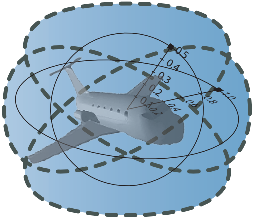
15-819/18-879: Logical Analysis of Hybrid Systems

08: First-Order Real Arithmetic

André Platzer

aplatzer@cs.cmu.edu
Carnegie Mellon University, Pittsburgh, PA



Outline

Outline

1. First-Order Real Arithmetic
   - Axioms of Reals
   - Real-Closed Fields

In hybrid systems, there is significant logical structure in the properties, the system, the reasoning, ...

We need to understand the reals first

Axioms of Reals

Axioms of Reals

1. Commutative group $(\mathbb{R}, +)$: $\forall x \, \forall y \, \forall z \; x + (y + z) = (x + y) + z$

Axioms of Reals

1. Commutative group $(\mathbb{R}, +)$: $\forall x\, \forall y\, \forall z\, x + (y + z) = (x + y) + z$
2. Neutral $\forall x\, x + 0 = x$

Axioms of Reals

1. Commutative group $(\mathbb{R}, +)$: $\forall x\, \forall y\, \forall z\, x + (y + z) = (x + y) + z$
2. Neutral $\forall x\, x + 0 = x$
3. Inverse $\forall x\, \exists y\, x + y = 0$

Axioms of Reals

1. Commutative group $(\mathbb{R}, +)$: $\forall x \, \forall y \, \forall z \; x + (y + z) = (x + y) + z$
2. Neutral $\forall x \; x + 0 = x$
3. Inverse $\forall x \, \exists y \; x + y = 0$
4. Abelian $\forall x \, \forall y \, (x + y = y + x)$

Axioms of Reals

1. Commutative group $(\mathbb{R}, +)$: $\forall x\, \forall y\, \forall z\, x + (y + z) = (x + y) + z$
2. Neutral $\forall x\, x + 0 = x$
3. Inverse $\forall x\, \exists y\, x + y = 0$
4. Abelian $\forall x\, \forall y\, (x + y = y + x)$
5. Commutative group $(\mathbb{R} \setminus \{0\}, \cdot)$: $\forall x\, \forall y\, \forall z\, x \cdot (y \cdot z) = (x \cdot y) \cdot z$

Axioms of Reals

1. Commutative group $(\mathbb{R},+)$: $\forall x\,\forall y\,\forall z\, x+(y+z)=(x+y)+z$
2. Neutral $\forall x\, x+0=x$
3. Inverse $\forall x\,\exists y\, x+y=0$
4. Abelian $\forall x\,\forall y\,(x+y=y+x)$
5. Commutative group $(\mathbb{R}\setminus\{0\},\cdot)$: $\forall x\,\forall y\,\forall z\, x\cdot(y\cdot z)=(x\cdot y)\cdot z$
6. Neutral $\forall x\, x\cdot 1=x$

Axioms of Reals

1. Commutative group $(\mathbb{R}, +)$: $\forall x\, \forall y\, \forall z\, x + (y + z) = (x + y) + z$
2. Neutral $\forall x\, x + 0 = x$
3. Inverse $\forall x\, \exists y\, x + y = 0$
4. Abelian $\forall x\, \forall y\, (x + y = y + x)$
5. Commutative group $(\mathbb{R} \setminus \{0\}, \cdot)$: $\forall x\, \forall y\, \forall z\, x \cdot (y \cdot z) = (x \cdot y) \cdot z$
6. Neutral $\forall x\, x \cdot 1 = x$
7. Inverse $\forall x\, (x \neq 0 \rightarrow \exists y\, x \cdot y = 1)$

