项目编号：T030PRP35059

上海交通大學

本科生研究计划（PRP）研究论文

（第 35 期）

论文题目：实数的康托尔构造理论在 Coq 中的形式化

项目负责人：曹钦翔　学院（系）：电子信息与电气工程学院

指导教师：曹钦翔　学院（系）：电子信息与电气工程学院

参与学生：周李韬

项目执行时间：2019 年 2 月 至 2019 年 6 月

实数的康托尔构造理论在 Coq 中的形式化

电子信息与电气工程学院　F1803016　周李韬
指导老师：电子信息与电气工程学院　曹钦翔

摘　要

数的形式化定义是软件形式化验证工作的基础。然而，经典实数理论中数学证明的复杂性和灵活性，造成了在 Coq 等定理证明系统中形式化实数定义的困难。本课题旨在实现由有理数柯西列等价类构造的实数在 Coq 中的形式化定义和完备性证明。本课题首先会将主流数学分析学教材中有关实数构造的定义形式化，然后通过形式化教材中已有的证明语言，或者在 Coq 中给出更适合形式化的证明，以求证该实数域满足实数公理。实践结果表明，通过有理数柯西列等价类定义的实数完备性可以在 Coq 中得到完整的形式化证明，此外，本文还给出了在该定义下构造的从实数非空单元集到实数的单射。从实验结果看出，在形式化验证工具中由有理数构造经典实数是可行的，并且得到的实数具有对接更高阶证明的扩展性。

关键词：实数域，柯西列，完备性，Coq，形式化

ABSTRACT

Formal definition of numbers is the foundation of formal verification in software. However, due to the complexity and flexibility of mathematical proofs in classical real number theory, it is difficult to formalize real number in formal proof systems like Coq. This paper is aimed to implement the formal definition and completeness proof of real numbers constructed by rational Cauchy sequence in Coq. We will first formalize the definition of real number, based on popular mathematical analysis textbooks, and then prove that the real number field we've constructed satisfies the real number axioms, either by formalizing the existing proof in maths or through a more suitable proof in Coq. It is shown in our work that the completeness of real numbers constructed by Cauchy sequence can be formally verified in Coq. Furthermore, we have constructed an injection from a non-empty, single-element set of real numbers to a particular real number in this paper. In conclusion, it is feasible to construct classical real numbers from rational numbers in formal language, and the real number field we construct can be applied to higher order proofs.

Key words: Real Number Field, Cauchy sequences, Completeness, Coq, Formal Verification

1. 绪论

1.1 研究背景和意义

程序的形式化证明在许多软件工程的关键领域已得到重要的应用。人们可以利用如 Coq 等交互式定理证明工具，书写形式化的定义、定理和证明，并严格地验证它们的正确性，以彻底消除软件漏洞的存在。实际工程中，无论是验证程序、算法还是数学定理的正确性，都离不开对“数”的形式化刻画。然而在现阶段，形式化证明的大部分应用主要只涉及到数学中的离散对象，如自然数、有理数等。对于数学中的连续对象，如实数的定义等，缺少完整、严格的形式化工作，这会使一些基

于实数公理的形式化证明不具有充分的可靠性，并给后续涉及连续对象的软件形式化验证工作造成困难。因此，给出完整的实数形式化定义和证明，对解决上述问题是十分必要的。

Coq 是本课题使用的研究工具，本文将在 Coq 中完成经典实数理论形式化的工作。在 Coq 标准库中，已经有了关于自然数、有理数、等价关系等内容的有关定义和定理。标准库中虽然也有一些有关实数的性质证明，但这些证明存在显著的缺陷。首先，这些证明基于事先声明的实数公理，没有给出从有理数构造实数的方法，因此我们无法确定这些公理本身、以及它们在 Coq 中的表达形式，在语义上是否具有可靠的正确性。其次，标准库中采用相等 (equality) 而非等价关系 (equivalence) 来定义实数，这会在有关经典实数的证明中产生大量困难和矛盾。因此，我们需要在 Coq 中，给出从有理数到实数的构造方式，并验证我们用形式化语言构造的实数域满足实数公理系统。

本课题中的形式化证明代码都经过了 Coq 的验证和编译，该工作的意义除了可以确保实数形式化的正确性外，还可以给出实数的数学性质在形式化语言中的正确表述形式。此外，由于 Coq 是一种表达力、扩展性极强的语言，本课题中的定义、定理还可以作为一个经过完全形式化验证的库，对接用于其他与实数相关的形式化验证工作中，提供可靠性的保障。

1.2 研究内容与主要创新点

19 世纪后半叶，经过康托尔等数学家的努力，实现了从有理数柯西列等价类构造实数。“实数康托尔构造理论”在严格的科学意义下奠定了分析学的基础。本文在 Coq 中从有理数构造实数的工作，也将采用了康托尔构造实数的方法，康托尔构造的实数定义如下：

定义 1 对有理数列 $[a_n]_n$，如果 $\forall \varepsilon \in \mathbb{Q}, \varepsilon >_{\mathbb{Q}} 0, \exists m \in \mathbb{N}$，使得 $\forall n_1, n_2 >_{\mathbb{N}} m, \left|a_{n_1} - a_{n_2}\right| <_{\mathbb{Q}} \varepsilon$，则称 $[a_n]_n$ 是有理数柯西列。

定义 2 对有理数柯西列 $[a_n]_n, [b_n]_n$，如果 $\lim_{n\to\infty} |a_n - b_n| =_{\mathbb{Q}} 0$，则称 $[a_n]_n$ 与 $[b_n]_n$ 等价。

在 Coq 中，我们可以基于标准库中的有理数定义，把用定义1构造出有理数柯西列定义为实数，用定义2描述实数之间的等价关系，从而在 Coq 中描述实数的等价类。随后根据该定义，我们可以定义实数间的运算、序关系，并证明由此定义出的实数满足实数域的公理系统。其中，实数的完备性将通过柯西准则的证明进行验证。

由于实数康托尔构造的方法和证明已经在许多数学教材中有了详细的阐述，因此本课题的主要研究内容是如何将相对笼统的、灵活的数学语言，转化为严格的形式化语言。本课题中的主要困难也多集中于此：

首先，数学语言中的一些基本定义在 Coq 中需要加以更加严格的形式化描述，例如数学中的有理数列，在 Coq 中的定义是一类符合函数性质的（自然数，有理数）二元关系对，因此在对数列进行证明时必须指明每一次应用了哪一条函数性质，否则不能通过 Coq 的检验。

其次，Coq 对类型有着更加严格的要求，在数学证明中，构造实数的后期往往把整数、有理数及其运算都看作实数的子集进行一并讨论，但这不能符合 Coq 类型检查的要求，因此我们需要为此专门构造有理数到实数的映射，并且在任何一处证明中明确区分讨论的对象是有理数还是一个与有理数等价的实数。

最后，数学证明的语言与能够通过 Coq 检验的形式化语言有许多不匹配之处。一方面，数学证明中存在“显然”的部分，需要我们补充给出必要的形式化证明。另一方面，数学证明中的一些技巧，在 Coq 中是难以实现的。如 Hewitt Edwitt 等 [1] 在证明康托尔实数满足柯西准则时，对有理数柯西列取了一个各元素互不相等的子数列，对此我们了提供新的证明方式，不仅能够完成证明，而且在 Coq 中能便于形式化，这是本文的创新之处。

本课题的研究除了解决上述困难，实现了从有理数到实数的构造和证明外，还构造了一个从实数单元集到实数的单射，这使我们得以用可计算函数的方式构造一个有理数柯西列等价类中的元素，从而对任意满足函数性的实数二元关系，我们都能基于实数单元集到实数单射的函数的性质，在 Coq 中构造可计算函数。这一工作提升了康托尔实数在 Coq 中的扩展性和实用性，并为此后基于实数公理系统的可计算实数的证明提供了帮助。

有关实数的康托尔构造理论能够在很多数学分析教材中找到，本文将重点阐述在 Coq 中对这些数学命题和证明的形式化表述，以及我们针对形式化工作本身特性，对实数构造理论给出的新证明、新方法。

