A Natural Language Formalization of Perfectoid Rings in ℕaproche

Peter Koepke
University of Bonn

March 16, 2025

Abstract

The formalization of P. Scholze's *perfectoid spaces* [8] in the Lean proof assistant [6] by K. Buzzard, J. Commelin, and P. Massot [1] is a milestone in bringing formal mathematics closer towards leading research-level mathematics. The Lean formalization, however, is not "readable" by mathematicians, since Lean resembles - and indeed is - a programming language for building proofs from proof commands.

The ℕaproche proof system [2], in contrast, accepts and checks readable texts written in a (controlled) natural mathematical language, with natural proof structurings. In this article we present a ℕaproche formalization of perfectoid *rings* which are main components of perfectoid spaces. We partly follow the structure of the mentioned Lean formalization. Our formalization can be loaded into Isabelle 2024 (see [4]) which then automatically calls the ℕaproche proof checking component of the Isabelle distribution.

Contents

Introduction

We define *perfectoid rings* in the proof assistant ℕaproche [2] with the intention to closely approximate the mathematical *language* of Definition 3.1 of P. Scholze's [9]:

> **Definition 3.1** A Tate ring R is perfectoid if R is complete, uniform, i.e. $R^o \subset R$ is bounded, and there exists a pseudo-uniformizer $\varpi \in R$ such that $\varpi^p | p$ in R^o and the Frobenius map
>
> $$\Phi : R^o/\varpi \to R^o/\varpi^p : x \mapsto x^p$$
>
> is an isomorphism.

ℕaproche (for Natural Proof Checking) uses the (extendible) controlled natural language ForTheL (Formula Theory Language) as its input language (see also [7]) which is a subset of LaTeX. ℕaproche can be viewed as a system that transforms ForTheL statements into proof tasks that are sent out to an external automated theorem prover (ATP). In this article we mostly use the E first-order prover [10] but also Vampire [11]. A ForTheL text is correct if all generated proof tasks can be discharged automatically.

In our formalization, the (LaTeX rendering of the) definition of perfectoid ring reads:

> **Definition 293.** R is perfectoid iff R is complete and uniform and there exists a pseudouniformizer ϖ of R such that $\varpi^{p,R} | p^{[R]}$ in R^o within R and
>
> $$\Phi^R : R^o/\varpi \cong R^o/\varpi^{p,R}.$$

Such a definition requires a long chain of intermediate definitions and propositions, starting from first principles. The formalization is logically self-contained; theories about sets, functions, natural numbers, groups, rings, and topology are developed as far as required for the intermediate and final definitions. Ideally foundational theories would be provided by some library but the existing libraries and library mechanisms in ℕaproche are still rudimentary.

We make several simplifying assumptions: all groups will be commutative and written additively; rings will be commutative containing a one. We circumvent some "higher" constructions like quotients of rings, and express a property like

$$\Phi : R^o/\varpi \cong R^o/\varpi^p$$

via congruences mod ϖ and mod ϖ^p, respectivly.

This text is written as a file `perfectoidrings.ftl.tex` in the LaTeX dialect of ℕaproche and typeset by pdf-LaTeX. The formal parts

are printed on a grey background. Everything else is interpreted as "literate" commentary that is not subject to the logical checking by the system. `perfectoidrings.ftl.tex` can be checked in the ℕaproche program by opening the file in Isabelle generic proof assistant [4]. ℕaproche proof checking constitutes a major computational process: each statement generates several first-order proof tasks each of which can take several seconds of ATP proving. To check the whole document takes about half an hour on older laptop, depending on the available processing power.

Part I
Preliminaries

Our formalization takes place in a familiar mathematical environment. ℕaproche supports standard proof arguments whilst avoiding explicit and tedious foundational subleties. Nevertheless, ℕaproche is a formal system and the logical foundations have to be set up unambiguously and consistently.

Initially the environment contains mathematical *objects* and collections of objects, called *classes*. Classes can be formed as abstraction terms $\{x \mid \phi\}$ where ϕ is a mathematical statement about the variable x. Classes which are objects themselves are *sets*. Similarly, *maps* send object to objects, and a *function* is a map which is an object. Some basic theory of sets and functions is built into ℕaproche. Further properties are postulated axiomatically in the next section. Later we shall introduce more types of objects like numbers or structures by **Signature**, **Definition** and **Axiom** commands.

We do not require all mathematical objects to be sets. Natural numbers, e.g., are introduced as objects of type "natural number" and characterized by arithmetical axioms. This correponds to widespread intuitions that numbers are "atomic" objects. Technically this may help to focus proof search on the domains under consideration.

For convenience we also state some obvious axioms which with some effort could be proved as lemmas. Other axioms are used to define classes of structures like groups or topological spaces. Finally we use axioms for inductive definitions of data types and functions, since we do not have definition mechanisms by recursion.

We start now by expanding our mathematical language by some singular/plural pairs (vocabulary) and some alternative phrases for mathematical properties (macros). These are imported as library files which contain ℕaproche commands of the form

```
[synonym number/-s]
```

and

```
Let $x$ and $y$ are distinct stand for $x \neq y$.
```

respectively:

[readtex meta-inf/source/vocabulary.ftl.tex]

[readtex meta-inf/source/macros.ftl.tex]

[memorylimit 8000]

The "memorylimit" instruction lets ℕaproche use up to 8000 Megabytes of working memory per prover call, the default being 2048. The grey background marks the strict formalization embedded in the text and is produced by a `\begin{forthel}` ... `\end{forthel}`-environment.

1 Sets and Functions

Our foundations correspond to a Kelley-Morse type set theory with atoms but without the axiom of choice. The axiom of infinity will be stated after the introduction of natural numbers. New notions and axioms will be *conservative* over classical Kelley-Morse set theory [5] and can in principle be reduced to definitions and propositions within that system, as is usual when developing mathematics in set theories.

1.1 Axioms

The following axioms express that certain "small" classes of axioms are sets.

Proposition 1. Every set is a class.

Let u, v, w denote mathematical objects.

Definition 2. $\emptyset = \{u | u \neq u\}$.

Let the empty set denote $\emptyset$.

Axiom 3 (Set Existence). $\emptyset$ is a set.

Definition 4. $\{u\} = \{v | v = u\}$.

Let the singleton of u denote $\{u\}$.

Definition 5. $\{u, v\} = \{w | w = u \text{ or } w = v\}$.

Let the unordered pair of u and v denote $\{u, v\}$.

Axiom 6 (Pairs). $\{u, v\}$ is a set.

Lemma 7. $\{u\}$ is a set.

Let X, Y, Z denote sets.

Definition 8. Assume that every element of Z is a set. $\bigcup Z = \{x | x \in z \text{ for some } z \in Z\}$.

Let the union of Z denote $\bigcup Z$.

Axiom 9 (Union). Let Z be a set such that every element of Z is a set. Then $\bigcup Z$ is a set.

Definition 10. Let C be a class. A subset of C is a set X such that every element of X is an element of C.

Let $X \subseteq C$ stand for X is a subset of C.

Axiom 11 (Powerset). Let X be a set. Let Y be a class such that every element of Y is a subset of X. Then Y is a set.

Axiom 12 (Separation). Let X be a set. Let Y be a class such that every element of Y is an element of X. Then Y is a set.

Further strength is gained using maps and functions.

Proposition 13. Assume F is a map and $x \in \text{dom}(F)$. Then $F(x)$ is an object.

Axiom 14. Assume that F is a function. Then $\text{dom}(F)$ is a set.

Let the domain of F denote $\text{dom}(F)$.

Axiom 15. Assume that F is a map and $\text{dom}(F)$ is a set. Then F is a function.

Axiom 16 (Replacement). Assume that F is a map and X is a set such that $X \subseteq \text{dom}(F)$. Then there is a set Y such that $Y = \{F(x) \mid x \in X\}$.

1.2 Miscellanous Notions and Properties

Lemma 17. $\emptyset$ and X are subsets of X.

Lemma 18. Let Z be a set such that every element of Z is a set. Let $z \in Z$. Then $z \subseteq \bigcup Z$.

Proof. Let $x \in z$. Then $x \in \bigcup Z$. □

Lemma 19. Let Y, Z be sets such that every element of Z is a subset of Y. Then $\bigcup Z$ is a subset of Y.

Definition 20. $X \cup Y = \{x | x \in X \text{ or } x \in Y\}$.

Let the union of X and Y denote $X \cup Y$.

Lemma 21. Let $X, Y \subseteq Z$. Then $X \cup Y \subseteq Z$.

Definition 22. Let Z be a set such that every element of Z is a set. $\bigcap Z = \{x | x \in z \text{ for all } z \in Z\}$.

Let the intersection of Z stand for $\bigcap Z$.

Definition 23. $X \cap Y = \{x \in X | x \in Y\}$.

Let the intersection of X and Y denote $X \cap Y$.

Lemma 24. $X \cap Y$ is a set.

Definition 25. X is nonempty iff $X \neq \emptyset$.

Lemma 26. Let Z be a nonempty set such that every element of Z is a set. Then $\bigcap Z$ is a set.

Lemma 27. Let Z be a nonempty set such that every element of Z is a set. Assume that Y is a subset of every element of Z. Then Y is a subset of $\bigcap Z$.

Proof. Let y be an element of Y. y is an element of every element of Z. Thus y is an element of $\bigcap Z$. □

2 Natural Numbers

We introduce the notion (or type) of natural numbers. Together with an induction axiom to be stated later, the natural numbers can be understood as the inductive type generated by 0 and +1.

In this chapter we proceed towards prime numbers and divisibility properties of factorials and binomial coefficients.

2.1 Axioms

Signature 28. A natural number is a mathematical object.

Let n, m, k, l, i, j denote natural numbers.

Definition 29. $\mathbb{N}$ is the collection of natural numbers.

Axiom 30 (Axiom of Infinity). $\mathbb{N}$ is a set.

Signature 31. 0 is a natural number.

Let x is nonzero stand for $x \neq 0$.

Signature 32. 1 is a nonzero natural number.

Signature 33. $m + n$ is a natural number.

Axiom 34. If n is a nonzero natural number then $n = m + 1$ for

some natural number m.

We postulate basic arithmetic properties of $\mathbb{N}$ axiomatically, although they could also be proved inductively.

Signature 35. $m * n$ is a natural number.

Axiom 36. $m + n = n + m$.

Axiom 37. $(m + n) + l = m + (n + l)$.

Axiom 38. $m + 0 = m = 0 + m$.

Axiom 39. $m * n = n * m$.

Axiom 40. $(m * n) * l = m * (n * l)$.

Axiom 41. $m * 1 = m = 1 * m$.

Axiom 42. $m * 0 = 0 = 0 * m$.

Axiom 43. $m * (n + l) = (m * n) + (m * l)$ and $(n + l) * m = (n * m) + (l * m)$.

Axiom 44. If $l + m = l + n$ or $m + l = n + l$ then $m = n$.

Axiom 45. Assume that l is nonzero. If $l*m = l*n$ or $m*l = n*l$ then $m = n$.

Axiom 46. If $m + n = 0$ then $m = 0$ and $n = 0$.

We name two more natural numbers:

Definition 47. $2 = 1 + 1$.

Definition 48. $3 = 2 + 1$.

2.1.1 Two Equalities

Since Naproche is weak on algebraic manipulations, we state and prove two complex equalities for later use.

Lemma 49. Let u, v, w, x, y be natural numbers. Then $y + (u * (v * (w * x))) = y + (v * ((u * w) * x))$.
Proof. $(u * (v * (w * x))) = (v * ((u * w) * x))$. □

Lemma 50. Let u, v, w, x, y be natural numbers. Then $(u * (v * (w * x))) + y = (v * (w * (u * x))) + y$.

2.2 The Natural Order

Definition 51. $m \leq n$ iff there exists a natural number l such that $m + l = n$.

Let $m < n$ stand for $m \leq n$ and $m \neq n$. Let $n > m$ stand for $m < n$. Let $n \geq m$ stand for $m \leq n$.

Definition 52. Assume that $n \leq m$. $m - n$ is a natural number l such that $n + l = m$.

The following three lemmas show that $\leq$ is a partial order:

Lemma 53. $m \leq m$.

Lemma 54. If $m \leq n \leq m$ then $m = n$.

Proof. Let $m \leq n \leq m$. Take natural numbers k, l such that $n = m + k$ and $m = n + l$. Then $m = m + (k + l)$ and $k + l = 0$ and $k = 0$. Hence $m = n$. □

Lemma 55. If $m \leq n \leq l$ then $m \leq l$.

We axiomatically postulate monotonicity properties for the arithmetical operations.

