

Numbers

Wolfgang Schreiner

Research Institute for Symbolic Computation (RISC-Linz)

Johannes Kepler University, Linz, Austria

Wolfgang.Schreiner@risc.uni-linz.ac.at

<http://www.risc.uni-linz.ac.at/people/schreine>

Overview

- Number Domains

- Natural Numbers
- Integer Numbers
- Rational Numbers
- Real Numbers
- Complex Numbers

- Related Notions

- Minimum and Maximum
- Sum and Product
- Binomials
- Matrix Operations
- Polynomial Operations

The Natural Numbers

Natural Numbers

- The numbers of **counting** distinct objects.

no object, one object, two objects, ...

- Axiomatic characterization.

1. Describe **properties** of natural numbers.
2. Peano axioms.

- Set-theoretic construction.

1. Numbers are defined as sets.
2. Definition satisfies Peano laws.

Two ways to introduce the natural numbers.

Peano Arithmetic

- Theory of natural numbers.
 - Object constant 0 (**zero**).
 - Unary function constant ' (**successor**).

- Axioms

1. 0 is not the successor of any natural number:

$$\forall x : x' \neq 0.$$

2. Different natural numbers have different successors:

$$\forall x, y : x' = y' \Rightarrow x = y.$$

3. F holds for every number, if F holds for 0 and with every number also for its successor:

$$(F[x \leftarrow 0] \wedge (\forall x : F \Rightarrow F[x \leftarrow x + 1])) \Rightarrow \forall x : F.$$

Illustration

The natural numbers are a single infinite chain

$$0 \rightarrow 0' \rightarrow 0'' \rightarrow 0''' \rightarrow \dots$$

1. Chain starts with 0.
2. Every application of ' yields a new natural number.
3. Every natural number is captured by the chain.

Construction from Sets

$$\begin{aligned}0 &:= \emptyset; \\ x' &:= x \cup \{x\}.\end{aligned}$$

Proof of first Peano law:

We prove $\forall x : x' \neq 0$. Take arbitrary x . By definition of 0 and $'$, we have to prove

$$x \cup \{x\} \neq \emptyset$$

which is true because $x \in (x \cup \{x\})$ but $x \notin \emptyset$.

Proof of second Peano law: see lecture notes.

Set of Natural Numbers

Definition: \mathbb{N} , the set of **natural numbers**

(omitted)

Proposition: \mathbb{N} is the smallest set that satisfies the properties:

$$0 \in \mathbb{N};$$

$$\forall x \in \mathbb{N} : x' \in \mathbb{N};$$

$$\forall F :$$

$$(F(0) \wedge \forall x \in \mathbb{N} : F(x) \Rightarrow F(x + 1)) \Rightarrow \forall x \in \mathbb{N} : F(x).$$

Third Peano law is a consequence of this proposition.

Auxiliary Notions

All further definitions work for both constructions of the naturals.

- Subsets of the natural numbers:

$$\begin{aligned}\mathbb{N}_{>0} &:= \{x \in \mathbb{N} : x > 0\}; \\ \mathbb{N}_n &:= \{x \in \mathbb{N} : x < n\}.\end{aligned}$$

e.g. $\mathbb{N}_3 = \{0, 1, 2\}$.

- Predecessor function:

$$x^- := \mathbf{such} \ y : x = y'.$$

e.g. $3^- = 2$; $0^- = ?$.

Natural Number Arithmetic

Constants

$$1 := 0', \quad 2 := 1';$$

Addition

$$x + y := \text{if } y = 0 \text{ then } x \text{ else } (x + y^-)'$$

Multiplication

$$x * y := \text{if } y = 0 \text{ then } 0 \text{ else } x + (x * y^-)$$

Total Order

$$\begin{aligned} x \leq y &: \Leftrightarrow \\ &\text{if } x = 0 \text{ then T} \\ &\text{else if } y = 0 \text{ then F} \\ &\text{else } x^- \leq y^- \end{aligned}$$

Termination function $r(x, y) := y$ for recursive definitions.

Example

$$3 := 2'; 4 := 3'; 5 := 4'$$

$$3 < 5 :\Leftrightarrow$$

$$3^- < 5^- \Leftrightarrow 2 < 4 \Leftrightarrow$$

$$2^- < 4^- \Leftrightarrow 1 < 3 \Leftrightarrow$$

$$1^- < 3^- \Leftrightarrow 0 < 2 \Leftrightarrow$$

T

Recursive unfolding of definitions.

Natural Number Laws

For all natural numbers x and y , we have:

Addition

$$\begin{aligned}x + 0 &= x, \\x + y' &= (x + y)';\end{aligned}$$

Multiplication

$$\begin{aligned}x * 0 &= 0, \\x * y' &= x + (x * y);\end{aligned}$$

Total Order

$$\begin{aligned}0 \leq x &\Leftrightarrow \text{T}, \\x \leq 0 &\Leftrightarrow x = 0, \\x' \leq y' &\Leftrightarrow x \leq y.\end{aligned}$$

Natural Number Laws

For all natural numbers x, y, z , we have:

$$x + 0 = x,$$

$$x * 1 = x,$$

$$x + y = y + x,$$

$$x * y = y * x,$$

$$x + (y + z) = (x + y) + z,$$

$$x * (y * z) = (x * y) * z,$$

$$x * (y + z) = (x * y) + (x * z),$$

$$x \leq x,$$

$$(x \leq y \wedge y \leq x) \Rightarrow x = y,$$

$$(x \leq y \wedge y \leq z) \Rightarrow x \leq z.$$

Order Predicates

In every domain with a binary relation \leq :

$$x < y :\Leftrightarrow x \leq y \wedge x \neq y;$$

$$x > y :\Leftrightarrow x \not\leq y;$$

$$x \geq y :\Leftrightarrow x \not< y.$$

We often write $a \leq x < b$ to denote $x \leq a \wedge x < b$ and similar for all other combinations of the order predicates.

Logic Evaluator

```
pred N(x) <=> Nat(x);
```

```
fun N0 = 0;
```

```
fun '(x: N) = +(x, 1);
```

```
fun ^-(x: N) = such(n in nat(0, x): =(x, '(n)), n);
```

```
fun N1 = '(N0);
```

```
fun N2 = '(N1);
```

```
fun +N(x: N, y: N) recursive y =  
  if(=(y, N0), x, '(+N(x, ^-(y))));
```

```
fun *N(x: N, y: N) recursive y =  
  if(=(y, N0), N0, +N(x, *N(x, ^-(y))));
```

```
pred <=N(x: N, y: N) recursive y <=>  
  if(=(x, N0), true, if(=(y, N0), false, <=N(^-(x), ^-(y))));
```

Difference

Definition: z is a **difference** of x and y if $x = y + z$.

$$x - y := \mathbf{such} \ z : x = z + y.$$

- Difference is not defined for every x and y :

There is no z with $1 = z + 2$, thus $1 - 2$ is undefined.

