations $+$, $\cdot$, $()^{-1}$ and the relation $<$ between two rational numbers. In the next chapter we construct a structure that allows us to construct the real numbers in Coq. From now on we have to assume classical laws.

5 Dedekind Cuts

Until now we were able to construct the natural numbers and the rational numbers without assuming any additional assumption. We will see that we will not be able to construct the real numbers without additional assumptions. In this chapter we consider certain subsets of the rational numbers allowing us to give a definition for the real numbers. These subsets are called **Dedekind cuts**. As already mentioned at the beginning of this thesis there are many other ways to go from the rational numbers to the real numbers. There were already computer scientists constructing the real numbers in Coq using **streams** (Ciaffaglione and Di Gianantonio [5]) or **Cauchy completion** (Geuvers and Niqui [7]). All of these mentioned methods have advantages and disadvantages. We will not say too much about the differences and constructions of Caiffaglione and Di Gianantonio or Geuvers and Niqui regarding the construction based on Dedekind cuts. However, the constructions of Ciaffaglione and Di Gianantonie or Geuvers and Niqui, respectively, have as goal to give a structure for computable reals. We will state and prove theorems about the classical real numbers. We cannot explicitly compute them.
To have an intuition of a Dedekind cut Θ, one can interpret it as

$$\Theta = (0, s) \cap \mathbb{Q}$$

for any $s \in \mathbb{R}^+$.
A Dedekind cut is a subset $\Theta \subset \mathbb{Q}^+$ of the rational numbers with the following properties

$$\exists X.\ X \in \Theta \tag{5.1}$$
$$\exists X.\ X \notin \Theta \tag{5.2}$$
$$\forall X\ Y.\ Y \in \Theta \to X < Y \to X \in \Theta \tag{5.3}$$
$$\forall X.\ X \in \Theta \to \exists Y.\ Y \in \Theta \wedge X < Y \tag{5.4}$$

That is, Θ is nonempty (5.1) and does not contain every rational number (5.2). If we consider a certain $Y \in \Theta$ then every rational number less then this Y is in Θ (5.3). Furthermore Θ does not contain a greatest element (5.4). That is, in addition, for every rational number $X \in \Theta$ there is a rational number $Y \in \Theta$ with $X < Y$. Given an arbitrary Θ we call a rational number $X \in \Theta$ a **lower number of**

Θ and a rational number $X \notin \Theta$ an **upper number of** Θ. We define these cuts in Coq as a type consisting of a predicate $pcut : prat \to Prop$ representing the set and the proofs of the four cut properties mentioned above. Landau introduced cuts the same way but using an alternative version for 5.3. His definition of the third cut property looks as follows.

$$\forall X\ Y.\ X \in \Theta \to Y \notin \Theta \to X < Y \tag{5.5}$$

We can prove that this property follows from the property 5.3. To prove the equivalence, that is, to prove the other direction we would have to assume excluded middle. For this reason we rather take 5.3 as definition and 5.5 as a (provable) lemma.

5.1 Order and Operations

Intuitively we can interpret the relation $\leq$ as $\subseteq$. Recall that $\subseteq$ is not linear. However, because of the properties of cuts, $\subseteq$ induces a linear order for cuts. Following Landau, we define $<$ before $\leq$. Intuitively $\Theta < \Xi$ means that Θ is a subset of Ξ but not the same set. Due to the properties of cuts it suffices to have an X that is in Ξ but not in Θ.

$$\Theta < \Xi \quad := \quad \exists X.\ X \in \Xi \wedge X \notin \Theta \tag{5.6}$$

$$\Theta \leq \Xi \quad := \quad \Theta < \Xi \vee \Theta = \Xi \tag{5.7}$$

We come now to **addition**, **multiplication** and **subtraction** for cuts. We consider $\Theta + \Xi$ as the set of all sums $X + Y$ such that $X \in \Theta$ and $Y \in \Xi$. Furthermore we consider $\Theta \cdot \Xi$ as the set of all products $X \cdot Y$ such that $X \in \Theta$ and $Y \in \Xi$. Finally we have $\Theta - \Xi$ the set of all differences $X - Y$ such that $X \in \Theta$ and $Y \notin \Xi$ but $Y < X$.

$$\Theta + \Xi \quad := \quad \lambda Z.\ \exists X \in \Theta\ \exists Y \in \Xi.\ Z = X + Y \tag{5.8}$$

$$\Theta \cdot \Xi \quad := \quad \lambda Z.\ \exists X \in \Theta\ \exists Y \in \Xi.\ Z = X \cdot Y \tag{5.9}$$

$$\Theta - \Xi \quad := \quad \lambda Z.\ \exists X \in \Theta\ \exists Y \notin \Xi.\ Z = X - Y \qquad \text{if } \Xi < \Theta \tag{5.10}$$

There is no obvious way to avoid the existential quantifiers in these definitions. Hence we do not have the choice to represent cuts with predicates mapping into *bool*. To define the operations above we also have to prove the four properties of cuts. These proofs are straightforward. Notice that $\Theta - \Xi$ can only be a cut if $\Xi < \Theta$ since in the other cases there is no upper number Y of Ξ and a lower number X of Θ with $Y < X$. Furthermore we did not explicitly mention the proof for the difference of X and Y in Definition 5.10.

Lemma 5.1.1 (Correctness of Subtraction) $\forall \Theta\ \Xi.\ \Xi < \Theta \to (\Theta - \Xi) + \Xi = \Theta$

The proof of the correctness is not obvious and needs additional assumptions discussed in Section 5.2.1.

5.2 Additional Assumptions

5.2.1 Excluded Middle

Until now we could avoid assuming excluded middle. In this section we argue the necessity of excluded middle.
The first time we really need the assumption *XM* is trichotomy for $<$ on cuts.

Lemma 5.2.1 (Trichotomy) For all cuts Θ and Ξ we exactly have one of the cases

$$\Theta < \Xi, \quad \Theta = \Xi, \quad \Xi < \Theta$$

Proof Given Θ and Ξ we distinguish two cases: $\exists X.\ X \in \Xi \wedge X \notin \Theta$ and $\neg\exists X.\ X \in \Xi \wedge X \notin \Theta$. The first case gives us $\Theta < \Xi$. Then we consider again two cases: $\exists X.\ X \in \Theta \wedge X \notin \Xi$ and $\neg\exists X.\ X \in \Theta \wedge X \notin \Xi$. The first case gives us $\Xi < \Theta$. Now, we can prove $\Theta = \Xi$. To apply *CE* we have to prove

$$\forall X.\ X \in \Theta \leftrightarrow X \in \Xi$$

We consider an arbitrary X. We only prove one direction because the other one is analogous. We assume $X \in \Theta$ and want to prove $X \in \Xi$. Using *XM* again we have to prove that $X \notin \Xi$ gives us a contradiction. With our assumption $\neg\exists X.\ X \in \Theta \wedge X \notin \Xi$ we have a contradiction since $\exists X.\ X \in \Theta \wedge X \notin \Xi$, namely X itself. ∎

The necessity of *XM*, that is, trichotomy implies *XM* is proven in the script. At this point we only sketch the proof. We assume trichotomy for cuts and want to prove $A \vee \neg A$ for an arbitrary proposition $A \in \mathit{Prop}$. Given A we construct cuts as follows.

$$\Theta := \{\ X \mid X < S\ \mathcal{O} \vee (X < S\ (S\ \mathcal{O}) \wedge A)\ \}$$
$$\Xi := \{\ X \mid X < S\ \mathcal{O} \vee (X < S\ (S\ \mathcal{O}) \wedge \neg A)\ \}$$

The fact that these sets constitute cuts is trivial. If $\Theta = \Xi$ we will have a contradiction. In the other cases we can prove A or $\neg A$, respectively. Due to the decidability of $<$ for rational numbers we can split into different cases $X < S\ \mathcal{O}$ equals *true* or *false*. In Coq this relates to a conditional like mentioned in Section 1.2.
To prove the correctness of subtraction and other theorems for cuts we need the following lemma.