Axiom 56. $m \leq n$ or $n < m$.

Lemma 57. Assume that $l < n$. Then $m + l < m + n$ and $l + m < n + m$.

Lemma 58. Assume that m is nonzero and $l < n$. Then $m * l < m * n$ and $l * m < n * m$.

2.3 Induction

ℕaproche provides an in-built binary relation symbol $\prec$ as a universal inductive relation: if

> (inheritance property) at any point m property P holds at m provided all $\prec$-predecessors of m satisfy P

then

> P holds everywhere.

ℕaproche has a proof tactic "by induction [on ...]", which reduces the inductive proof goal "P holds everywhere" to proving the inheritance property for P.

Initially, there is no specification of $\prec$. The induction proof method for some concrete relation is made available by embedding that relation into $\prec$. Therefore we axiomatically embed the natural order into $\prec$.

Axiom 59. If $m < n$ then $m \prec n$.

Let m is inductively smaller than n stand for $m \prec n$.

As a first example of induction we show:

Lemma 60. For every natural number n: $n = 0$ or $1 \leq n$.
Proof by induction. Let n be a natural number. Case $n = 0$. Trivial.

Take $n' = n - 1$. □

Lemma 61. If $m \leq n + 1$ then $m \leq n$ or $m = n + 1$.

Lemma 62. Let $m \neq 0$. Then $n \leq n * m$.

Proof. $1 \leq m$. □

Here are some intuitive facts about the numbers $0, 1, 2, 3$:

Lemma 63. If $m \leq 0$ then $m = 0$.

Lemma 64. If $m \leq 1$ then $m = 0$ or $m = 1$.

Lemma 65. If $m \leq 2$ then $m = 0$ or $m = 1$ or $m = 2$.

Lemma 66. $0 < 1 < 2 < 3$.

2.4 Division

Definition 67. n divides m iff for some l: $m = n * l$.

Let $x|y$ denote x divides y. Let a divisor of x denote a natural number that divides x.

Lemma 68. Assume $l|m|n$. Then $l|n$.

Lemma 69. Let $l|m$ and $l|m + n$. Then $l|n$.

Proof. Assume that l is nonzero. Take a natural number q such that $m = l * q$. Take a natural number r such that $m + n = l * r$.

Let us show that $q \leq r$.

Proof by contradiction. Assume the contrary. Then $r < q$. $m + n = l * r < l * q = m$. Contradiction. qed.

Take $s = r - q$. We have $(l * q) + (l * s) = l * r = m + n = (l * q) + n$. Hence $n = l * s$. □

Lemma 70. Let $m|n \neq 0$. Then $m \leq n$.

Definition 71. n is even iff 2 divides n.

Let n is odd stand for n is not even.

Lemma 72. For all natural numbers n n is even or $n = (2*m)+1$ for some m.

Proof by induction. Let n be a natural number.

Case $n = 0$. Trivial.

Take $n' = n - 1$.

Case n' is even. Take a natural number m' such that $n' = 2 * m'$. Then $n = (2 * m) + 1$ for some m. qed.

Take a natural number m' such that $n' = (2 * m') + 1$. Then $n = ((2 * m') + 1) + 1 = 2 * (m' + 1)$. Hence n is even.

□

2.5 Primes

Let p, d denote natural numbers.

Let n is nontrivial stand for $n \neq 0$ and $n \neq 1$.

Definition 73. p is prime iff p is nontrivial and for every divisor d of p $d = 1$ or $d = p$.

Let a prime number stand for a natural number that is prime.

Lemma 74. 2 is prime.

Lemma 75. Every even prime number is equal to 2.

Lemma 76. 3 is prime.

Lemma 77. Every nontrivial n has a prime divisor.

Proof by induction. Let n be a nontrivial natural number. Assume that n is not prime. Take a divisor m of n such that $m \neq 1$ and $m \neq n$. m is inductively smaller than n. Every prime divisor of m is a prime divisor of n. □

2.6 Euclid's Lemma

We need that prime numbers are prime elements in the ring of integers, or the halfring of natural numbers. The following argument is taken over almost verbatim from the Wikipedia article on Euclid's Lemma [13].

Definition 78. m and n are coprime iff every common divisor of m and n is equal to 1.

Lemma 79. If m and m are coprime then $m = 1$.

Let a, b denote natural numbers.

Lemma 80. For all nonzero natural numbers n, a, b if $n|a * b$ and n and a are coprime then n divides b.

Proof by induction on $a * b$.

Let n, a, b be nonzero natural numbers such that $n|a*b$ and n and a are coprime. Take a natural number q such that $n * q = a * b$.

Case $n = a$. Then $n = 1$ and $n|b$. qed.

Case $a > n$. Then $q \geq b$.

$$n * (q - b) = (n * q) - (n * b) = (a * b) - (n * b) = (a - n) * b.$$

Thus n divides $(a-n)*b$. n and $a-n$ are coprime. $(a-n)*b < a*b$. $(a-n)*b$ is inductively smaller than $a*b$. Thus n divides b. qed.

Hence $n > a$ and $b \geq q$.

$$(n - a) * q = (n * q) - (a * q) = (a * b) - (a * q) = a * (b - q).$$

$n-a$ divides $a*(b-q)$. $n-a$ and a are coprime. $a*(b-q) < a*b$. $a * (b - q)$ is inductively smaller than $a * b$. Thus $n - a$ divides $b - q$.

Take a natural number r such that $b - q = r * (n - a)$.

$(n - a) * q = (n * q) - (a * q) = (a * b) - (a * q) = a * (b - q) = a * (r * (n - a)) = (a * r) * (n - a)$.

$n - a \neq 0$ and $q = a * r$.

$a * (n * r) = n * (a * r) = n * q = a * b$.

Then $n * r = b$ and n divides b. □

Theorem 81 (Euclids Lemma). Let p be a prime number and $p|m * n$. Then $p|m$ or $p|n$.

2.7 Binomial Coefficients

We introduce factorials $n!$ and binomial coefficients $\binom{n}{i}$ together with some divisibility properties which will be used later in connection with Frobenius homomorphisms.

Signature 82. $n!$ is a natural number.

Axiom 83. $0! = 1$.

Axiom 84. $(n+1)! = (n+1) * n!$.

Lemma 85. Let $n \neq 0$. Then $n|n!$.

Proof. Take $m = n - 1$. Then $n! = n * m!$. □

Lemma 86. Let p be a prime number. For all k if $k < p$ then p does not divide $k!$.

Proof by induction on k. Let k be a natural number. Case $k = 0$. Trivial. Let $k < p$. Take $l = k - 1$. Then p does not divide k. p does not divide $l!$. p does not divide $k * l!$. □

Signature 87. $\binom{n}{i}$ is a natural number.

Axiom 88. $\binom{n}{0} = 1$.

Axiom 89. $\binom{0}{i} = 0$ for all i such that $i \geq 1$.

Axiom 90. Let $i \geq 1$. $\binom{n+1}{i} = \binom{n}{i} + \binom{n}{i-1}$.

Theorem 91. For all natural numbers n and all natural numbers i if $i \geq n + 1$ then $\binom{n}{i} = 0$.

Proof by induction on n. Let n be a natural number. Case $n = 0$. Trivial.

Take a natural number n' such that $n = n' + 1$. Let i be a natural number such that $i \geq n + 1$. Then $\binom{n}{i} = \binom{n'}{i} + \binom{n'}{i-1} = 0 + 0 = 0$. □

Theorem 92. For all n $\binom{n}{n} = 1$.

Proof by induction. Let n be a natural number. Case $n = 0$. Trivial.

Take a natural number m such that $n = m + 1$. Then $\binom{n}{n} = \binom{m}{n} + \binom{m}{m} = 0 + 1 = 1$.

□

The next property would normally be expressed as

$$\binom{n}{i} = \frac{n!}{i! * (n-i)!}.$$

Since we don't have rational numbers available we reformulate the property within the natural numbers.

Lemma 93. For all natural numbers n and all natural numbers i such that $0 \leq i \leq n$

$$n! = \binom{n}{i} * (i! * (n-i)!).$$

Proof by induction on n. Let n be a natural number. Let i be a natural number such that $0 \leq i \leq n$.

Case $n = 0$. Trivial.

Take $m = n - 1$.

For all natural numbers j such that $0 \leq j \leq m$ $m! = \binom{m}{j} * (j! * (m - j)!)$. Indeed m is inductively smaller than n.

Case $i = 0$. Trivial.

Case $i = n$. Trivial.

$i - 1 \leq m$ and $m - (i - 1) = n - i$. $m - i$ is a natural number. $n - i = (m - i) + 1$.

Then

$n! = n * m! = ((n - i) + i) * m! = ((n - i) * m!) + (i * m!)$

$= ((n - i) * m!) + (i * (\binom{m}{i-1} * ((i - 1)! * (m - (i - 1))!)))$

$= ((n - i) * m!) + (\binom{m}{i-1} * ((i * (i - 1)!) * (m - (i - 1))!))$

$= ((n - i) * m!) + (\binom{m}{i-1} * (i! * (m - (i - 1))!))$

$= ((n - i) * m!) + (\binom{m}{i-1} * (i! * (n - i)!))$

$= ((n - i) * (\binom{m}{i} * (i! * (m - i)!))) + (\binom{m}{i-1} * (i! * (n - i)!))$

$= ((\binom{m}{i} * (i! * ((n - i) * (m - i)!)))) + (\binom{m}{i-1} * (i! * (n - i)!))$

$= ((\binom{m}{i} * (i! * (n - i)!))) + (\binom{m}{i-1} * (i! * (n - i)!))$

$= (\binom{m}{i} + \binom{m}{i-1}) * (i! * (n - i)!)$

$= \binom{n}{i} * (i! * (n - i)!)$.

Indeed $\binom{n}{i} = \binom{m}{i} + \binom{m}{i-1}$.

□

Lemma 94. Let p be a prime number. Let $0 < k < p$. Then p divides $\binom{p}{k}$.

Proof. $p! = \binom{p}{k} * (k! * (p - k)!)$. p divides $p!$. p does not divide $k!$. p does not divide $(p - k)!$. p does not divide $k! * (p - k)!$. Hence p divides $\binom{p}{k}$. □

3 Finite Sequences and Sets

We can get standard notations in the pretty-printed text by employing LaTeX macros as ForTheL terms. The notation $\{m, \ldots, n\}$ can

be generated from the ForTheL function pattern `\Seq{m}{n}` by the macro:

```
\newcommand{\Seq}[2]{\{#1,\dots,#2\}}
```

.

Let m, n, i denote natural numbers.

Definition 95. $\{m, \dots, n\}$ is the collection of natural numbers i such that $m \leq i \leq n$.

Lemma 96. $\{m, \dots, n\}$ is a set.

Lemma 97. $\{1, \dots, 0\} = \emptyset$.

Lemma 98. Let $m \leq n$. Then $\{1, \dots, m\} \subseteq \{1, \dots, n\}$.

Lemma 99. $\{1, \dots, n\} \cup \{n+1\} = \{1, \dots, n+1\}$.

Proof.

(1) $\{1, \dots, n\} \cup \{n+1\} \subseteq \{1, \dots, n+1\}$.

Proof. $\{1, \dots, n\} \subseteq \{1, \dots, n+1\}$. $\{n+1\} \subseteq \{1, \dots, n+1\}$. Qed.

(2) $\{1, \dots, n+1\} \subseteq \{1, \dots, n\} \cup \{n+1\}$.

Proof. Let $m \in \{1, \dots, n+1\}$. $1 \leq m \leq n+1$. Let us show that $m \in \{1, \dots, n\} \cup \{n+1\}$.

Case $m \leq n$. Trivial.

$m = n+1$. Trivial.

Qed.

□

Definition 100. A sequence of length n is a map a such that $\mathrm{dom}(a) = \{1, \dots, n\}$.

Let a denote a map. Let a_i stand for $a(i)$.

Definition 101. Let $\{1, \dots, n\} \subseteq \mathrm{dom}(a)$.

$$\{a_1, \dots, a_n\} = \{a_i \mid i \in \{1, \dots, n\}\}.$$

Lemma 102. Assume that $\{1, \dots, n\} \subseteq \mathrm{dom}(a)$. Then $\{a_1, \dots, a_n\}$ is a set.

Proof. Consider $X = \{1, \dots, n\}$. X is a set such that $X \subseteq \mathrm{dom}(a)$. [timelimit 10] Take a set Y such that $Y = \{a_i | i \in X\}$. [timelimit 3] $Y = \{a_1, \dots, a_n\}$. □

Lemma 103. Assume that $\{1, \dots, n\} \subseteq \mathrm{dom}(a)$. Let $m \leq n$. Then $\{1, \dots, m\} \subseteq \mathrm{dom}(a)$ and $\{a_1, \dots, a_m\} \subseteq \{a_1, \dots, a_n\}$.

