More on Functions 1

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

Further Notions

Overview

- Further Notions
- Counting Set Elements
- Embedding Sets

Image

Definition: Let $f : A \to B$, $A' \subseteq A$. The image of A' at f is the set of all values to which elements of A' are mapped by f:

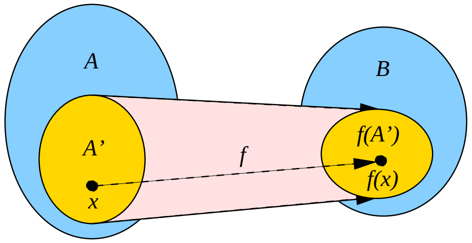
$$f(A') := \textbf{if } A' \subseteq \mathrm{domain}(f) \textbf{ then } \{f(x) : x \in A'\}.$$

The inverse image of B' at f is the set of all elements that are mapped to some elements of B' by f:

$$f^{-1}(B') := \{x \in \mathrm{domain}(f) : f(x) \in B'\}.$$

Function applied to set of arguments.

Image



$f^{-1}(f(A')) = A'$

Function Properties

Definition: Let f: $A \to B$. f is injective (one-to-one) if it does not map different arguments to the same result:

$$f : A \overset{\text{injective}}{\longrightarrow} B :\Leftrightarrow$$
$$f : A \to B \wedge (\forall x_0 \in A, x_1 \in A : f(x_0) = f(x_1) \Rightarrow x_0 = x_1).$$

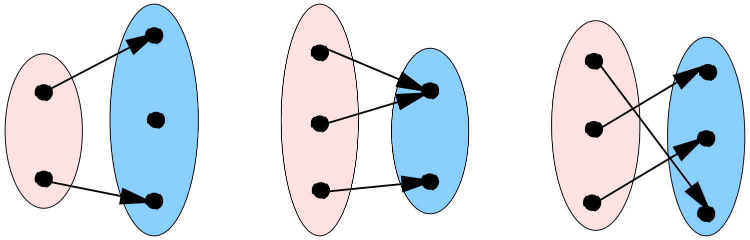
f is surjective (onto) if every element of B is hit by some argument:

$$f : A \overset{\text{surjective}}{\longrightarrow} B :\Leftrightarrow f : A \to B \wedge (\forall y \in B : \exists x \in A : f(x) = y).$$

f is bijective if it is injective and surjective:

$$f : A \overset{\text{bijective}}{\longrightarrow} B :\Leftrightarrow f : A \overset{\text{injective}}{\longrightarrow} B \wedge f : A \overset{\text{surjective}}{\longrightarrow} B.$$

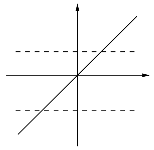
Illustration



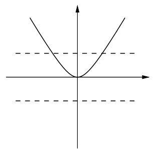
injective (not surjective) | surjective (not injective) | bijective

Example

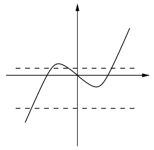
- The identity function $f(x) := x$ is bijective:



- The square function $f(x) := x^2$ is neither injective nor surjective:



- The function $f(x) := x^3 - x$ is surjective but not injective:



Function Composition

Proposition: The composition of two bijective functions is bijective:

$$\forall A, B, C, f : A \xrightarrow{\text{bijective}} B, g : B \xrightarrow{\text{bijective}} C :$$
$$f \circ g : A \xrightarrow{\text{bijective}} C.$$

Proof: Take arbitrary $f : A \xrightarrow{\text{bijective}} B, g : B \xrightarrow{\text{bijective}} C$.

- We show $f \circ g$ is injective. Take arbitrary $x_0 \in A$ and $x_1 \in A$ with $(f \circ g)(x_0) = (f \circ g)(x_1)$. We have to show $x_0 = x_1$.

  We know, by definition of $\circ$, that $g(f(x_0)) = g(f(x_1))$ and thus, because g is injective, $f(x_0) = f(x_1)$. Since f is injective, we then have $x_0 = x_1$.
- We show $f \circ g$ is surjective. Take arbitrary $z \in C$; we have to find some x such that $(f \circ g)(x) = z$. Since g is surjective, we have some $y \in B$ such that $g(y) = z$. Since f is surjective, we have some $x \in A$ such that $f(x) = y$. Thus $(f \circ g)(x) = g(f(x)) = g(y) = z$.