Lemma 5.2.2 $\forall X\ \forall \Theta\ \exists Y\ Z.\ Y \notin \Theta \wedge Z \in \Theta \wedge X = Y - Z$
That is, given an arbitrary rational number X and an arbitrary cut Θ we can write X as the difference of an upper number of Θ and a lower number of Θ.

Since in the proof of this lemma we strictly follow Landau, we only sketch the proof. The detailed proof can be found in the script or in Landau's book. Due to the properties of cuts we have a lower number X_1 of Θ. One can prove without excluded middle that there is a natural number n such that $X_1 + n \cdot X$ is not in Θ. For example consider any upper number $U = \frac{u_1}{u_2}$ of Θ and the representative $\frac{x_1}{x_2}$ of X and take n to be $x_2 \cdot u_1$. At this point Landau uses the (classical) Well-Ordering Principle and takes the least n such that $X_1 + n \cdot X$ is not in Θ. We can now define Y and Z with X_1, X and n. That is, we set $Y = X_1 + n \cdot X$ and $Z = X_1 + (n - 1) \cdot X$. Since we cannot subtract 1 from 1 we have to distinguish the cases $n = 1$ and $1 < n$.

5.2.2 Cut Extensionality

If we take a closer look at the representation of cuts in Coq we can state two problems: The predicate Θ maps into *Prop* instead of *bool*. When it comes to the definitions of the operations for cuts we will see that we have to define Θ mapping into *Prop* instead of *bool* due to existential quantifiers. The other problem is that the four properties for a cut have type *Prop*. Hence we cannot apply *BPI* to show the equality of the proofs of two different cuts as we did with rational numbers and their corresponding proofs.
First we remember that *FE* characterizes equality of functions and *PE* characterizes equality of propositions. In this special situation we consider functions of type $prat \to Prop$. We would like to have the following property characterizing equality of cuts.

$$CE \quad := \quad \forall \Theta\ \Xi.\ (\forall X.\ X \in \Theta \leftrightarrow X \in \Xi) \to \Theta = \Xi \tag{5.11}$$

We call this characterization or assumption **Cut Extensionality**. The attentive reader may have noticed the difference between *FE* and *CE*. While it makes no sense to have an equivalence for arbitrary values yielded by functions we now range over propositions and characterize the equality by the equivalence $\leftrightarrow$. For that *CE* looks like a combination of *FE* and *PE*. We need this for a lot of proofs and we cannot circumvent it. To be sure that we do not assume something contradictory we note that $FE \to PE \to CE$. The interested reader can read this proof in the script. The additional assumption *PI* to prove the equality of the proofs is provable from *PE*. That is, $PE \to PI$. This proof is defined in the standard library of Coq. Because we also can prove *PE* from *CE* we do not need to assume *PI*.

5.3 Rational Numbers as Cuts

We also want to have the rational numbers as a subset of all cuts. Mapping a natural number to a rational number was obvious. We want to map a given rational number X to a set where the least upper bound is X (see also Section 5.5). To be more explicit we have

$$\begin{aligned} &prat\_to\_cut : prat \to cut \\ &prat\_to\_cut\ X \quad := \quad \lambda Y.\ Y < X \end{aligned}$$

This set is obviously a cut: It is not empty (5.1) since for every rational number there is a smaller one (Lemma 4.7.2). The set does not contain every rational number (5.2) since X is not in the set. The third property 5.3 follows from transitivity of $<$. The fourth property 5.4 follows from the fact that there is always a rational number between two other rational numbers (Lemma 4.7.1). We can easily prove

$$\begin{aligned} prat\_to\_cut(\Theta + \Xi) &= prat\_to\_cut\ \Theta + prat\_to\_cut\ \Xi \\ prat\_to\_cut(\Theta - \Xi) &= prat\_to\_cut\ \Theta - prat\_to\_cut\ \Xi \qquad \text{if } \Xi < \Theta \\ prat\_to\_cut(\Theta \cdot \Xi) &= prat\_to\_cut\ \Theta \cdot prat\_to\_cut\ \Xi \\ prat\_to\_cut\left(\frac{\Theta}{\Xi}\right) &= \frac{prat\_to\_cut\ \Theta}{prat\_to\_cut\ \Xi} \\ prat\_to\_cut(\Theta < \Xi) &\leftrightarrow prat\_to\_cut\ \Theta < prat\_to\_cut\ \Xi \end{aligned}$$

That is, the function *prat_to_cut* **respects** the operations $+$, $-$, $\cdot$, taking the quotient and the relation $<$. We call X the **corresponding rational number to** *prat_to_cut* X. Furthermore we do not explicitly write *prat_to_cut* as one can see in the following lemma expressing a further interesting property of *prat_to_cut*.

Lemma 5.3.1 $\forall\Theta\ \forall X.\ X < \Theta \leftrightarrow X \in \Theta$

Proof Let Θ and X be given. First we show $X < \Theta \to X \in \Theta$ and assume $X < \Theta$. That is, there is a Z such that $Z \notin X$ but $Z \in \Theta$. From trichotomy for rational numbers we have $X \leq Z$ because $Z \notin X$. Now from Property 5.3 we know $X \in \Theta$ since $Z \in \Theta$. We now prove $X \in \Theta \to X < \Theta$. We assume $X \in \Theta$. For Property 5.4 there is a rational number $Y \in \Theta$ with $X < Y$. Obviously $Y \notin X$ and hence we have $X < \Theta$. ∎

5.4 Inverse of Multiplication

For an arbitrary cut Θ we also want to define an **inverse element Θ^{-1} for** $\cdot$. This definition is not obvious.

$$\Theta^{-1} \quad := \quad \lambda X.\ \exists Y \notin \Theta.\ Y < X^{-1} \tag{5.12}$$

The interested reader can verify in the script that this set constitutes a cut. The definition is not exactly the same as in Landau's book. In his book he considers all rational numbers of the form $\frac{1}{X}$ where X is not the least upper number of Θ. We consider the inverse itself and not the quotient. We do so for two reasons: We have the equality $\frac{1}{X} = X^{-1}$ and in Coq the formalization of the quotient is much longer than the one of the inverse. Furthermore we consider every rational number X whose inverse is an upper number of Θ but not the least one. This formulation is equivalent to Landau's since $(X^{-1})^{-1} = X$.