Lemma 104. $\{a_1, \ldots, a_0\} = \emptyset$.

Lemma 105. Assume that $\{1, \ldots, n+1\} \subseteq \mathrm{dom}(a)$.

Then $\{a_1, \ldots, a_n\}$, $\{a_{n+1}\}$ are sets and

$$\{a_1, \ldots, a_n\} \cup \{a_{n+1}\} = \{a_1, \ldots, a_{n+1}\}.$$

Proof. $n+1 \in \mathrm{dom}(a)$. $\{a_{n+1}\}$ is a set and $\{a_1, \ldots, a_n\}$ is a set.

(1) $\{a_1, \ldots, a_n\} \cup \{a_{n+1}\} \subseteq \{a_1, \ldots, a_{n+1}\}$.

Proof. $\{a_1, \ldots, a_n\} \subseteq \{a_1, \ldots, a_{n+1}\}$. $\{a_{n+1}\} \subseteq \{a_1, \ldots, a_{n+1}\}$. Qed.

(2) $\{a_1, \ldots, a_{n+1}\} \subseteq \{a_1, \ldots, a_n\} \cup \{a_{n+1}\}$.

Proof. Let $x \in \{a_1, \ldots, a_{n+1}\}$. Take $m \in \{1, \ldots, n+1\}$ such that $x = a_m$. Let us show that $x \in \{a_1, \ldots, a_n\} \cup \{a_{n+1}\}$.

$m \in \{1, \ldots, n\} \cup \{n+1\}$.

Case $m \in \{1, \ldots, n\}$. Trivial.

$m \in \{n+1\}$. Then $m = n+1$. Trivial. Qed. □

Definition 106. Let A be a class. A is finite iff $A = \{a_1, \ldots, a_n\}$ for some natural number n and some map a such that $\{1, \ldots, n\} \subseteq \mathrm{dom}(a)$.

Lemma 107. $\emptyset$ is finite.

Proof. Define $a(x) = x$ for $x \in \{1, \ldots, 0\}$. Then $\{a_1, \ldots, a_0\} = \emptyset$. □

Lemma 108. Let u be an object. Then $\{u\}$ is finite.

Proof. Define $a(x) = u$ for $x \in \{1, \ldots, 1\}$. Then $\{a_1, \ldots, a_1\} = \{u\}$. □

Lemma 109. For every object u: $u \in \{1, \ldots, 2\}$ iff $u = 1$ or $u = 2$.

Lemma 110. Let u, v be objects. Then $\{u, v\}$ is finite.

Proof. Define $a(x) = \begin{cases} u & : x = 1 \\ v & : x = 2 \end{cases}$ for $x \in \{1, \ldots, 2\}$.

Then $\{a_1, \ldots, a_2\} = \{u, v\}$. □

Definition 111. Let C be a class. C is infinite iff C is not finite.

4 (Additive) Groups

It is common to define structures as an underlying set with further structural elements that "belong" to that set: "a group is a set with

...". This naive approach to structures is employed here. It works alright as long as one does not consider two different structures of the same kind on the same underlying set. In general one will need stronger structure mechanisms as provided in other proof systems.

4.1 Axioms

[synonym group/-s]

Signature 112. A group is a set.

Let an additive group stand for group.

Let G denote a group.

Signature 113. 0^G is an element of G.

Signature 114. Let $x, y \in G$. $x +^G y$ is an element of G.

Signature 115. Let $x \in G$. $-^G x$ is an element of G.

Axiom 116 (Associativity). $(x +^G y) +^G z = x +^G (y +^G z)$ for all $x, y, z \in G$.

Axiom 117. $x +^G 0^G = x$ for all $x \in G$.

Axiom 118. $x +^G (-^G x) = 0^G$ for all $x \in G$.

Axiom 119. $x +^G y = y +^G x$ for all $x, y \in G$.

Let $x -^G y$ stand for $x +^G (-^G y)$.

Lemma 120. $-^G(-^G x) = x$ for all $x \in G$.

Proof. Let $x \in G$. $-^G(-^G x) = -^G(-^G x) +^G (-^G x +^G x) = (-^G(-^G x) +^G -^G x) +^G x = x$. □

Since Naproche does not provide automatic type elaboration the obvious group parameter G has to be carried along in the LaTeX source. In the LaTeX output, however, we can hide it by some LaTeX trickery:

```
\catcode`^\active
\def^#1{\ifthenelse{\equal{#1}{G}} {\unskip} {\sp{#1}}}
```

The first command makes the symbol `^` active as a possible macro name. The second line defines the macro `^{...}`: if the argument is G, it is discarded. Otherwise we treat it as a superscript. Since `^` is used as a macro symbol, we generate the superscript instead by the LaTeX command `\sp{ }`. The definition of the macro requires to `\usepackage{ifthen}`. The previous lemma and proof then print out more concisely as:

Lemma 121. $-(-x) = x$ for all $x \in G$.
Proof. Let $x \in G$. $-(-x) = -(-x) + (-x + x) = (-(-x) + -x) + x = x$. □

Lemma 122. Let $x, y \in G$. Then $-(x + y) = -x - y$.

Proof. $(x + y) + (-x - y) = 0$. □

4.2 Subgroups

We define subgroups and the subgroup generated by some set of generators.

Let G denote a group.

[synonym subgroup/-s]

Definition 123. A subgroup of G is a subset H of G such that $0 \in H$ and for all $x, y \in H$

$x + y \in H$ and $-x \in H$.

Since we shall later consider subgroups of rings where we also have a multiplication, we also use the adjective "additive":

Let an additive subgroup of G stand for a subgroup of G.

Lemma 124. G is a subgroup of G.

Lemma 125. $\{0\}$ is a subgroup of G.

Proof. Let $x, y \in \{0\}$. Then $x, y = 0$. $x + y = 0 \in \{0\}$ and $-x = 0 \in \{0\}$. □

Lemma 126. Let F be a nonempty set such that every element of F is a subgroup of G. Then $\bigcap F$ is a subgroup of G.

Definition 127. Let A be a subset of G. $[A] = \{x \in G \mid x \in H$ for all subgroups H of G such that $A \subseteq H\}$.

Lemma 128. Let A be a subset of G. Then $[A]$ is a subgroup of G such that $A \subseteq [A]$.

Proof.

(1) $[A]$ is a subset of G.

(2) $0 \in [A]$.

(3) $x + y \in [A]$ for all $x, y \in [A]$.

(4) $-x \in [A]$ for all $x \in [A]$.

Hence $[A]$ is a subgroup of G.

Let $x \in A$. Then $x \in [A]$. □

Let the additive closure of A in G stand for $[A]$.

Definition 129. Let $C \subseteq G$ and $c \in G$. $c \oplus C = \{c + d \mid d \in C\}$.

5 Rings

5.1 Axioms

We shall only consider commutative rings with 1. After defining a group as a *set* with further structure, we can now define a ring as a *group* together with multiplication and a 1.

[prover vampire]

Signature 130. A ring is an additive group.

Let R denote a ring.

Signature 131. 1^R is an element of R such that $1^R \neq 0^R$.

Signature 132. Let $x, y \in R$. $x \cdot^R y$ is an element of R.

Axiom 133. $(x \cdot^R y) \cdot^R z = x \cdot^R (y \cdot^R z)$ for all $x, y, z \in R$.

Axiom 134. $x \cdot^R 1^R = x$ for all $x \in R$.

Axiom 135 (Commutativity). $x \cdot^R y = y \cdot^R x$ for all $x, y \in R$.

Axiom 136 (Distributivity). $(x +^R y) \cdot^R z = (x \cdot^R z) +^R (y \cdot^R z)$ for all $x, y, z \in R$.

Again readability is improved if we hide the recurring superscript ^{R} by the above method.

Lemma 137. $z \cdot (x + y) = (z \cdot x) + (z \cdot y)$ for all $x, y, z \in R$.
Proof. Let $x, y, z \in R$. $z \cdot (x + y) = (x + y) \cdot z = (x \cdot z) + (y \cdot z) = (z \cdot x) + (z \cdot y)$. □

Lemma 138. $0 \cdot x = 0$ for all $x \in R$.

Proof. Let $x \in R$. $(0 \cdot x) + x = (0 \cdot x) + (1 \cdot x) = (0 + 1) \cdot x = 1 \cdot x = x$. $0 \cdot x = (0 \cdot x) + ((-x) + x) = 0$. □

Lemma 139. $(-1) \cdot x = -x$ for all $x \in R$.

Proof. Let $x \in R$. $(-1) \cdot x = ((-1) \cdot x) + (x + (-x)) = (((-1) \cdot x) + x) + (-x) = (((-1) \cdot x) + (1 \cdot x)) + (-x)$. □

Lemma 140. $-(x \cdot y) = (-x) \cdot y$ for all $x, y \in R$.

Proof. Let $x, y \in R$. $-(x \cdot y) = (-1) \cdot (x \cdot y)$. □

Lemma 141. $(-1) \cdot (-1) = 1$.

[prover eprover]

Lemma 142. $x - (x - y) = y$ for all $x, y \in R$.

[prover vampire]

Lemma 143. $(x - y) \cdot z = (x \cdot z) - (y \cdot z)$ for all $x, y, z \in R$.

Proof. Let $x, y, z \in R$. $(x - y) \cdot z$

$= (x + (-y)) \cdot z$

$= (x \cdot z) + ((-y) \cdot z)$

$= (x \cdot z) + (-(y \cdot z))$.

□

5.2 Subrings

Let R denote a ring.

Definition 144. Let A be a subset of R. A is closed under multiplication in R iff $x \cdot y \in A$ for all $x, y \in A$.

Definition 145. A subring of R is an additive subgroup S of R such that $1 \in S$ and S is closed under multiplication in R.

Lemma 146. R is a subring of R.

5.3 Operations on Subsets of Rings

Let R denote a ring.

Definition 147. Let $B, C \subseteq R$. $BC = \{b \cdot c \in R | b \in B$ and $c \in C\}$.

Definition 148. Let $B, C \subseteq R$. $B \cdot C = [BC]$.

We iterate the formation of additive closures of pointwise products:

Let n denote natural numbers.

Signature 149. Let $B \subseteq R$ and $n \geq 1$. $B^{n,R,subset}$ is a subset of R.

Axiom 150. Let $B \subseteq R$. $B^{1,R,subset} = B$.

Axiom 151. Let $B \subseteq R$ and $n \geq 1$. $B^{n+1,R,subset} = B^{n,R,subset} \cdot B$.

Lemma 152. Let $B \subseteq R$. Then $B^{n,R,subset}$ is a subgroup of R where n is a natural number and $n > 1$.

Proof by induction on n.

Let n be a natural number.

CASE $n \leq 1$. trivial.

Take a natural number m such that $n = m+1$. Then $B^{n,R,subset} = B^{m,R,subset} \cdot B$ and $B^{n,R,subset}$ is a subgroup of R. □

Definition 153. Let $B \subseteq R$. $\{B^{n,R} \mid n \in \mathbb{N}\} = \{B^{n,R,subset} | n \in \mathbb{N} \text{ and } n \geq 1\}$.

Lemma 154. Let $B \subseteq R$. Then $\{B^{n,R} \mid n \in \mathbb{N}\}$ is a set.

Proof. $\mathbb{N}$ is a set. □

5.4 Divisibility

Let R denote a ring.

Definition 155. A unit in R is an element x of R such that $x \cdot y = 1$ for some element y of R.

Definition 156. Let X be a subset of R. Let $x, y \in R$. x divides y in X within R iff $x \cdot z = y$ for some element z of X.

Let $x|y$ in X within R stand for x divides y in X within R.

Lemma 157. Let S be a subring of R. Let $x, y, z \in R$. Let $x|y$ in S within R and $y|z$ in S within R. Then $x|z$ in S within R.

Lemma 158. Let S be a subring of R. Let $x, y, z \in R$. Let $x|y$ in S within R and $x|z$ in S within R. Then $x|(y+z)$ in S within R.

Proof. Take an element u of S such that $x \cdot u = y$. Take an element v of S such that $x \cdot v = z$. Then $x \cdot (u+v) = y+z$ and $u+v \in S$. □

Lemma 159. Let S be a subring of R. Let $x, y \in R$. Let $x|y$ in S within R. Then $x|(-y)$ in S within R.