- If a difference exists, it is unique:

$$\forall x, y, z_0, z_1 : (x = z_0 + y \wedge x = z_1 + y) \Rightarrow z_0 = z_1.$$

- If $x \geq y$, the difference of x and y is defined:

$$\forall x, y : x \geq y \Rightarrow x = (x - y) + y.$$

Quotient and Remainder

Definition: quotient and remainder

$$x \operatorname{div} y := \mathbf{such} \ q : \exists r : r < y \wedge x = (q * y) + r;$$
$$x \operatorname{mod} y := \mathbf{such} \ r : \exists q : r < y \wedge x = (q * y) + r.$$

Examples:

- $5 \operatorname{div} 3 = 1, 5 \operatorname{mod} 3 = 2.$
- $15 \operatorname{div} 6 = 2, 15 \operatorname{mod} 6 = 3.$
- $1 \operatorname{div} 3 = 0, 1 \operatorname{mod} 3 = 1.$
- $0 \operatorname{div} 3 = 0, 1 \operatorname{mod} 3 = 0.$

Properties of Quotient and Remainder

- Quotient and remainder are not defined for every x and y :

$(x \operatorname{div} 0)$ and $(x \operatorname{mod} 0)$ are undefined for every x .

- If quotient respectively remainder exist, they are unique.

$$\forall x, y, q_0, q_1, r_0 < y, r_1 < y : \\ (x = (q_0 * y) + r_0 \wedge x = (q_1 * y) + r_1) \Rightarrow (q_0 = q_1 \wedge r_0 = r_1).$$

- If the divisor is not null, quotient and remainder exist:

$$\forall x, y \neq 0 : (\exists q, r : r < y \wedge x = (q * y) + r).$$

- We thus have the following relationship:

$$\forall x, y \neq 0 : x = (x \operatorname{div} y) * y + (x \operatorname{mod} y).$$

Exponentiation

$$\cdot : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N},$$

$$x^n := \mathbf{if} \ n = 0_{\mathbb{N}} \ \mathbf{then} \ 1 \ \mathbf{else} \ x * x^{n-}.$$

Termination function: $r(x, n) := n$

Example:

$$\underline{5}^3 = 5 * (\underline{5}^2) = 5 * (5 * (\underline{5}^1)) = 5 * (5 * (5 * (\underline{5}^0))) = 5 * (5 * (5 * (1))) = 5 * 5 * 5.$$

More Notions

- x **divides** y if $x * z = y$ for some z :

$$x|y \Leftrightarrow \exists z : x * z = y.$$

- The **greatest common divisor** of x and y is the largest number that divides both x and y :

$$\text{gcd}(x, y) := \mathbf{such} \ z : z|x \wedge z|y \wedge (\forall w : (w|x \wedge w|y) \Rightarrow w \leq z).$$

- The **least common multiple** of x and y is the smallest number that both x and y divide:

$$\text{lcm}(x, y) := \mathbf{such} \ z : x|z \wedge y|z \wedge (\forall w : (x|w \wedge y|w) \Rightarrow z \leq w).$$

Examples

- $1|18, 2|18, 3|18, 6|18, 9|18, 18|18.$
- $1|24, 2|24, 3|24, 4|24, 6|24, 8|24, 12|24, 24|24.$
- $\gcd(18, 24) = 6.$
- $\gcd(16, 27) = 1.$
- $\text{lcm}(4, 6) = 12.$
- $\text{lcm}(8, 12) = 24.$

More Notions

- Two numbers are **relatively prime** if their gcd is 1:

$$x \text{ and } y \text{ are relatively prime} :\Leftrightarrow \gcd(x, y) = 1.$$

- A number greater than 1 is **prime** if its only divisors are 1 and itself:

$$x \text{ is prime} :\Leftrightarrow x > 1 \wedge (\forall y : y|x \Rightarrow (y = 1 \vee y = x)).$$

- 16 and 27 are relatively prime.
- (Only) the underlined numbers are prime:

$$0, 1, \underline{2}, \underline{3}, 4, \underline{5}, 6, \underline{7}, 8, 9, 10, \underline{11}, 12, \underline{13}, 14, 15, 16, \underline{17}, \dots$$

Logic Evaluator

```
pred divides(x, y) <=> exists(z in nat(N0, y): =( *N(x, z), y));
```

```
fun gcd(x, y) =  
  let(m = if(=(x, N0), y, x):  
    such(z in nat(N0, m):  
      and(divides(z, x), divides(z, y),  
        forall(w in nat(+N(z, N1), m):  
          or(not(divides(w, x)), not(divides(w, y))))),  
      z));
```

```
pred isprime(x) <=>  
  and(not(<=N(x, N1)),  
    forall(y in nat(N0, x):  
      implies(divides(y, x), or(=(y, N1), =(y, x)))));
```

The Integer Numbers

Motivation

- Not every pair of elements has a difference in \mathbb{N} :
 - $\neg \exists x : 0 = x + 1$.
 - $x - y := \mathbf{such} \ z : x = z + y$.
 - $0 - 1$ is undefined.
- Introduce a set \mathbb{Z} of **integer numbers** such that
 1. \mathbb{N} can be “embedded” into \mathbb{Z} , and
 2. for all integers a and b there is an integer x with $a = x + b$ (and consequently $a - b$ is defined).

Set-theoretic construction on top of \mathbb{N} .

Definition

Idea:

- Representation: let $\langle a, b \rangle$ denote the difference between a and b .
- Normalize: $\langle a, 0_{\mathbb{N}} \rangle$ for non-negative ints, $\langle 0_{\mathbb{N}}, a \rangle$ for negative ones.

$$\mathbb{Z} := \mathbb{Z}_{\geq 0} \cup \mathbb{Z}_{< 0};$$

$$\mathbb{Z}_{\geq 0} := \{ \langle x, 0_{\mathbb{N}} \rangle : x \in \mathbb{N} \};$$

$$\mathbb{Z}_{< 0} := \{ \langle 0_{\mathbb{N}}, x \rangle : x \in \mathbb{N} \setminus \{0_{\mathbb{N}}\} \};$$

Constructor function:

$$I : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{Z}$$

$$I(x, y) := \mathbf{if} \ x \geq_{\mathbb{N}} y \ \mathbf{then} \ \langle x -_{\mathbb{N}} y, 0_{\mathbb{N}} \rangle \ \mathbf{else} \ \langle 0_{\mathbb{N}}, y -_{\mathbb{N}} x \rangle;$$

Example

- The difference of 5 and 3 is denoted by

$$I(5_{\mathbb{N}}, 3_{\mathbb{N}}) = \langle 2_{\mathbb{N}}, 0_{\mathbb{N}} \rangle = 2_{\mathbb{Z}}.$$

- The difference of 3 and 5 is denoted by

$$I(3_{\mathbb{N}}, 5_{\mathbb{N}}) = \langle 0_{\mathbb{N}}, 2_{\mathbb{N}} \rangle = -2_{\mathbb{Z}}.$$

Now it remains to define the arithmetic operations.

