Implementing field extensions of the form $\mathbb{Q}[\sqrt{b}]^*$

René Thiemann

September 19, 2015

Abstract

We apply data refinement to implement the real numbers, where we support all numbers in the field extension $\mathbb{Q}[\sqrt{b}]$, i.e., all numbers of the form $p + q\sqrt{b}$ for rational numbers $p$ and $q$ and some fixed natural number $b$. To this end, we also developed algorithms to precisely compute roots of a rational number, and to perform a factorization of natural numbers which eliminates duplicate prime factors.

Our results have been used to certify termination proofs which involve polynomial interpretations over the reals.

Contents

1 Introduction 1
2 Auxiliary lemmas which might be moved into the Isabelle distribution. 2
3 Prime products 2
4 A representation of real numbers via triples 3
5 A unique representation of real numbers via triples 8

1 Introduction

It has been shown that polynomial interpretations over the reals are strictly more powerful for termination proving than polynomial interpretations over the rationals. To this end, also automated termination prover started to generate such interpretations. [3, 4, 5, 7, 8]. However, for all current implementations, only reals of the form $p + q \cdot \sqrt{b}$ are generated where $b$ is some fixed natural number and $p$ and $q$ may be arbitrary rationals, i.e., we get numbers within $\mathbb{Q}[\sqrt{b}]$.

*This research is supported by FWF (Austrian Science Fund) project P22767-N13.
To support these termination proofs in our certifier CēTA [6], we therefore required executable functions on \( \mathbb{Q}[\sqrt{b}] \), which can then be used as an implementation type for the reals. Here, we used ideas from [1, 2] to provide a sufficiently powerful partial implementations via data refinement.

## 2 Auxiliary lemmas which might be moved into the Isabelle distribution.

theory Real-Impl-Auxiliary
imports
  ~/src/HOL/Number-Theory/UniqueFactorization
begin

lemma multiplicity-prime: assumes p: prime (i :: nat) and ji: j ≠ i
  shows multiplicity j i = 0
⟨proof⟩
end

## 3 Prime products

theory Prime-Product
imports
  Real-Impl-Auxiliary
  ../Sqrt-Babylonian/Sqrt-Babylonian
begin

Prime products are natural numbers where no prime factor occurs more than once.

definition prime-product where prime-product (n :: nat) = (\forall p. multiplicity p n ≤ 1)

The main property is that whenever \( b_1 \) and \( b_2 \) are different prime products, then \( p_1 + q_1 \sqrt{b_1} = p_2 + q_2 \sqrt{b_2} \) implies \( (p_1, q_1, b_1) = (p_2, q_2, b_2) \) for all rational numbers \( p_1, q_1, p_2, q_2 \). This is the key property to uniquely represent numbers in \( \mathbb{Q}[\sqrt{b}] \) by triples. In the following we develop an algorithm to decompose any natural number \( n \) into \( n = s^2 \cdot p \) for some \( s \) and prime product \( p \).

function prime-product-factor-main :: nat ⇒ nat ⇒ nat ⇒ nat ⇒ nat ⇒ nat × nat where
  prime-product-factor-main factor-sq factor-pr limit n i =
  (if i ≤ limit ∧ i ≥ 2 then
   (if i dvd n
    then (let n' = n div i in
       (if i dvd n' then
        let n'' = n' div i in
        . . .
       . . .
       )
    . . .)
   . . .)
  . . .)
prime-product-factor-main (factor-sq * i) factor-pr (nat (root-nat-floor 3 n')) n'' i  
else  
  (case sqrt-nat n' of  
  Cons sn -> (factor-sq * sn, factor-pr * i)  
  [] -> prime-product-factor-main factor-sq (factor-pr * i) (nat (root-nat-floor 3 n')) n' (Suc i))  
)  
)  
prime-product-factor-main factor-sq factor-pr limit n (Suc i))  
else  
  (factor-sq, factor-pr * n)) ⟨proof⟩

termination  
⟨proof⟩

lemma prime-product-factor-main: assumes ¬ (∃ s. s * s = n)  
and limit = nat (root-nat-floor 3 n)  
and m = factor-sq * factor-sq * factor-pr * n  
and prime-product-factor-main factor-sq factor-pr limit n i = (sq, p)  
and i ≥ 2  
and ∃ j. j ≥ 2 ⇒ j < i ⇒ ¬ j dvd n  
and ∃ j. j < i ⇒ multiplicity j factor-pr ≤ 1  
and ∃ j. j ≥ i ⇒ multiplicity j factor-pr = 0  
and factor-pr > 0  
shows m = sq * sq * p ∧ prime-product p  
⟨proof⟩