1.3 论文组织结构

从本文的第 2 节开始将按照证明的承接关系，也即 Coq 编译的先后顺序，详细介绍本课题所进行的形式化工作和取得的成果，每一节将首先说明该节给出的新定义和证明目标，随后阐述证明的关键部分，最后给出该段形式化证明的概要。第 2~7 节将分别介绍将实数的加法、乘法、序关系、单元集到实数的单射、极限定义及完备性证明。第 8 节总结本课题的成果和存在需要改进的地方，并提出了下一步工作的设想。

2. 实数的定义

2.1 实数的形式化定义

根据定义1，我们在 Coq 中构造了一个 $(\mathbb{N},\mathbb{Q})$ 的二元关系，要求该二元关系满足函数性且具有有理数柯西列的性质，形式化定义如下。

```
Class Cauchy (CSeq : nat -> Q -> Prop) : Prop := {
  Cauchy_exists : forall (n:nat), exists (q:Q), (CSeq n q);
  Cauchy_unique : forall (n:nat) (q1 q2:Q), CSeq n q1 -> CSeq n q2 -> q1 == q2;
  Cauchy_proper: forall (p q: Q) n, p==q -> (CSeq n p -> CSeq n q);
  Cauchy_def : forall (eps:Q), eps > 0 -> (exists (n:nat), forall (m1 m2:nat), (m1 > n)%nat -> (m2 > n)%nat
   -> forall (q1 q2:Q), CSeq m1 q1 -> CSeq m2 q2 -> Qabs (q1 - q2) < eps);
}.
```

2.2 实数等价关系的形式化定义

对于满足柯西性质的有理数列，我们定义为实数（Real），并且用定义 2 来描述 Coq 中实数的等价关系（Real_ equiv）。

```
Inductive Real : Type :=
| Real_intro (CSeq : nat -> Q -> Prop) (H: Cauchy CSeq).

Definition Real_equiv (x1 x2 : Real) : Prop :=
  match x1, x2 with
  | Real_intro CSeq1 H1,Real_intro CSeq2 H2 => forall (eps:Q), eps>0 -> (exists (n:nat), forall (m:nat), (m
   > n)%nat -> forall (q1 q2:Q), CSeq1 m q1 -> CSeq2 m q2 -> Qabs (q1 - q2) < eps)
  end.
```

我们需要证明该实数二元关系的定义满足等价关系的自反性、对称性和传递性。自反性和对称性的证明可通过展开定义完成，传递性的证明需要我们利用柯西列极限的性质，这些都不难在 Coq 中实现，以传递性为例，形式化证明如下[1]。

[1]由于形式化证明的 Coq 代码较为冗长，且大部分将数学证明形式化的方法在本项目中大同小异，下文中除非必要，将省略证明的形式化代码，或以非形式化的数学证明替代。

```
Theorem Real_def_trans: transitive Real Real_equiv.
Proof. hnf. intros. unfold Real_equiv in *.
  destruct x as [x Hx], y as [y Hy], z as [z Hz]. intros.    % 展开定义
  assert (Heps: eps == eps *(1#2) + eps *(1#2)) by ring.     % 有理数的算数性质
  destruct (H _ (eps_divide_2_positive eps H1)) as [n1 Hab]. % 得到命题Hab: 对任意 n>n1, |x[n]-y[n]|<eps/2
  destruct (H0 _ (eps_divide_2_positive eps H1)) as [n2 Hbc].% 得到命题Hbc: 对任意 n>n2, |y[n]-z[n]|<eps/2
  clear H. clear H0.
  assert (H: le n1 n2 \/ ~ (le n1 n2)).
    { apply classic. } destruct H.                           % 对n1,n2大小关系讨论，这里用到了排中律公理
  - exists n2. intros m H0 q1 q3.                            % n1<=n2时，取N=n2，考虑数列中第N项之后的任意第m项
    assert (H': (m > n1)%nat). { omega. }
    intros Hxq Hzq.
    destruct (Cauchy_exists _ Hy m) as [q2 Hyq].
    apply (Hab _ H' q1 q2) in Hxq.                           % 将m>n1应用到Hab性质中，得|x[m]-y[m]|<eps/2
    apply (Hbc _ H0 q2 q3) in Hyq.                           % 将m>n1应用到Hbc性质中，得|y[m]-z[m]|<eps/2
    apply Qlt_le_weak in Hyq.
    apply (Qle_lt_trans _ _ _ (Qabs_triangle q1 q2 q3)).     % 利用有理数库中的三角不等式，可得|x[m]-z[m]|<eps
    rewrite Heps. apply (Qplus_lt_le_compat _ _ _ _ Hxq Hyq).
    apply Hzq. apply Hyq.
  - exists n1. ...                                           % n1>n2的情况，取N=n1，证明类似，省略
Qed.
```

进一步，我们可以将实数的等价关系写作 Coq 中 RelationClass 标准库的一个实例（Instance）。这样做的好处是在接下来的证明中，如果一个函数已被证明能保持实数的等价性，那么当我们需要进行重写操作（rewrite），在命题中替换等价实数时，Coq 能够借助这一实例将等价关系的证明自动化。以上，我们便完成了实数等价类的定义和性质证明，在 Coq 中，我们用记号 == 表示这一等价关系。

为了满足 Coq 类型检查的需要，我们还需要定义有理数到实数的映射用于之后的证明。

例 1 (有理数的实数表示) 对任意 $q \in \mathbb{Q}$，$\{(n, q_n) \in \mathbb{N} \times \mathbb{Q} \mid q_n = q\}$ 是它合法的实数表示。

证明 第一，对任意 $n \in \mathbb{N}$，存在 q 是它的第 n 项。

第二，对第 n 项，如果 $q_1 = q, q_2 = q$ 同时成立，则 $q_1 = q_2$。

第三，如果 $q_1 = q_2$，则如果 q_1 是有理数列的第 n 项，即 $q_1 = q$，那么有 $q_2 = q$，则 q_2 也是该有理数列的第 n 项

可以证明，该关系是一个 $\mathbb{N} \to \mathbb{Q}$ 的一个函数。下证符合该数列是一个柯西列，

取 $N = 0$，由定义，对任意 ε，都有 $|q_1 - q_2| = 0 < \varepsilon$。 □

在 Coq 中，我们定义 (inject_Q q) 为有理数的实数表示，例1是形式化地构造该表示的证明。

3. 实数的加法

3.1 实数加法的定义

在实数的康托尔构造中，将两个有理数柯西列每一项之和构成的有理数列定义为两个实数的和。不难利用柯西列的性质证明新构造的数列也是满足柯西列性质的实数。实数加法的数学定义如下。

定义 3 (实数加法) 对实数 $\{a_n\}_n$、$\{b_n\}_n$，定义 $\{a_n\}_n + \{b_n\}_n = \{a_n + b_n\}_n$。

在 Coq 中，对实数运算的形式化定义，我们需要首先构造一个有理数列的函数，随后证明该函数所得的有理数列是柯西列。以下是省略证明后，实数加法的完整形式化构造。

```
Definition CauchySeqPlus (A B: nat -> Q -> Prop): (nat -> Q -> Prop) :=
  fun (n:nat) (q:Q) =>  forall (q1 q2:Q), A n q1 -> B n q2 -> q == q1 + q2.
Theorem Cauchy_Plus_Cauchy: forall A B, Cauchy A -> Cauchy B  -> Cauchy (CauchySeqPlus A B).
```

```
Definition Rplus(a b : Real) : Real :=
  match a with
  | (Real_intro A HA) => match b with
                        | (Real_intro B HB) =>
                          Real_intro (CauchySeqPlus A B) (Cauchy_Plus_Cauchy A B HA HB)
                         end
  end.
Infix "+" := Rplus : Real_scope.
```

3.2 实数加法的性质

不难利用柯西列的性质证明，实数加法能够保持实数的等价关系。

定理 1 对实数 $\{a_n\}_n$、$\{b_n\}_n$、$\{a'_n\}_n$、$\{b'_n\}_n$，如果有 $\{a_n\}_n =_{\mathbb{R}} \{a'_n\}_n$，$\{b_n\}_n =_{\mathbb{R}} \{b'_n\}_n$，则 $\{a_n\}_n + \{b_n\}_n =_{\mathbb{R}} \{a'_n\}_n + \{b'_n\}_n$