Lemma 5.4.1 (Inverse of Multiplication) $\forall \Theta.\ \Theta^{-1} \cdot \Theta = 1$
In our formalization 1 corresponds to $\mathcal{O}$ considered as a cut.

The proof uses many basic transformations and can be read in Landau's book or in the proof script.
Based on the definition of $()^{-1}$ we can define the **quotient of Θ and Ξ** for arbitrary given Θ and Ξ.

$$\frac{\Theta}{\Xi} \quad := \quad \Theta \cdot \Xi^{-1} \tag{5.13}$$

The common property of the quotient is summarized in the following lemma.

Lemma 5.4.2 (Correctness of Quotient) $\forall \Theta\ \Xi.\ \Theta = \frac{\Theta}{\Xi} \cdot \Xi$

The proof is similar to the one of Lemma 4.6.2 using Lemma 5.4.1 and associativity of $\cdot$.

5.5 Least Upper Number

A cut has the special property that it is a nonempty set which has an upper number and the cut itself is downward closed. Recall that an upper number X of a certain cut Θ is a rational number where $X \notin \Theta$. Given an arbitrary subset of the rational numbers P, a rational number X is called an **upper bound** of P if $\forall Y \in P.\ Y \leq X$. Due to the properties of cuts, every upper number is an upper bound and vice versa. Now we want to know if every arbitrary cut Θ has a

least upper number or a **least upper bound**. This is a rational number with the following property.

$$lun\,\Theta\,X \quad := \quad X \notin \Theta \wedge \forall Y \notin \Theta.\, X \leq Y \tag{5.14}$$

We can state an interesting lemma expressing an equivalent formulation for the introduced property above.

Lemma 5.5.1 $\forall\Theta\ \forall X.\ lun\,\Theta\,X \leftrightarrow (\forall Y.\ Y \in \Theta \leftrightarrow Y < X)$

This equivalence is not difficult to prove but a bit tedious in Coq. The interested reader can find the proof in the script. The definition is the more common version of the least upper number but the equivalent formulation allows us to prove the properties of the least upper bound in a very easy way. In Section 5.3 we could embed the rational numbers into cuts. We can state the following lemma.

Lemma 5.5.2 $\forall X.\ lun\,X\,X$
That is, every rational number X is the least upper bound of itself considered as a cut.

Proof Let X be given. By Lemma 5.5.1 we have to show $\forall Y.\ Y \in X \leftrightarrow Y < X$. Let Y be given. The rational number X considered as a cut means $\lambda Y.\ Y < X$. For that we have to prove $Y < X \leftrightarrow Y < X$ which is obviously trivial. ∎

Now we know that every rational number considered as a cut has a least upper bound. Furthermore we know this bound. The question now is whether cuts having a least upper bound always correspond to a rational number.

Lemma 5.5.3 $\forall\Theta\ \forall X.\ lun\,\Theta\,X \rightarrow \Theta = X$
That is, every cut Θ with the least upper bound X corresponds to the rational number X.

Proof Let Θ and X be given and assume $lun\,\Theta\,X$. From Lemma 5.5.1 we have $\forall Y.\ Y \in \Theta \leftrightarrow Y < X$. We can now apply *CE* and we are done. ∎

5.6 Square Root

We come now to an operation for cuts that gives us a unique solution Ξ for the equation $\Xi \cdot \Xi = \Theta$ for an arbitrary Θ. In contrast to the rational numbers such a cut always exists. We call this cut the **square root of** Θ and also write $\sqrt{\Theta}$ representing this cut. We define it as follows.

$$\sqrt{\Theta} \quad := \quad \lambda X.\, X \cdot X \in \Theta \tag{5.15}$$

Proving that this set constitutes a cut is not difficult. To prove the property of the square root we have to state several helping lemmas.

Lemma 5.6.1 $\forall \Theta\ \Xi. \forall X.\ \Theta \cdot \Xi < X \to \exists Y\ Z.\ X = Y \cdot Z \wedge \Theta \leq Y \wedge \Xi \leq Z$

This lemma expresses the following. Given two arbitrary cuts Θ and Ξ and a rational number X where the product of Θ and Ξ is less than X considered as a cut, there are always rational numbers Y und Z with the following property. The product of Y and Z equals X and both Θ is less than or equal to Y and Ξ is less than or equal to Z. The square root has the following property.

Lemma 5.6.2 $\forall \Theta.\ \sqrt{\Theta} \cdot \sqrt{\Theta} = \Theta$

The proofs of these lemmas can be read in Landau's book or in the script since we are strictly following Landau.

5.7 Rational and Irrational Cuts

In Section 5.3 we embedded the rational numbers into cuts and in Section 5.5 we showed that every cut having a least upper bound relates to a rational number and vice versa. We call such cuts **rational**. We are not convinced until now of the existence of a cut that is not rational. That is, is there a cut not having a least upper bound? We would call such a cut **irrational**. In this section we show the existence of such a cut.

Theorem 5.7.1 $\exists \Theta\ \forall X.\ X \neq \Theta$
That is, there is an irrational cut. That is, there is an irrational positive real number.

Proof By Lemma 5.6.2 we know that $\Theta \cdot \Theta = S\ \mathcal{O}$ has a solution for Θ, namely $\sqrt{S\ \mathcal{O}}$. This cut is irrational. If it were rational we would have a contradiction by Lemma 4.7.3. ∎

5.8 Remarks

In this chapter we constructed Dedekind cuts, a structure that represents the last step before we can construct the real numbers. We could not avoid the use of excluded middle since trichotomy for cuts is equivalent to excluded middle. We defined an additional assumption, namely *CE* that characterizes equality for cuts. This assumption is reasonable since we can prove $FE \to PE \to CE$. Because we deal with sets or rather predicates of type $prat \to Prop$ we could not avoid an assumption similar to extensionality. Furthermore in Coq we represent cuts

with a type including proofs of type *Prop* we need proof irrelevance to prove equality of proofs. Since *PI* follows from propositional extensionality *PE* and *PE* gives us a characterization for equality of propositions it suffices to have *PE* as assumption for *CE*. Unfortunately these assumption do not suffice in our construction to define the real numbers with all their properties. We will see that we need something stronger than *XM* that allows us to decide a proposition in a computational function.

6 Real Numbers

In this chapter we consider the real numbers $\mathbb{R}$. At this point we introduce negative numbers and zero.

6.1 Properties of the Real Numbers

The set of the real numbers $\mathbb{R}$ is a complete ordered field. A popular formulation of completeness is the **supremum property**. That is, every bounded subset of the real numbers has a least upper bound. This property is what differentiates the real numbers from the rational numbers. The ordered field properties are summarized below.