Integer Arithmetic

Constants

$$0 := I(0_{\mathbb{N}}, 0_{\mathbb{N}}); \quad 1 := I(1_{\mathbb{N}}, 0_{\mathbb{N}}); \quad 2 := I(2_{\mathbb{N}}, 0_{\mathbb{N}}).$$

Basic Arithmetic

$$x + y := I(x_0 +_{\mathbb{N}} y_0, x_1 +_{\mathbb{N}} y_1);$$

$$x * y := I((x_0 *_{\mathbb{N}} y_0) +_{\mathbb{N}} (x_1 *_{\mathbb{N}} y_1), (x_0 *_{\mathbb{N}} y_1) +_{\mathbb{N}} (x_1 *_{\mathbb{N}} y_0))$$

$$-x := \langle x_1, x_0 \rangle;$$

$$x - y := x + (-y).$$

Total Order

$$x \leq y :\Leftrightarrow (x_0 + y_1 <_{\mathbb{N}} y_0 + x_1).$$

Examples

- $-2 = -\langle 2_{\mathbb{N}}, 0_{\mathbb{N}} \rangle = \langle 0_{\mathbb{N}}, 2_{\mathbb{N}} \rangle.$
- $(-2) + 1 = (-\langle 2_{\mathbb{N}}, 0_{\mathbb{N}} \rangle) + \langle 1_{\mathbb{N}}, 0_{\mathbb{N}} \rangle = \langle 0_{\mathbb{N}}, 2_{\mathbb{N}} \rangle + \langle 1_{\mathbb{N}}, 0_{\mathbb{N}} \rangle = I(0_{\mathbb{N}} + 1_{\mathbb{N}}, 2_{\mathbb{N}} + 0_{\mathbb{N}}) = I(1_{\mathbb{N}}, 2_{\mathbb{N}}) = \langle 0_{\mathbb{N}}, 1_{\mathbb{N}} \rangle = -\langle 1_{\mathbb{N}}, 0_{\mathbb{N}} \rangle = -1.$
- $2 * 3 = \langle 2_{\mathbb{N}}, 0_{\mathbb{N}} \rangle * \langle 3_{\mathbb{N}}, 0_{\mathbb{N}} \rangle = I((2_{\mathbb{N}} *_{\mathbb{N}} 3_{\mathbb{N}}) + (0_{\mathbb{N}} *_{\mathbb{N}} 0_{\mathbb{N}}), (2_{\mathbb{N}} *_{\mathbb{N}} 0_{\mathbb{N}}) + (3_{\mathbb{N}} *_{\mathbb{N}} 0_{\mathbb{N}})) = I(6_{\mathbb{N}}, 0_{\mathbb{N}}) = \langle 6_{\mathbb{N}}, 0_{\mathbb{N}} \rangle = 6.$
- $(-2) * 3 = (-\langle 2_{\mathbb{N}}, 0_{\mathbb{N}} \rangle) * \langle 3_{\mathbb{N}}, 0_{\mathbb{N}} \rangle = \langle 0_{\mathbb{N}}, 2_{\mathbb{N}} \rangle * \langle 3_{\mathbb{N}}, 0_{\mathbb{N}} \rangle = I((0_{\mathbb{N}} *_{\mathbb{N}} 3_{\mathbb{N}}) + (2_{\mathbb{N}} *_{\mathbb{N}} 0_{\mathbb{N}}), (0_{\mathbb{N}} *_{\mathbb{N}} 0_{\mathbb{N}}) + (2_{\mathbb{N}} *_{\mathbb{N}} 3_{\mathbb{N}})) = I(0_{\mathbb{N}}, 6_{\mathbb{N}}) = \langle 0_{\mathbb{N}}, 6_{\mathbb{N}} \rangle = -\langle 6_{\mathbb{N}}, 0_{\mathbb{N}} \rangle = -6.$

Substituting and evaluating the definitions.

More Arithmetic

$$|x| := \mathbf{if} \ 0 \leq x \ \mathbf{then} \ x \ \mathbf{else} \ -x;$$

$$\mathbf{sign}(x) := \mathbf{if} \ x = 0 \ \mathbf{then} \ 0 \ \mathbf{else} \ \mathbf{if} \ 0 \leq x \ \mathbf{then} \ 1 \ \mathbf{else} \ -1;$$

$$x \ \mathbf{div} \ y := \mathbf{such} \ q : \exists r :$$

$$|r| < |y| \wedge x = q * y + r \wedge (\mathbf{sign}(r) = 0 \vee \mathbf{sign}(r) = \mathbf{sign}(y));$$

$$x \ \mathbf{mod} \ y := \mathbf{such} \ r : \exists q :$$

$$|r| < |y| \wedge x = q * y + r \wedge (\mathbf{sign}(r) = 0 \vee \mathbf{sign}(r) = \mathbf{sign}(y)).$$

Integer Laws

Same laws that also hold in \mathbb{N} .

Proposition:

$$\forall x \in \mathbb{Z}, y \in \mathbb{Z} : x + y = y + x.$$

Proof: Take arbitrary $x \in \mathbb{Z}, y \in \mathbb{Z}$. We have

$$\begin{aligned} x + y &= (\text{definition of } +) \\ I(x_0 +_{\mathbb{N}} y_0, x_1 +_{\mathbb{N}} y_1) &= (\text{commutativity of } +_{\mathbb{N}}) \\ I(y_0 +_{\mathbb{N}} x_0, y_1 +_{\mathbb{N}} x_1) &= (\text{definition of } +) \\ & y + x. \end{aligned}$$

Difference

Proposition: For every integer x and y the difference is defined:

$$\forall x \in \mathbb{Z}, y \in \mathbb{Z} : x = (x - y) + y.$$

Proof: Take arbitrary $x \in \mathbb{Z}$ and $y \in \mathbb{Z}$. We have

$$\begin{aligned}(x - y) + y &= (\text{definition of } -) \\(x + (-y)) + y &= (\text{associativity of } +) \\x + ((-y) + y) &= (*) \\x + 0 &= (\text{definition of } + \text{ and } 0) \\x &.\end{aligned}$$

Proof (Continued)

(*) We show $-y + y = 0$:

$$-y + y = (\text{definition of } -)$$

$$\langle y_1, y_0 \rangle + y = (\text{definition of } +)$$

$$I(y_1 +_{\mathbb{N}} y_0, y_0 +_{\mathbb{N}} y_1) = (\text{definition of } I, \text{ computation in } \mathbb{N})$$

$$\langle 0_{\mathbb{N}}, 0_{\mathbb{N}} \rangle = (\text{definition of } 0)$$

0.