definition prime-product-factor :: nat ⇒ nat × nat where  
prime-product-factor n = (case sqrt-nat n of  
  (Cons s _) ⇒ (s,1)  
  [] ⇒ prime-product-factor-main 1 1 (nat (root-nat-floor 3 n)) n 2)  
lemma prime-product-one[simp, intro]: prime-product 1  
⟨proof⟩

lemma prime-product-factor: assumes pf: prime-product-factor n = (sq,p)  
shows n = sq * sq * p ∧ prime-product p  
⟨proof⟩

end

4 A representation of real numbers via triples

theory Real-Impl  
imports
We represent real numbers of the form $p + q \cdot \sqrt{b}$ for $p, q \in \mathbb{Q}$, $n \in \mathbb{N}$ by triples $(p, q, b)$. However, we require the invariant that $\sqrt{b}$ is irrational. Most binary operations are implemented via partial functions where the common the restriction is that the numbers $b$ in both triples have to be identical. So, we support addition of $\sqrt{2} + \sqrt{2}$, but not $\sqrt{2} + \sqrt{3}$.

The set of natural numbers whose sqrt is irrational

**definition** sqrt-irrat = { $q :: \text{nat.} \neg (\exists p. \ p \cdot p = \text{rat-of-nat} \ q)$}

**lemma** sqrt-irrat: assumes choice: $q = 0 \lor b \in \text{sqrt-irrat}$
and eq: real-of-rat $p + \text{real-of-rat} \ q \cdot \sqrt{\text{of-nat} \ b} = 0$
shows $q = 0$
⟨proof⟩

Collect existing code equations for reals, so that they can be deleted.

**lemmas** real-code-dels =
refl[of op + :: real ⇒ real ⇒ real]
refl[of uminus :: real ⇒ real]
refl[of op − :: real ⇒ real ⇒ real]
refl[of op * :: real ⇒ real ⇒ real]
refl[of inverse :: real ⇒ real]
refl[of op / :: real ⇒ real ⇒ real]
refl[of floor :: real ⇒ int]
refl[of sqrt]
refl[of HOL.equal :: real ⇒ real ⇒ bool]
refl[of op ≤ :: real ⇒ real ⇒ bool]
refl[of op < :: real ⇒ real ⇒ bool]
refl[of 0 :: real]
refl[of 1 :: real]

**lemma** real-code-unfold-dels:
of-rat ≡ Ratreal
of-int a ≡ (of-rat (of-int a) :: real)
0 ≡ (of-rat 0 :: real)
1 ≡ (of-rat 1 :: real)
umeral k ≡ (of-rat (numeral k) :: real)
− numeral k ≡ (of-rat (− numeral k) :: real)
⟨proof⟩

**lemma** real-standard-impls:
$(x :: \text{real}) / (y :: \text{real}) = x \cdot \text{inverse} \ y$
$(x :: \text{real}) - (y :: \text{real}) = x + (− y)$
⟨proof⟩

To represent numbers of the form $p + q \cdot \sqrt{b}$, use mini algebraic numbers, i.e., triples $(p, q, b)$ with irrational $\sqrt{b}$. 

4
typedef mini-alg =
\{(p,q,b) | (p :: \text{rat}) (q :: \text{rat}) (b :: \text{nat}).
q = 0 \lor b \in \text{sqrt-irrat}\}
\langle \text{proof} \rangle

setup-lifting type-definition-mini-alg

lift-definition real-of :: mini-alg \Rightarrow real is
\lambda (p,q,b). of-rat p + of-rat q * sqrt (of-nat b) \langle \text{proof} \rangle

lift-definition ma-of-rat :: \text{rat} \Rightarrow \text{mini-alg is} \lambda x. (x,0,0) \langle \text{proof} \rangle

lift-definition ma-base :: mini-alg \Rightarrow \text{nat} is snd o snd \langle \text{proof} \rangle

lift-definition ma-coeff :: mini-alg \Rightarrow \text{rat} is \lambda x. (x,0,0) \langle \text{proof} \rangle

lift-definition ma-minus :: mini-alg \Rightarrow mini-alg is
\lambda (p1,q1,b1). (- p1, - q1, b1) \langle \text{proof} \rangle