由于我们利用等价关系来定义实数，因此对于新定义的运算，必须要证明经过该运算，实数间的等价关系仍能够被保持。在 Coq 中，我们可以将定理1的证明形式化为 RelationClass 库中的 Proper 实例，这样在之后的证明中，Coq 能够借助这一实例将该运算下等价关系的重写证明自动化。Proper 实例的表述如下。

```
Instance Rplus_comp : Proper (Real_equiv ==> Real_equiv ==> Real_equiv) Rplus.
```

此外，实数关于加法的运算是一个阿贝尔群，为此，数学中定义了实数加法的单位元和加法的逆元。

定义 4 (实数加法的单位元和逆元) 1. 定义 $\{0\}_n$ 为实数加法的零元；2. 对实数 $\{a_n\}_n$，定义 $\{-a_n\}_n$ 为该实数的加法逆元。

这些数学定义可以在 Coq 中用同样的方法得到形式化的定义。通过将定义展开，可以证明实数加法满足阿贝尔群的性质，以下是实数在加法下满足阿贝尔群性质的形式化命题。这些命题都可以用展开定义的方法，将命题中实数的加法转化为有理数列每一项的加法，直接应用有理数的加法性质进行证明。

```
Theorem Rplus_comm : forall (A B: Real),  (A + B == B + A)%R.
Theorem Rplus_assoc: forall (A B C: Real),  (A + B + C == A + (B + C))%R.
Theorem Rplus_Zero: forall (A : Real),  (A + Rzero == A)%R.
Theorem Rplus_opp_r : forall (A:Real),  (A + (Ropp A)== Rzero)%R.
```

根据数学定义4，我们可以在 Coq 中形式化实数相反数、实数减法的定义。

```
Definition Cauchy_opp (A : nat -> Q -> Prop): (nat -> Q -> Prop) :=
    fun (n:nat) (q:Q) => forall (q1:Q), (A n q1) -> q == - q1.
Theorem Cauchy_opp_Cauchy: forall A, Cauchy A -> Cauchy (Cauchy_opp A).
Definition Ropp(a : Real) : Real :=
  match a with
    | (Real_intro A HA) => Real_intro (Cauchy_opp A) (Cauchy_opp_Cauchy A HA)
  end.
Notation "- x" := (Ropp x) : Real_scope.
Definition Rminus (a b:Real) := Rplus a (Ropp b).
Infix "-" := Rminus : Real_scope.
```

为方便此后的证明，我们还可以从以上所证得阿贝尔群四条性质出发，无需展开实数的定义，证明一些有用的推论，举例如下。

```
Instance Rminus_comp : Proper (Real_equiv ==> Real_equiv ==> Real_equiv) Rminus.
Theorem Ropp_involutive: forall x, (x == - - x)%R.
Lemma Rplus_inj_r (x y z: Real): (x + z == y + z)%R <-> (x == y)%R.
```

数学教材在有关实数运算的性质中，一般直接将有理数作为实数的子集进行讨论。但在 Coq 中，我们需要对有理数与有理数构造的实数加以区分，因此需要对 inject_Q 函数的一些性质加以必要的证明。这些证明通常通过简单的展开定义即可完成，举例如下。

```
Lemma inject_Q_plus (x y: Q): (inject_Q (x + y) == inject_Q x + inject_Q y)%R.
Lemma inject_Q_opp (x: Q): (inject_Q (- x) == - inject_Q x)%R.
Instance inject_Q_comp: Proper (Qeq ==>Real_equiv) inject_Q.
Lemma inject_Q_nonzero: forall q, ~ q == 0 -> ~ (inject_Q q == 0)%R.
```

在定义实数的加法操作 Rplus 及其记号后，此后书写命题和证明时，就可以不用再每次考虑实数背后复杂的构造过程，而是能通过应用现有的定理，将证明以一种相对简洁的方式呈现。

4. 实数的乘法

4.1 实数乘法的定义

与实数的加法类似，对两个有理数柯西列，它们每一项的乘积构成的数列就是这两个实数的乘积。数学中，为了证明新的数列满足柯西列的性质，需要首先证明一个引理。

引理 2 (有理数柯西列必有界) 如果 $\{a_n\}_n$ 是有理数柯西列，那么 $\exists M \in \mathbb{Q}$，使得 $\forall n \in \mathbb{N}$，$|a_n| \leq M$。

证明 令 $\varepsilon = 1$，则可以找到 $N \in \mathbb{N}$，使得 $\forall n \geq N, m \geq N$，有 $|a_n - a_m| < 1$。

则对任意 $n > N$，有 $|a_n| = |a_n - a_N + a_N| \leqslant |a_n - a_N| + |a_N| < |a_N| + 1$。

令

$$M = \max\left(|a_1|, \cdots, |a_{N-1}|, |a_N| + 1\right) \tag{1}$$

则对一切 $n \in \mathbb{N}$，有 $|a_n| \leq M$

所以 $\{a_n\}_n$ 是有界的。 □

由此，可以证明有理数柯西列相乘的结果也是有理数柯西列。

定理 3 如果 $\{a_n\}_n$，$\{b_n\}_n$ 是有理数柯西列，那么 $\{a_n \cdot b_n\}_n$ 是有理数柯西列。

证明 由引理2，$\exists M \in \mathbb{Q}, M > 0$，$|a_{\mathrm{n}}| \leqslant M$，　$|b_n| \leqslant M$

对任意 ε，由柯西列性质，对 $\frac{M}{2\varepsilon}$，可以找到 N，

$\forall n > N, m > N$，有 $|a_n - a_m| < \frac{\varepsilon}{2M}$，$|b_{\mathrm{n}} - b_{\mathrm{m}}| < \frac{\varepsilon}{2M}$。于是

$$\begin{aligned} |a_n b_n - a_m b_m| &= |a_n b_n - a_m b_n + a_m b_n - a_m b_m| \\ &\leqslant |b_n|\,|a_m - a_m| + |a_m|\,|b_n - b_m| \\ &< M \cdot \frac{\varepsilon}{2M} + M \cdot \frac{\varepsilon}{2M} = \varepsilon \end{aligned} \tag{2}$$

所以 $\{a_n b_n\}_n$ 是有理数柯西列。 □

与加法类似，要在 Coq 中定义实数的乘法运算 Rmult，我们需要定义一个对有理数列的乘法运算，并且证明该运算的结果符合柯西列性质。乘法运算的定义如下。

```
Definition CauchySeqMult (A B: nat -> Q -> Prop): (nat -> Q -> Prop) :=
  fun (n:nat) (q:Q) => forall (q1 q2:Q), A n q1 -> B n q2 -> q == q1 * q2.
```

数学证明中，在证明乘法符合柯西列性质的过程中，公式1中取了若干项的最大值，但这在 Coq 的形式化证明中不是显然的。对于 $n > N$ 的情况，我们可以形式化已有定理2的数学证明，而对于 $n \leq N$ 的情况，则需要我们对数列前有限项的有界性另外作出证明。

引理 4 有理数柯西列的前有限项必有界

证明 对前 N 项作归纳证明。

$N = 0$ 时，显然成立。

归纳假设：对柯西列 $\{a_n\}_n$，$\exists M \in \mathbb{Q}, \forall n \in \mathbb{N}, n < N$，有 $|a_n| < M$

令 $M' = max\{M, a_N + 1\}$，则对任意 $n < N + 1$，有 $a_n < M'$，命题成立 □

结合以上两部分，我们就能在 Coq 中形式化地证明柯西列的有界性。将柯西列的有界性应用于定理3的证明，我们就能形式化实数乘法的定义，证明节选如下。

```
Lemma CauchySeqBounded_weak:                                    %对n足够大时，柯西列有界的证明
 forall A, Cauchy A -> exists (N:nat), exists (M:Q), forall (n:nat) (q:Q),(n>N)%nat -> A n q -> (Qabs q)<M.
Lemma FiniteSeqBounded:  forall (A:nat->Q->Prop) (N:nat),    %对n<=任意N时，柯西列有界的证明
 Cauchy A -> exists (M:Q), forall (n:nat)(q:Q), (n < N)%nat -> A n q -> Qabs q < M.
Lemma CauchySeqBounded: forall A, Cauchy A -> exists (M:Q), 0 < M
 /\forall (n:nat) (q:Q), A n q -> (Qabs q) < M.
Proof. intros.
  destruct (CauchySeqBounded_weak _ H) as [N [M1 HM1]].
  destruct (FiniteSeqBounded _ (S N) H) as [M2 HM2].
  assert (HM: Qle M1 M2 \/ ~ (Qle M1 M2)). { apply classic. } destruct HM as [HM | HM].
- exists M2. ...
- exists M1. ...
Qed.
Theorem Cauchy_Mult_Cauchy : forall A B, Cauchy A -> Cauchy B -> Cauchy (CauchySeqMult A B).
Definition Rmult(a b:Real):Real:=
match a with
| (Real_intro A HA) => match b with
                       | (Real_intro B HB) =>
                          Real_intro (CauchySeqMult A B) (Cauchy_Mult_Cauchy A B HA HB)
                       end
end.
```