Lemma 160. Let S be a subring of R. Let $x, y, z \in R$. Let $x|y$ in S within R and $x|z$ in S within R. Then $x|(y-z)$ in S within R.

Proof. $x|(-z)$ in S within R. □

5.5 Congruences

Let $x \equiv_S y \bmod a$ within R stand for a divides $x - y$ in S within R.

We show that for S being a subring of R and $a \in S$, $\equiv_S \bmod a$ is an equivalence relation and a congruence relation on S.

Lemma 161. Let S be a subring of R and $a \in S$. $x \equiv_S x \bmod a$ within R for all $x \in S$.

Lemma 162. Let S be a subring of R and $a \in S$. Let x, y be elements of S such that $x \equiv_S y \bmod a$ within R. Then $y \equiv_S x \bmod a$ within R.

Proof. a divides $x - y$ in S within R. a divides $-(x - y)$ in S within R. $y - x = -(x - y)$. □

Lemma 163. Let S be a subring of R and $a \in S$. Let x, y, z be elements of S such that $x \equiv_S y \bmod a$ within R and $y \equiv_S z \bmod a$ within R. Then $x \equiv_S z \bmod a$ within R.

Proof. Take $u \in S$ such that $x - y = a \cdot u$. Take $v \in S$ such that $y - z = a \cdot v$. Then $x - z = ((x - y) + y) - z = (x - y) + (y - z) = (a \cdot u) + (a \cdot v) = a \cdot (u + v)$. □

Lemma 164. Let S be a subring of R and $a \in S$. Let x, x', y, y' be elements of S such that $x \equiv_S x' \bmod a$ within R and $y \equiv_S y' \bmod a$ within R. Then $x + y \equiv_S x' + y' \bmod a$ within R.

Proof. Take $u \in S$ such that $x - x' = a \cdot u$. Take $v \in S$ such that $y - y' = a \cdot v$. Then $(x + y) - (x' + y') = (x + y) + (-x' + -y') = ((x + y) - x') - y' = (x + (y - x')) - y' = ((x - x') + y) - y' = (x - x') + (y - y') = (a \cdot u) + (a \cdot v)$. □

Lemma 165. Let S be a subring of R and $a \in S$. Let x, x' be elements of S such that $x \equiv_S x' \bmod a$ within R. Then $(-x) \equiv_S (-x') \bmod a$ within R.

Proof. Take $z \in S$ such that $x - x' = a \cdot z$.

$(-1) \cdot (x - x') = (-1) \cdot (a \cdot z)$. $(-x) - (-x') = ((-1) \cdot x) - ((-1) \cdot x') = (-1) \cdot (a \cdot z)$. □

[prover eprover]

Lemma 166. Let S be a subring of R and $a \in S$. Let x, x', y, y' be elements of S such that $x \equiv_S x' \bmod a$ within R and $y \equiv_S y' \bmod a$ within R. Then $x \cdot y \equiv_S x' \cdot y' \bmod a$ within R.

Proof. Take $u \in S$ such that $x - x' = a \cdot u$. Take $v \in S$ such that $y - y' = a \cdot v$.

$x \cdot y = (x \cdot y) + 0$

$= (x \cdot y) + (-(x' \cdot y) + (x' \cdot y))$

$= ((x \cdot y) - (x' \cdot y)) + (x' \cdot y)$

$= ((x - x') \cdot y) + (x' \cdot y)$.

$(x' \cdot y) - (x' \cdot y') = x' \cdot (y - y')$.

Hence

$(x \cdot y) - (x' \cdot y') =$

$(((x - x') \cdot y) + (x' \cdot y)) - (x' \cdot y')$

$= ((x - x') \cdot y) + ((x' \cdot y) - (x' \cdot y'))$ (by Associativity).

[timelimit 10]

$(x \cdot y) - (x' \cdot y') =$

$((x - x') \cdot y) + ((x' \cdot y) - (x' \cdot y'))$

$= ((x - x') \cdot y) + (x' \cdot (y - y'))$

$= ((a \cdot u) \cdot y) + (x' \cdot (a \cdot v))$

$= ((a \cdot u) \cdot y) + ((x' \cdot a) \cdot v)$

$= (a \cdot (u \cdot y)) + ((a \cdot x') \cdot v)$

$= (a \cdot (u \cdot y)) + (a \cdot (x' \cdot v))$

$= a \cdot ((u \cdot y) + (x' \cdot v))$.

[timelimit 3]

a divides $(x \cdot y) - (x' \cdot y')$ in S within R. Indeed $(u \cdot y) + (x' \cdot v) \in S$. □

We could now define equivalence sets

$[x] = \{x' \in S \mid x' \equiv_S x \bmod a\}$

and form a quotient

$$S/a = \{[x] \mid x \in S\}.$$

But as we shall not continue working with the quotients in this article we will only consider congruences mod a. To talk about quotient rings that have distinguished elements $0, 1$ with $0 \neq 1$, we show:

Lemma 167. Let S be a subring of R and $a \in S$. Assume that a does not divide 1 in S within R. Then not $0 \equiv_S 1 \bmod a$ within R.

5.6 Embedding Natural Numbers into a Ring

Natural numbers are represented in a ring R as sums of 1's. As ℕaproche does not yet provide recursive function definitions, we work

axiomatically: the notation or function symbol $n^{[R]}$ is introduced into the language, and then two axioms postulate the initial case and the successor case of the recursion.

Finite powers of ring elements are introduced in a similar way.

Let m denote natural numbers.

Let R denote a ring.

Signature 168. Let n be a natural number. $n^{[R]}$ is an element of R.

Axiom 169. $0^{[R]} = 0$.

Axiom 170. $(n+1)^{[R]} = n^{[R]} + 1$.

Lemma 171. $1^{[R]} = 1$.

Lemma 172. Let S be a subring of R. Then $n^{[R]} \in S$ for all n.

Proof by induction. Let n be a natural number.

Case $n = 0$. Trivial.

Take $m = n - 1$. Then $n^{[R]} = m^{[R]} + 1 \in S$. □

Lemma 173. For all n we have $(m+n)^{[R]} = m^{[R]} + n^{[R]}$.

Proof by induction. Let n be a natural number.

Case $n = 0$. Trivial.

Take $l = n - 1$.

$(m+n)^{[R]} = ((m+l)+1)^{[R]} = (m+l)^{[R]} + 1 = (m^{[R]} + l^{[R]}) + 1 = m^{[R]} + n^{[R]}$. □

Lemma 174. For all n we have $(m * n)^{[R]} = m^{[R]} \cdot n^{[R]}$.

Proof by induction. Let n be a natural number.

Case $n = 0$. Trivial.

Take $l = n - 1$.

$(m * n)^{[R]} = ((m * l) + m)^{[R]} = (m * l)^{[R]} + m^{[R]} = (m^{[R]} \cdot l^{[R]}) + m^{[R]} = (m^{[R]} \cdot l^{[R]}) + (m^{[R]} \cdot 1) = m^{[R]} \cdot (l+1)^{[R]}$. □

Lemma 175. Let S be a subring of R. Let m divide n. Then $m^{[R]}$ divides $n^{[R]}$ in S within R.

Lemma 176. Let S be a subring of R and $x \in S$. Then $x \equiv_S -x \mod (2^{[R]})$ within R.

Proof. $x - (-x) = x + x = (1+1) \cdot x = 2^{[R]} \cdot x$. □

5.7 Exponentiation

Exponentiation in R is defined by recursive axioms that specify the new function symbol `x^{n,R}` which prints as $x^{n,R}$.

Signature 177. Let $x \in R$. $x^{n,R}$ is an element of R.

Axiom 178. Let $x \in R$. Then $x^{0,R} = 1$.

Axiom 179. Let $x \in R$. Then $x^{n+1,R} = x^{n,R} \cdot x$.

If the parameter R is understood from the context one would like to turn R into an implicit parameter and hide `,R`. Since we also want to remove superscripts `^{R}` we redefine the "macro" `^`.

```
\catcode`^\active

\def^#1{\ifthenelse{\equal{#1}{R}} {\unskip}
{{\IfEndWith{#1}{,R}{\sp{\StrBefore{#1}{,R}}}{\sp{#1}}}}}
```

The string operations in this macro require to `\usepackage{xstring}`.

Lemma 180. Assume that $n \neq 0$. Then $0^n = 0$.
Proof. Take m such that $n = m + 1$. Then $0^{m+1} = 0^m \cdot 0 = 0$. □

Lemma 181. Assume that $x \in R$. Then for all natural numbers n

(if n is even then $(-x)^n = x^n$) and

(if n is odd then $(-x)^n = -(x^n)$).

Proof by induction. Let n be a natural number.

(1) Case $n = 0$. Trivial.

Take $m = n - 1$.

(2a) Case n is even.

m is inductively smaller than n and odd. $(-x)^m = -(x^m)$. $(-x)^n = (-x)^m \cdot (-x) = (-(x^m)) \cdot (-x) = (x^m) \cdot x = x^n$. End.

(2b) Case n is odd.

m is inductively smaller than n and even. $(-x)^m = x^m$. $(-x)^n = (-x)^m \cdot (-x) = (x^m) \cdot (-x) = -((x^m) \cdot x) = -(x^n)$. End.

□

Lemma 182. For all natural numbers n we have $1^n = 1$.

Proof By induction on n. □

Lemma 183. Let n be a natural numbers. Then $(-1)^n = 1$ or $(-1)^n = -1$.

Proof. □

Lemma 184. Let $x \in R$ and m be a natural number. For all natural numbers n we have $x^m \cdot x^n = x^{m+n}$.

Proof by induction on n. Let n be a natural number.

CASE $n = 0$. Trivial.

Take a natural number k such that $n = k + 1$. Then

$x^m \cdot x^n =$

$x^m \cdot x^{k+1} =$

$x^m \cdot (x^k \cdot x) =$

$(x^m \cdot x^k) \cdot x =$

$x^{m+k} \cdot x =$

$x^{(m+k)+1} = x^{m+n}$. □

Lemma 185. Let $x \in R$ and m be a natural number. For all natural numbers n we have $(x^m)^n = x^{m*n}$.

Proof by induction on n. Let n be a natural number.

CASE $n = 0$. Trivial.

Take a natural number k such that $n = k + 1$. Then $(x^m)^n = (x^m)^{k+1} = (x^m)^k \cdot (x^m)$. □

Lemma 186. Let $x, y \in R$. For all natural numbers n we have $(x \cdot y)^n = (x^n \cdot y^n)$.

Proof by induction on n. Let n be a natural number.

CASE $n = 0$. Trivial.

Take m such that $n = m+1$. $(x \cdot y)^n = (x \cdot y)^{m+1} = (x \cdot y)^m \cdot (x \cdot y)$.

$(x^m \cdot y^m) \cdot (x \cdot y) = (x^m \cdot x) \cdot (y^m \cdot y)$. □

Definition 187. Let $x \in R$. $\{x^{n,R} \mid n \in \mathbb{N}\} = \{x^n | n \in \mathbb{N}\}$.

Lemma 188. $\{x^{n,R} \mid n \in \mathbb{N}\}$ is a set for every $x \in R$.

[timelimit 11]

Lemma 189. Let $x \in R$. Then $\{x^{n,R} \mid n \in \mathbb{N}\}$ is a subset of R that is closed under multiplication in R.

[timelimit 3]

Lemma 190. Let A be a subset of R that is closed under multi-

plication in R. Then the additive closure of A in R is closed under multiplication in R.

Proof. Define $B = \{b \in R \mid b \cdot a \in [A] \text{ for all } a \in A\}$.

(1) B is a subset of R.

(2) $0 \in B$.

(3) $x + y \in B$ for all $x, y \in B$.

Proof. Let $x, y \in B$. Let $a \in A$. Then $x \cdot a, y \cdot a \in [A]$. Then $(x + y) \cdot a = (x \cdot a) + (y \cdot a) \in [A]$. Qed.

(4) $-x \in B$ for all $x \in B$.

Proof. Let $x \in B$. Let $a \in A$. Then $x \cdot a \in [A]$. Then $(-x) \cdot a = -(x \cdot a) \in [A]$. Qed.

(5) B is a subgroup of R.

(6) $A \subseteq B$. Indeed A is closed under multiplication in R.

(7) $[A] \subseteq B$.

(8) For all $b \in [A]$ and all $a \in A$ $b \cdot a \in [A]$.

(9) For all $a \in A$ and all $b \in [A]$ $a \cdot b \in [A]$.

Define $C = \{c \in R \mid c \cdot a \in [A] \text{ for all } a \in [A]\}$.

(10) C is a subset of R.

(11) $0 \in C$.