lift-definition ma-compatible :: mini-alg \Rightarrow mini-alg \Rightarrow \text{bool is}
\lambda (p1,q1,b1) (p2,q2,b2). q1 = 0 \lor q2 = 0 \lor b1 = b2 \langle \text{proof} \rangle

definition ma-normalize :: \text{rat} \times \text{rat} \times \text{nat} \Rightarrow \text{rat} \times \text{rat} \times \text{nat where}
ma-normalize x \equiv \text{case } x \text{ of } (a,b,c) \Rightarrow \text{if } b = 0 \text{ then } (a,0,0) \text{ else } (a,b,c)

lemma ma-normalize-case[simp]: (case ma-normalize r of (a,b,c) \Rightarrow real-of-rat a + real-of-rat b * sqrt (of-nat c))
= (case r of (a,b,c) \Rightarrow real-of-rat a + real-of-rat b * sqrt (of-nat c)) \langle \text{proof} \rangle

lift-definition ma-plus :: mini-alg \Rightarrow mini-alg \Rightarrow mini-alg is
\lambda (p1,q1,b1) (p2,q2,b2). if q1 = 0 then
(p1 + p2, q2, b2) else ma-normalize (p1 + p2, q1 + q2, b1) \langle \text{proof} \rangle

lift-definition ma-times :: mini-alg \Rightarrow mini-alg \Rightarrow mini-alg is
\lambda (p1,q1,b1) (p2,q2,b2). if q1 = 0 then
ma-normalize (p1*p2, p1*q2, b2) else
ma-normalize (p1*p2 + of-nat b2*q1*q2, p1*q2 + q1*p2, b1) \langle \text{proof} \rangle

lift-definition ma-floor :: mini-alg \Rightarrow int is
\lambda (p,q,b). \text{let } d = \text{inverse } (p * p - of-nat b * q * q) \text{ in}
\text{ma-normalize } (p * d, - q * d, b) \langle \text{proof} \rangle

lift-definition ma-floor :: mini-alg \Rightarrow int is
\lambda (p,q,b). \text{case } (\text{quotient-of }p, \text{quotient-of }q) \text{ of } ((z1,n1),(z2,n2)) \Rightarrow
\text{let } z2n1 = z2 * n1; z1n2 = z1 * n2; n12 = n1 * n2; prod = z2n1 * z2n1 * \text{int } b \text{ in}
(z1n2 + (if z2n1 \geq 0 \text{ then } \text{sqrt-int-floor-pos prod else } - \text{sqrt-int-ceiling-pos prod}) \text{ div } n12 \langle \text{proof} \rangle
lift-definition \( ma-sqrt :: \text{mini-alg} \Rightarrow \text{mini-alg} \) is 
\[
\lambda (p,q,b). \text{let } (a,b) = \text{quotient-of } p; \text{ aa } = \text{abs } (a*b) \text{ in } \text{case sqrt-int aa of } [] \Rightarrow (0, \text{inverse } (\text{of-int } b), \text{nat } aa) | (\text{Cons } s) \Rightarrow (\text{of-int } s / \text{of-int } b, 0, 0) \\
\langle \text{proof} \rangle
\]

lift-definition \( ma-equal :: \text{mini-alg} \Rightarrow \text{mini-alg} \Rightarrow \text{bool} \) is 
\[
\lambda (p1,q1,b1) (p2,q2,b2). \text{p1 } = p2 \land q1 = q2 \land (q1 = 0 \lor b1 = b2) \langle \text{proof} \rangle
\]

lift-definition \( ma-ge-0 :: \text{mini-alg} \Rightarrow \text{bool} \) is 
\[
\lambda (p,q,b). \text{let } bqq = \text{of-nat } b * q * q; \text{ pp } = p * p \text{ in } \text{0 } \leq \text{p } \land \text{bqq } \leq \text{pp } \lor \text{0 } \leq \text{q } \land \text{pp } \leq \text{bqq} \langle \text{proof} \rangle
\]

lift-definition \( ma-is-rat :: \text{mini-alg} \Rightarrow \text{bool} \) is 
\[
\lambda (p,q,b). \text{q } = 0 \langle \text{proof} \rangle
\]

definition \( ge-0 :: \text{real} \Rightarrow \text{bool} \) where [code del]: \( ge-0 \) \( x \) = \( (x \geq 0) \)

lemma \( ma-ge-0: \text{ge-0 } (\text{real-of } x) = \text{ma-ge-0 } x \) \langle \text{proof} \rangle