Integer Numbers

- Difference of two numbers is always well-defined.
- Definition on top of \mathbb{N} .
 - $\mathbb{Z} \subseteq \mathbb{N} \times \mathbb{N}$.
 - $\mathbb{N} \not\subseteq \mathbb{Z}$!
- We will see later how to “embed” \mathbb{N} into \mathbb{Z} .
- We will see later a “better” construction of \mathbb{Z} .

The Rational Numbers

Motivation

- Not every pair of elements has a quotient in \mathbb{Z} :
 - $\neg \exists x : 2 = x * 3$.
 - $x/y := \mathbf{such} \ z : x = z * y$.
 - $2/3$ is undefined.
- Introduce a set \mathbb{Q} of **rational numbers** such that
 1. \mathbb{Z} can be “embedded” into \mathbb{Q} , and
 2. for all rationals a and b there is a rational x with $a = x * b$ (and consequently a/b is defined).

Set-theoretic construction on top of \mathbb{Z} .

Definition

Idea:

- Representation: let $\langle a, b \rangle$ denote the quotient between a and b .
- Normalization: a and b are relatively prime and b is positive.

Conversion functions:

$$\begin{aligned} Z : \mathbb{N} &\rightarrow \mathbb{Z}_{\geq 0}, & Z(x) &:= \langle x, 0_{\mathbb{N}} \rangle; \\ N : \mathbb{Z} &\rightarrow \mathbb{N}, & N(x) &:= |x|_0; \end{aligned}$$

Set definition:

$$\mathbb{Q} := \{ \langle x, y \rangle : x \in \mathbb{Z} \wedge y \in \mathbb{Z}_{>0} \wedge N(x) \text{ and } N(y) \text{ are relatively prime} \}.$$

Constructor function

$$\begin{aligned} \frac{*}{*} &: \mathbb{Z} \times \mathbb{Z}_{>0} \rightarrow \mathbb{Q} \\ \frac{x}{y} &:= \langle \text{sign}(x *_{\mathbb{Z}} y) *_{\mathbb{Z}} (|x| \text{div}_{\mathbb{Z}} g), |y| \text{div}_{\mathbb{Z}} g \rangle \\ &\text{where } g = \mathbb{Z}(\text{gcd}(N(x), N(y))). \end{aligned}$$

Example:

- $\frac{10_{\mathbb{Z}}}{6_{\mathbb{Z}}} = \langle 1_{\mathbb{Z}} *_{\mathbb{Z}} (10_{\mathbb{Z}} \text{div}_{\mathbb{Z}} 2_{\mathbb{Z}}), 6_{\mathbb{Z}} \text{div}_{\mathbb{Z}} 2_{\mathbb{Z}} \rangle = \langle 5_{\mathbb{Z}}, 3_{\mathbb{Z}} \rangle.$
- $\frac{-_{\mathbb{Z}}10_{\mathbb{Z}}}{6_{\mathbb{Z}}} = \langle -_{\mathbb{Z}}1_{\mathbb{Z}} *_{\mathbb{Z}} (10_{\mathbb{Z}} \text{div}_{\mathbb{Z}} 2_{\mathbb{Z}}), 6_{\mathbb{Z}} \text{div}_{\mathbb{Z}} 2_{\mathbb{Z}} \rangle = \langle -_{\mathbb{Z}}5_{\mathbb{Z}}, 3_{\mathbb{Z}} \rangle.$
- $\frac{-_{\mathbb{Z}}10_{\mathbb{Z}}}{-_{\mathbb{Z}}6_{\mathbb{Z}}} = \langle 1_{\mathbb{Z}} *_{\mathbb{Z}} (10_{\mathbb{Z}} \text{div}_{\mathbb{Z}} 2_{\mathbb{Z}}), 6_{\mathbb{Z}} \text{div}_{\mathbb{Z}} 2_{\mathbb{Z}} \rangle = \langle 5_{\mathbb{Z}}, 3_{\mathbb{Z}} \rangle.$

Numerator and Denominator

Let $r \in \mathbb{Q}$ and take x and y such that $r = \langle x, y \rangle$. We call x the **numerator** of r and y its **denominator**:

$$\begin{aligned}\text{numerator}(r) &:= \mathbf{such} \ x : \exists y : r \in \mathbb{Q} \wedge r = \langle x, y \rangle; \\ \text{denominator}(r) &:= \mathbf{such} \ y : \exists x : r \in \mathbb{Q} \wedge r = \langle x, y \rangle.\end{aligned}$$

Numerator and denominator are uniquely defined.

Rational Arithmetic

Definition:

See Lecture Notes!

Satisfies same laws as integer arithmetic.

Quotient

Proposition: For all rationals x and $y \neq 0$ the quotient is defined:

$$\forall x \in \mathbb{Q}, y \in \mathbb{Q} \setminus \{0\} : x = (x/y) * y.$$

Proof: see lecture notes.

Proposition: Between any two rational numbers, there is another rational number:

$$\forall x \in \mathbb{Q}, y \in \mathbb{Q} : x < y \Rightarrow \exists z \in \mathbb{Q} : x < z < y.$$

Proof: Take $x \in \mathbb{Q}$ and $y \in \mathbb{Q}$ with $x < y$. Then $x < (x+y)/2 < y$.

Rational Numbers

- Quotient of two numbers is always well-defined.
- Between any two rationals, there is another rational.
- Definition on top of \mathbb{Z} .
 - $\mathbb{Q} \subseteq \mathbb{Z} \times \mathbb{Z}$.
 - $\mathbb{Z} \not\subseteq \mathbb{Q}$!
- We will see later how to “embed” \mathbb{Z} into \mathbb{Q} .
- We will see later a “better” construction of \mathbb{Q} .

The Real Numbers

Motivation

- Not every element has a square root in \mathbb{Q} :
 - $\neg \exists x : x * x = 2$.
 - $\sqrt{x} := \mathbf{such} \ z : x = z * z$.
 - $\sqrt{2}$ is undefined.
- **Proof:** see lecture notes.
- Introduce a set \mathbb{R} of **real numbers** such that
 1. \mathbb{Q} can be “embedded” into \mathbb{R} , and
 2. for every non-negative real number a there is a real number x with $a = x * x$ (and consequently \sqrt{a} is defined).