4.2 实数乘法的性质

接下来，需要证明实数关于乘法的运算是一个阿贝尔群。我们定义有理数 1 的常数列为乘法的单位元，在 Coq 中，实数乘法的交换律、结合律、分配律以及乘法单位元的证明都可以通过展开定义，转换成对有理数列第 n 项运算性质的证明问题得到求证。有关乘法性质的证明，较为复杂的部分在于对乘法逆运算的定义。数学中，对于非零实数乘法逆元的定义，需要首先证明一些引理。

引理 5 设 $\{a_n\}_n$ 是非零有理数的柯西列，且 $\lim_{n\to\infty} a_n \neq 0$，则存在 $\varepsilon_0 \in \mathbb{Q}, \varepsilon > 0$，使得 $|a_n| \geqslant \varepsilon_0$ 对一切 $n \in \mathbb{N}$ 成立。

证明 由 $\lim_{n\to\infty} a_n \neq 0$ 知，$\exists \varepsilon_1, \forall N \in \mathbb{N}, \exists n_N > N, \left|a_{n_N}\right| > \varepsilon_1$。

由 $\{a_n\}_n$ 是有理数的柯西列，令 $\varepsilon = \frac{\varepsilon_1}{2}$，$\exists N_1, \forall n > N_1, m > N_1, |a_n - a_m| < \frac{\varepsilon_1}{2}$

则当 $n > n_{N_1}$ 时，有

$$|a_n| = \left|a_n - a_{N_1} + a_{n_{N_1}}\right| \geqslant \left|a_{n_{N_1}}\right| - \left|a_n - a_{n_N}\right| > \frac{\varepsilon_1}{2} \tag{3}$$

令 $\varepsilon_0 = \min\left(|a_1|, \cdots, \left|a_{n_N}\right|, \frac{\varepsilon_1}{2}\right)$，对任意 n 有

$$|a_n| \geqslant \varepsilon_0 \tag{4}$$

引理 6 设 $\{a_n\}_n$ 是非零有理数的柯西列，且 $\lim_{n\to\infty} a_n \neq 0$，则 $\{\frac{1}{a_n}\}_n$ 是有理数柯西列。

证明 对任意给定正有理数 ε，由 $\{a_n\}_n$ 是柯西列，$\exists N \in \mathbb{N}, \forall n > N, m > N, |a_n - a_m| < \varepsilon_0^2\varepsilon$。于是

$$\left|\frac{1}{a_n} - \frac{1}{a_m}\right| = \frac{|a_m - a_n|}{|a_n a_m|} < \frac{1}{\varepsilon_0^2} \cdot \varepsilon_0^2\varepsilon = \varepsilon \tag{5}$$

所以，$\{\frac{1}{a_n}\}_n$ 是有理数柯西列。 □

定义 5 (实数乘法的逆元) 对有理数柯西列 $\{a_n\}_n$，取它的非零子列 $\{a'_n\}_n$，则由引理6和定理3，可以说明 $\{\frac{1}{a'_n}\}_n$ 是 $\{a_n\}_n$ 的逆元，即 $\{a_n\}_n \cdot \{\frac{1}{a_n}\}_n =_{\mathbb{R}} 1$

以上的数学证明中，引理5、引理6的条件是有理数的非零数列。虽然这在数学中不失一般性，但在 Coq 中，对形式化定义的有理数列，我们难以构造形式化方法来剔除其中的零项，因此不能直接形式化以上证明来构造实数的倒数。

我们所采用的另一种构造方法是直接将该有理数列的每一项取倒数。在 Coq 的有理数标准库中，0 的倒数被定义为 0 本身，因此我们的定义不会因为数列中可能存在 0 而不通过 Coq 的验证。注意到对极限不为 0 的有理数柯西列必然存在 N，使得当 $n > N$ 时该数列没有一项等于 0。因此，我们可以通过证明第 N 项之后的有理数列具有引理5、引理6描述的性质，从而证明原有理数列取倒数后，在 n 足够大时能够满足柯西性质，回避剔除零项的问题。

```
Definition limit_not_0 (A:nat->Q->Prop):Prop:=  % 描述一个有理数列极限不为0
(exists (eps:Q), eps>0 /\ forall (N:nat), exists(nN:nat),(nN > N)%nat /\ (forall(q:Q), A nN q -> Qabs q >
   eps)).
Definition limit_not_0_real (A:Real):Prop:=
match A with | Real_intro CA HA => limit_not_0 CA end.
```

为此，我们在形式化的过程中，需要对引理5的条件加以改写，由“非零有理数列”改成“从某一项开始为非零数列”。形式化后的命题如下。注意到数学证明中，公式4中对若干项有理数取了最小值的操作，因此我们在引理5的证明中，也需要用类似引理4的证明方法，对 n 足够大时和 n 属于前有限项的情况做分别证明。

```
Lemma limit_not_0_seq : forall A (H:Cauchy A), limit_not_0_real (Real_intro A H) -> exists (N:nat), forall n
   , (n>N)%nat ->forall q, A n q -> ~(q == 0).
Lemma FiniteNo0SeqBounded_Below_positive:
forall (A:nat->Q->Prop) (N:nat), Cauchy A -> (exists N',forall n, (n>N')%nat ->  ~(A n 0)) -> exists (N':nat
   ),exists (M:Q), M>0 /\ forall (n:nat)(q:Q), (n>N')%nat -> (n < N)%nat -> A n q -> Qabs q >= M.
Lemma Cauchy_nonzero_pre: forall A (HA:Cauchy A), limit_not_0_real (Real_intro A HA) -> exists (N:nat), (
   exists (eps0:Q), eps0>0 /\ (forall (n:nat), (n>N)%nat -> forall(q:Q), A n q -> Qabs q >= eps0)).
```

进一步将引理6的数学证明形式化，可以证明在柯西列极限不为零时，对数列每一项取倒数，结果仍为一个柯西列。

```
Lemma Cauchy_inv_nonzero: forall A  (H:Cauchy A) , limit_not_0_real (Real_intro A H) -> Cauchy (fun (n:nat)(
   q:Q) => A n (/q)).
```

注意到柯西列的极限不为零，与实数意义下柯西列不等于零，两者在展开定义后是等价的。前者在证明构造时较为方便，而后者则更符合直观，且便于之后的证明使用，因此我们在定义实数倒数 Rinv 时，证明了两个条件命题的定价性，并用实数不等于零作为构造 Rinv 偏函数的条件。

```
Lemma limit_not_0_spec: forall x: Real, (~ x == Rzero)%R <-> limit_not_0_real x.
Definition Rinv (a: {a0: Real | (~ a0 == Rzero)%R }): Real :=
  match a with
  | exist _ (Real_intro a0 H) H0 =>
      Real_intro (fun (n : nat) (q : Q) => a0 n (/ q))
        (Cauchy_inv_nonzero a0 H (proj1 (limit_not_0_spec (Real_intro a0 H)) H0))
  end.
Notation "/ x" := (Rinv x) : Real_scope.
Definition Rdiv x y := Rmult x (Rinv y).
Infix "/" := Rdiv : R_scope.
```