Axioms of Reals

1. Commutative group $(\mathbb{R}, +)$: $\forall x\, \forall y\, \forall z\, x + (y + z) = (x + y) + z$
2. Neutral $\forall x\, x + 0 = x$
3. Inverse $\forall x\, \exists y\, x + y = 0$
4. Abelian $\forall x\, \forall y\, (x + y = y + x)$
5. Commutative group $(\mathbb{R} \setminus \{0\}, \cdot)$: $\forall x\, \forall y\, \forall z\, x \cdot (y \cdot z) = (x \cdot y) \cdot z$
6. Neutral $\forall x\, x \cdot 1 = x$
7. Inverse $\forall x\, (x \neq 0 \rightarrow \exists y\, x \cdot y = 1)$
8. Abelian $\forall x\, \forall y\, (x \cdot y = y \cdot x)$

Axioms of Reals

1. Commutative group $(\mathbb{R}, +)$: $\forall x \, \forall y \, \forall z \, x + (y + z) = (x + y) + z$
2. Neutral $\forall x \, x + 0 = x$
3. Inverse $\forall x \, \exists y \, x + y = 0$
4. Abelian $\forall x \, \forall y \, (x + y = y + x)$
5. Commutative group $(\mathbb{R} \setminus \{0\}, \cdot)$: $\forall x \, \forall y \, \forall z \, x \cdot (y \cdot z) = (x \cdot y) \cdot z$
6. Neutral $\forall x \, x \cdot 1 = x$
7. Inverse $\forall x \, (x \neq 0 \rightarrow \exists y \, x \cdot y = 1)$
8. Abelian $\forall x \, \forall y \, (x \cdot y = y \cdot x)$
9. Distributive $\forall x \, \forall y \, \forall z \, (x \cdot (y + z) = (x \cdot y) + (x \cdot z))$

Axioms of Reals

1. Commutative group $(\mathbb{R}, +)$: $\forall x \, \forall y \, \forall z \, x + (y + z) = (x + y) + z$
2. Neutral $\forall x \, x + 0 = x$
3. Inverse $\forall x \, \exists y \, x + y = 0$
4. Abelian $\forall x \, \forall y \, (x + y = y + x)$
5. Commutative group $(\mathbb{R} \setminus \{0\}, \cdot)$: $\forall x \, \forall y \, \forall z \, x \cdot (y \cdot z) = (x \cdot y) \cdot z$
6. Neutral $\forall x \, x \cdot 1 = x$
7. Inverse $\forall x \, (x \neq 0 \to \exists y \, x \cdot y = 1)$
8. Abelian $\forall x \, \forall y \, (x \cdot y = y \cdot x)$
9. Distributive $\forall x \, \forall y \, \forall z \, (x \cdot (y + z) = (x \cdot y) + (x \cdot z))$
10. Transitive $\forall x \, \forall y \, \forall z \, (x \geq y \land y \geq z \to x \geq z)$

Axioms of Reals

1. Commutative group $(\mathbb{R}, +)$: $\forall x\, \forall y\, \forall z\, x + (y + z) = (x + y) + z$
2. Neutral $\forall x\, x + 0 = x$
3. Inverse $\forall x\, \exists y\, x + y = 0$
4. Abelian $\forall x\, \forall y\, (x + y = y + x)$
5. Commutative group $(\mathbb{R} \setminus \{0\}, \cdot)$: $\forall x\, \forall y\, \forall z\, x \cdot (y \cdot z) = (x \cdot y) \cdot z$
6. Neutral $\forall x\, x \cdot 1 = x$
7. Inverse $\forall x\, (x \neq 0 \rightarrow \exists y\, x \cdot y = 1)$
8. Abelian $\forall x\, \forall y\, (x \cdot y = y \cdot x)$
9. Distributive $\forall x\, \forall y\, \forall z\, (x \cdot (y + z) = (x \cdot y) + (x \cdot z))$
10. Transitive $\forall x\, \forall y\, \forall z\, (x \geq y \land y \geq z \rightarrow x \geq z)$
11. Antisym. $\forall x\, \forall y\, (x \geq y \land y \geq x \rightarrow x = y)$