Function Inversion

Proposition: If a function is injective, its inverse is also a function:

$$\forall A, B, f : A \xrightarrow{\text{injective}} B : : f^{-1} : B \to A.$$

Proof: Take arbitrary $f : A \xrightarrow{\text{injective}} B$. We have to show $f^{-1} : B \to A$.
We have $f^{-1} \subseteq B \times A$. Thus it remains to be shown

$$(\forall x, y_0, y_1 : (\langle x, y_0 \rangle \in f^{-1} \wedge \langle x, y_1 \rangle \in f^{-1}) \Rightarrow y_0 = y_1).$$

Take arbitrary x, y_0, and y_1 and assume

$$(1)\ \langle x, y_0 \rangle \in f^{-1} \wedge \langle x, y_1 \rangle \in f^{-1}.$$

We have to show (2) $y_0 = y_1$. From (1) and the definition of inverse, we know

$$(3)\ \langle y_0, x \rangle \in f\ \wedge \langle y_1, x \rangle \in f,$$

i.e., $f(y_0) = x$ and $f(y_1) = x$. Since f is injective, we thus know (2).

Inverse Function Properties

$$1_A : A \to A, 1_A(x) := x$$

Proposition: For every $A, B, f : A \to B$, we have

$$f \circ 1_B = f$$
$$1_A \circ f = f.$$

If f is injective, then we have

$$f \circ f^{-1} = 1_A$$

If f is also surjective (i.e., bijective), then we have

$$f^{-1} \circ f = 1_B.$$

Counting Set Elements

Number of Set Elements

Definition: A set S is finite if it is empty or there is a bijection to $\mathbb{N}_n$ for some $n > 0$. We then call 0 resp. n the size or cardinality of S:

$$S \text{ is finite} :\Leftrightarrow S = \emptyset \lor$$
$$(\exists n \in \mathbb{N}_{>0}, f : f : \mathbb{N}_n \overset{\text{bijective}}{\longrightarrow} S);$$

$$|S| := \textbf{if } S = \emptyset \textbf{ then } 0 \textbf{ else}$$
$$(\textbf{such } n \in \mathbb{N}_{>0} : \exists f : f : \mathbb{N}_n \overset{\text{bijective}}{\longrightarrow} S).$$

A set is infinite if is not finite:

$$S \text{ is infinite } :\Leftrightarrow \neg S \text{ is finite.}$$

Unicity of Bijection

Proposition: If S is not empty and both $f : \mathbb{N}_n \to S$ and $g : \mathbb{N}_m \to S$ are bijections, then $n = m$:

$$(\forall S \neq \emptyset, n \in \mathbb{N}, m \in \mathbb{N}, f : \mathbb{N}_n \overset{\text{bijective}}{\longrightarrow} S, g : \mathbb{N}_m \overset{\text{bijective}}{\longrightarrow} S : m = n).$$

Proof: see lecture notes.

The size of a set is uniquely defined.

Example

- The set $S := \{0, 2, 4\}$ is finite; its size is 3 because we can define a function $f : \mathbb{N}_3 \overset{\text{bijective}}{\longrightarrow} S$ as

$$f(0) := 0$$
$$f(1) := 2$$
$$f(2) := 4$$

  i.e., $f = [0, 2, 4]$. The length of f is the same as the length of $[0, 4, 2]$, $[4, 2, 0]$ or of any other bijection to S.
- The set $\mathbb{N}$ is infinite. If it were finite, we had some $n \in \mathbb{N}$ and some $f : \mathbb{N}_n \overset{\text{bijective}}{\longrightarrow} \mathbb{N}$. Take $k := 1 + \max\{f(i) : i \in \mathbb{N}_n\}$. Then $k \in \mathbb{N}$ but $\forall i \in \mathbb{N}_n : f(i) \neq k$, i.e., f is not surjective on $\mathbb{N}$.

Number Quantifier

Definition: For every variable x and formula F, the phrase

$$\#x : F$$

is a term where x is bound and whose value equals

$$|\{x : F\}|.$$

The term value is only well defined if the base formula is true for a finite number of assignments for the bound variable.