$0 \neq 1$		(6.1)
$\forall \epsilon\ \eta.\ \epsilon + \eta = \eta + \epsilon$	Commutativity of $+$	(6.2)
$\forall \epsilon\ \eta\ \zeta.\ (\epsilon + \eta) + \zeta = \epsilon + (\eta + \zeta)$	Associativity of $+$	(6.3)
$\forall \epsilon.\ 0 + \epsilon = \epsilon$	Identity of $+$	(6.4)
$\forall \epsilon\ \exists \epsilon'.\ \epsilon' + \epsilon = 0$	Inverse of $+$	(6.5)
$\forall \epsilon\ \eta.\ \epsilon \cdot \eta = \eta \cdot \epsilon$	Commutativity of $\cdot$	(6.6)
$\forall \epsilon\ \eta\ \zeta.\ (\epsilon \cdot \eta) \cdot \zeta = \epsilon \cdot (\eta \cdot \zeta)$	Associativity of $\cdot$	(6.7)
$\forall \epsilon.\ 1 \cdot \epsilon = \epsilon$	Identity of $\cdot$	(6.8)
$\forall \epsilon.\ \epsilon \neq 0 \to \exists \epsilon'.\ \epsilon' \cdot \epsilon = 1$	Inverse of $\cdot$	(6.9)
$\forall \epsilon\ \eta\ \zeta.\ \epsilon \cdot (\eta + \zeta) = \epsilon \cdot \eta + \epsilon \cdot \zeta$	Distributivity of $+$ and $\cdot$	(6.10)
$\forall \epsilon\ \eta\ \zeta.\ \epsilon \leq \eta \to \eta \leq \zeta \to \epsilon < \zeta$	Transitivity of $\leq$	(6.11)
$\forall \epsilon\ \eta.\ \epsilon \leq \eta \wedge \eta \leq \epsilon \to \epsilon = \eta$	Antisymmetry of $\leq$	(6.12)
$\forall \epsilon\ \eta.\ \epsilon \leq \eta \vee \eta \leq \epsilon$	Linearity of $\leq$	(6.13)
$\forall \epsilon\ \eta\ \zeta.\ \epsilon \leq \eta \to \epsilon + \zeta \leq \eta + \zeta$	Monotonicity of $\leq$ and $+$	(6.14)
$\forall \epsilon\ \eta.\ 0 \leq \epsilon \to 0 \leq \eta \to 0 \leq \epsilon \cdot \eta$		(6.15)

An axiomatization of the real numbers including the properties above is given by Dieudonné in [10]. Dieudonné's axiomatization does not include the supremum property of the real numbers. It contains the equivalent **axiom of nested intervals**. That is, he wants the following property to be satisfied:

We consider an (infinite) sequence of closed intervals $[a_n, b_n]$ where $a_n \leq a_{n+1}$ and $b_{n+1} \leq b_n$ (and of course $a_n \leq b_n$) for all $n \in \mathbb{N}^+$. In Coq we consider sequences of real numbers to be functions of type *nat → real*. We have that the set

$$\bigcap_{n \in \mathbb{N}^+} [a_n, b_n]$$

is nonempty. That is, $\exists \zeta\ \forall n.\ a_n \leq \zeta \wedge \zeta \leq b_n$.
In addition, Dieudonné also mentions the **Archimedean property** for the real numbers: Given two real numbers ϵ and η with $0 \leq \epsilon \wedge 0 \neq \epsilon$ and $0 \leq \eta$, there exists a natural number n such that $\eta \leq n \cdot \epsilon$.

$$AP \quad := \quad \forall \epsilon\ \eta.\ 0 \leq \epsilon \wedge 0 \neq \epsilon \to 0 \leq \eta \to \exists n \in \mathbb{N}^+.\ \eta \leq n \cdot \epsilon$$

We now come to an alternative axiomatization of the real numbers by Harrison [9] including $<$ instead of $\leq$ and the supremum property. He want definitions for

0	: *real*	
1	: *real*	
$<$	: *real → real → Prop*	
$+$	: *real → real → real*	
$-$	: *real → real*	Inverse of $+$
$\cdot$	: *real → real → real*	
$()^{-1}$	: *real → real*	Inverse of $\cdot$

and want the following properties to be satisfied.

$0 \neq 1$		(6.16)
$\forall \epsilon\ \eta.\ \epsilon + \eta = \eta + \epsilon$	Commutativity of $+$	(6.17)
$\forall \epsilon\ \eta\ \zeta.\ (\epsilon + \eta) + \zeta = \epsilon + (\eta + \zeta)$	Associativity of $+$	(6.18)
$\forall \epsilon.\ 0 + \epsilon = \epsilon$	Identity of $+$	(6.19)
$\forall \epsilon.\ -\epsilon + \epsilon = 0$	Inverse of $+$	(6.20)
$\forall \epsilon\ \eta.\ \epsilon \cdot \eta = \eta \cdot \epsilon$	Commutativity of $\cdot$	(6.21)
$\forall \epsilon\ \eta\ \zeta.\ (\epsilon \cdot \eta) \cdot \zeta = \epsilon \cdot (\eta \cdot \zeta)$	Associativity of $\cdot$	(6.22)
$\forall \epsilon.\ 1 \cdot \epsilon = \epsilon$	Identity of $\cdot$	(6.23)
$\forall \epsilon.\ \epsilon \neq 0 \to \epsilon^{-1} \cdot \epsilon = 1$	Inverse of $\cdot$	(6.24)
$\forall \epsilon\ \eta\ \zeta.\ \epsilon \cdot (\eta + \zeta) = \epsilon \cdot \eta + \epsilon \cdot \zeta$	Distributivity of $+$ and $\cdot$	(6.25)
$\forall \epsilon\ \eta.\ \epsilon < \eta \vee \epsilon = \eta \vee \eta < \epsilon$	Trichotomy of $<$	(6.26)
$\forall \epsilon.\ \neg\ \epsilon < \epsilon$	Irreflexivity of $<$	(6.27)

$$\forall \epsilon\ \eta\ \zeta.\ \eta < \zeta \to \epsilon + \eta < \epsilon + \zeta \qquad \text{Monotonicity of } < \text{ and } + \qquad (6.28)$$

$$\forall \epsilon\ \eta.\ 0 < \epsilon \to 0 < \eta \to 0 < \epsilon \cdot \eta \qquad (6.29)$$

At first Harrison considers $()^{-1}$ to be defined for every real number except 0. Recall that we cannot define partial functions in Coq and for that we would need an additional argument (like for subtraction of cuts). Harrison also discusses this issue concerning HOL's functions and the problem of defining subtypes. For that he explicitly gives a multiplicative inverse of 0, namely 0. That is, finally he defines $()^{-1}$ to be total on $\mathbb{R}$.
At this point Harrison discusses the existence of the supremum for a nonempty subset R of the real numbers that is bounded from above. Given R and ϵ, the predicate ub holds if every real number in R is less than or equal to ϵ, i.e. ϵ is an upper bound of R. The supremum property says that every subset of the real numbers that is bounded from above has a least upper bound.

$$ub\ R\ \epsilon \quad := \quad \forall \eta \in R.\ \eta < \epsilon \vee \eta = \epsilon$$

$$\forall R \subseteq \mathbb{R}.\ R \neq \emptyset \to (\exists \epsilon.\ ub\ R\ \epsilon) \to \exists \zeta.\ ub\ R\ \zeta \wedge \forall \eta.\ ub\ R\ \eta \to \zeta < \eta \vee \zeta = \eta$$

6.2 Constructing the Real Numbers

We consider the cuts introduced in Chapter 5 to be the positive real numbers. For every positive rational number ϵ we introduce a negative real number, namely $-\epsilon$. Furthermore we define a special real number $\mathcal{Z}$ representing the zero. To be more explicit, in Coq we have

```
Inductive real : Type :=
| Z : real
| P : cut -> real
| N : cut -> real.
```

The constructors $\mathcal{P}$ and $\mathcal{N}$ yield either a positive real numbers or a negative real number to a given cut.