Axioms of Reals

1. Commutative group $(\mathbb{R}, +)$: $\forall x \, \forall y \, \forall z \, x + (y + z) = (x + y) + z$
2. Neutral $\forall x \, x + 0 = x$
3. Inverse $\forall x \, \exists y \, x + y = 0$
4. Abelian $\forall x \, \forall y \, (x + y = y + x)$
5. Commutative group $(\mathbb{R} \setminus \{0\}, \cdot)$: $\forall x \, \forall y \, \forall z \, x \cdot (y \cdot z) = (x \cdot y) \cdot z$
6. Neutral $\forall x \, x \cdot 1 = x$
7. Inverse $\forall x \, (x \neq 0 \rightarrow \exists y \, x \cdot y = 1)$
8. Abelian $\forall x \, \forall y \, (x \cdot y = y \cdot x)$
9. Distributive $\forall x \, \forall y \, \forall z \, (x \cdot (y + z) = (x \cdot y) + (x \cdot z))$
10. Transitive $\forall x \, \forall y \, \forall z \, (x \geq y \wedge y \geq z \rightarrow x \geq z)$
11. Antisym. $\forall x \, \forall y \, (x \geq y \wedge y \geq x \rightarrow x = y)$
12. Total $\forall x \, \forall y \, (x \geq y \vee y \geq x)$

Axioms of Reals

1. Commutative group $(\mathbb{R}, +)$: $\forall x \, \forall y \, \forall z \, x + (y + z) = (x + y) + z$
2. Neutral $\forall x \, x + 0 = x$
3. Inverse $\forall x \, \exists y \, x + y = 0$
4. Abelian $\forall x \, \forall y \, (x + y = y + x)$
5. Commutative group $(\mathbb{R} \setminus \{0\}, \cdot)$: $\forall x \, \forall y \, \forall z \, x \cdot (y \cdot z) = (x \cdot y) \cdot z$
6. Neutral $\forall x \, x \cdot 1 = x$
7. Inverse $\forall x \, (x \neq 0 \rightarrow \exists y \, x \cdot y = 1)$
8. Abelian $\forall x \, \forall y \, (x \cdot y = y \cdot x)$
9. Distributive $\forall x \, \forall y \, \forall z \, (x \cdot (y + z) = (x \cdot y) + (x \cdot z))$
10. Transitive $\forall x \, \forall y \, \forall z \, (x \geq y \land y \geq z \rightarrow x \geq z)$
11. Antisym. $\forall x \, \forall y \, (x \geq y \land y \geq x \rightarrow x = y)$
12. Total $\forall x \, \forall y \, (x \geq y \lor y \geq x)$
13. Additive $\forall x \, \forall y \, \forall z \, (x \geq y \rightarrow x + z \geq y + z)$

Axioms of Reals

1. Commutative group $(\mathbb{R}, +)$: $\forall x\, \forall y\, \forall z\, x + (y + z) = (x + y) + z$
2. Neutral $\forall x\, x + 0 = x$
3. Inverse $\forall x\, \exists y\, x + y = 0$
4. Abelian $\forall x\, \forall y\, (x + y = y + x)$
5. Commutative group $(\mathbb{R} \setminus \{0\}, \cdot)$: $\forall x\, \forall y\, \forall z\, x \cdot (y \cdot z) = (x \cdot y) \cdot z$
6. Neutral $\forall x\, x \cdot 1 = x$
7. Inverse $\forall x\, (x \neq 0 \to \exists y\, x \cdot y = 1)$
8. Abelian $\forall x\, \forall y\, (x \cdot y = y \cdot x)$
9. Distributive $\forall x\, \forall y\, \forall z\, (x \cdot (y + z) = (x \cdot y) + (x \cdot z))$
10. Transitive $\forall x\, \forall y\, \forall z\, (x \geq y \land y \geq z \to x \geq z)$
11. Antisym. $\forall x\, \forall y\, (x \geq y \land y \geq x \to x = y)$
12. Total $\forall x\, \forall y\, (x \geq y \lor y \geq x)$
13. Additive $\forall x\, \forall y\, \forall z\, (x \geq y \to x + z \geq y + z)$
14. Positive $\forall x\, \forall y\, (x \geq 0 \land y \geq 0 \to x \cdot y \geq 0)$