(12) $x + y \in C$ for all $x, y \in C$.

Proof. Let $x, y \in C$. Let $a \in [A]$. Then $x \cdot a, y \cdot a \in [A]$. Then $(x + y) \cdot a = (x \cdot a) + (y \cdot a) \in [A]$. Qed.

(13) $-x \in C$ for all $x \in C$.

Proof. Let $x \in C$. Let $a \in [A]$. Then $x \cdot a \in [A]$. Then $(-x) \cdot a = -(x \cdot a) \in [A]$. Qed.

(14) C is a subgroup of R.

(15) $A \subseteq C$ (by 9).

(16) $[A] \subseteq C$.

(17) For all $b \in [A]$ and all $a \in [A]$ $b \cdot a \in [A]$. □

6 Binomial Properties in Rings

6.1 Binomial Coefficients

As natural numbers, the binomial coefficients can be canonically embedded into a ring R together with their recursive properties.

Let R denote a ring. Let n, m, k, l, i, j denote natural numbers.

Lemma 191. $\binom{n}{0}^{[R]} = 1$.

Lemma 192. $\binom{0}{i}^{[R]} = 0$ for all i such that $i \geq 1$.

Lemma 193. Let $i \geq 1$. $\binom{n+1}{i}^{[R]} = \binom{n}{i}^{[R]} + \binom{n}{i-1}^{[R]}$.

Lemma 194. If $i \geq n+1$ then $\binom{n}{i}^{[R]} = 0$.

Theorem 195. $\binom{n}{n}^{[R]} = 1$.

Lemma 196. Let S be a subring of R. Let p be a prime number. Let $0 < i < p$. Then $p^{[R]}$ divides $\binom{p}{i}^{[R]}$ in S within R.

6.2 Binomial Sums

We shall deal with "partial" binomial sums of the form

$$\sum_{i=0}^{m} \binom{n}{i} x^{n-i} y^i.$$

We view the summation as a first-order function symbol in the arguments m, n, x, y, R and specify the function axiomatically.

Signature 197. Let $x, y \in R$.

$$\sum\nolimits_{i=0}^{k} \binom{m}{i} x^{m-i} y^i$$

is an element of R.

Axiom 198. Let m be a natural number and $x, y \in R$. Then

$$\sum\nolimits_{i=0}^{0} \binom{m}{i} x^{m-i} y^i = x^m.$$

Axiom 199 (Summation recursion). Let $1 \leq k \leq m$ and $x, y \in R$. Then

$\sum_{i=0}^{k} \binom{m}{i} x^{m-i} y^i =$

$(\sum_{i=0}{}^{k-1}\binom{m}{i}x^{m-i}y^i) + (\binom{m}{k}^{[R]} \cdot (x^{m-k} \cdot y^k))$.

The next proofs will be rather tedious since ℕaproche so far does not have efficient term rewriting or an inbuilt ring theory.

Lemma 200. Let $x, y \in R$. For all natural numbers m if $m \leq n$ then

$(\sum_{i=0}{}^{m}\binom{n}{i}x^{n-i}y^i) \cdot (x+y) =$

$(\sum_{i=0}{}^{m}\binom{n+1}{i}x^{n+1-i}y^i) + (\binom{n}{m}^{[R]} \cdot (x^{n-m} \cdot y^{m+1}))$.

Proof by induction. Let m be a natural number such that $m \leq n$.

Case $m = 0$.

$(\sum_{i=0}{}^{0}\binom{n}{i}x^{n-i}y^i) \cdot (x+y) =$

$x^n \cdot (x+y) =$

$(x^n \cdot x) + (x^n \cdot y) =$

$x^{n+1} + (x^n \cdot y) =$

$(\sum_{i=0}{}^{0}\binom{n+1}{i}x^{n+1-i}y^i) + (1 \cdot (x^n \cdot y)) =$

$(\sum_{i=0}{}^{0}\binom{n+1}{i}x^{n+1-i}y^i) + (\binom{n}{0}^{[R]} \cdot (x^{n-0} \cdot y)) =$

$(\sum_{i=0}{}^{0}\binom{n+1}{i}x^{n+1-i}y^i) + (\binom{n}{0}^{[R]} \cdot (x^{n-0} \cdot y^{0+1}))$.

Indeed $y = 1 \cdot y$.

End.

Take $m' = m - 1$.

[timelimit 30]

$(\sum_{i=0}{}^{m}\binom{n}{i}x^{n-i}y^i) \cdot (x+y) =$

$((\sum_{i=0}{}^{m-1}\binom{n}{i}x^{n-i}y^i) + (\binom{n}{m}^{[R]} \cdot (x^{n-m} \cdot y^m))) \cdot (x+y)$.

[timelimit 3]

$((\sum_{i=0}{}^{m-1}\binom{n}{i}x^{n-i}y^i) + (\binom{n}{m}^{[R]} \cdot (x^{n-m} \cdot y^m))) \cdot (x+y) =$

$((\sum_{i=0}{}^{m'}\binom{n}{i}x^{n-i}y^i) \cdot (x+y)) + (((\binom{n}{m}^{[R]} \cdot (x^{n-m} \cdot y^m)) \cdot (x+y)) =$

$((\sum_{i=0}{}^{m'}\binom{n+1}{i}x^{n+1-i}y^i) + (\binom{n}{m'}^{[R]} \cdot (x^{n-m'} \cdot y^{m'+1}))) + (((\binom{n}{m}^{[R]} \cdot (x^{n-m} \cdot y^m)) \cdot (x+y)) =$

$((\sum_{i=0}{}^{m'}\binom{n+1}{i}x^{n+1-i}y^i) + (\binom{n}{m'}^{[R]} \cdot (x^{n-m'} \cdot y^{m'+1}))) + ((((\binom{n}{m}^{[R]} \cdot (x^{n-m} \cdot y^m)) \cdot x) + (((\binom{n}{m}^{[R]} \cdot (x^{n-m} \cdot y^m)) \cdot y))$.

[timelimit 20]

$((\sum_{i=0}{}^{m'}\binom{n+1}{i}x^{n+1-i}y^i) + (\binom{n}{m'}^{[R]} \cdot (x^{n-m'} \cdot y^{m'+1}))) + ((((\binom{n}{m}^{[R]} \cdot$

$(x^{n-m} \cdot y^m)) \cdot x) + (((\binom{n}{m}^{[R]} \cdot (x^{n-m} \cdot y^m)) \cdot y)) =$

$((\sum_{i=0}^{m'} \binom{n+1}{i} x^{n+1-i} y^i) + (((\binom{n}{m'}^{[R]} \cdot (x^{n-m'} \cdot y^{m'+1})) + (((\binom{n}{m}^{[R]} \cdot (x^{n-m} \cdot y^m)) \cdot x))) + (((\binom{n}{m}^{[R]} \cdot (x^{n-m} \cdot y^m)) \cdot y).$

$(\binom{n}{m}^{[R]} \cdot (x^{n-m} \cdot y^m)) \cdot y = \binom{n}{m}^{[R]} \cdot ((x^{n-m} \cdot y^m) \cdot y) = \binom{n}{m}^{[R]} \cdot (x^{n-m} \cdot y^{m+1}).$

$((\sum_{i=0}^{m'} \binom{n+1}{i} x^{n+1-i} y^i) + (((\binom{n}{m'}^{[R]} \cdot (x^{n-m'} \cdot y^{m'+1})) + (((\binom{n}{m}^{[R]} \cdot (x^{n-m} \cdot y^m)) \cdot x))) + (((\binom{n}{m}^{[R]} \cdot (x^{n-m} \cdot y^m)) \cdot y) =$

$((\sum_{i=0}^{m'} \binom{n+1}{i} x^{n+1-i} y^i) + (((\binom{n}{m'}^{[R]} \cdot (x^{n-m'} \cdot y^{m'+1})) + (((\binom{n}{m}^{[R]} \cdot (x^{n-m} \cdot y^m)) \cdot x))) + (\binom{n}{m}^{[R]} \cdot (x^{n-m} \cdot y^{m+1})).$

$x^{n-m'} \cdot y^{m'+1} = x^{(n+1)-m} \cdot y^m.$

$\binom{n}{m'}^{[R]} \cdot (x^{n-m'} \cdot y^{m'+1}) = \binom{n}{m'}^{[R]} \cdot (x^{(n+1)-m} \cdot y^m).$

$(\binom{n}{m}^{[R]} \cdot (x^{n-m} \cdot y^m)) \cdot x =$

$\binom{n}{m}^{[R]} \cdot ((x^{n-m} \cdot y^m) \cdot x).$

$(x^{n-m} \cdot y^m) \cdot x = x^{n-m} \cdot (y^m \cdot x) = x^{n-m} \cdot (x \cdot y^m) = (x^{n-m} \cdot x) \cdot y^m.$

$(n-m)+1 = (n+1)-m.$

$(x^{n-m} \cdot x) \cdot y^m = x^{(n+1)-m} \cdot y^m.$

$(\binom{n}{m}^{[R]} \cdot (x^{n-m} \cdot y^m)) \cdot x =$

$\binom{n}{m}^{[R]} \cdot (x^{(n+1)-m} \cdot y^m).$

$x^{n-m'} \cdot y^{m'+1} = x^{(n+1)-m} \cdot y^m.$

$((\sum_{i=0}^{m'} \binom{n+1}{i} x^{n+1-i} y^i) + (((\binom{n}{m'}^{[R]} \cdot (x^{n-m'} \cdot y^{m'+1})) + (((\binom{n}{m}^{[R]} \cdot (x^{n-m} \cdot y^m)) \cdot x))) + (\binom{n}{m}^{[R]} \cdot (x^{n-m} \cdot y^{m+1})) =$

$((\sum_{i=0}^{m'} \binom{n+1}{i} x^{n+1-i} y^i) + (((\binom{n}{m'}^{[R]} \cdot (x^{(n+1)-m} \cdot y^m)) + (\binom{n}{m}^{[R]} \cdot (x^{(n+1)-m} \cdot y^m)))) + (\binom{n}{m}^{[R]} \cdot (x^{n-m} \cdot y^{m+1})) =$

$((\sum_{i=0}^{m'} \binom{n+1}{i} x^{n+1-i} y^i) + ((\binom{n}{m'}^{[R]} + \binom{n}{m}^{[R]}) \cdot (x^{(n+1)-m} \cdot y^m))) + (\binom{n}{m}^{[R]} \cdot (x^{n-m} \cdot y^{m+1})).$

$\binom{n}{m'}^{[R]} + \binom{n}{m}^{[R]} = \binom{n+1}{m}^{[R]}.$

$\sum_{i=0}^{m} \binom{n+1}{i} x^{n+1-i} y^i = (\sum_{i=0}^{m'} \binom{n+1}{i} x^{n+1-i} y^i) + (\binom{n+1}{m}^{[R]} \cdot (x^{(n+1)-m} \cdot y^m)).$

$((\sum_{i=0}^{m'} \binom{n+1}{i} x^{n+1-i} y^i) + ((\binom{n}{m'}^{[R]} + \binom{n}{m}^{[R]}) \cdot (x^{(n+1)-m} \cdot y^m))) + (\binom{n}{m}^{[R]} \cdot (x^{n-m} \cdot y^{m+1})) =$

$((\sum_{i=0}^{m'} \binom{n+1}{i} x^{n+1-i} y^i) + (\binom{n+1}{m}^{[R]} \cdot (x^{(n+1)-m} \cdot y^m))) + (\binom{n}{m}^{[R]} \cdot$

$(x^{n-m} \cdot y^{m+1})) =$

$(\sum_{i=0}^{m} \binom{n+1}{i} x^{n+1-i} y^i) + (\binom{n}{m}^{[R]} \cdot (x^{n-m} \cdot y^{m+1}))$. □

This leads to the standard binomial formula:

Theorem 201. Let $x, y \in R$. For all natural numbers n we have

$$(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^{n-i} y^i.$$

Proof by induction. Let n be a natural number.

Case $n = 0$. Trivial.

Take $n' = n - 1$.

$(x+y)^n =$

$(x+y)^{n'} \cdot (x+y) =$

$\sum_{i=0}^{n'} \binom{n'}{i} x^{n'-i} y^i \cdot (x+y) =$

$(\sum_{i=0}^{n'} \binom{n'+1}{i} x^{n'+1-i} y^i) + (\binom{n'}{n'}^{[R]} \cdot (x^{n'-n'} \cdot y^{n'+1})) =$

$(\sum_{i=0}^{n-1} \binom{n}{i} x^{n-i} y^i) + (\binom{n}{n}^{[R]} \cdot (x^{n-n} \cdot y^n))$.