6.3 Order and Operations

It turns out that defining the relation $<$ is relatively easy since we can directly reduce $<$ for reals to $<$ for cuts in special cases. We define

$$\mathcal{N}\ \Theta < \mathcal{N}\ \Xi \quad := \quad \Xi < \Theta \qquad (6.30)$$

$$\mathcal{N}\ \Theta < \mathcal{P}\ \Xi \quad := \quad \mathit{True} \qquad (6.31)$$

$$\mathcal{N}\ \Theta < \mathcal{Z} \quad := \quad \mathit{True} \tag{6.32}$$
$$\mathcal{Z} < \mathcal{N}\ \Xi \quad := \quad \mathit{False} \tag{6.33}$$
$$\mathcal{Z} < \mathcal{Z} \quad := \quad \mathit{False} \tag{6.34}$$
$$\mathcal{Z} < \mathcal{P}\ \Xi \quad := \quad \mathit{True} \tag{6.35}$$
$$\mathcal{P}\ \Theta < \mathcal{N}\ \Xi \quad := \quad \mathit{False} \tag{6.36}$$
$$\mathcal{P}\ \Theta < \mathcal{Z} \quad := \quad \mathit{False} \tag{6.37}$$
$$\mathcal{P}\ \Theta < \mathcal{P}\ \Xi \quad := \quad \Theta < \Xi \tag{6.38}$$

and can easily prove **trichotomy** for $<$ on $\mathbb{R}$ with trichotomy for $<$ on cuts and a case analysis or a *destruct* tactic on ϵ and η using the inductive definition.

Lemma 6.3.1 (Trichotomy) For all real numbers ϵ and η we exactly have one of the cases

$$\epsilon < \eta, \quad \epsilon = \eta, \quad \eta < \epsilon$$

Furthermore we define $\leq$ as follows.

$$\epsilon \leq \eta \quad := \quad \epsilon < \eta \vee \epsilon = \eta \tag{6.39}$$

As it comes to **addition** and **subtraction** for real numbers we have more work to do. We will discuss these operations in Section 6.5.
Defining **multiplication** is again straightforward since we can have a case analysis on ϵ and η.

$$\mathcal{Z} \cdot \eta \quad := \quad \mathcal{Z} \tag{6.40}$$
$$\epsilon \cdot \mathcal{Z} \quad := \quad \mathcal{Z} \qquad \text{if } \eta \neq \mathcal{Z} \tag{6.41}$$
$$\mathcal{P}\ \Theta \cdot \mathcal{P}\ \Xi \quad := \quad \mathcal{P}\ (\Theta \cdot \Xi) \tag{6.42}$$
$$\mathcal{N}\ \Theta \cdot \mathcal{N}\ \Xi \quad := \quad \mathcal{P}\ (\Theta \cdot \Xi) \tag{6.43}$$
$$\mathcal{N}\ \Theta \cdot \mathcal{P}\ \Xi \quad := \quad \mathcal{N}\ (\Theta \cdot \Xi) \tag{6.44}$$
$$\mathcal{P}\ \Theta \cdot \mathcal{N}\ \Xi \quad := \quad \mathcal{N}\ (\Theta \cdot \Xi) \tag{6.45}$$

6.4 Strong Trichotomy

We define a stronger version of trichotomy for cuts and refer to it as **strong trichotomy**.

$$\mathit{STR} \quad := \quad \forall \Theta\ \Xi\ \Phi.\ \{\ \Theta < \Xi\ \}\ +\ \{\ \Theta = \Xi\ \}\ +\ \{\ \Xi < \Theta\ \} \tag{6.46}$$

One can interpret $+$ above as $\vee$ with the difference that *STR* has type *Type* instead of *Prop*. This fact allows us a case analysis within definitions. Using the assumption of **strong excluded middle** of type *Type*

$$\mathit{SXM} \quad := \quad \forall X : \mathit{Prop}.\ \{\ X\ \}\ +\ \{\sim X\ \} \tag{6.47}$$

we can prove *STR*. Instead of assuming *SXM* and proving *STR* we just assume *STR* in the rest of our construction. The necessity of *STR* as additional assumption is discussed in Section 6.5. Furthermore we have $STR \to SXM$.

6.5 Addition and Subtraction

We now argue the necessity of *STR* as additional assumption. We want addition to have the following three properties

$$\forall \Theta\ \Xi.\ \Theta < \Xi \to \mathcal{P}\ \Theta + \mathcal{N}\ \Xi = \mathcal{N}\ (\Xi - \Theta)$$
$$\forall \Theta\ \Xi.\ \Theta = \Xi \to \mathcal{P}\ \Theta + \mathcal{N}\ \Xi = \mathcal{Z}$$
$$\forall \Theta\ \Xi.\ \Xi < \Theta \to \mathcal{P}\ \Theta + \mathcal{N}\ \Xi = \mathcal{P}\ (\Theta - \Xi)$$

We assume we have addition with these properties. From this we can easily define *STR* by a case analysis on $\mathcal{P}\ \Theta + \mathcal{N}\ \Xi$ and trichotomy for cuts. That is, *STR* is a necessary assumption for addition of real numbers. The details can be found in the script. Note that strong trichotomy (for cuts) gives us a strong trichotomy principle for real numbers.
After having assumed *STR* defining **addition** and **subtraction** for real numbers becomes easy. First we define addition.

$$\epsilon + \mathcal{Z} := \epsilon \tag{6.48}$$
$$\mathcal{Z} + \eta := \eta \quad \text{if } \eta \neq \mathcal{Z} \tag{6.49}$$
$$\mathcal{N}\ \Theta + \mathcal{N}\ \Xi := \mathcal{N}\ (\Theta + \Xi) \tag{6.50}$$
$$\mathcal{P}\ \Theta + \mathcal{P}\ \Xi := \mathcal{P}\ (\Theta + \Xi) \tag{6.51}$$
$$\mathcal{P}\ \Theta + \mathcal{N}\ \Xi := \mathcal{Z} \quad \text{if } \Theta = \Xi \tag{6.52}$$
$$\mathcal{P}\ \Theta + \mathcal{N}\ \Xi := \mathcal{N}\ (\Xi - \Theta) \quad \text{if } \Theta < \Xi \tag{6.53}$$
$$\mathcal{P}\ \Theta + \mathcal{N}\ \Xi := \mathcal{P}\ (\Theta - \Xi) \quad \text{if } \Theta > \Xi \tag{6.54}$$
$$\mathcal{N}\ \Theta + \mathcal{P}\ \Xi := \mathcal{P}\ \Xi + \mathcal{N}\ \Theta \tag{6.55}$$

Because we now have negative numbers we can define for every real number ϵ the **inverse element** $-\epsilon$ **of** $+$ as follows.

$$-\mathcal{Z} := \mathcal{Z} \tag{6.56}$$
$$-\mathcal{P}\ \Theta := \mathcal{N}\ \Theta \tag{6.57}$$
$$-\mathcal{N}\ \Theta := \mathcal{P}\ \Theta \tag{6.58}$$

We will see that we reduce subtraction for real numbers to addition of two real numbers using this inverse element. The operator $-$ becomes overloaded and

stands for either subtraction or taking the inverse element for addition. The context will always be clear and there should not be any confusion since the subtraction operator is binary and the operator taking the inverse is unary.