Axioms of Reals

1. Commutative group $(\mathbb{R}, +)$: $\forall x\, \forall y\, \forall z\, x + (y + z) = (x + y) + z$
2. Neutral $\forall x\, x + 0 = x$
3. Inverse $\forall x\, \exists y\, x + y = 0$
4. Abelian $\forall x\, \forall y\, (x + y = y + x)$
5. Commutative group $(\mathbb{R} \setminus \{0\}, \cdot)$: $\forall x\, \forall y\, \forall z\, x \cdot (y \cdot z) = (x \cdot y) \cdot z$
6. Neutral $\forall x\, x \cdot 1 = x$
7. Inverse $\forall x\, (x \neq 0 \to \exists y\, x \cdot y = 1)$
8. Abelian $\forall x\, \forall y\, (x \cdot y = y \cdot x)$
9. Distributive $\forall x\, \forall y\, \forall z\, (x \cdot (y + z) = (x \cdot y) + (x \cdot z))$
10. Transitive $\forall x\, \forall y\, \forall z\, (x \geq y \land y \geq z \to x \geq z)$
11. Antisym. $\forall x\, \forall y\, (x \geq y \land y \geq x \to x = y)$
12. Total $\forall x\, \forall y\, (x \geq y \lor y \geq x)$
13. Additive $\forall x\, \forall y\, \forall z\, (x \geq y \to x + z \geq y + z)$
14. Positive $\forall x\, \forall y\, (x \geq 0 \land y \geq 0 \to x \cdot y \geq 0)$
15. Sup "Non-empty subsets with upper bounds have supremum"

First-order Axioms of Reals

What is a good set of first-order axioms for the reals $\mathbb{R}$?

First-order Axioms of Reals

What is a good set of first-order axioms for the reals $\mathbb{R}$?

Theorem (downward Skolem-Löwenheim'1915-20)

Let Γ be a countable set of first-order formulas.
Γ *has a model* $\Rightarrow$ Γ *has an infinite countable model*
"first-order logic cannot distinguish different infinities"

First-order Axioms of Reals

What is a good set of first-order axioms for the reals $\mathbb{R}$?

Theorem (downward Skolem-Löwenheim'1915-20)

Let Γ be a countable set of first-order formulas.
Γ *has a model* $\Rightarrow$ Γ *has an infinite countable model*
"first-order logic cannot distinguish different infinities"

Corollary

The reals cannot be characterized (up to isomorphism) in first-order logic (nor any other infinite structure really, not even in the generated case)

First-order Axioms of Reals

What is a good set of first-order axioms for the reals $\mathbb{R}$?

Theorem (downward Skolem-Löwenheim'1915-20)

Let Γ be a countable set of first-order formulas.
Γ *has a model* $\Rightarrow$ Γ *has an infinite countable model*
"first-order logic cannot distinguish different infinities"

Corollary

The reals cannot be characterized (up to isomorphism) in first-order logic (nor any other infinite structure really, not even in the generated case)

But the first-order "view" of the reals is still fairly amazing

Of Rationals and Reals

Rationals and Reals are . . .

Similar	Dissimilar	$\mathbb{Q}$	$\mathbb{R}$
✓		similar axioms (ordered field of characteristic 0)	

Of Rationals and Reals

Rationals and Reals are . . .

Similar	Dissimilar	$\mathbb{Q}$	$\mathbb{R}$
✓		similar axioms (ordered field of characteristic 0)	
	×	countable	uncountable

Of Rationals and Reals

Rationals and Reals are ...

Similar	Dissimilar	$\mathbb{Q}$	$\mathbb{R}$
✓		similar axioms (ordered field of characteristic 0)	
	×	countable	uncountable
✓		algebraic closures indistinguishable algebraically	

Of Rationals and Reals

Rationals and Reals are ...