Axiomatic characterization.

Theory of Reals

- Object constants 0 and 1.
- Unary function constant $^{-1}$.
- Binary function constants $+$, $-$, $*$.
- Binary predicate constant \leq .
- Axioms: see lecture notes.

Existence of Real Roots

Proposition: In \mathbb{R} every non-negative number has an n -th root:

$$\forall a \in \mathbb{R}_{\geq 0}, n \in \mathbb{N}_{>0} : \exists x \in \mathbb{R} : x^n = a.$$

Definition:

$$\begin{aligned} \sqrt[n]{x} &:= \text{such } y : x^n = y \\ \sqrt{x} &:= \sqrt[2]{x}. \end{aligned}$$

Consequence:

$$\forall a \in \mathbb{R}_{\geq 0}, n \in \mathbb{N}_{>0} : (\sqrt[n]{a})^n = a.$$

All roots of non-negative reals are well-defined.

Real Numbers

- Roots of non-negative reals are well defined.
- Axiomatic characterization.
- There are also “constructive” definitions of \mathbb{R} .
- We will see later how to “embed” \mathbb{Q} into \mathbb{R} .

The Complex Numbers

Motivation

- Not every element has a square root in \mathbb{R} :
 - $\neg \exists x : x * x = -1$.
 - $\sqrt{x} := \mathbf{such} \ z : x = z * z$.
 - $\sqrt{-1}$ is undefined.
- **Proof:** We prove $\forall x \in \mathbb{R} : x * x \neq -1$. Take arbitrary $x \in \mathbb{R}$. If $x \geq 0$, then $x * x \geq 0$. If $x < 0$, then also $x * x \geq 0$.
- Introduce a set \mathbb{C} of **complex numbers** such that
 1. \mathbb{R} can be “embedded” into \mathbb{C} , and
 2. for every complex number a there is a complex number x with $a = x * x$ (and consequently \sqrt{a} is defined).

Set-theoretic definition on top of \mathbb{R} .

Definition

$$\mathbb{C} := \mathbb{R} \times \mathbb{R}.$$

Constructor Function:

$$\begin{aligned} _ + _ i &: \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{C} \\ x + yi &:= \langle x, y \rangle. \end{aligned}$$

Let $c \in \mathbb{C}$ and take x and y such that $c = \langle x, y \rangle$. We call x the **real part** of c and y its **imaginary part**:

$$\begin{aligned} \text{real}(c) &:= \text{such } x : \exists y : c \in \mathbb{C} \wedge c = \langle x, y \rangle; \\ \text{imaginary}(c) &:= \text{such } y : \exists x : c \in \mathbb{C} \wedge c = \langle x, y \rangle. \end{aligned}$$

Complex Number Operations

Constants

$$0 := 0_{\mathbb{R}} + 0_{\mathbb{R}}i; \quad 1 := 1_{\mathbb{R}} + 0_{\mathbb{R}}i; \quad 2 := 2_{\mathbb{R}} + 0_{\mathbb{R}}i; \quad i := 0_{\mathbb{R}} + 1_{\mathbb{R}}i.$$

Arithmetic

$$x + y := (x_0 +_{\mathbb{R}} y_0) + (x_1 +_{\mathbb{R}} y_1)i;$$

$$x - y := (x_0 -_{\mathbb{R}} y_0) + (x_1 -_{\mathbb{R}} y_1)i;$$

$$x * y := ((x_0 *_{\mathbb{R}} y_0) -_{\mathbb{R}} (x_1 *_{\mathbb{R}} y_1)) + ((x_0 *_{\mathbb{R}} y_1) +_{\mathbb{R}} (x_1 *_{\mathbb{R}} y_0))i$$

$$x/y := (((x_0 *_{\mathbb{R}} y_0) +_{\mathbb{R}} (x_1 *_{\mathbb{R}} y_1))/_{\mathbb{R}} d) +$$

$$(((x_1 *_{\mathbb{R}} y_0) -_{\mathbb{R}} (x_0 *_{\mathbb{R}} y_1))/_{\mathbb{R}} d)i$$

$$\text{where } d = (y_0 *_{\mathbb{R}} y_0) +_{\mathbb{R}} (y_1 *_{\mathbb{R}} y_1).$$

Example

- $i * i = (0_{\mathbb{R}} + 1_{\mathbb{R}}i) * (0_{\mathbb{R}} + 1_{\mathbb{R}}i) = (0_{\mathbb{R}} -_{\mathbb{R}} 1_{\mathbb{R}}) + (0_{\mathbb{R}} +_{\mathbb{R}} 0_{\mathbb{R}})i = (-_{\mathbb{R}}1_{\mathbb{R}}) + 0_{\mathbb{R}}i = -(1_{\mathbb{R}} + 0_{\mathbb{R}}i) = -1.$
- $2 * 3 = (2_{\mathbb{R}} + 0_{\mathbb{R}}i) * (3_{\mathbb{R}} + 0_{\mathbb{R}}i) = (6_{\mathbb{R}} -_{\mathbb{R}} 0_{\mathbb{R}}) + (0_{\mathbb{R}} +_{\mathbb{R}} 0_{\mathbb{R}})i = 6_{\mathbb{R}} + 0_{\mathbb{R}}i = 6.$
- $(1_{\mathbb{R}} + 3_{\mathbb{R}}i) * (2_{\mathbb{R}} + 4_{\mathbb{R}}i) = (2_{\mathbb{R}} -_{\mathbb{R}} 12_{\mathbb{R}}) + (4_{\mathbb{R}} +_{\mathbb{R}} 6_{\mathbb{R}})i = (-_{\mathbb{R}}10_{\mathbb{R}}) + 10_{\mathbb{R}}i.$

Fundamental Theorem of Algebra

For every $a_0 \in \mathbb{C}, \dots, a_{n-1} \in \mathbb{C}$, there exists an $x \in \mathbb{C}$ such that

$$a_0 * x^0 + \dots + a_{n-1} * x^{n-1} = 0.$$

- \mathbb{C} is **complete** with respect to $+$ and $*$.
 - Every equation with $+$ and $*$ has a solution in \mathbb{C} .

No further extension required.

Complex Square Root

$\sqrt{x} :=$
if $x_1 \geq_{\mathbb{R}} 0_{\mathbb{R}}$ **then** $u + vi$ **else** $u + (-_{\mathbb{R}}v)i$
where

$$u = \sqrt{(x_0 +_{\mathbb{R}} \sqrt{x_0^2 +_{\mathbb{R}} x_1^2}) /_{\mathbb{R}} 2_{\mathbb{R}}}$$

$$v = \sqrt{(-_{\mathbb{R}}x_0 +_{\mathbb{R}} \sqrt{x_0^2 +_{\mathbb{R}} x_1^2}) /_{\mathbb{R}} 2_{\mathbb{R}}}.$$

Proposition: the (positive or negative) root of x squared equals x .