Lemma 6.5.1 (Inverse of Addition) $\forall \epsilon.\ -\epsilon + \epsilon = 0$

In our formalization 0 is a real number corresponding to $\mathcal{Z}$. The proof of this lemma is straightforward by definition of $-$, a case analysis for ϵ and the definition of $+$. We are now able to define subtraction in a quite easy way.

$$\epsilon - \eta \quad := \quad \epsilon + (-\eta) \tag{6.59}$$

The correctness of subtraction is proven below.

Lemma 6.5.2 (Correctness of Subtraction) $\forall \epsilon\ \eta.\ \epsilon = (\epsilon - \eta) + \eta$

Proof Given arbitrary real numbers ϵ and η, we have

$$(\epsilon - \eta) + \eta = (\epsilon + (-\eta)) + \eta = \epsilon + (-\eta + \eta) = \epsilon + \mathcal{Z} = \epsilon$$

The first equality follows from the definition of subtraction, the second equality from associativity (which we did not prove explicitly in this section), the third equality follows from Lemma 6.5.1 and the last equality follows from the definition of $+$ (6.48). ∎

6.6 Inverse of Multiplication

Defining the **inverse element** ϵ^{-1} **for** $\cdot$ for an arbitrary real number ϵ brings up the problem of dividing through zero 0 or $\mathcal{Z}$, respectively. We could procrastinate dealing with 0 until now. Similar to the definition of subtraction for natural numbers or rational numbers we require an additional argument, a proof that the second operand is not 0. We define the inverse for multiplication as below.

$$(\mathcal{P}\ \Theta)^{-1} \quad := \quad \mathcal{P}\ \Theta^{-1} \tag{6.60}$$

$$(\mathcal{N}\ \Theta)^{-1} \quad := \quad \mathcal{N}\ \Theta^{-1} \tag{6.61}$$

We constructed the real numbers in a way we can directly decide whether a given real number is $\mathcal{Z}$ or not. We call this function *neq_zero* and also write $\neq_b 0$ instead.

$$\mathcal{Z} \neq_b 0 \quad := \quad \mathit{false} \tag{6.62}$$

$$\epsilon \neq_b 0 \quad := \quad \mathit{true} \qquad \text{if } \epsilon \neq \mathcal{Z} \tag{6.63}$$

Defining this predicate mapping into *bool* allows us to use the same method like mentioned in Section 2.2. To be more explicit, in Coq we have the following.

```
Definition inv_mul_real (x:real) : neq_zero x -> real := match x with
| Z => fun (l : neq_zero Z) => match l with end
| P a => fun _ => P (inv_cut a)
| N a => fun _ => N (inv_cut a)
end.
```

At this point we also state the main property of the inverse for real numbers.

Lemma 6.6.1 (Inverse of Multiplication) $\forall \epsilon.\ \epsilon \neq_b 0 \to \epsilon^{-1} \cdot \epsilon = 1$

The number 1 corresponds to the cut $\mathcal{O}$. Here a case analysis on ϵ, the definition of $\cdot$ and Lemma 5.4.1 gives us the proof.
For Harrison's axiomatization we need $()^{-1}$ to be defined for every real number. Hence we add the defining equation

$$\mathcal{Z}^{-1} \quad := \quad \mathcal{Z} \tag{6.64}$$

and adapt the Coq definition to have type $real \to real$ as follows.

```
Definition inv_mul_real' (x:real) : real := match x with
| Z => Z
| P a => P (inv_cut a)
| N a => N (inv_cut a)
end.
```

Defining the **quotient for ϵ and η** is analogous to the previous chapters. Here we will again use $()^{-1}$ with the additional argument that the operand is not zero.

$$\frac{\epsilon}{\eta} \quad := \quad \epsilon \cdot \eta^{-1} \qquad \text{if } \eta \neq_b 0 \tag{6.65}$$

Lemma 6.6.2 (Correctness of Quotient) $\forall \epsilon\ \eta.\ \eta \neq_b 0 \to \frac{\epsilon}{\eta} \cdot \eta = \epsilon$

Again, the proof is is trivial using associativity of $\cdot$, Lemma 6.6.1 and the identity for $\cdot$.

6.7 From Cuts to Real Numbers

At the beginning of this chapter in Section 6.2 we already mentioned that we consider the cuts to be the positive real numbers and we gave them a special constructor $\mathcal{P}$ yielding this positive real number. We also declare this function or constructor $\mathcal{P}$ as a coercion.

$$cut\_to\_real : cut \to real$$
$$cut\_to\_real \quad := \quad \mathcal{P}$$

Since every operation for two positive real numbers reduce to the corresponding operation for cuts it is not necessary to explicitly prove that *cut_to_real* respects the operations $+$, $-$, $\cdot$, taking the quotient and the relation $\leq$ or $<$, respectively.

6.8 Completeness

As we already mentioned there are different formulations of the completeness property of the real numbers. We introduced the supremum property and the axiom of nested intervals. Landau gives a theorem we discuss in the next section. To argue about sets P and Q of real numbers we introduce the following notations.

$$P < Q \quad := \quad \forall \epsilon\ \eta.\ \epsilon \in P \to \eta \in Q \to \epsilon < \eta \tag{6.66}$$

$$P \neq \emptyset \quad := \quad \exists \epsilon.\ \epsilon \in P \tag{6.67}$$

$$P \cup Q = \mathbb{R} \quad := \quad \forall \epsilon.\ \epsilon \in P \vee \epsilon \in Q \tag{6.68}$$

6.8.1 Dedekind's Fundamental Theorem

We now introduce a special property for the real numbers that is called **Dedekind's Fundamental Theorem**. It says the following.

Theorem 6.8.1 (Dedekind's Fundamental Theorem) We consider any nontrivial partition of the real numbers, that is, two connected nonempty subsets P and Q of the real numbers with $P \cup Q = \mathbb{R}$ and $P < Q$. There is a unique real number ζ such that every real number ϕ less than ζ is in P and every real number ϕ where ζ is less than ϕ is in Q. Notice that P and Q are disjoint due to $P < Q$.

$$\begin{aligned} DF \quad := \quad & \forall P\ Q.\ P \neq \emptyset \to Q \neq \emptyset \to P \cup Q = \mathbb{R} \to P < Q \\ & \to \exists \zeta\ \forall \phi.\ (\phi < \zeta \to \phi \in P) \wedge (\zeta < \phi \to \phi \in Q) \end{aligned}$$

Note that DF does not include the uniqueness of the candidate ζ. However, we could easily state and prove it.

6.8.2 Tarski's Fundamental Theorem

A similar property of the real numbers called the **Law of Continuity** is formulated below given by Tarski [16]. Due to the analogy to Dedekind's Fundamental Theorem we refer to it as **Tarski's Fundamental Theorem**.