Similar	Dissimilar	$\mathbb{Q}$	$\mathbb{R}$
✓		similar axioms (ordered field of characteristic 0)	
	×	countable	uncountable
✓		algebraic closures indistinguishable algebraically	
	×	doesn't know about π	has π

Of Rationals and Reals

Rationals and Reals are . . .

Similar	Dissimilar	$\mathbb{Q}$	$\mathbb{R}$
✓		similar axioms (ordered field of characteristic 0)	
	×	countable	uncountable
✓		algebraic closures indistinguishable algebraically	
	×	doesn't know about π	has π
	×	not closed (lim)	closed

Of Rationals and Reals

Rationals and Reals are . . .

Similar	Dissimilar	$\mathbb{Q}$	$\mathbb{R}$
✓		similar axioms (ordered field of characteristic 0)	
	×	countable	uncountable
✓		algebraic closures indistinguishable algebraically	
	×	doesn't know about π	has π
	×	not closed (lim)	closed
✓		dense in $\mathbb{R}$	

Of Rationals and Reals

Rationals and Reals are ...

Similar	Dissimilar	$\mathbb{Q}$	$\mathbb{R}$
✓		similar axioms (ordered field of characteristic 0)	
	×	countable	uncountable
✓		algebraic closures indistinguishable algebraically	
	×	doesn't know about π	has π
	×	not closed (lim)	closed
✓		dense in $\mathbb{R}$	
	×	$FOL_{\mathbb{Q}}$ undecidable	$FOL_{\mathbb{R}}$ decidable

Of Rationals and Reals

Rationals and Reals are . . .

Similar	Dissimilar	$\mathbb{Q}$	$\mathbb{R}$
✓		similar axioms (ordered field of characteristic 0)	
	×	countable	uncountable
✓		algebraic closures indistinguishable algebraically	
	×	doesn't know about π	has π
	×	not closed (lim)	closed
✓		dense in $\mathbb{R}$	
	×	$FOL_{\mathbb{Q}}$ undecidable	$FOL_{\mathbb{R}}$ decidable

Relaxing Reals to Real Fields

Definition (Formally real field)

Field R is a *(formally) real field* iff, equivalently:

Relaxing Reals to Real Fields

Definition (Formally real field)

Field R is a *(formally) real field* iff, equivalently:

1. -1 is not a sum of squares in R.

Relaxing Reals to Real Fields

Definition (Formally real field)

Field R is a *(formally) real field* iff, equivalently:

1. -1 is not a sum of squares in R.
2. For every $x_1, \ldots, x_n \in R$, $\sum_{i=1}^{n} x_i^2 = 0$ implies $x_1 = \cdots = x_n = 0$.

Relaxing Reals to Real Fields

Definition (Formally real field)

Field R is a *(formally) real field* iff, equivalently:

1. -1 is not a sum of squares in R.
2. For every $x_1, \ldots, x_n \in R$, $\sum_{i=1}^{n} x_i^2 = 0$ implies $x_1 = \cdots = x_n = 0$.
3. R admits an ordering that makes R an ordered field (ordering compatible with $+, \cdot$).

Relaxing Reals to Real Fields

Definition (Formally real field)

Field R is a *(formally) real field* iff, equivalently:

1. -1 is not a sum of squares in R.
2. For every $x_1, \dots, x_n \in R$, $\sum_{i=1}^{n} x_i^2 = 0$ implies $x_1 = \cdots = x_n = 0$.
3. R admits an ordering that makes R an ordered field (ordering compatible with $+, \cdot$).

- What's missing?

Relaxing Reals to Real Fields

Definition (Formally real field)

Field R is a *(formally) real field* iff, equivalently:

1. -1 is not a sum of squares in R.
2. For every $x_1, \ldots, x_n \in R$, $\sum_{i=1}^{n} x_i^2 = 0$ implies $x_1 = \cdots = x_n = 0$.
3. R admits an ordering that makes R an ordered field (ordering compatible with $+, \cdot$).

- What's missing?
- That we have enough elements in R.