到此为止，我们已形式化地证明了实数及其定义的加法、乘法构成了一个域。在 Coq 中，对于环包含的运算，可以借助标准库中的 ring_theory 进行自动化证明。

```
Definition Rsrt : (ring_theory 0 1 Rplus Rmult Rminus Ropp Real_equiv)%R.
Proof.
  constructor.
  - exact Rplus_0_l.
  - exact Rplus_comm.
  - intros. rewrite Rplus_assoc. reflexivity.
  - exact Rmult_1_l.
  - exact Rmult_comm.
  - intros. rewrite Rmult_assoc. reflexivity.
  - exact Rmult_plus_distr_l.
  - reflexivity.
  - exact Rplus_opp_r.
Qed.
Add Ring Rring :Rsrt.
```

5. 实数的序关系

5.1 实数正负性的定义

两个实数的序关系可以通过比较他们相减结果的正负进行定义，因此在定义实数的序关系前，需要首先定义实数的正负性。实数四则运算中，实数的四则运算是直接通过其每一项有理数四则运算直接定义的，但在序关系的定义中，这一方法不再适用，我们需要使用极限的语言描述实数的正负性。

定义 6 (正实数) 实数 $\{a_n\}_n$ 为正实数，如果 $\exists \varepsilon_0 \in \mathbb{Q}, \varepsilon_0 > 0, \exists N \in \mathbb{N}, \forall n \geq N$，有 $a_n \geq \varepsilon_0$。

这一定义可以在 Coq 中形式化地写作如下形式，同时也不难用柯西列的性质证明，等价的实数其正负性保持一致。

```
Definition Rpositive (A:Real):Prop:=
  exists eps0:Q, (eps0>0) /\ (exists N, forall n, (n>=N)%nat ->  forall q,
    (match A with | Real_intro A0 _ => A0 end) n q -> q >= eps0).

Theorem Rpositive_equiv: forall A B, (A == B)%R -> Rpositive A -> Rpositive B.
Instance Rpositive_proper_iff: Proper (Real_equiv ==> iff) Rpositive.
```

可以简单地定义负实数是正实数的相反数。

```
Definition Rnegative (A:Real):Prop:= Rpositive (Ropp A).
Instance Rnegative_proper_iff: Proper (Real_equiv ==> iff) Rnegative.
```

不难经过一些基于极限方法的引理证明，正实数集、零、负实数集是实数的一个分割，这是我们下一步证明实数集是一个有序集的基础。

```
Theorem Real_positive_0_negative: forall A,
 ( Rpositive A /\ ~(A==Rzero)%R  /\ ~ Rnegative A ) \/
 ( ~ Rpositive A /\ (A==Rzero)%R  /\ ~ Rnegative A ) \/
 ( ~ Rpositive A /\ ~(A==Rzero)%R  /\ Rnegative A ).
```

5.2 实数序关系的定义

通过实数的正负性和实数减法运算，可以定义实数的序关系。不难通过 Rpositive、Rminus 的 Proper 性质，证明以下序关系也具有 Proper 性质。

```
Definition Rlt (a b:Real) : Prop := Rpositive (Rminus b a).
Notation "a < b" := (Rlt a b):Real_scope.
Definition Rle (a b:Real) : Prop :=  (a < b)%R \/ (a == b)%R.
Notation "a <= b" := (Rle a b):Real_scope.
Definition Rgt (a b:Real) : Prop :=  (b < a)%R.
Notation "a > b" := (Rgt a b):Real_scope.
Definition Rge (a b:Real) : Prop :=  (b <= a)%R.
Notation "a >= b" := (Rge a b):Real_scope.
Instance Rlt_comp: Proper (Real_equiv ==> Real_equiv ==> iff) Rlt.
Instance Rgt_comp: Proper (Real_equiv ==> Real_equiv ==> iff) Rgt.
Instance Rle_comp: Proper (Real_equiv ==> Real_equiv ==> iff) Rle.
Instance Rge_comp: Proper (Real_equiv ==> Real_equiv ==> iff) Rge.
```

可以在 Coq 中将以下证明形式化，验证我们定义的序关系满足顺序公理。

定理 7 (实数序关系的传递性) 如果对实数 A,B,C，$A <_{\mathbb{R}} B$ 且 $B <_{\mathbb{R}} C$，则有 $A <_{\mathbb{R}} C$.

证明 由 $A < B$，$\exists \varepsilon_{AB} >_{\mathbb{Q}} 0, \exists N_{AB}, \forall n > N_{AB}, b_n - a_n \geq \varepsilon_{AB}$

由 $B < C$，$\exists \varepsilon_{BC} >_{\mathbb{Q}} 0, \exists N_{BC}, \forall n > N_{BC}, c_n - b_n \geq \varepsilon_{BC}$

令 $\varepsilon_{AC} = 2 \cdot min\{\varepsilon_{AB}, \varepsilon_{BC}\}$。对 $n > max\{N_{AB}, N_{BC}\}$，有

$$c_n - a_n = (c_n - b_n) + (b_n - a_n) \geq \varepsilon_{AB} + \varepsilon_{BC} \geq \varepsilon_{AC} \tag{6}$$

所以实数 $A <_{\mathbb{R}} C$ □

可以用展开定义的方法，证明实数加法和乘法维持了序关系。

```
Theorem Rlt_plus_r: forall (A B C:Real), (A < B)%R -> (A+C < B+C)%R.
Theorem Rlt_mult_r: forall (A B C:Real),  (Rpositive C) ->(A < B)%R -> (A*C < B*C)%R.
```

综上，我们形式化定义的序关系满足了实数的公理系统。

5.3 实数绝对值的定义

实数的绝对值在有关实数性质的证明中具有重要的作用，有必要在 Coq 中形式化地定义实数绝对值。通常数学中将实数绝对值定义为一个由实数到实数的分段函数，分段标准以实数的正负性为界。在 Coq 中，由于实数的正负性是通过 Real→Prop 定义的，我们不能用分段函数的方式写出实数绝对值函数定义。尽管这种分段函数的定义方式可以用一个满足函数性的 Real→Real→Prop 二元关系替代，但这将为此后的证明带来极大的不便。为此，我们采用如下的函数定义，将有理数列每一项取绝对值。

```
Definition Cauchy_abs (A : nat -> Q -> Prop): (nat -> Q -> Prop) :=
    fun (n:nat) (q:Q) => forall (qabs:Q), (A n qabs) -> q == (Qabs qabs).
```

定理 8 将有理数柯西列每一项取绝对值所得的数列仍是有理数柯西列。

证明 容易说明，由于 $\{a_n\}_n$ 满足函数性，$\{|a_n|\}_n$ 也满足函数性。

下证 $\{|a_n|\}_n$ 是柯西列，

对任意 ε，由 $\{a_n\}_n$ 是柯西列，可以找到 $N_0, \forall m,n > N_0, |a_n - a_m| < \varepsilon$。

令 $N = N_0$，对任意 $m,n > N$，

$$||a_n| - |a_m|| \leq |a_n - a_m| < \varepsilon \tag{7}$$

因此 $\{|a_n|\}_n$ 是有理数柯西列。 □

以上的取绝对值函数定义和定理8完成了实数绝对值的构造。

容易通过将定义展开，证明我们形式化定义的实数绝对值是正确的。

```
Theorem Rabs_zero: (Rabs 0 == 0)%R.
Theorem Rabs_positive: forall A, Rpositive A -> (Rabs A == A)%R.
Theorem Rabs_negative: forall A, Rnegative A -> (Rabs A == Ropp A)%R.
```

利用排中律公理对实数的正负性进行讨论，我们可以证明更多实数绝对值有用的性质，用于之后的证明。

```
Theorem Rabs_triangle: forall A B, (Rabs(A+B)<= Rabs A + Rabs B)%R.
Theorem Rabs_Rle: forall A,  (A <= Rabs A)%R.
```

6. 形式化实数的重要性质

目前为止，我们已构造并证明了实数公理中的所有基本运算及其性质。在开始实数完备性的证明之前，我们首先证明一些重要的性质。

6.1 实数的阿基米德性质

作为实数公理系统的组成部分，数学中阿基米德公理的表述如下。以下是本课题中对这一公理的非形式化证明过程。

定理 9 (阿基米德公理) 若实数 $B >_{\mathbb{R}} A >_{\mathbb{R}} 0$，则存在 $N \in \mathbb{N}, N \cdot A >_{\mathbb{R}} B$。