Theorem 6.8.2 (Tarski's Fundamental Theorem) We consider two subsets P and Q of the real numbers with the property $P < Q$. There is a real number ζ with the following property. If we consider arbitrary real numbers $\epsilon \in P$ and $\eta \in Q$ both different from ζ, we have ζ between ϵ and η.

$$\begin{aligned} TF \quad := \quad & \forall P\ Q.\ P < Q \\ & \to \exists \zeta\ \forall \epsilon\ \eta.\ \epsilon \in P \to \eta \in Q \to \epsilon \neq \zeta \to \eta \neq \zeta \to \epsilon < \zeta \wedge \zeta < \eta \end{aligned}$$

The main differences to DF are that P and Q do not have to include every real number and there is no restriction about the emptiness of P and Q.

6.8.3 Proofs of Fundamental Theorems

To prove Dedekind's Fundamental Theorem in Coq we diverge a bit from Landau. We state a more general theorem that allows us to prove both Dedekind's and Tarski's Fundamental Theorem.

Lemma 6.8.3 We consider two nonempty subsets P and Q of the real numbers with the property $P < Q$. There is a real number ζ such that every real number less than ζ is not in Q and every real number ϕ where ζ is less than ϕ is not in P.

$$\forall P\ Q.\ P \neq \emptyset \to Q \neq \emptyset \to P < Q \\ \to \exists \zeta\ \forall \phi.\ (\phi < \zeta \to \phi \notin Q) \wedge (\zeta < \phi \to \phi \notin P)$$

The proof of this lemma is similar to Landau's proof of Dedekind's Fundamental Theorem. Using *XM* we distinguish the cases whether P contains a positive or Q contains a negative real number. If both are not the case the candidate for ζ is $\mathcal{Z}$. We only consider the case that P contains a positive real number. We construct the following set Ξ.

$$\Xi \quad := \quad \lambda X.\ \exists \epsilon \in P.\ X < \epsilon$$

It is not difficult to prove that this set constitutes a cut. We choose ζ to be the corresponding real number to Ξ.
Landau defines Ξ in a different way. He considers every rational number X in P which is not the least one if one exists. Hence he has the restriction $X \in P$. If $P \cup Q = \mathbb{R}$ this definition is equivalent to Landau's. Otherwise, Landau's set is not necessarily a cut.
We have to prove $(\phi < \zeta \to \phi \notin Q) \wedge (\zeta < \phi \to \phi \notin P)$. We only consider $\phi < \zeta \to \phi \notin Q$ since the proof of the other side is similar. We assume $\phi < \zeta$ and $\phi \in Q$. From certain lemmas and a case analysis we know that there is rational number X with $\phi < X < \zeta$. Since $X < \zeta = \Xi$ we have $X \in \Xi$. By the definition of Ξ we have a real number $\epsilon \in P$ with $X < \epsilon$. Now we have $\phi < \epsilon$ from transitivity of $<$. Because of $P < Q$, $\epsilon \in P$ and $\phi \in Q$ we have $\epsilon < \phi$ in contradiction to $\phi < \epsilon$. The detailed proof can be found in the script.

Proof (Dedekind's Fundamental Theorem) Let P and Q be given. We assume the premisses from *DF*. In contrast to the general lemma we additionally assume $P \cup Q = \mathbb{R}$. We consider the ζ from Lemma 6.8.3. We have to prove $(\phi < \zeta \to \phi \in P) \wedge (\zeta < \phi \to \phi \in Q)$. We only prove the left side $\phi < \zeta \to \phi \in P$ since the proof of the other side is similar. We assume $\phi < \zeta$. From the properties of ζ in Lemma 6.8.3 we have $\phi \notin Q$. By our assumption $P \cup Q = \mathbb{R}$ we are done since $\phi \in Q$ yield a contradiction. ∎

Proof (Tarski's Fundamental Theorem) To prove *TF* we need a case analysis on whether P or Q are empty. That is, we need *XM* to distinguish these cases. If one of them is empty every rational number ζ does the job since $\epsilon \in P$ or $\eta \in Q$ as premiss gives us a contradiction. Hence we consider P and Q to be nonempty and we can use the ζ from Lemma 6.8.3. We assume the premisses in the lemma and want to prove $\epsilon < \zeta \wedge \zeta < \eta$. We only prove $\epsilon < \zeta$ since the proof of the other side is similar. Using trichotomy for ϵ and ζ we consider three cases where $\epsilon < \zeta$ is exactly what we want. In the case $\epsilon = \zeta$ we have a contradiction to $\epsilon \neq \zeta$ and in the case $\zeta < \epsilon$ we have $\epsilon \notin P$ from the properties of ζ in Lemma 6.8.3 and have a contradiction to $\epsilon \in P$. ∎

6.8.4 Other Completeness Formulations

In this section we discuss how we can get the other formulations of the completeness property assuming Dedekind's Fundamental Theorem. The interested reader can find the detailed proofs in the script.

Supremum

To prove the supremum property, given a nonempty set R that is bounded from above, we give definitions for P and Q. The candidate we get from the Fundamental Theorem is the desired supremum. We define

$$\begin{aligned} P &:= \lambda\epsilon.\ \exists\eta \in R.\ \epsilon < \eta \\ Q &:= \lambda\epsilon.\ \neg\ \exists\eta \in R.\ \epsilon < \eta \end{aligned}$$

Axiom of Nested Intervals

To prove the axiom of nested intervals, given a sequence $[a_n, b_n]$ of real number, we define

$$R := \lambda\epsilon.\ \exists n.\ \epsilon < a_n$$

This set is nonempty and has an upper bound, for example b_0. Hence from the supremum property we have a least upper bound. This bound will also be in the set

$$\bigcap_{n\in\mathbb{N}} [a_n, b_n]$$

6.8.5 Archimedean Property

We already mentioned the Archimedean property of the real numbers. This property does not express the completeness property of the real numbers. However,

it is provable from the completeness property.
To prove it, we define $\mathbb{N}^+$ to be a subset of the real numbers by a predicate of type *real* → *Prop*.

$$\mathbb{N}^+ \quad := \quad \lambda\epsilon.\ \exists n.\ \epsilon = \underbrace{1 + \cdots + 1}_{n \text{ times}}$$

To prove the Archimedean property we first prove that $\mathbb{N}^+$ is unbounded.

Lemma 6.8.4 ($\mathbb{N}^+$ is unbounded) $\forall\epsilon\ \exists\eta \in \mathbb{N}^+.\ \epsilon < \eta$

Proof We assume $\mathbb{N}^+$ is bounded. From the supremum property we have a least upper bound ζ. We know that there is a natural number n with $\zeta - 1 < n$ (if not, $\zeta - 1$ would be an upper bound of $\mathbb{N}^+$ that is less than the least upper bound). Because $\mathbb{N}^+$ is inductively defined we know $n + 1$ is in $\mathbb{N}^+$. We have $\zeta < n + 1$ in contradiction to ζ being an upper bound of $\mathbb{N}^+$. ∎

Proof (Archimedean property) Let two real numbers ϵ and η with $0 \le \epsilon \wedge 0 \ne \epsilon$ and $0 \le \eta$ be given. Since $\mathbb{N}^+$ is not bounded we can find a natural numbers n with

$$\frac{\eta}{\epsilon} \le n$$

such that $\eta \le n \cdot \epsilon$. ∎

6.9 Remarks

In this chapter we constructed the real numbers based on Dedekind cuts. Defining $<$ and multiplication $\cdot$ did not require additional assumptions. For the operations addition $+$ and hence subtraction we needed a stronger version of trichotomy for cuts, namely *STR*, to have a case analysis within the definition. Furthermore we introduced negative numbers and a zero. Hence we had to pay attention defining the inverse of multiplication regarding dividing through zero. Finally we considered the fundamental theorem expressing a very important property of the real numbers. In the end we could construct the real numbers from the assumptions *CE* and *STR* since *XM* can be proven from *STR*.