[timelimit 8]

$(\sum_{i=0}^{n-1} \binom{n}{i} x^{n-i} y^i) + (\binom{n}{n}^{[R]} \cdot (x^{n-n} \cdot y^n)) =$

$\sum_{i=0}^{n} \binom{n}{i} x^{n-i} y^i$ (by summation recursion).

[timelimit 3] □

6.3 Divisibility

Lemma 202. Let S be a subring of R. Let $x, y, z \in S$. Let $x|y$ in S within R. Then $x|(y \cdot z)$ in S within R.

Lemma 203. Let S be a subring of R. Let $x \in S$. For all natural numbers n $x^n \in S$.

Proof by induction. Let n be a natural number.

Case $n = 0$. Trivial.

Take $n' = n - 1$. $x^{n'} \in S$. $x^n = x^{n'} \cdot x \in S$. □

Lemma 204. Let p be a prime number. Let S be a subring of R and $x, y \in S$. Then for all natural numbers m if $m < p$ then $\sum_{i=0}^{m} \binom{p}{i} x^{p-i} y^i \equiv_S x^p \bmod p^{[R]}$ within R.

Proof by induction. Let m be a natural number such that $m < p$.

Case $m = 0$. Trivial.

Take $m' = m - 1$.

(f1) $\sum_{i=0}{}^{m'} \binom{p}{i} x^{p-i} y^i \equiv_S x^p \bmod p^{[R]}$ within R.

$p^{[R]}$ divides $\binom{p}{m}^{[R]}$ in S within R.

$x^{p-m} \in S$.

$p^{[R]}$ divides $(\binom{p}{m}^{[R]} \cdot (x^{p-m} \cdot y^m))$ in S within R.

(f2) $(\binom{p}{m}^{[R]} \cdot (x^{p-m} \cdot y^m)) \equiv_S 0 \bmod p^{[R]}$ within R.

$(\sum_{i=0}{}^{m-1} \binom{p}{i} x^{p-i} y^i) + (\binom{p}{m}^{[R]} \cdot (x^{p-m} \cdot y^m)) \equiv_S x^p \bmod p^{[R]}$ within R.

Proof. Take $a = \sum_{i=0}{}^{m-1} \binom{p}{i} x^{p-i} y^i$. Take $b = (\binom{p}{m}^{[R]} \cdot (x^{p-m} \cdot y^m))$. Take $c = x^p$. $a \equiv_S c \bmod p^{[R]}$ within R. $b \equiv_S 0 \bmod p^{[R]}$ within R. $b \in S$. $a + b \equiv_S c \bmod p^{[R]}$ within R. Qed.

$\sum_{i=0}{}^{m} \binom{p}{i} x^{p-i} y^i \equiv_S x^p \bmod p^{[R]}$ within R.

Proof. $m \leq p$.

[timelimit 20]

$\sum_{i=0}{}^{m} \binom{p}{i} x^{p-i} y^i = (\sum_{i=0}{}^{m-1} \binom{p}{i} x^{p-i} y^i) + (\binom{p}{m}^{[R]} \cdot (x^{p-m} \cdot y^m))$. [timelimit 3]

QED. □

The following lemma will be used later to show that the Frobenius map is an additive homomorphism.

Lemma 205. Let p be a prime number. Let S be a subring of R and $x, y \in S$. Then $(x + y)^p \equiv_S x^p + y^p \bmod p^{[R]}$ within R.
Proof. $p \geq 1$.

[timelimit 30]

$(x + y)^p = \sum_{i=0}{}^{p} \binom{p}{i} x^{p-i} y^i =$

$(\sum_{i=0}{}^{p-1} \binom{p}{i} x^{p-i} y^i) + (\binom{p}{p}^{[R]} \cdot (x^{p-p} \cdot y^p)) =$

$(\sum_{i=0}{}^{p-1} \binom{p}{i} x^{p-i} y^i) + y^p$.

Indeed $\binom{p}{p}^{[R]} \cdot (x^{p-p} \cdot y^p) = y^p$.

$\sum_{i=0}{}^{p-1} \binom{p}{i} x^{p-i} y^i \equiv_S x^p \bmod p^{[R]}$ within R.

$\sum_{i=0}{}^{p-1} \binom{p}{i} x^{p-i} y^i + y^p \equiv_S x^p + y^p \bmod p^{[R]}$ within R.

Proof. Take $a = \sum_{i=0}{}^{p-1} \binom{p}{i} x^{p-i} y^i$. Take $b = x^p$.

$a \equiv_S b \bmod p^{[R]}$ within R.

Take $c = y^p$.

$a + y^p \equiv_S b + y^p \bmod p^{[R]}$ within R. Qed. [timelimit 3] □

Lemma 206. Let p be a prime number. Let S be a subring of R and $x, y \in S$. Then $(x - y)^p \equiv_S x^p - y^p \bmod p^{[R]}$ within R.

Proof.

Case p is even. Then p is equal to 2.

$(x - y)^2 \equiv_S x^2 + (-y)^2 \bmod 2^{[R]}$ within R.

$(x - y)^2 \equiv_S x^2 + y^2 \bmod 2^{[R]}$ within R.

$x^2 + y^2 \equiv_S x^2 - y^2 \bmod 2^{[R]}$ within R. Indeed $y^2 \equiv_S -(y^2) \bmod 2^{[R]}$ within R.

$(x - y)^2$, $x^2 + y^2$, $x^2 - y^2 \in S$.

Hence $(x - y)^2 \equiv_S x^2 - y^2 \bmod 2^{[R]}$ within R.

End.

p is odd.

$(x - y)^p \equiv_S x^p + (-y)^p \bmod p^{[R]}$ within R.

$(x - y)^p \equiv_S x^p - y^p \bmod p^{[R]}$ within R. □

7 Topological Spaces

We formalize some beginnings of set-theoretic topology. For simplicity, we do not work with a set-theoretic family of open sets, but instead use a predicate "is open in T". We partially follow the presentation by Wedhorn [12], 5.4.

7.1 Topological Axioms

Signature 207. A topological space is a set.

Let T denote a topological space.

Signature 208. Assume that T is a topological space and X is a subset of T. X is open in T is an atom.

Definition 209. An open subset of T is a subset of T that is open in T.

Axiom 210. T is open in T.

Axiom 211. Let X be an open subsets of T and Y be an open

subset of T. Then $X \cap Y$ is open in T.

Axiom 212. Let Z be a set such that every element of Z is an open subset of T. Then $\bigcup Z$ is open in T.

Lemma 213. $\emptyset$ is open in T.

Proof. $\emptyset = \bigcup \emptyset$. □

7.2 Convergence

[synonym neighborhood/-s]

Definition 214. Let $x \in T$. A neighborhood of x in T is a subset V of T such that there is a subset U of V such that U is open in T and $x \in U$.

Lemma 215. Let $x \in T$. Let V, V' be neighborhoods of x in T. Then $V \cap V'$ is a neighborhood of x in T.

Proof. Take a subset U of V such that U is open in T and $x \in U$. Take a subset U' of V' such that U' is open in T and $x \in U'$. Then $U \cap U'$ is open in T. $x \in U \cap U' \subseteq V \cap V'$. □

Lemma 216. Let x be an element of T. Let U, V be subsets of T such that U is a neighborhood of x in T and $U \subseteq V$. Then V is a neighborhood of x in T.

A topology is determined by its neighborhoods.

Lemma 217. Let $A \subseteq T$. Then A is open in T iff for every $x \in A$ there exists a neighborhood V of x in T such that $V \subseteq A$.
Proof. Case A is open in T. Obvious.

Case For every $x \in A$ there exists a neighborhood V of x in T such that $V \subseteq A$. For every $x \in A$ there exists a subset U of A such that U is open in T and $x \in U$. Define $Z = \{U \mid U \subseteq A \text{ and } U \text{ is open in } T\}$. Z is a set. Every element of Z is a subset of T that is open in T. $\bigcup Z \subseteq A$.

$A = \bigcup Z$.

Proof. Let x be an element of A. Take an element U of Z such that $x \in U$. $U \subseteq \bigcup Z$. qed.

Hence A is open in T. Indeed every element of Z is an open subset of T. qed. □

Definition 218. T is Hausdorff iff for all distinct elements x, y of T there are sets A, B such that A is a neighborhood of x in T and B is a neighborhood of y in T and $A \cap B = \emptyset$.

Definition 219. A filter basis on T is a nonempty set B such that every element of B is a nonempty subset of T and for all elements X, Y of B there exists an element Z of B such that $Z \subseteq X \cap Y$.

Definition 220. Let B be a filter basis on T and $x \in T$. B converges to x in T iff for every neighborhood U of x in T there exists an element X of B such that $X \subseteq U$.

Definition 221. Let B be a filter basis on T. B converges in T iff B converges to some element of T in T.

Definition 222. Let x be an element of T. The neighborhood filter of x in T is the collection of neighborhoods of x in T.

Let N_x^T denote the neighborhood filter of x in T.

Lemma 223. N_x^T is a set for all $x \in T$.

Lemma 224. Let x be an element of T. N_x^T is a filter basis on T that converges to x in T.

8 Topological Groups

A topological group requires its operations to be topologically continuous.

Let G denote a group that is a topological space.

Let us now hide the parameter G as we did previously. (Note that R is no longer "hidden").

Definition 225. Let $x, x' \in G$. G is additively continuous at x and x' iff for every neighborhood U of $x + x'$ in G there are subsets V, V' of G such that V is a neighborhood of x in G and V' is a neighborhood of x' in G and for all $v \in V$ for all $v' \in V'$ $v + v' \in U$.

Definition 226. G is additively continuous iff G is additively continuous at x and x' for all $x, x' \in G$.

Definition 227. Let $x \in G$. G is negation continuous at x iff for every neighborhood U of $-x$ in G there exists a neighborhood V of x in G such that $-v \in U$ for all $v \in V$.

Definition 228. G is negation continuous iff G is negation continuous at x for every $x \in G$.

Definition 229 (Topological group). A topological group is a group G such that G is a topological space and G is additively continuous and negation continuous.

Let G denote a topological group.

Definition 230. A fundamental system of neighborhoods of G is a subset F of N_0^G such that for every neighborhood U of 0 in G there exists $V \in F$ such that $V \subseteq U$.

Definition 231. A fundamental system of open neighborhoods of G is a fundamental system of neighborhoods F of G such that every element of F is open in G.

Proposition 232. N_0^G is a fundamental system of neighborhoods of G.

Definition 233. G is nonarchimedean iff every neighborhood U of 0 in G has a subset S that is a subgroup of G and open in G.

Lemma 234. Let B be a subgroup of G that is a neighborhood of 0 in G. Then B is open in G.

Proof. Let $x \in B$. G is additively continuous at x and $-x$. B is a neighborhood of $x + (-x)$ in G. [timelimit 10] Take subsets V, V' of G such that V is a neighborhood of x in G and V' is a neighborhood of $-x$ in G and for all $v \in V$, all $v' \in V'$ $v + v' \in B$. [timelimit 3]

(1) $V \subseteq B$. Proof. Let $v \in V$. Then $v + (-x) \in B$. $v = (v + (-x)) + x \in B$. end. □

8.1 Completeness

Let G denote a topological group.

Definition 235. Let B be a filter basis on G. B is Cauchy in G iff for every neighborhood U of 0 in G there exists $A \in B$ such that $x - y \in U$ for all $x, y \in A$.

Definition 236. G is complete iff G is Hausdorff and every filter basis on G that is Cauchy in G converges in G.

9 Topological Rings

A topological ring has continuous multiplication.

Let R denote a ring that is a topological space.

Let us hide `^{R}` and `,R}` as we have done before.

Definition 237. Let $x, x' \in R$. R is multiplicatively continuous at x and x' iff for every neighborhood U of $x \cdot x'$ in R there are subsets V, V' of R such that V is a neighborhood of x in R and V' is a neighborhood of x' in R and for all $v \in V$ for all $v' \in V'$ $v \cdot v' \in U$.

Definition 238. R is multiplicatively continuous iff R is multiplicatively continuous at x and x' for all $x, x' \in R$.

Definition 239 (Topological ring). A topological ring is a ring R such that R is a topological group and R is multiplicatively continuous.

Part II
Perfectoid Rings

10 Boundedness

This chapter corresponds to parts of the file `power_bounded.lean` in the Lean formalization of perfectoid spaces [6] which contains the theory of topologically nilpotent, bounded, and power-bounded elements and subsets of topological rings. The line numbers "L ..." after some definitions and theorems refer to that file. We also use material from [12]. We omit those parts that depend on an adic topology on R, since this will not be needed in our definition of perfectoid rings. Initially we do not require a connection between the algebraic and the topological structure on R.