Real-Closed Fields

Definition (Real-closed field)

Field R is *real-closed field* iff, equivalently:

1. R is an ordered field where every positive element is a square and every univariate polynomial in $R[X]$ of odd degree has a root in R (then this order is, in fact, unique).

Real-Closed Fields

Definition (Real-closed field)

Field R is *real-closed field* iff, equivalently:

1. R is an ordered field where every positive element is a square and every univariate polynomial in $R[X]$ of odd degree has a root in R (then this order is, in fact, unique).
2. R is not algebraically closed but its field extension $R[\sqrt{-1}] = R[i]/(i^2 + 1)$ is algebraically closed.

Real-Closed Fields

Definition (Real-closed field)

Field R is *real-closed field* iff, equivalently:

1. R is an ordered field where every positive element is a square and every univariate polynomial in $R[X]$ of odd degree has a root in R (then this order is, in fact, unique).
2. R is not algebraically closed but its field extension $R[\sqrt{-1}] = R[i]/(i^2 + 1)$ is algebraically closed.
3. R is not algebraically closed but its algebraic closure is a finite extension, i.e., finitely generated over R.

Real-Closed Fields

Definition (Real-closed field)

Field R is *real-closed field* iff, equivalently:

1. R is an ordered field where every positive element is a square and every univariate polynomial in $R[X]$ of odd degree has a root in R (then this order is, in fact, unique).
2. R is not algebraically closed but its field extension $R[\sqrt{-1}] = R[i]/(i^2 + 1)$ is algebraically closed.
3. R is not algebraically closed but its algebraic closure is a finite extension, i.e., finitely generated over R.
4. R has the *intermediate value property*, i.e., R is an ordered field such that for any polynomial $p \in R[X]$ with $a, b \in R, a < b$ and $p(a)p(b) < 0$, there is a ζ with $a < \zeta < b$ such that $p(\zeta) = 0$.

Real-Closed Fields

Definition (Real-closed field)

Field R is *real-closed field* iff, equivalently:

1. R is an ordered field where every positive element is a square and every univariate polynomial in $R[X]$ of odd degree has a root in R (then this order is, in fact, unique).
2. R is not algebraically closed but its field extension $R[\sqrt{-1}] = R[i]/(i^2 + 1)$ is algebraically closed.
3. R is not algebraically closed but its algebraic closure is a finite extension, i.e., finitely generated over R.
4. R has the *intermediate value property*, i.e., R is an ordered field such that for any polynomial $p \in R[X]$ with $a, b \in R, a < b$ and $p(a)p(b) < 0$, there is a ζ with $a < \zeta < b$ such that $p(\zeta) = 0$.
5. R is a real field such that no proper algebraic extension is a formally real field.

Real-Closed Fields beyond the Reals

Example (Real-closed fields)

- Real numbers $\mathbb{R}$.

Real-Closed Fields beyond the Reals

Example (Real-closed fields)

- Real numbers $\mathbb{R}$.
- Real algebraic numbers $\bar{\mathbb{Q}} \cap \mathbb{R}$, that is, real numbers in the algebraic closure of $\mathbb{Q}$, i.e., real numbers that are roots of a non-zero polynomial with rational or integer coefficients

$$p(r) = 0 \text{ for some } p \in \mathbb{Q}[X] \setminus \{0\}$$

Real-Closed Fields beyond the Reals

Example (Real-closed fields)

- Real numbers $\mathbb{R}$.
- Real algebraic numbers $\bar{\mathbb{Q}} \cap \mathbb{R}$, that is, real numbers in the algebraic closure of $\mathbb{Q}$, i.e., real numbers that are roots of a non-zero polynomial with rational or integer coefficients

$$p(r) = 0 \text{ for some } p \in \mathbb{Q}[X] \setminus \{0\}$$

- Computable numbers, i.e., those that can be approximated by a computable function up to any desired precision.