lemma \( ma-0: 0 = \text{real-of } (\text{ma-of-rat } 0) \) \langle \text{proof} \rangle

lemma \( ma-1: 1 = \text{real-of } (\text{ma-of-rat } 1) \) \langle \text{proof} \rangle

lemma \( ma-uminus: \text{− } (\text{real-of } x) = \text{real-of } (\text{ma-uminus } x) \) \langle \text{proof} \rangle

lemma \( ma-inverse: \text{inverse } (\text{real-of } r) = \text{real-of } (\text{ma-inverse } r) \) \langle \text{proof} \rangle

lemma \( ma-sqrt-main: \text{ma-rat } r \geq 0 \Rightarrow \text{ma-coeff } r = 0 \Rightarrow \text{sqrt } (\text{real-of } r) = \text{real-of } (\text{ma-sqrt } r) \) \langle \text{proof} \rangle

lemma \( ma-sqrt: \text{sqrt } (\text{real-of } r) = (\text{if } \text{ma-coeff } r = 0 \text{ then } (\text{if } \text{ma-rat } r \geq 0 \text{ then } \text{real-of } (\text{ma-sqrt } r) \text{ else } \text{real-of } (\text{ma-sqrt } (\text{ma-uminus } r))) \text{ else Code.abort } (\text{STR } "\text{cannot represent sqrt of irrational number"}) (\lambda -. \text{sqrt } (\text{real-of } r))) \) \langle \text{proof} \rangle

lemma \( ma-plus: \text{ (real-of } r1 + \text{ real-of } r2) = (\text{if } \text{ma-compatible } r1 \text{ r2 then } \text{real-of } (\text{ma-plus } r1 \text{ r2}) \text{ else } \text{Code.abort } (\text{STR } "\text{different base"}) (\lambda -. \text{real-of } r1 + \text{real-of } r2)) \)
lemma ma-times:
\[
(\text{real-of } r_1 \ast \text{real-of } r_2) = (\text{if ma-compatible } r_1 r_2 \text{ then real-of } \text{ma-times } r_1 r_2 \text{ else Code.abort (STR "different base") } (\lambda \cdot \text{real-of } r_1 \ast \text{real-of } r_2))
\]

lemma ma-equal:
\[
\text{HOL.equal } (\text{real-of } r_1) (\text{real-of } r_2) = (\text{if ma-compatible } r_1 r_2 \text{ then ma-equal } r_1 r_2 \text{ else Code.abort (STR "different base") } (\lambda \cdot \text{HOL.equal } (\text{real-of } r_1) (\text{real-of } r_2)))
\]

lemma ma-floor: floor (\text{real-of } r) = \text{ma-floor } r

lemma comparison-impl:
\[
(x :: real) \leq (y :: real) = \text{ge-0 } (y - x) \\
(x :: real) < (y :: real) = (x \neq y \land \text{ge-0 } (y - x))
\]

lemma ma-of-rat: \text{real-of-rat } r = \text{real-of } (\text{ma-of-rat } r)

definition is-rat :: real \Rightarrow bool where
\[
\text{[code del]: is-rat } x = (x \in \mathbb{Q})
\]

lemma [code-unfold]: \(x \in \mathbb{Q} \leftrightarrow \text{is-rat } x\) (proof)

lemma ma-is-rat: is-rat (\text{real-of } x) = \text{ma-is-rat } x

definition sqrt-real x = (if \(x \in \mathbb{Q} \land x \geq 0\) then (if \(x = 0\) then \(0\) else (let sx = sqrt x in \(\left[sx, -sx\right]\))) else [])

lemma sqrt-real[simp]: assumes \(x :: \mathbb{Q}\)

  shows set (sqrt-real x) = \{y . y * y = x\}
  (proof)

lemmas ma-code-eqns = ma-ge-0 ma-floor ma-0 ma-1 ma-uminus ma-inverse ma-sqrt ma-plus ma-times ma-equal ma-is-rat comparison-impl

code-datatype real-of

declare real-code-delss[code, code del]
declare real-code-unfold-delss[code-unfold del]
Some tests with small numbers. To work on larger number, one should additionally import the theories for efficient calculation on numbers

\[
\begin{align*}
\text{value} & \left\lfloor 101.1 \times (3 \times \sqrt{2} + 6 \times 0.5) \right\rfloor \\
\text{value} & \left\lfloor 606.2 \times \sqrt{2} + 0.001 \right\rfloor \\
\text{value} & 101.1 \times (3 \times \sqrt{2} + 6 \times 0.5) = 606.2 \times \sqrt{2} + 0.001 \\
\text{value} & (\sqrt{0.1} \in \mathbb{Q}, \sqrt{(-0.09)} \in \mathbb{Q})
\end{align*}
\]

end

5 A unique representation of real numbers via triples

theory Real-Unique-Impl
imports
Prime-Product
Real-Impl
../Show/Show-Instances
begin