Set Sizes

Proposition: If A and B are disjoint with sizes m and n, respectively, then the size of their union is $m + n$:

$$\begin{aligned}&\forall A, B, m \in \mathbb{N}, n \in \mathbb{N} :\\&\quad (A \cap B = \emptyset \wedge |A| = m \wedge |B| = n) \Rightarrow |A \cup B| = m + n.\end{aligned}$$

The size of the Cartesian product of two sets is the product of their sizes:

$$\begin{aligned}&\forall A, B, m \in \mathbb{N}, n \in \mathbb{N} :\\&\quad (|A| = m \wedge |B| = n) \Rightarrow |A \times B| = m * n.\end{aligned}$$

Set Sizes (Continued)

Proposition: If A and B have size m and n, respectively, then the size of the set of functions from A to B is n^m:

$$\begin{aligned}&\forall A, B, m \in \mathbb{N}, n \in \mathbb{N} :\\&\quad (|A| = m \wedge |B| = n) \Rightarrow |A \to B| = n^m.\end{aligned}$$

If A is of size n, then A has 2^n subsets:

$$\begin{aligned}&\forall A, n \in \mathbb{N} :\\&\quad |A| = n \Rightarrow |\mathbb{P}(A)| = 2^n.\end{aligned}$$

Countable Sets

Definition: A set is countable if it has an enumeration, i.e., a bijective mapping from $\mathbb{N}$:

$$S \text{ is countable } :\Leftrightarrow \exists f : f : \mathbb{N} \overset{\text{bijective}}{\longrightarrow} S.$$

A criterium to distinguish "degrees of infinity".

Example

$\mathbb{Z}$ is infinite but it is countable because we can define

$$\begin{aligned}&f : \mathbb{N} \overset{\text{bijective}}{\longrightarrow} \mathbb{Z}\\&f(x) := \textbf{if } x \text{ is even } \textbf{then } -x/2 \textbf{ else } (x+1)/2\end{aligned}$$

i.e.,

$$f = [0, 1, -1, 2, -2, 3, -3, \ldots].$$

While $\mathbb{Z}$ is infinite, we can enumerate all its elements.

Example

The set $\mathbb{Q}$ is infinite but countable: we can list all positive rationals in an infinite matrix that holds at position $\langle i, j \rangle$ the rational $\frac{i+1}{j+1}$:

$$
\begin{array}{ccccccccc}
\frac{1}{1} & & \frac{1}{2} & & \frac{1}{3} & & \frac{1}{4} & & \ldots \\
& \swarrow & & \swarrow & & \swarrow & & & \\
\frac{2}{1} & & \frac{2}{2} & & \frac{2}{3} & & \ldots & & \ldots \\
& \swarrow & & \swarrow & & & & & \\
\frac{3}{1} & & \frac{3}{2} & & \ldots & & \ldots & & \ldots \\
& \swarrow & & & & & & & \\
\frac{4}{1} & & \ldots & & \ldots & & \ldots & & \ldots \\
& & & & & & & & \\
\ldots & & \ldots & & \ldots & & \ldots & & \ldots
\end{array}
$$

We can enumerate all elements in this matrix in a sequence f.

Example (Continued)

From f, we remove all "doubles" constructing a sequence $f' : \mathbb{N} \rightarrow \mathbb{Q}$ that contains each positive rational number in exactly one position. Finally we can define an enumeration of all rationals

$$
\begin{array}{l}
g : \mathbb{N} \xrightarrow{\text{bijective}} \mathbb{Q} \\
g(x) := \\
\quad \textbf{if } x = 0 \textbf{ then } 0 \\
\quad \textbf{else if } x \text{ is even} \\
\qquad \textbf{then } -f'(x/2) \\
\qquad \textbf{else } f'((x-1)/2)
\end{array}
$$

$$g = [0, 1, -1, \frac{1}{2}, -\frac{1}{2}, \frac{2}{1}, -\frac{2}{1}, \frac{1}{3}, -\frac{1}{3}, \frac{3}{1}, -\frac{3}{1}, \ldots].$$

Example

The set of all infinite sequences over $\{0, 1\}$ is not countable.