$\forall x \in \mathbb{C} :$

let $r = \sqrt{x} :$

$$x = r * r \wedge x = (-r) * (-r).$$

Complex Conjugate

Definition: the complex conjugate.

$$\bar{x} := x_0 + (-\mathbb{R}x_1)i.$$

Example: $\overline{3_{\mathbb{R}} + 5_{\mathbb{R}}i} = 3_{\mathbb{R}} + (-\mathbb{R}5_{\mathbb{R}})i.$

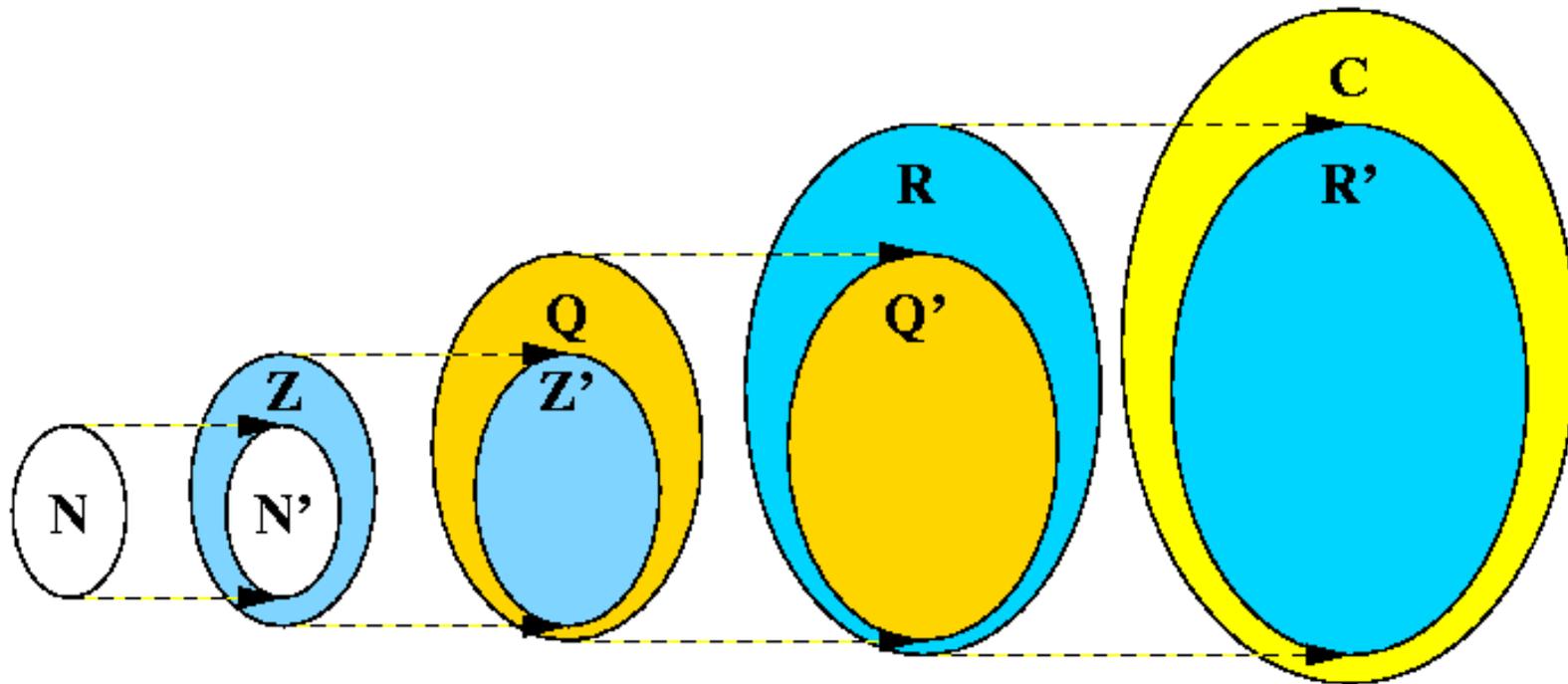
Proposition: For every $x \in \mathbb{C}, y \in \mathbb{C}, z \in \mathbb{C}$, the following holds:

$$\begin{aligned}\overline{\bar{x}} &= x, \\ \overline{x + y} &= \bar{x} + \bar{y}, \\ \overline{x * y} &= \bar{x} * \bar{y}, \\ y \neq 0 &\Rightarrow \overline{x/y} = \bar{x}/\bar{y},\end{aligned}$$

Complex Numbers

- \mathbb{C} is complete with respect to $+$ and $*$.
 - All equations have solutions in \mathbb{C} .
- Definition on top of \mathbb{R} .
 - $\mathbb{C} = \mathbb{R} \times \mathbb{R}$.
 - $\mathbb{R} \not\subseteq \mathbb{C}$!
 - Cartesian coordinates.
- We will see later how to “embed” \mathbb{R} into \mathbb{C} .
- We will see later another definition of \mathbb{C} (polar coordinates).

Relationship between Number Domains



Each domain has an “identical twin” in subsequent domain.

Related Notions

Minimum and Maximum Quantifier

Definition: If x is a variable and F is a formula, then the following are terms with bound variable x :

$$\min_x F$$

$$\max_x F$$

The value of the first term is the smallest value of x such that F holds; the value of the second term is the largest such value:

$$\min_x F := \mathbf{such} \ x : F \wedge (\forall y : F[x \leftarrow y] \Rightarrow x \leq y);$$

$$\max_x F := \mathbf{such} \ x : F \wedge (\forall y : F[x \leftarrow y] \Rightarrow x \geq y).$$

Quantifiers for every domain with a binary predicate \leq .

Minimum and Maximum Function

$$\min(S) := \min_x x \in S;$$

$$\max(S) := \max_x x \in S;$$

Examples:

- We have

$$\max_x (\text{isprime}(x) \wedge x|100) = 5.$$

- The value of

$$\min(\{1/x : x \in \mathbb{N}_{>0}\})$$

is undefined, because for every x in $\{1/1, 1/2, 1/3, 1/4, \dots\}$ there is always an y in this set with $y < x$, namely $1/(x+1)$.