证明 由 B 为实数，得有理数列 $\{b_n\}_n$ 有界，设上界为 $M \in \mathbb{Q}$，则有

$$b_n \leq_{\mathbb{Q}} \lceil M \rceil + 1 \tag{8}$$

由 A 为正实数，根据定义，则 $\exists N_1 \in \mathbb{N}, \varepsilon \in \mathbb{Q}, \forall m,n > N_1, a_n > \varepsilon$。

令 $N = (\lceil M \rceil + 1) \times_{\mathbb{N}} \lceil \frac{1}{\varepsilon} \rceil$，其中 $\lceil M \rceil$ 表示取 M 的上整。

考虑 $n > N_1$ 时，实数 $\{N \cdot a_n\}_n$，有

$$\begin{aligned} N \cdot a_n &= (\lceil M \rceil + 1) \cdot_{\mathbb{N}} \lceil \frac{1}{\varepsilon} \rceil \cdot_{\mathbb{Q}} a_n \\ &\geq (\lceil M \rceil + 1) \cdot_{\mathbb{N}} \frac{a_n}{\varepsilon} \\ &\geq \lceil M \rceil + 1 > M + \frac{1}{2} > b_n + \frac{1}{2} \end{aligned} \tag{9}$$

令 $N = N_1, \varepsilon_0 = \frac{1}{2}$，可由定义证明 $N \cdot A >_{\mathbb{R}} B$。 □

一般的数学证明中，公式8和公式9是不必要的。但在 Coq 中，由于实数和有理数、整数的乘法不能看作同一个操作，需要区分类型，因此在此处的证明中，我们利用了 Coq 有理数标准库中取上整的性质，对不等式进行放缩，完成了证明。形式化后的阿基米德公理如下。

```
Theorem R_Archimedian: forall A B, Rpositive A -> (B>A)%R -> exists (N:nat), (inject_Q (inject_Z (Z.of_nat N
    )) * A > B)%R.
```

6.2 实数的取下整函数

为了构造实数单元集到实数的单射，我们首先需要构造一个实数到整数的取下整函数。但限于有理数柯西列的任意性，Coq 中无法写出 $\mathbb{R} \to \mathbb{Z}$ 的函数。我们用以下的二元关系作为取代，并且证明该二元关系具有函数性。

```
Definition Rfloor (A:Real)(z:Z):Prop :=
 (inject_Q (inject_Z z) <= A)%R /\ (inject_Q ((inject_Z z) + 1) > A)%R.
```

非形式化的证明过程如下。

定义 7 (实数的取下整关系) 定义二元关系 $\mathbf{L} = \{(\{a_n\}_n, z) \in \mathbb{R} \times \mathbb{Z} \mid z \leq_{\mathbb{R}} \{a_n\} \wedge z+1 \geq_{\mathbb{R}} \{a_n\}\}$，记作 $\{a_n\}_n \mathbf{L} z$，表示 z 是实数 $\{a_n\}_n$ 的下整。

定理 10 (实数下整的存在性) 对任意实数 $\{a_n\}_n$，存在整数 z，使得 $\{a_n\}_n \mathbf{L} z$。

证明 由 $\{a_n\}_n$ 的柯西列性质，令 $\varepsilon = \frac{1}{4}$，存在 N，对任意 $m,n > N$，有 $|a_n - a_m| < \frac{1}{4}$。记 $z' = \lfloor a_{N+1} \rfloor$。

1. 若 $z' \leq_{\mathbb{R}} \{a_n\}_n$ 且 $z'+1 \leq_{\mathbb{R}} \{a_n\}_n$，取 $z = z'+1$，$z = z'+1 \leq_{\mathbb{R}} \{a_n\}_n$ 可直接得证。
   令 $\varepsilon_0 = \frac{1}{2}$，对任意 $n \geq N+1$，$z'+2-a_n > a_{N+1} - a_n + 1 > 1 - |a_{N+1} - a_n| > 1 - \frac{1}{4} > \varepsilon_0$
   即 $z+1 \geq_{\mathbb{R}} \{a_n\}_n$。所以存在 $z = z'+1$，使得 $\{a_n\}_n \mathbf{L} z$。
2. 若 $z' \leq_{\mathbb{R}} \{a_n\}_n$ 且 $z'+1 >_{\mathbb{R}} \{a_n\}_n$，取 $z = z'$
3. 若 $z' >_{\mathbb{R}} \{a_n\}_n$ 且 $z'+1 \leq_{\mathbb{R}} \{a_n\}_n$，取 $z = z'-1$。
4. 若 $z' >_{\mathbb{R}} \{a_n\}_n$ 且 $z'+1 >_{\mathbb{R}} \{a_n\}_n$，取 $z = z'-2$。

2~4 情况的证明与 1 的方法类似。

定理 11 (实数下整的唯一性) 对任意实数 $\{a_n\}_n$，若整数 z_1, z_2 都满足 $\{a_n\}_n \mathbf{L} z_1$，$\{a_n\}_n \mathbf{L} z_2$，则 $z_1 = z_2$。

证明 假设法，若 $z_1 \neq z_2$，不妨设 $z_1 + 1 \leq z_2$，则由下取整函数的定义

$$\{a_n\}_n < z_1 + 1 \leq_{\mathbb{R}} z_2 \leq_{\mathbb{R}} \{a_n\}_n \tag{10}$$

□

产生矛盾。

实数下整保持实数定义的等价性可以展开定义，由实数运算、序关系的 Proper 性质进行证明。

综上，我们形式化地定义了实数的取整关系，并证明了该关系具有函数性。在此后的证明中，我们可以像使用柯西数列的函数性一样应用这些性质。

6.3 构造实数单元集到实数的单射

从实数单元集到实数的单射函数在 Coq 中十分重要，对任意有理数柯西列的等价类，我们都能通过这一单射函数构造出该单元集中的实数。更进一步，对任意满足函数性的实数二元关系，我们都能基于实数单元集到实数的单射函数性质，构造 Coq 中的可计算函数。我们目标构造的单射函数类型定义如下。

```
Definition RSingleFun : {X: Real -> Prop|(exists x, X x) /\ (forall x1 x2, X x1 ->
 X x2 -> x1 == x2) /\ Proper (Real_equiv ==> iff) (X) }%R -> Real.
Admitted.
```

该构造函数要求提供一个实数集合，同时该实数集要求非空，其中所有元素具有等价性，且包含所有等价的元素，通过该函数我们能构造出该实数等价类的代表元素。我们的构造方法如下：

定义 8 对实数等价类 $[\{a_n\}_n]_{\mathbb{R}}$，令 $b_n = \frac{\lfloor a_n \cdot n \rfloor}{n}$，则有理数列 $\{b_n\}_n$ 是该等价类对应的实数。

该构造方法在 Coq 中的形式化表述如下：

```
(fun n q => exists A, S A /\ forall z, (Rfloor (A * (inject_Q (inject_Z (Z.of_nat (n)%nat)))) z) -> q == z #
    (Pos.of_nat (n)%nat)).
```

不难证明，我们所构造出的有理数列，其函数性可以通过单元集的性质得到保证。下面证明通过该方法构造出的有理数列是柯西列。

定理 12 对任意实数等价类 $[\{a_n\}_n]_{\mathbb{R}}$ 中的元素 $\{a_n\}_n$，$\{b_n\}_n = \{\frac{\lfloor a_n \cdot n \rfloor}{n}\}_n$ 是一个柯西列。

证明 对任意 ε，令 $N = max\{2, 1 + \lceil \frac{1}{\varepsilon} \rceil\}$。对任意 $m, n > N$，

$$\begin{aligned} b_n - b_m &= \frac{\lfloor \{a_n\}_n \cdot n \rfloor}{n} - \frac{\lfloor \{a_n\}_n \cdot m \rfloor}{m} \\ &< \frac{\{a_n\}_n \cdot n}{n} - \frac{\{a_n\}_n \cdot m - 1}{m} \\ &< \{a_n\}_n - \{a_n\}_n + \frac{1}{m} \\ &< \frac{1}{1 + \lceil \frac{1}{\varepsilon} \rceil} < \varepsilon \end{aligned} \tag{11}$$