7 Conclusion

7.1 Differences to Landau

The first time we diverged from Landau's construction was that we did not assume the Peano axioms. Due to the underlying Calculus of Constructions we could easily prove the axioms. We also diverged from Landau's definition concerning the relation $\leq$. While Landau defined the relation $<$, $\leq$, $>$ and $\leq$ independently we defined them as special notations of $\leq$. Furthermore we defined $\leq$ recursively instead of using addition. Hence many proofs became different from Landau's. We also defined the function *first* giving us a constructive version of the Well-Ordering Principle that allowed us to avoid excluded middle as assumption.
Another time we fundamentally diverged from Landau was the definition of the rational numbers. While Landau explicitly defined the rational numbers to be sets of equivalent fraction we represent such a set by a unique representative, namely the reduced fraction. We could reuse the function *first* to compute the reduced fraction without additional algorithms like the Euclidean algorithm.
A further time we diverge from Landau is the definition of the properties of cuts. We have chosen an equivalent version of the third property of cuts.
Concerning the real numbers and the fundamental theorem we stated a more general theorem that allowed us to prove both Dedekind's and Tarski's Fundamental Theorem.

7.2 Assumptions

7.2.1 Excluded Middle

In Coq and the Calculus of Inductive Constructions we could define the natural numbers without assuming excluded middle The only time we needed it were in the Well-Ordering Principle *WP*. We were able to prove $XM \leftrightarrow WP$. Since our collection of the properties of the natural numbers does not include *WP*, we could avoid excluded middle.
As it came to (positive) rational numbers there was no need of excluded middle because we could decide the relation $\leq$ for rational numbers as for natural num-

bers. That is, we could define ≤ mapping into *bool* instead of *Prop*.
Nevertheless it was not possible to avoid assuming excluded middle in the construction of the real numbers. Working with Dedekind cuts required classical logic. We could prove the equivalence between *XM* and trichotomy for cuts. That is, there is no construction of cuts that gives us trichotomy only from intuitionistic laws without assuming classical laws in advance. Since we used Dedekind cuts to construct the real numbers their structure is also classical.

7.2.2 Other Assumptions

In the construction of the different number systems we also needed additional assumptions besides excluded middle. For the natural numbers we did not need any additional assumption. Since we represent rational numbers by a unique representative, i.e. a reduced fraction instead of sets of equivalent fractions we did not need an extensionality characterizing equality for sets, predicates or functions, respectively.
There was no obvious way to represent Dedekind cuts in another way than sets or predicates of type $prat \to Prop$. In addition to classical assumptions we had to assume some extensionality characterizing the equality of cuts, namely *CE*. The assumption *CE* was provable from Functional Extensionality *FE* and Propositional Extensionality *PE*, i.e. $FE \to PE \to CE$. The necessary assumption *PI* to prove the equality of the proofs of the cut properties can be proven from *PE*. That is, $PE \to PI$. Furthermore, we could prove $CE \to PE$. Hence the reasonable assumption *CE* gives us Proof Irrelevance. Defining the real numbers and addition for them required a further assumption. We defined strong trichotomy *STR* corresponding to trichotomy for cuts and $<$ of type *Type*. With this assumption we could easily define addition for real numbers. If we assume having addition for real numbers with certain properties we can prove *STR*. That is, strong trichotomy for cuts and $<$ is a necessary assumption. We could also prove $SXM \leftrightarrow STR$ where *SXM* corresponds to *XM* of type *Type*, a stronger version of excluded middle.

Bibliography

[1] The Coq Proof Assistant. http://coq.inria.fr/. Accessed: 21/03/2011.

[2] Yves Bertot and Pierre Castéran. *Interactive Theorem Proving and Program Development. Coq'Art: The Calculus of Inductive Constructions*. Texts in Theoretical Computer Science. An EATCS Series. Springer, 2004.

[3] Chad E. Brown. Faithful Reproductions of the Automath Landau Formalization. 2011. Submitted.

[4] Jawahar Chirimar and Douglas J. Howe. Implementing constructive real analysis: Preliminary report. In *Constructivity in Computer Science, Summer Symposium*, pages 165–178, London, UK, 1992. Springer-Verlag.

[5] Alberto Ciaffaglione and Pietro Di Gianantonio. A co-inductive approach to real numbers. In *Selected papers from the International Workshop on Types for Proofs and Programs*, TYPES '99, pages 114–130, London, UK, 2000. Springer-Verlag.

[6] Robert L. Constable, Stuart F. Allen, S. F. Allen, H. M. Bromley, W. R. Cleaveland, J. F. Cremer, R. W. Harper, Douglas J. Howe, T. B. Knoblock, N. P. Mendler, P. Panangaden, Scott F. Smith, James T. Sasaki, and S. F. Smith. Implementing mathematics with the nuprl proof development system, 1986.

[7] Herman Geuvers and Milad Niqui. Constructive Reals in Coq: Axioms and Categoricity. In *Selected papers from the International Workshop on Types for Proofs and Programs*, TYPES '00, pages 79–95, London, UK, 2002. Springer-Verlag.

[8] M. J. C. Gordon and T. F. Melham. *Introduction to HOL: A theorem proving environment for higher order logic*. Cambridge University Press, 1993.

[9] John Harrison. *Theorem Proving with the Real Numbers*. Springer-Verlag, 1998.

[10] Jean Dieudonné. *Foundation of Modern Analysis*. Academic Press Inc., New York, 1960.

[11] Claire Jones. Completing the rationals and metric spaces in lego. In *Papers presented at the second annual Workshop on Logical environments*, pages 297–316, New York, NY, USA, 1993. Cambridge University Press.

[12] L.S. van Benthem Jutting. *Checking Landau's "Grundlagen" in the AUTOMATH System*. PhD thesis, Eindhoven University of Technology, 1977.

[13] Edmund Landau. *Grundlagen der Analysis*. Leipzig, 1930.

[14] Giuseppe Peano. Arithmetices principia, nova methodo exposita. Turin, 1889. Translated in [17], pp. 83–97.

[15] Gert Smolka and Chad E. Brown. Introduction to Computational Logic, 2010. Lecture notes.

[16] Alfred Tarski. *Introduction to Logic and to the Methodology of the Deductive Sciences*. Oxford University Press, 1994. Edited by Jan Tarski, originally 1946.

[17] Jean van Heijenoort, editor. *From Frege to Gödel: A Source Book in Mathematical Logic, 1879–1931*. Source Books in the History of the Sciences. Harvard University Press, 2002.