Sum Quantifier

Definition: If x is a variable, F is a formula and T is a term, then the following is a term with bound variable x :

$$\sum_{x,F} T.$$

The value of this term is 0, if F does not hold for any x ; otherwise it is, for every x that satisfies F , the sum of the value of T and of the value of the term for all other x :

$$\begin{aligned} (\forall x : \neg F) &\Rightarrow \sum_{x,F} T = 0; \\ (\forall y : F[x \leftarrow y]) &\Rightarrow \sum_{x,F} T = T[x \leftarrow y] + \sum_{x,F \wedge x \neq y} T). \end{aligned}$$

Examples

$$\sum_{1 \leq i \leq n} i^2 = \sum_{i, (i \in \mathbb{N} \wedge 1 \leq i \wedge i \leq n)} i^2$$

$$\sum_{1 \leq i \leq 0} i^2 = 0$$

$$\sum_{1 \leq i \leq 5} i^2 = 1^2 + \sum_{2 \leq i \leq 5} i^2$$

$$\sum_{1 \leq i \leq 5} i^2 = 1^2 + 2^2 + 3^2 + 4^2 + 5^2;$$

Examples

$$\sum_{1 \leq i \leq 9} (x - i)^2 = (x - 1)^2 + \sum_{2 \leq i \leq 9} (x - i)^2$$

$$\sum_{1 \leq i \leq n} x^i = \sum_{1 \leq i \leq n \wedge \text{iseven}(i)} x^i + \sum_{1 \leq i \leq n \wedge \text{isodd}(i)} x^i$$

Identities which are true for every x .

Example: Decimal Number Representation

Let $a := [3, 1, 2, 9, 0, 7]$. We have

$$\sum_{0 \leq i \leq 5} a_i * 10^i = 709213.$$

In general, for any finite sequence d of “decimal digits” the term

$$\sum_{0 \leq i < \text{length}(d)} d_i * 10^i$$

denotes the value of this sequence in the decimal number system.

Example: Binary Number Representation

Likewise, for any finite sequence b of binary digits 0 and 1, the value

$$\sum_{0 \leq i < \text{length}(b)} b_i * 2^i$$

denotes the value of this sequence in the binary number system, e.g., the value of $[0, 1, 1, 0, 1]$ is

$$1 * 2^4 + 0 * 2^3 + 1 * 2^2 + 1 * 2^1 + 0 * 2^0 = 22.$$

Generalization to any number base.

Multiple Variable Bindings

$$\sum_{1 \leq i \leq 5, 1 \leq j \leq 3} i * j = 1 * 1 + 1 * 2 + 1 * 3 + \sum_{2 \leq i \leq 5, 1 \leq j \leq 3} i * j$$

$$\sum_{1 \leq i \leq 3, 1 \leq j \leq i} i * j = 1 * 1 + 2 * 1 + 2 * 2 + 3 * 1 + 3 * 2 + 3 * 3.$$

Bound variables have to be deduced from context.

Sum Identities

For all vars i and j and formulas F (in which j does not occur freely), G (in which i does not occur freely), and H and terms T and U :

$$\sum_{i,F} T * \sum_{j,G} U = \sum_{i,F} \sum_{j,G} T * U.$$

$$\sum_{i,F} \sum_{j,G} T = \sum_{j,G} \sum_{i,F} T = \sum_{i,j,F \wedge G} T.$$

$$\sum_{i,F} T + \sum_{i,H} T = \sum_{i,F \vee H} T + \sum_{i,F \wedge H} T.$$

Sum Identities

Furthermore, if term C is a term in which i does not occur freely:

$$\sum_{i,F} C * T = C * \sum_{i,F} T.$$

$$\sum_{i,F} C = n * C$$

(where n is the number of i for which F holds).

Examples

$$\sum_{1 \leq i \leq n} x^i * \sum_{1 \leq j \leq m} x^j = \sum_{1 \leq i \leq n} \sum_{1 \leq j \leq m} x^{i+j} = \sum_{1 \leq i \leq n \wedge 1 \leq j \leq m} x^{i+j}.$$

$$\sum_{1 \leq i \leq n} \sum_{1 \leq j \leq m} i * x^j = \sum_{1 \leq i \leq n} (i * \sum_{1 \leq j \leq m} x^j).$$

Many more identities can be deduced from basic definition.

Product Quantifier

If x is a variable, F is a formula and T is a term, then the following is a term with bound variable x :

$$\prod_{x,F} T.$$

The value of this term is 1, if F does not hold for any x ; otherwise it is, for every x that satisfies F , the product of the value of T and of the value of the term for all other x :

$$\begin{aligned} (\forall x : \neg F) &\Rightarrow \prod_{x,F} T = 1; \\ (\forall y : F[x \leftarrow y]) &\Rightarrow \prod_{x,F} T = T[x \leftarrow y] * \prod_{x,F \wedge x \neq y} T). \end{aligned}$$

Example

$$\prod_{1 \leq i \leq n} i^2 = \prod_{i, (i \in \mathbb{N} \wedge 1 \leq i \wedge i \leq n)} i^2$$

$$\prod_{1 \leq i \leq 0} i^2 = 1$$

$$\prod_{1 \leq i \leq 5} i^2 = 1^2 * \prod_{2 \leq i \leq 5} i^2$$

$$\prod_{1 \leq i \leq 5} i^2 = 1^2 * 2^2 * 3^2 * 4^2 * 5^2;$$

Product Identities

See lecture notes.

Factorial

Definition: The **factorial** of a natural number n is the product of all non-zero numbers less than or equal n :

$$n! := \prod_{1 \leq i \leq n} i.$$

Handy notation for a particular product.

Binomial

Definition: The **binomial coefficient** (Binomialkoeffizient) “ n choose k ” of two natural numbers n and k :

$$\binom{n}{k} := \mathbf{if} \ 0 \leq k \leq n \ \mathbf{then} \ \frac{n!}{k! * (n - k)!} \ \mathbf{else} \ 0.$$

Proposition: We have for every n and k with $0 \leq k \leq n$

$$\binom{n}{k} = \frac{\prod_{n-k+1 \leq i \leq n} i}{\prod_{1 \leq i \leq k} i}.$$

Important notion in combinatorics (the math of “counting things”).

Motivation

$\binom{n}{k}$ is the number of ways

- to choose a k element set
- from an n -element set.