同理可证

$$\begin{aligned} b_n - b_m &= \frac{\lfloor \{a_n\}_n \cdot n \rfloor}{n} - \frac{\lfloor \{a_n\}_n \cdot m \rfloor}{m} \\ &> \frac{\{a_n\}_n - 1 \cdot n}{n} - \frac{\{a_n\}_n \cdot m}{m} \\ &> \{a_n\}_n - \{a_n\}_n - \frac{1}{n} \\ &> -\frac{1}{1 + \lceil \frac{1}{\varepsilon} \rceil} > -\varepsilon \end{aligned} \tag{12}$$

所以对任意 $m, n > N$，$|b_n - b_m| < \varepsilon$。该有理数列是柯西列。 □

进一步，我们验证经过该函数所得的柯西列与原单元集中的元素是相等的实数。首先我们证明一个引理。

引理 13 对实数 $\{a_n\}_n$，对任意的有理数 $\varepsilon > 0$，存在 $N \in \mathbb{N}, \forall n > N, |\{a_n\}_n -_{\mathbb{R}} a_n| <_{\mathbb{R}} \varepsilon$。

证明 对任意的 $\varepsilon > 0$，可以找到自然数 N'，对任意 $m,n > N'$，

$$|a_m - a_n| < \frac{\varepsilon}{2} \tag{13}$$

取 $N = N' + 1, \varepsilon_0 = \frac{\varepsilon}{2}$。对任意的 $n > N$，由公式13有

$$|a_m - a_n| < \frac{\varepsilon}{2} = \varepsilon - \varepsilon_0 \tag{14}$$

因此当 $n_0 > n$ 时，有 $\varepsilon - \left|a_{n_0} - a_n\right| > \varepsilon_0$。

所以 $N = N' + 1$ 时，对任意 $n > N$，有 $|\{a_n\}_n -_{\mathbb{R}} a_n| <_{\mathbb{R}} \varepsilon$。

定理 14 (单元集到实数单射的正确性) 对任意实数 $\{a_n\}_n$，$\{\frac{\lfloor\{a_n\}_n \cdot n\rfloor}{n}\}_n$ 与 $\{a_n\}_n$ 等价。

证明 对任意的 $\varepsilon > 0$，由引理13，可以找到自然数 N_0，对任意 $m,n > N_0, |\{a_n\}_n - a_n| < \frac{\varepsilon}{2}$

令 $N = max\{N_0, 2 \cdot (\lceil\frac{1}{\varepsilon}\rceil + 1)\}$，则对任意 $n > N$，有

$$\frac{\lfloor\{a_n\}_n \cdot n\rfloor}{n} - a_n \leq \{a_n\}_n - a_n < \frac{\varepsilon}{2} < \varepsilon \tag{15}$$

$$\begin{aligned} \frac{\lfloor\{a_n\}_n \cdot n\rfloor}{n} - a_n &> \frac{\{a_n\}_n \cdot n - 1}{n} - a_n \\ &= \{a_n\}_n - a_n - \frac{1}{m} \\ &\geq -\frac{\varepsilon}{2} - \frac{1}{2 \cdot (\lceil\frac{1}{\varepsilon}\rceil + 1)} > -\varepsilon \end{aligned} \tag{16}$$

所以对任意 $\varepsilon > 0$，存在 $N = max\{N_0, 2 \cdot (\lceil\frac{1}{\varepsilon}\rceil + 1)\}$，

对任意 $n > N$ 可得 $\left|\frac{\lfloor\{a_n\}_n \cdot n\rfloor}{n} - a_n\right| < \varepsilon$。命题得证。 □

以上的证明都在 Coq 中得到了形式化验证，综上，我们形式化地定义了实数单元集到实数的单射，并且可以通过定理14说明该单射定义的正确性。

7. 实数的完备性

我们将证明通过有理数柯西列等价类定义的实数满足柯西准则，来说明形式化实数定义的完备性。

命题 15 (实数的柯西准则) 实数列极限存在的充分必要条件是该实数列是一个柯西列。

首先我们形式化地给出实数列、实数列极限和实数柯西准则的定义。实数列是一个满足单射性质的 $(\mathbb{N},\mathbb{R})$ 二元关系。实数列极限是一个实数列和实数的二元关系命题。实数柯西准则是一条关于实数的单元命题。其形式化定义如下。

```
Class R_seq (RS: nat -> Real -> Prop) : Prop := {                % 实数列的定义
  Rseq_exists : forall (n:nat), exists A1, RS n A1;
  Rseq_unique : forall (n:nat)  A1 A2, RS n A1 -> RS n A2 -> (A1 == A2)%R;
  Rseq_proper: forall n, Proper (Real_equiv ==> iff) (RS n);
}.
Inductive Real_seq : Type := | Rseq_intro (RS : nat -> Real -> Prop) (H: R_seq RS).
Definition Rlimit (Rseq:Real_seq) (Lim:Real):Prop:=               % 实数列极限的定义
  forall Eps:Real, (0 < Eps)%R -> exists N, forall n, (n>=N)%nat -> forall A,
  (match Rseq with Rseq_intro RS _ => RS end) n A -> (Rabs (A - Lim) < Eps)%R.
```

```
Definition Cauchy_of_R (Rseq:Real_seq):Prop:=                    % 实数列满足柯西性质的定义
  forall Eps:Real, (0 < Eps)%R -> exists N, forall n m, (n>=N)%nat -> (m>=N)%nat -> forall A B,
  (match Rseq with Rseq_intro RS _ => RS end) n A -> (match Rseq with Rseq_intro RS _ => RS end) m B ->  (
   Rabs (A - B) < Eps)%R.
```

在实数极限和柯西列的定义中，出于完备性的要求，不同于此前的证明，我们要求任意小量 ε 的类型是实数。为简化证明，我们首先说明有理数在实数中的稠密性，从而将 $\varepsilon_{\mathbb{R}}$ 放缩为 $\varepsilon_{\mathbb{Q}}$。

定理 16 (有理实数的稠密性) 对任意实数 $\{a_n\}_n, \{b_n\}_n$，如果 $\{b_n\}_n <_{\mathbb{R}} \{a_n\}_n$ 存在有理数 q，使得 $\{b_n\}_n <_{\mathbb{R}} q <_{\mathbb{R}} \{a_n\}_n$

证明 由 $\{b_n\}_n <_{\mathbb{R}} \{a_n\}_n$，可找到有理数 $\delta > 0$ 和自然数 N_1，对任意 $n > N_1$，$a_n - b_n \geq \delta$

由引理13，可以找到 N_2，使对任意 $n > N_2$，有

$$|\{a_n\}_n - a_n| <_{\mathbb{R}} \frac{\delta}{4} \quad |\{b_n\}_n - b_n| <_{\mathbb{R}} \frac{\delta}{4} \tag{17}$$

令 $q = a_n - \frac{\delta}{2}$，可以证明

$$\{b_n\}_n <_{\mathbb{R}} b_n + \frac{\delta}{4} \leq a_n - \frac{3}{4}\delta < a_n - \delta/2 < a_n - \frac{\delta}{4} <_{\mathbb{R}} \{a_n\}_n \tag{18}$$

□

所以存在 $q = a_n - \frac{\delta}{2}$，使 $\{b_n\}_n <_{\mathbb{R}} q <_{\mathbb{R}} \{a_n\}_n$，命题得证。

定理 17 (实数柯西准则的必要性) 若存在实数 ρ，对实数列 $\{A_n\}_n$，有 $\lim_{n\to\infty}\{A_n\}_n = \rho$，那么 $\{A_n\}_n$ 是实数柯西列。

证明 对任意取得的 $\varepsilon_{\mathbb{R}} > 0$，由极限定义，存在 N，使得

$$\forall n > N, |A_n - \rho| <_{\mathbb{R}} \frac{\varepsilon_{\mathbb{R}}}{2} \tag{19}$$

可得对任意 $m, n > N$，

$$|A_n - A_m| \leq_{\mathbb{R}} |A_n - \rho| + |A_m - \rho| <_{\mathbb{R}} \frac{\varepsilon_{\mathbb{R}}}{2} + \frac{\varepsilon_{\mathbb{R}}}{2} = \varepsilon_{\mathbb{R}} \tag{20}$$