Let R denote a ring that is a topological space.

Definition 240 (L 42). Assume that B is a subset of R. B is bounded in R iff for all neighborhoods U of 0 in R there exists a neighborhood V of 0 in R such that $v \cdot b \in U$ where $v \in V$ and $b \in B$.

The last condition can be expressed by products of sets:

Lemma 241 (L 48). Assume that B is a subset of R. B is bounded in R if and only if for all neighborhoods U of 0 in R there exists a neighborhood V of 0 in R such that $VB \subseteq U$.
Proof. CASE B is bounded in R. Let U be a neighborhood of 0 in R. Take a neighborhood V of 0 in R such that $v \cdot b \in U$ where $v \in V$ and $b \in B$. Then $VB \subseteq U$. end.

CASE For every neighborhood U of 0 in R there exists a neighborhood V of 0 in R such that $VB \subseteq U$.

Let us show that B is bounded in R. Let U be a neighborhood of 0 in R. Take a neighborhood V of 0 in R such that $VB \subseteq U$. Then $v \cdot b \in U$ where $v \in V$ and $b \in B$. end. end. □

Now we strengthen our assumptions on R to:

Let R denote a topological ring.

Lemma 242 (L 91). Let R be nonarchimedean and $B \subseteq R$. Then B is bounded in R iff for all neighborhoods U of 0 in R there exists a subgroup V of R such that V is open in R and the additive closure of VB in R is a subset of U.

Proof. CASE B is bounded in R. Let U be a neighborhood of 0 in R. Take a subset U' of U such that U' is a subgroup of R and open in R. U' is a neighborhood of 0 in R. Take a neighborhood V' of 0 in R such that $V'B \subseteq U'$. Take a subset V of V' such that V is a subgroup of R and open in R. Then $VB \subseteq U'$. The additive closure of VB in R is a subset of U'. end.

CASE For all neighborhoods U of 0 in R there exists a subgroup V of R such that V is open in R and the additive closure of VB in R is a subset of U. Let U be a neighborhood of 0 in R. Take a subgroup V of R such that V is open in R and the additive closure of VB in R is a subset of U. V is a neighborhood of 0 in R. $VB \subseteq R$. VB is a subset of the additive closure of VB in R. Then $VB \subseteq U$. end. □

Definition 243. A bounded subset of R is a subset of R that is bounded in R.

Lemma 244. $\emptyset$ is a bounded subset of R.

Lemma 245 (Boundedness of Singletons). Let $r \in R$. Then $\{r\}$ is bounded in R.

Proof. Let U be a neighborhood of $0 \cdot r$ in R. R is multiplicatively continuous at 0 and r. [timelimit 10] Take $V, V' \subseteq R$ such that V is a neighborhood of 0 in R and V' is a neighborhood of r in R and for all $v \in V$ for all $v' \in V'$ $v \cdot v' \in U$. [timelimit 3] Then $V\{r\} \subseteq U$. □

Lemma 246. Let B, B' be subsets of R that are bounded in R. Then $B \cup B'$ is bounded in R.

Proof. Let U be a neighborhood of 0 in R. Take a neighborhood V of 0 in R such that $v \cdot b \in U$ where $v \in V$ and $b \in B$. Take a neighborhood V' of 0 in R such that $v \cdot b \in U$ where $v \in V'$

and $b \in B'$. $V \cap V'$ is a neighborhood of 0 in R. $v \cdot b \in U$ where $v \in V \cap V'$ and $b \in B \cup B'$. □

Lemma 247. For every natural number n for every map s such that $\{1, \ldots, n\} \subseteq \mathrm{dom}(s)$ and $\{s_1, \ldots, s_n\} \subseteq R$ $\{s_1, \ldots, s_n\}$ is bounded in R.

Proof by induction. Let n be a natural number. Let s be a map such that $\{1, \ldots, n\} \subseteq \mathrm{dom}(s)$ and $\{s_1, \ldots, s_n\} \subseteq R$.

CASE $n = 0$. trivial.

Take a natural number m such that $n = m{+}1$. $m \prec n$. $\{1, \ldots, m\} \subseteq \mathrm{dom}(s)$. $\{s_1, \ldots, s_m\} \subseteq R$. $\{s_1, \ldots, s_m\}$ is bounded in R.

$\{s_1, \ldots, s_{m+1}\} = \{s_1, \ldots, s_m\} \cup \{s_{m+1}\}$. $\{s_{m+1}\}$ is a bounded subset of R. Hence $\{s_1, \ldots, s_{m+1}\}$ is bounded in R. □

Lemma 248 (5 28 1). Every finite subset of R is bounded in R.

Lemma 249. Let $r, s \in R$. Then $\{r, s\}$ is bounded in R.

Proof. $\{r, s\}$ is a finite subset of R. □

Lemma 250 (L 136). Every subset of every bounded subset of R is a bounded subset of R.

Proof. Let B be a bounded subset of R. Let $A \subseteq B$. Let U be a neighborhood of 0 in R. Take a neighborhood V of 0 in R such that $VB \subseteq U$. Then $VA \subseteq VB \subseteq U$. $VA \subseteq U$. □

It is interesting to contrast this declarative natural language proof with the corresponding formal tactic proof in `power_bounded.lean`:

```
lemma subset {S1 S2 : set R}
(h : S1 \subset S2) (H : is_bounded S2) :
is_bounded S1 :=
begin
  intros U hU,
  rcases H U hU with <V, hV1, hV2>,
  use [V, hV1],
  intros v hv b hb,
  exact hV2 _ hv _ (h hb),
end
```

Definition 251 (L 179). Let r be an element of R. r is powerbounded in R iff $\{r^{n,R} \mid n \in \mathbb{N}\}$ is bounded in R.

Lemma 252. Let r be an element of R. Then r is powerbounded in R iff for all neighborhoods U of 0 in R there exists a neighborhood V of 0 in R such that $v \cdot r^n \in U$ where $v \in V$ and n is a natural number.

Proof. CASE r is powerbounded in R. Let U be a neighborhood of 0 in R. Take a neighborhood V of 0 in R such that $V\{r^{n,R} \mid n \in \mathbb{N}\} \subseteq U$. Indeed $\{r^{n,R} \mid n \in \mathbb{N}\}$ is bounded in R. Assume $w \in V$. Let m be a natural number. Then $r^m \in \{r^{n,R} \mid n \in \mathbb{N}\}$. $w \cdot r^m \in V\{r^{n,R} \mid n \in \mathbb{N}\} \subseteq U$.

end.

CASE For all neighborhoods U of 0 in R there exists a neighborhood V of 0 in R such that $v \cdot r^n \in U$ where $v \in V$ and n is a natural number.

(1) $\{r^{n,R} \mid n \in \mathbb{N}\}$ is bounded in R.

Proof. Let U be a neighborhood of 0 in R. Take a neighborhood V of 0 in R such that $v \cdot r^n \in U$ where $v \in V$ and n is a natural number. qed. end. □

Lemma 253 (L 189). 0 is powerbounded in R.

Lemma 254 (L 199). 1 is powerbounded in R.

Lemma 255. -1 is powerbounded in R.

Proof. $\{-1, 1\}$ is bounded in R. $\{-1^{n,R} \mid n \in \mathbb{N}\} \subseteq \{-1, 1\}$. [timelimit 20] Hence $\{-1^{n,R} \mid n \in \mathbb{N}\}$ is bounded in R. [timelimit 3] □

Lemma 256 (L 248). Let a, b be elements of R that are powerbounded in R. Then $a \cdot b$ is powerbounded in R.

Proof. Let U be a neighborhood of 0 in R. [timelimit 10] Take a neighborhood V of 0 in R such that $v \cdot b^n \in U$ where $v \in V$ and n is a natural number. [timelimit 15] Take a neighborhood W of 0 in R such that $w \cdot a^n \in V$ where $w \in W$ and n is a natural number. [timelimit 3]

(1) $w \cdot (a \cdot b)^n \in U$ where $w \in W$ and n is a natural number.

Proof. Let $w \in W$ and n be a natural number. $w \cdot a^n \in V$.

$w \cdot (a \cdot b)^n = w \cdot (a^n \cdot b^n) = (w \cdot a^n) \cdot b^n \in U$.

qed. □

Lemma 257 (L 290). Let R be nonarchimedean. Let a, b be elements of R that are powerbounded in R. Then $a + b$ is powerbounded in R.

Proof. Let U be a neighborhood of 0 in R. Take a subset U' of U that is a subgroup of R and open in R. U' is a neighborhood of 0 in R. [timelimit 30] Take a neighborhood V of 0 in R such that

$v \cdot b^n \in U'$ where $v \in V$ and n is a natural number. [timelimit 30] Take a neighborhood W of 0 in R such that $w \cdot a^m \in V$ where $w \in W$ and m is a natural number. [timelimit 3] (1) $w \cdot (a^m \cdot b^n) \in U'$ where $w \in W$ and m, n are natural numbers.

Proof. Let $w \in W$ and m, n be natural numbers.

$w \cdot a^m \in V$ and $w \cdot (a^m \cdot b^n) = (w \cdot a^m) \cdot b^n \in U$.

qed.

Define $G = \{x \in R \mid w \cdot x \in U' \text{ for all } w \in W\}$.

(3) G is a subgroup of R.

Proof.

(a) $0 \in G$.

(b) For all $x, y \in G$ $x + y \in G$.

Proof. Let $x, y \in G$. Let $w \in W$. Then $w \cdot (x+y) = (w \cdot x) + (w \cdot y) \in U'$.

qed.

(c) For all $x \in G$ $-x \in G$.

Proof. Let $x \in G$. Let $w \in W$.

$w \cdot (-x) = w \cdot ((-1) \cdot x) = (-1) \cdot (w \cdot x) = -(w \cdot x)$.

qed.

qed.

Define $Z = \{a^m \cdot b^n \mid m, n \in \mathbb{N}\}$.

(2) Z is a subset of G that is closed under multiplication in R.

Proof. Let $u, v \in Z$. Take $m, n \in \mathbb{N}$ such that $u = a^m \cdot b^n$. Take $m', n' \in \mathbb{N}$ such that $v = a^{m'} \cdot b^{n'}$. Then $u \cdot v = (a^m \cdot b^n) \cdot (a^{m'} \cdot b^{n'}) =$

$(a^m \cdot a^{m'}) \cdot (b^n \cdot b^{n'}) =$

$a^{m+m'} \cdot b^{n+n'} \in Z$.

Hence $u \cdot v \in Z$. Qed.

(3) $1, a, b \in Z$. Proof. $1 = a^0 \cdot b^0$. $a = a^1 \cdot b^0$. $b = a^0 \cdot b^1$. Qed.

(4) $Z \subseteq G$.

(5) $[Z] \subseteq G$.

(6) $[Z]$ is closed under multiplication in R.

(7) For all natural numbers n $(a + b)^n \in [Z]$. Proof by induction.

Let n be a natural number. Case $n = 0$. Trivial.

$a + b \in [Z]$.

Let $m = n - 1$. Then $(a + b)^m \in [Z]$.

$(a + b)^n = (a + b)^{m+1} = (a + b)^m \cdot (a + b) \in [Z]$. Qed.

(8) For all natural numbers n $(a + b)^n \in G$.

(9) For all natural numbers n and all $w \in W$ $w \cdot (a + b)^n \in U'$.

□

Lemma 258 (L 342). Let a be an element of R that is powerbounded in R. Then $-a$ is powerbounded in R.

Proof. $-a = (-1) \cdot a$. □

Definition 259 (L 310). $R^o = \{x \in R \mid x$ is powerbounded in $R\}$.

Lemma 260. R^o is a subset of R.

Lemma 261 (L 320). $0 \in R^o$.

Lemma 262 (L 322). $1 \in R^o$.

Lemma 263 (L 324). Let $a, b \in R^o$. Then $a \cdot b \in R^o$.

Lemma 264 (L 324). Let $a \in R^o$. Then $a^n \in R^o$ for all $n \in \mathbb{N}$.

Proof by induction. Let $n \in \mathbb{N}$.

Case $n = 0$. Trivial.

Take $m = n - 1$. m is inductively smaller than n and $a^m \in R^o$. Hence $a^n = a^m \cdot a \in R^o$. □

Lemma 265 (L 337). Let R be nonarchimedean. Let $a, b \in R^o$. Then $a + b \in R^o$.

Lemma 266 (L 342). Let $a \in R^o$. Then $-a \in R^o$.