We implement the real numbers again using triples, but now we require an additional invariant on the triples, namely that the base has to be a prime product. This has the consequence that the mapping of triples into \( \mathbb{R} \) is injective. Hence, equality on reals is now equality on triples, which can even be executed in case of different bases. Similarly, we now also allow different basis in comparisons. Ultimately, injectivity allows us to define a show-function for real numbers, which pretty prints real numbers into strings.

typedef mini-alg-unique =
\{ \text{r} :: \text{mini-alg} \cdot \text{ma-coeff } \text{r} = 0 \land \text{ma-base } \text{r} = 0 \lor \text{ma-coeff } \text{r} \neq 0 \land \text{prime-product (ma-base } \text{r}) \}
(proof)

setup-lifting type-definition-mini-alg-unique

lift-definition real-of-u :: mini-alg-unique \Rightarrow real is real-of (proof)
lift-definition mau-floor :: mini-alg-unique \Rightarrow int is ma-floor (proof)
lift-definition mau-of-rat :: rat \Rightarrow mini-alg-unique is ma-of-rat (proof)
lift-definition mau-rat :: mini-alg-unique \Rightarrow rat is ma-rat (proof)
lift-definition mau-base :: mini-alg-unique \Rightarrow nat is ma-base (proof)
lift-definition mau-coeff :: mini-alg-unique \Rightarrow rat is ma-coeff (proof)
lift-definition mau-uminus :: mini-alg-unique \Rightarrow mini-alg-unique is ma-uminus (proof)
lift-definition mau-compatible :: mini-alg-unique \Rightarrow mini-alg-unique \Rightarrow bool is ma-compatible (proof)
lift-definition mau-ge-0 :: mini-alg-unique \Rightarrow bool is ma-ge-0 (proof)
lift-definition mau-inverse :: mini-alg-unique ⇒ mini-alg-unique is ma-inverse
  ⟨proof⟩

lift-definition mau-plus :: mini-alg-unique ⇒ mini-alg-unique ⇒ mini-alg-unique
is ma-plus
  ⟨proof⟩

lift-definition mau-times :: mini-alg-unique ⇒ mini-alg-unique ⇒ mini-alg-unique
is ma-times
  ⟨proof⟩

lift-definition ma-identity :: mini-alg ⇒ mini-alg ⇒ bool is op =
  ⟨proof⟩

lift-definition mau-equal :: mini-alg-unique ⇒ mini-alg-unique ⇒ bool is ma-identity
  ⟨proof⟩

lift-definition mau-is-rat :: mini-alg-unique ⇒ bool is ma-is-rat
  ⟨proof⟩

lemma mau-floor: floor (real-of-u r) = mau-floor r
  ⟨proof⟩

lemma mau-inverse: inverse (real-of-u r) = real-of-u (mau-inverse r)
  ⟨proof⟩

lemma mau-uminus: − (real-of-u r) = real-of-u (mau-uminus r)
  ⟨proof⟩

lemma mau-times:
  (real-of-u r1 * real-of-u r2) = (if mau-compatible r1 r2
then real-of-u (mau-times r1 r2) else
  Code.abort (STR "different base") (λ -. real-of-u r1 * real-of-u r2))
  ⟨proof⟩

lemma mau-plus:
  (real-of-u r1 + real-of-u r2) = (if mau-compatible r1 r2
then real-of-u (mau-plus r1 r2) else
  Code.abort (STR "different base") (λ -. real-of-u r1 + real-of-u r2))
  ⟨proof⟩

lemma real-of-u-inj[simp]: real-of-u x = real-of-u y ←→ x = y
  ⟨proof⟩

lift-definition mau-sqrt :: mini-alg-unique ⇒ mini-alg-unique is
  λ ma. let (a,b) = quotient-of (ma-rat ma); (sq, fact) = prime-product-factor
  (nat (abs a * b));
ma′ = ma-of-rat (of-int (sgn(a)) * of-nat sq / of-int b)
in ma-times ma′ (ma-sqrt (ma-of-rat (of-nat fact)))
  ⟨proof⟩

lemma sqrt-sgn[simp]: sqrt (of-int (sgn a)) = of-int (sgn a)
  ⟨proof⟩

lemma mau-sqrt-main: mau-coeff r = 0 ⇒ sqrt (real-of-u r) = real-of-u (mau-sqrt r)
  ⟨proof⟩

lemma mau-sqrt: sqrt (real-of-u r) = (if mau-coeff r = 0 then
real-of-u (mau-sqrt r)
else Code.abort (STR "cannot represent sqrt of irrational number") (λ - sqrt (real-of-u r))