□

所以 $\{A_n\}_n$ 是实数柯西列。

对充分性的证明，我们需要为一个具有柯西列性质的实数列构造出一个有理数柯西列，使得该有理数柯西列所代表的实数是实数列的极限。数学教材中常用的构造方法是对实数列相邻的两项应用有理实数的稠密性（定理16），可以证明取出的这一列有理数列是柯西列且等于该实数列的极限。然而，在 Coq 中，这种构造方法过于复杂和灵活，难以被形式化。因此我们提出了如下构造方法。

定义 9 (实数列的极限数列) 对实数列 $\{A_n\}_n$，构造有理数列 $\{a_n\}_n$，令

$$a_n = \frac{\lfloor A_n \cdot_{\mathbb{R}} n \rfloor}{n}$$

称 $\{a_n\}_n$ 为实数列 $\{A_n\}_n$ 的极限数列。

定义9在 Coq 中的形式化表述如下：

```
(fun n q => forall A, RS n A -> forall z, (Rfloor (A * (inject_Q (inject_Z (Z.of_nat (n)%nat)))) z) ->
            q == z # (Pos.of_nat (n)%nat))  %其中，RS表示实数列
```

不难证明通过该方法构造的 $(\mathbb{N},\mathbb{R})$ 二元关系，可以满足函数的单射性，下面证明该数列是一个柯西列。

定理 18 对实数柯西列 $\{A_n\}_n$，它的极限数列 $\{\frac{\lfloor A_n \cdot_{\mathbb{R}} n \rfloor}{n}\}_n$ 是一个有理数柯西列。

证明 对任取的有理数 $\varepsilon > 0$，令 $N_0 = 2 \cdot \lceil \frac{1}{\varepsilon} + 1 \rceil$。

由实数列的柯西性质，可找到 $M \in \mathbb{N}$，对任意 $m_1, m_2 > M$，$\left| A_{m_1} -_{\mathbb{R}} A_{m_2} \right| < \frac{1}{N_0}$。

令 $N = max\{M, N_0\}$，对任意 $n_1, n_2 > N$，

$$\begin{aligned}
\frac{\lfloor A_{m_1} \cdot_{\mathbb{R}} m_1 \rfloor}{m_1} - \frac{\lfloor A_{m_2} \cdot_{\mathbb{R}} m_2 \rfloor}{m_2} &< \frac{A_{m_1} \cdot_{\mathbb{R}} m_1}{m_1} - \frac{A_{m_2} \cdot_{\mathbb{R}} m_2 - 1}{m_2} \\
&= A_{m_1} - A_{m_2} + \frac{1}{m_2} < \frac{1}{N} + \frac{1}{M} < \frac{2}{N_0} < \varepsilon \\
\frac{\lfloor A_{m_1} \cdot_{\mathbb{R}} m_1 \rfloor}{m_1} - \frac{\lfloor A_{m_2} \cdot_{\mathbb{R}} m_2 \rfloor}{m_2} &> \frac{A_{m_1} \cdot_{\mathbb{R}} m_1 - 1}{m_1} - \frac{A_{m_2} \cdot_{\mathbb{R}} m_2}{m_2} \\
&= A_{m_1} - A_{m_2} - \frac{1}{m_1} > -\frac{1}{N} - \frac{1}{M} > -\frac{2}{N_0} > -\varepsilon
\end{aligned} \tag{21}$$

所以 $\left| \frac{\lfloor A_{m_1} \cdot_{\mathbb{R}} m_1 \rfloor}{m_1} - \frac{\lfloor A_{m_2} \cdot_{\mathbb{R}} m_2 \rfloor}{m_2} \right| < \varepsilon$，即 $\{A_n\}_n$ 的极限数列是一个有理数柯西列。

下面，我们完成实数柯西准则充分性的证明。

定理 19 对实数柯西列 $\{A_n\}_n$，它的极限数列 $\{\frac{\lfloor A_n \cdot_{\mathbb{R}} n \rfloor}{n}\}_n$ 是该实数列的极限。

证明 对任取的 $\varepsilon_{\mathbb{R}} > 0$，由定理16，可以找到有理数 $\varepsilon \in \mathbb{Q}$，$\varepsilon_{\mathbb{R}} > \varepsilon > 0$。

由定理13，对极限数列 $\{\frac{\lfloor A_n \cdot_{\mathbb{R}} n \rfloor}{n}\}_n$ 可找到 M，对任意 $n > M$，有

$$\left| \{\frac{\lfloor A_n \cdot_{\mathbb{R}} n \rfloor}{n}\}_n - \frac{\lfloor A_n \cdot_{\mathbb{R}} n \rfloor}{n} \right| < \frac{\varepsilon}{2} \tag{22}$$

令 $M = max\{M, 2 \cdot (\lceil \frac{1}{\varepsilon} \rceil + 1)\}$，则任取 $n > M$，有

$$\begin{aligned}
A_n - \{\frac{\lfloor A_n \cdot_{\mathbb{R}} n \rfloor}{n}\}_n &\geq \{A_n\}_n - \{\frac{A_n\}_n \cdot_{\mathbb{R}} n}{n}\}_n \\
&= A_n - A_n = 0 > -\frac{\varepsilon}{2} \\
A_n - \{\frac{\lfloor A_n \cdot_{\mathbb{R}} n \rfloor}{n}\}_n &< A_n - \{\frac{A_n \cdot_{\mathbb{R}} n - 1}{n}\}_n \\
&= A_n - A_n + \frac{1}{n} \\
&< \frac{1}{2 \cdot (\lceil \frac{1}{\varepsilon} \rceil + 1)} < \frac{\varepsilon}{2}
\end{aligned} \tag{23}$$

由公式22和公式23可得，

$$\begin{aligned}
\left| A_n - \{\frac{\lfloor A_n \cdot_{\mathbb{R}} n \rfloor}{n}\}_n \right| &\leq \left| \{\frac{\lfloor A_n \cdot_{\mathbb{R}} n \rfloor}{n}\}_n - \frac{\lfloor A_n \cdot_{\mathbb{R}} n \rfloor}{n} \right| + \left| A_n - \{\frac{\lfloor A_n \cdot_{\mathbb{R}} n \rfloor}{n}\}_n \right| \\
&< \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon < \varepsilon_{\mathbb{R}}
\end{aligned} \tag{24}$$

□

所以极限数列 $\{\frac{\lfloor A_n \cdot_{\mathbb{R}} n \rfloor}{n}\}_n$ 是实数列 $\{A_n\}_n$ 的极限。

综上，我们完成了实数及其定义在 Coq 中的形式化和完备性证明的工作。

8. 总结与展望

本文基于交互式定理证明工具 Coq，用形式化方法完成了从有理数构造实数的工作，并且证明了实数的完备性。本课题的最终成果是在 Coq 中构造了一个完备的实数库，其包含的主要成果有如下几点：

1. 形式化地给出了用有理数柯西列等价类定义实数域的构造方法。
2. 形式化地验证了定义的实数满足实数公理系统，并提供了大量经典实数理论中，数学证明的形式化实例。
3. 构造了实数单元集到实数的函数单射，实现了 Coq 中实数可计算函数的构造。

本文在 Coq 中实现了从有理数到完备经典实数的构造，并给出了必要的定理证明。然而，本文的内容仍有需要在接下来的研究中加以完善之处：

1. 本文对经典实数仅证明了验证完备性必要的性质，对实数构造理论中其他重要的定理，如对于实数完备性命题之间的等价性，需要进一步进行形式化的表述和证明。
2. 本文构造的实数还缺少具体的实现，如幂函数、指对函数等，距离实际的连续型软件验证应用还需要更多形式化工作。

参考文献

[1] E. Hewitt.Real and Abstract Analysis.Berlin, Heidelberg : Springer Berlin Heidelberg, 1965:32-46

[2] 王建午, 曹之江, 刘景麟. 实数的构造理论, 北京: 人民教育出版社,1981:52-86

致谢

一学期的 PrP 课题已接近尾声，在此我要向所有为我提供帮助和支持的老师和同学们表达最诚挚的谢意。

首先感谢导师曹钦翔老师，在课题的进展过程中，对我的学习、研究情况关照有加，每周都通过组会了解我的课题情况，并且为课题提出了许多有价值的指导意见。

其次我要感谢同在课题组的四位同学，从他们的研究中我获得了很多进步。

最后，感谢我的学院和学校，为我提供了良好的环境完成本课题。