Real-Closed Fields beyond the Reals

Example (Real-closed fields)

- Real numbers $\mathbb{R}$.
- Real algebraic numbers $\bar{\mathbb{Q}} \cap \mathbb{R}$, that is, real numbers in the algebraic closure of $\mathbb{Q}$, i.e., real numbers that are roots of a non-zero polynomial with rational or integer coefficients

$$p(r) = 0 \text{ for some } p \in \mathbb{Q}[X] \setminus \{0\}$$

- Computable numbers, i.e., those that can be approximated by a computable function up to any desired precision. π lives here!

Real-Closed Fields beyond the Reals

Example (Real-closed fields)

- Real numbers $\mathbb{R}$.
- Real algebraic numbers $\bar{\mathbb{Q}} \cap \mathbb{R}$, that is, real numbers in the algebraic closure of $\mathbb{Q}$, i.e., real numbers that are roots of a non-zero polynomial with rational or integer coefficients

$$p(r) = 0 \text{ for some } p \in \mathbb{Q}[X] \setminus \{0\}$$

- Computable numbers, i.e., those that can be approximated by a computable function up to any desired precision. π lives here!
- ZFC-Definable numbers, i.e., those real numbers $a \in \mathbb{R}$ for which there is a first-order formula φ in set theory with one free variable such that a is the unique real number for which φ holds true.

$$I, \beta \models \varphi \text{ iff } I(x) = a$$

The advantages of implicit definition over construction are roughly those of theft over honest toil [Russell]

First-Order Axiom Schemes of Real-Closed Fields

1. Commutative group $(\mathbb{R}, +)$: $\forall x\, \forall y\, \forall z\; x + (y + z) = (x + y) + z$
2. Neutral $\forall x\; x + 0 = x$
3. Inverse $\forall x\, \exists y\; x + y = 0$
4. Abelian $\forall x\, \forall y\, (x + y = y + x)$
5. Commutative group $(\mathbb{R} \setminus \{0\}, \cdot)$: $\forall x\, \forall y\, \forall z\; x \cdot (y \cdot z) = (x \cdot y) \cdot z$
6. Neutral $\forall x\; x \cdot 1 = x$
7. Inverse $\forall x\, (x \neq 0 \to \exists y\; x \cdot y = 1)$
8. Abelian $\forall x\, \forall y\, (x \cdot y = y \cdot x)$
9. Distributive $\forall x\, \forall y\, \forall z\, (x \cdot (y + z) = (x \cdot y) + (x \cdot z))$
10. $\neg\exists x_1 \ldots \exists x_n\, (-1 = x_1^2 + \cdots + x_n^2)$ for any n
11. $\forall x\, \forall y\, (x < y \land p(x)p(y) < 0 \to \exists z\, (x < z < y \land p(z) = 0))$ for polynomial p (intermediate value property)

First-Order Axiom Schemes of Real-Closed Fields

1. Commutative group $(\mathbb{R}, +)$: $\forall x\, \forall y\, \forall z\, x + (y + z) = (x + y) + z$
2. Neutral $\forall x\, x + 0 = x$
3. Inverse $\forall x\, \exists y\, x + y = 0$
4. Abelian $\forall x\, \forall y\, (x + y = y + x)$
5. Commutative group $(\mathbb{R} \setminus \{0\}, \cdot)$: $\forall x\, \forall y\, \forall z\, x \cdot (y \cdot z) = (x \cdot y) \cdot z$
6. Neutral $\forall x\, x \cdot 1 = x$
7. Inverse $\forall x\, (x \neq 0 \rightarrow \exists y\, x \cdot y = 1)$
8. Abelian $\forall x\, \forall y\, (x \cdot y = y \cdot x)$
9. Distributive $\forall x\, \forall y\, \forall z\, (x \cdot (y + z) = (x \cdot y) + (x \cdot z))$
10. $\neg \exists x_1 \ldots \exists x_n\, (-1 = x_1^2 + \cdots + x_n^2)$ for any n
11. $\forall x\, \forall y\, (x < y \land p(x)p(y) < 0 \rightarrow \exists z\, (x < z < y \land p(z) = 0))$ for polynomial p (intermediate value property)