⟨proof⟩

lemma mau-0: 0 = real-of-u (mau-of-rat 0) ⟨proof⟩

lemma mau-1: 1 = real-of-u (mau-of-rat 1) ⟨proof⟩

lemma mau-equal:
HOL.equal (real-of-u r1) (real-of-u r2) = mau-equal r1 r2 ⟨proof⟩

lemma mau-ge-0: ge-0 (real-of-u x) = mau-ge-0 x ⟨proof⟩

definition real-lt :: real ⇒ real ⇒ bool where real-lt = op <

The following code equation terminates if it is started on two different inputs.

lemma real-lt[code]: real-lt x y = (let fx = floor x; fy = floor y in
(if fx < fy then True else if fx > fy then False else real-lt (x * 1024) (y * 1024)))
⟨proof⟩

For comparisons we first check for equality. Then, if the bases are compatible we can just compare the differences with 0. Otherwise, we start the recursive algorithm real-lt which works on arbitrary bases. In this way, we have an implementation of comparisons which can compare all representable numbers.

Note that in Real-Impl we did not use real-lt as there the code-equations for equality already require identical bases.

lemma comparison-impl:
real-of-u x ≤ real-of-u y ⟷ real-of-u x = real-of-u y ∨
(if mau-compatible x y then ge-0 (real-of-u y - real-of-u x) else real-lt (real-of-u x) (real-of-u y))

real-of-u x < real-of-u y ⟷ real-of-u x ≠ real-of-u y ∧
(if mau-compatible x y then ge-0 (real-of-u y - real-of-u x) else real-lt (real-of-u x) (real-of-u y))
⟨proof⟩

lemma mau-is-rat: is-rat (real-of-u x) = mau-is-rat x ⟨proof⟩

lift-definition ma-show-real :: mini-alg ⇒ string is
λ (p,q,b). let sb = shows "sqrt(" o shows b o shows ")";
qb = (if q = 1 then sb else if q = -1 then shows "-" o sb else shows q o shows "^" o sb) in
(if q = 0 then shows p [] else
if p = 0 then qb [] else
if q < 0 then ((shows p o qb) [])
else ((shows p o shows "^" o qb) []) ⟨proof⟩

lift-definition mau-show-real :: mini-alg-unique ⇒ string is mau-show-real ⟨proof⟩
**definition** show-real :: real ⇒ string where
show-real x = (if (∃ y. x = real-of-u y) then mau-show-real (THE y. x = real-of-u y) else [])

**lemma** mau-show-real: show-real (real-of-u x) = mau-show-real x
⟨proof⟩

**lemmas** mau-code-eqns = mau-floor mau-0 mau-1 mau-uminus mau-inverse mau-sqrt
mau-plus mau-times mau-equal mau-ge-0 mau-is-rat
mau-show-real comparison-impl

**code-datatype** real-of-u
declare real-code-dels[code, code del]
declare ma-code-eqns[code del]
declare real-code-unfold-dels[code-unfold del]
declare real-standard-impls[code]
declare mau-code-eqns[code]

Some tests with small numbers. To work on larger number, one should additionally import the theories for efficient calculation on numbers

value [101.1 * (sqrt 18 + 6 * sqrt 0.5)]
value [324 * sqrt 7 + 0.001]
value 101.1 * (sqrt 18 + 6 * sqrt 0.5) = 324 * sqrt 7 + 0.001
value 101.1 * (sqrt 18 + 6 * sqrt 0.5) > 324 * sqrt 7 + 0.001
value show-real (101.1 * (sqrt 18 + 6 * sqrt 0.5))
value (sqrt 0.1 ∈ Q, sqrt (− 0.09) ∈ Q)

end

**Acknowledgements**

We thank Bertram Felgenhauer for interesting discussions and especially for mentioning Cauchy’s mean theorem during the formalization of the algorithms for computing roots.

**References**