Example:

The set $\{0, 1, 2, 3\}$ has $6 = \binom{4}{2}$ subsets with 2 elements:

$$\{0, 1\}, \{0, 2\}, \{0, 3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}.$$

Binomial Identities

For every $n \in \mathbb{N}$ and $k \in \mathbb{N}$ with $0 \leq k \leq n$:

$$\binom{n+1}{k+1} = \binom{n}{k} + \binom{n}{k+1},$$

$$\binom{n}{k} = \binom{n}{n-k},$$

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

Pascal's Triangle

$$\begin{array}{cccc}
 & & 1 & \\
 & 1 & & 1 \\
 & & 1 & 2 & 1 \\
 1 & & 3 & & 3 & & 1 \\
 \dots & & \dots & & \dots & & \dots
 \end{array}
 =
 \begin{array}{cccc}
 & & \binom{0}{0} & \\
 & \binom{1}{0} & & \binom{1}{1} \\
 & & \binom{2}{0} & \binom{2}{1} & \binom{2}{2} \\
 \binom{3}{0} & \binom{3}{1} & \binom{3}{2} & \binom{3}{3} \\
 \dots & & \dots & & \dots
 \end{array}$$

Construction

This triangle is bounded by sides of 1 and where every interior element is the sum of both parents:

$$\begin{array}{ccc} \binom{n}{k} & & \binom{n}{k+1} \\ \dots & & \dots \\ & \binom{n+1}{k+1} & \dots \end{array}$$

Quick construction of binomial values.

Matrix Operations

See lecture notes.

Polynomials

A **polynomial** over the reals is an infinite sequence of real numbers, the **coefficients**, of which only finitely many are different from 0:

$$p \text{ is polynomial} \iff p : \mathbb{N} \rightarrow \mathbb{R} \wedge (\exists k \in \mathbb{N} : \forall i \geq k : p_i = 0).$$

The **degree** of a polynomial is zero, if all coefficients are zero; otherwise, it is the index of the largest non-zero coefficient:

$$\begin{aligned} \text{deg}(p) &:= \\ &\mathbf{if} \ \forall i \in \mathbb{N} : p_i = 0 \\ &\quad \mathbf{then} \ 0 \\ &\quad \mathbf{else} \ (\mathbf{such} \ k \in \mathbb{N} : p_k \neq 0 \wedge (\forall i > k : p_i = 0)). \end{aligned}$$

Special Polynomials

$$\text{Poly} := \{p \in \mathbb{N} \rightarrow \mathbb{R} : p \text{ is polynomial}\}.$$

Definition: constant and variable polynomial

$$\cdot_{\text{Poly}} : \mathbb{R} \rightarrow \text{Poly}$$

$$c_{\text{Poly}} := \mathbf{such} \ p \in \text{Poly} : p_0 = c \wedge (\forall i > 0 : p_i = 0)$$

$$\mathbf{x} := \mathbf{such} \ p \in \text{Poly} : p_0 = 0 \wedge p_1 = 1 \wedge (\forall i > 1 : p_i = 0)$$

$$3_{\text{Poly}} = [3, 0, 0, 0, 0, \dots]$$

$$\mathbf{x} = [0, 1, 0, 0, 0, \dots]$$

Polynomial Operations

$$+ : \text{Poly} \times \text{Poly} \rightarrow \text{Poly}$$

$$(p + q)_i := p_i + q_i$$

$$- : \text{Poly} \times \text{Poly} \rightarrow \text{Poly}$$

$$(p - q)_i := p_i - q_i$$

$$- : \text{Poly} \rightarrow \text{Poly}$$

$$(-p)_i := -(p_i)$$

$$* : \text{Poly} \times \text{Poly} \rightarrow \text{Poly}$$

$$(p * q)_i := \sum_{0 \leq j \leq i} p_j * q_{i-j}$$

Examples

$$3_{\text{Poly}} = [3, 0, 0, 0, 0, \dots]$$

$$x = [0, 1, 0, 0, 0, \dots]$$

$$x + 3 = [3, 1, 0, 0, 0, \dots]$$

$$x * x = [0, 0, 1, 0, 0, \dots]$$

$$x * x + 2 * x + 1 = [1, 2, 1, 0, 0, \dots]$$

$$(x + 1) * (x + 2) = [2, 3, 1, 0, 0, \dots]$$

Terms are just convenient notations to describe polynomials and compute with them.

Relationship to Reals

For all real numbers a and b we have

$$a_{\text{Poly}} + b_{\text{Poly}} = (a +_{\mathbb{R}} b)_{\text{Poly}},$$

$$a_{\text{Poly}} - b_{\text{Poly}} = (a -_{\mathbb{R}} b)_{\text{Poly}},$$

$$-a_{\text{Poly}} = (-_{\mathbb{R}} a)_{\text{Poly}},$$

$$a_{\text{Poly}} * b_{\text{Poly}} = (a *_{\mathbb{R}} b)_{\text{Poly}}.$$

A property like $1 + 1 = 2$ also holds for polynomials 1_{Poly} and 2_{Poly} and $+$ interpreted as the polynomial addition.

Polynomial Evaluation

Definition: polynomial evaluation

$$[\] : \text{Poly} \times \mathbb{R} \rightarrow \mathbb{R}$$
$$p[a] := \sum_{0 \leq i \leq \deg(p)} p_i *_{\mathbb{R}} a^i.$$

Example: $p := 2 + 3 * x + 4 * x * x$:

$$p = [2, 3, 4, 0, 0, 0, 0, \dots]$$
$$p[5] = 2 * 5^0 + 3 * 5^1 + 4 * 5^2 = 117.$$

Polynomial Evaluation

Proposition: For all polynomials p and q and all reals c and a :

$$\begin{aligned} c_{\text{Poly}}[a] &= c, \\ \mathbf{x}[a] &= a, \\ (p + q)[a] &= p[a] +_{\mathbb{R}} q[a], \\ (p * q)[a] &= p[a] *_{\mathbb{R}} q[a]. \end{aligned}$$

When evaluating a polynomial p on a real a , we substitute a_{Poly} for every occurrence of x in p and then use arithmetic on reals.

$$\begin{aligned} (\mathbf{x} + 1)[2] &= 2 + 1 = 3 \\ (\mathbf{x} * \mathbf{x} + 2 * \mathbf{x} + 1)[3] &= 3 * 3 + 2 * 3 + 1 = 16 \end{aligned}$$

Typical Notation

- No fixed “polynomial variable” x .
- Polynomial domains $\mathbb{R}[x]$, $\mathbb{Q}[y]$, $\mathbb{C}[z]$.
 - Coefficient domain \mathbb{R} , \mathbb{Q} , \mathbb{C} .
 - Polynomial variable x , y , z .
 - $\mathbb{Q}[y]$: $y = [0, 1, 0, 0, 0, \dots]$.
- Multivariate polynomials $\mathbb{R}[x, y]$
 - $\mathbb{R}[x, y] = (\mathbb{R}[x])[y]$.
 - Coefficients are themselves polynomials.

Generalization to arbitrary number of variables.

Summary

- Number domains.
 - Construction.
 - Basic operations.
 - Basic laws.
 - Relationship.
- Minimum and Maximum.
- Sum and Product.
- Binomials.
- Matrix operations.
- Polynomials.