Lemma 267 (L 365). Let R be nonarchimedean. Then R^o is a subgroup of R.

Lemma 268 (L 371). Let R be nonarchimedean. Then R^o is a subring of R.

Definition 269 (L 380). R is uniform iff R^o is a bounded subset of R.

10.1 Topological Nilpotency

Definition 270 (L 30). Let r be an element of R. r is topologically nilpotent in R iff for all neighborhoods U of 0 in R there

exists a natural number N such that $r^n \in U$ for all natural numbers n such that $n > N$.

For example:

Lemma 271. 0 is topologically nilpotent in R.

[prover vampire][timelimit 20]

Lemma 272. Assume that R is Hausdorff. 1 is not topologically nilpotent in R.

Proof. Take sets A, B such that A is a neighborhood of 0 in R and B is a neighborhood of 1 in R and $A \cap B = \emptyset$. □ [prover eprover][timelimit 3]

Theorem 273. Let r be an element of R that is topologically nilpotent in R. Then r is powerbounded in R.

Proof. Let U be a neighborhood of 0 in R. R is multiplicatively continuous at 0 and 0 and U is a neighborhood of $0 \cdot 0$ in R. [prover vampire][timelimit 10] Take sets V, V' such that V is a neighborhood of 0 in R and V' is a neighborhood of 0 in R and for all $v \in V$ for all $v' \in V'$ $v \cdot v' \in U$. [prover eprover][timelimit 3] Take a natural number N such that $r^n \in V$ for all natural numbers n such that $n > N$. Define $X = \{r^n \mid n \in \mathbb{N} \text{ and } 1 \leq n \leq N\}$.

(1) X is finite.

Proof. Define $s(n) = r^n$ for $n \in \{1, \ldots, N\}$. [timelimit 5] $X = \{s_1, \ldots, s_N\}$. [timelimit 3] qed.

X is bounded in R. Take a neighborhood V'' of 0 in R such that $v'' \cdot x \in U$ where $v'' \in V''$ and $x \in X$. Let $W = U \cap (V' \cap V'')$. [timelimit 5]W is a neighborhood of 0 in R. Indeed $V' \cap V''$ is a neighborhood of 0 in R. [timelimit 3]

(2) $w \cdot x \in U$ where $w \in W$ and $x \in \{r^{n,R} \mid n \in \mathbb{N}\}$.

□

Lemma 274. Let a, b be elements of R such that a is topologically nilpotent in R and b is powerbounded in R. Then $a \cdot b$ is topologically nilpotent in R.

Proof. Let U be a neighborhood of 0 in R. [timelimit 10] Take a neighborhood V of 0 in R such that $v \cdot b^n \in U$ where $v \in V$ and n is a natural number. [timelimit 15] Take a natural number N such that $a^n \in V$ for all natural numbers n such that $n > N$. [timelimit 3]

(1) $(a \cdot b)^n \in U$ for all natural numbers n such that $n > N$.

Proof. Let n be a natural number such that $n > N$.

$(a \cdot b)^n = a^n \cdot b^n \in U$.

qed. □

Lemma 275. Let R be Hausdorff. Let a be an element of R that is topologically nilpotent in R. Then a does not divide 1 in R^o within R.

Proof. Assume the contrary. Take $b \in R^o$ such that $a \cdot b = 1$. Then $a \cdot b$ is topologically nilpotent in R. Contradiction. □

11 Huber rings

Let R denote a topological ring.

The following is the original definition of f-adic ring by R. Huber [3]:

Definition 276. A Huber ring is a topological ring R such that for some subset U of R and some finite subset T of U $\{U^{n,R} \mid n \in \mathbb{N}\}$ is a fundamental system of neighborhoods of R and $T \cdot U = U \cdot U \subseteq U$.

Lemma 277. Let R be a Huber ring. Then R is nonarchimedean.

Proof. Take a subset U of R such that $U \cdot U \subseteq U$ and $\{U^{n,R} \mid n \in \mathbb{N}\}$ is a fundamental system of neighborhoods of R. Let V be a neighborhood of 0 in R. Take $B \in \{U^{n,R} \mid n \in \mathbb{N}\}$ such that $B \subseteq V$. B is a neighborhood of 0 in R. Take $n \in \mathbb{N}$ such that $n \geq 1$ and $B = U^{n,R,subset}$.

Case $n > 1$. Then B is a subgroup of R that is open in R. end.

$n = 1$. $B = U$. $U \cdot U$ is a subgroup of R that is open in R. $U \cdot U \subseteq U = B \subseteq V$. □

Lemma 278. Let R be a Huber ring. Then R^o is a subring of R.

12 Tate Rings

Let R denote a topological ring.

Definition 279. A pseudouniformizer of R is a unit in R that is topologically nilpotent in R.

[timelimit 10]

Lemma 280. Let ϖ be a pseudouniformizer of R. Then ϖ is powerbounded in R.

[timelimit 3]

Definition 281. A Tate ring is a Huber ring that has a pseudouniformizer.

13 Frobenius maps

Normally we would use (set-theoretic) quotients by principal ideals in R^o for the definition of perfectoid rings, and then Frobenius-style maps on those quotient rings. Instead we define a global map Φ, $x \mapsto x^p$ and consider whether it induces maps between such quotients. This can be expressed by calculations modulo the generators of the ideals. A complete formalization would have to prove certain well-definednesses which we assume for simplicity. We treat the Frobenius map as a function symbol of the logic, dependent on the ring and a fixed prime number p.

Let R denote a Huber ring.

Signature 282. p is a prime number.

Definition 283. Let $x \in R$. $\Phi(x) = x^p$.

Lemma 284. Let $x \in R^o$. Then $\Phi(x) \in R^o$.

Φ maps the subring of power-bounded elements into itself. To show further structural properties we recall the following

Lemma. Let S be a subring of R and x, y be elements of S. Then
$(x+y)^p \equiv_S x^p + y^p \bmod p^{[R]}$ within R
and
$(x-y)^p \equiv_S x^p - y^p \bmod p^{[R]}$ within R

Lemma 285. Let ϖ be an element of R^o such that $(\varpi^p)|p^{[R]}$ in R^o within R. Let x, y be elements of R^o such that

$x \equiv_{R^o} y \bmod \varpi$ within R.

Then

$\Phi(x) \equiv_{R^o} \Phi(y) \bmod \varpi^p$ within R.
Proof. ϖ divides $x-y$ in R^o within R. ϖ^p divides $(x-y)^p$ in R^o within R. $p^{[R]}$ divides $(x-y)^p - (x^p - y^p)$ in R^o within R. Let $t = (x-y)^p - (x^p - y^p)$. Then ϖ^p divides $-t$ in R^o within R. ϖ^p divides $(x-y)^p - t$ in R^o within R. ϖ^p divides $x^p - y^p$ in R^o

within R. Indeed $(x-y)^p - t = x^p - y^p$. □

This map also respects the ring operations modulo ϖ and ϖ^p.

Lemma 286. $\Phi(0) = 0$.

Lemma 287. $\Phi(1) = 1$.

Lemma 288. Let ϖ be an element of R^o such that $(\varpi^p)|p^{[R]}$ in R^o within R. Let x, y be elements of R^o. Then

$\Phi(x+y) \equiv_{R^o} \Phi(x) + \Phi(y) \bmod \varpi^p$ within R.

Proof. $p^{[R]}$ divides $(x+y)^p - (x^p + y^p)$ in R^o within R. Then ϖ^p divides $(x+y)^p - (x^p + y^p)$ in R^o within R.

□

Lemma 289. Let ϖ be an element of R^o such that $(\varpi^p)|p^{[R]}$ in R^o within R. Let x be an element of R^o. Then

$\Phi(-x) \equiv_{R^o} -\Phi(x) \bmod \varpi^p$ within R.

Proof.

$\Phi(x + (-x)) \equiv_{R^o} \Phi(x) + \Phi(-x) \bmod \varpi^p$ within R.

ϖ^p divides $0 - (\Phi(x) + \Phi(-x))$ in R^o within R. [timelimit 10] ϖ^p divides $-\Phi(x) - \Phi(-x)$ in R^o within R. [timelimit 3] □

Lemma 290. Let ϖ be an element of R^o such that $(\varpi^p)|p^{[R]}$ in R^o within R. Let x, y be elements of R^o. Then

$\Phi(x \cdot y) \equiv_{R^o} \Phi(x) \cdot \Phi(y) \bmod \varpi^p$ within R.

Proof. $\Phi(x \cdot y) = (x \cdot y)^p = x^p \cdot y^p = \Phi(x) \cdot \Phi(y)$. □

A perfectoid ring requires the Frobenius map to be an isomorphism So far we have established that it is a homomorphism. To express the crucial isomorphism property one would ordinarily apply a general predicate for ring congruence to the rings R^o/a and R^o/b. To cut things short, we (slightly miss-)use the notation $\Phi : S/a \cong T/b$ with LaTeX source

```
$\Phi^{R} : S / a \cong T / b$
```

by defining its meaning in terms of congruences using the parameters S, a, T, b.

Definition 291. Let $S, T \subseteq R$. Let $a \in S$ and $b \in T$. $\Phi : S/a \cong T/b$ iff (for every $x, y \in S$ if $\Phi(x) \equiv_T \Phi(y) \bmod b$ within R then $x \equiv_S y \bmod a$ within R) and (for every $z \in T$ there exists $w \in S$

such that $z \equiv_T \Phi(w)$ mod b within R).

14 Perfectoid rings

Now all ingredients are prepared for defining perfectoid rings in ℕaproche:

Let R denote a Tate ring.

Lemma 292. Let R be complete and ϖ be a pseudouniformizer of R. Then ϖ, ϖ^p do not divide 1 in R^o within R.

Proof. ϖ does not divide 1 in R^o within R.

Assume that ϖ^p divides 1 in R^o within R. Take $b \in R^o$ such that $\varpi^p \cdot b = 1$. Let $q = p - 1$. Then $\varpi^p = \varpi \cdot \varpi^q$. $\varpi \cdot (\varpi^q \cdot b) = (\varpi \cdot \varpi^q) \cdot b = 1$. [timelimit 6] Then ϖ divides 1 in R^o within R. Indeed $\varpi^q \in R^o$. [timelimit 3] □

In this case the quotients R^o/ϖ and R^o/ϖ^p are well-defined rings, and one can define:

Definition 293. R is perfectoid iff R is complete and uniform and there exists a pseudouniformizer ϖ of R such that $\varpi^p | p^{[R]}$ in R^o within R and

$$\Phi : R^o/\varpi \cong R^o/\varpi^p.$$

The present formalization has mainly been directed towards the definition of perfectoid rings in a readable and proof-checked mathematical language. We do not pursue the theory of perfectoid rings any further and we do not consider examples. If one wanted to do so one would have to refine and considerably expand the previous developments.

References

[1] Kevin Buzzard, Johan Commelin, and Patrick Massot: Formalising perfectoid spaces. CPP 2020: 299-312. arXiv:1910.12320. Also: `https://leanprover-community.github.io/lean-perfectoid-spaces/`

[2] Adrian De Lon, Peter Koepke, Anton Lorenzen, Adrian Marti, Marcel Schütz, Makarius Wenzel: The Isabelle/Naproche Natural Language Proof Assistant. In: André Platzer and Geoff Sutcliffe (eds.); Automated Deduction – CADE 28, Lecture Notes in Computer Science, vol 12699. Springer, Cham, 2021.

[3] R. Huber: Continuous Valuations. Mathematische Zeitschrift, Springer-Verlag, 1993. http://virtualmath1.stanford.edu/~conrad/Perfseminar/refs/Hubercontval.pdf

[4] The Isabelle homepage: https://isabelle.in.tum.de/

[5] John L. Kelley: General Topology, Springer Graduate Texts in Mathematics 27.

[6] The Lean homepage: https://lean-lang.org/

[7] Andrei Paskevich: The syntax and semantics of the ForTheL language. http://nevidal.org/download/forthel.pdf, 2007.

[8] Peter Scholze: Perfectoid Spaces. Publications Mathématiques de l'IHÉS, Volume 116 (2012), pp. 245-313.

[9] Peter Scholze: Étale cohomology of diamonds, arXiv:1709.07343.

[10] Stephan Schulz: The E Theorem Prover. http://wwwlehre.dhbw-stuttgart.de/~sschulz/E/E.html

[11] The Vampire homepage: https://vprover.github.io/

[12] Torsten Wedhorn: Adic Spaces, arXiv 1910.05934v1.

[13] Wikipedia entry "Euclid's Lemma": https://en.wikipedia.org/wiki/Euclid\%27s_lemma