If it were, we had an $f : \mathbb{N} \xrightarrow{\text{bijective}} (\mathbb{N} \rightarrow \{0, 1\})$. Let $s : \mathbb{N} \rightarrow \{0, 1\}$

$$s(i) := \overline{f(i)_i}$$

where $\overline{d} := 1 - d$. Then s differs from $f(i)$ in the i-th digit (for every $i \in \mathbb{N}$), thus s is not contained in f.

$$
\begin{array}{rlllll}
f(0) = & [\boldsymbol{f(0)_0} & f(0)_1 & f(0)_2 & f(0)_3 & \ldots] \\
f(1) = & [f(1)_0 & \boldsymbol{f(1)_1} & f(1)_2 & f(1)_3 & \ldots] \\
f(2) = & [f(2)_0 & f(2)_1 & \boldsymbol{f(2)_2} & f(2)_3 & \ldots] \\
f(3) = & [f(3)_0 & f(3)_1 & f(3)_2 & \boldsymbol{f(3)_3} & \ldots] \\
& \ldots & \ldots & \ldots & \ldots & \ldots \\
s := & [\overline{f(0)_0}, & \overline{f(1)_1} & \overline{f(2)_2} & \overline{f(3)_3}, & \ldots]
\end{array}
$$

Example

The set $\mathbb{R}$ is not countable.
Every infinite sequence d of decimal digits represents a real number

$$0.d_0 d_1 d_2 \ldots.$$

Since the set of all infinite sequences is not countable (and every real number is represented by a countable set of such sequences), also $\mathbb{R}$ is not countable.

Not all number domains are countable.

Set Cardinalities

Proposition: Two sets have same size, if there is a bijection between:

$$A \text{ and } B \text{ are of same size } :\Leftrightarrow \exists f : f : A \xrightarrow{\text{bijective}} B.$$

One set is not larger than another set, if there exists an injection from the first set into the second set:

$$A \text{ is not larger than } B :\Leftrightarrow \exists f : f : A \xrightarrow{\text{injective}} B.$$

One set is smaller than another set, if they are not of same size and the second one is not larger than the first one.

$$\begin{aligned}&A \text{ is smaller than } B :\Leftrightarrow \\ &\quad (A \text{ is not larger than } B) \wedge \neg(A \text{ and } B \text{ have same size}).\end{aligned}$$

Finite Sets

Proposition: For all finite sets A and B, the following holds:

$$\begin{aligned}|A| = |B| &\Leftrightarrow A \text{ and } B \text{ have same size;}\\ |A| \leq |B| &\Leftrightarrow A \text{ is not larger than } B;\\ |A| < |B| &\Leftrightarrow A \text{ is smaller than } B.\end{aligned}$$

For finite sets, the new notions coincide with the old ones.

Infinite Sets

We can now also compare the size of infinite sets:

- $\mathbb{N}$ has the same size as $\mathbb{Z}$.
- $\mathbb{Z}$ has the same size as $\mathbb{Q}$.
- $\mathbb{Q}$ is smaller than $\mathbb{R}$.
- $\mathbb{R}$ has the same size as $\mathbb{C}$.

The first results were just shown above.

Size of Powersets

Proposition: Every set is smaller than its powerset:

$$\forall S : S \text{ is smaller than } \mathbb{P}(S).$$

Proof: Take arbitrary S. S is not larger than $\mathbb{P}(S)$ because we can define

$$\begin{aligned}&f : S \xrightarrow{\text{injective}} \mathbb{P}(S)\\ &f(x) := \{x\}.\end{aligned}$$

Assume that S and $\mathbb{P}(S)$ are of the same size, i.e., there exists some $f : S \xrightarrow{\text{bijective}} \mathbb{P}(S)$. We show a contradiction.

Take $A := \{x \in S : x \notin f(x)\}$. Since f is surjective and $A \subseteq S$, i.e., $A \in \mathbb{P}(S)$, we have some $a \in S$ with $f(a) = A$. But then we know $a \in A \Leftrightarrow a \notin f(a) \Leftrightarrow a \notin A$.

Permutations

Definition: A permutation of length n is a bijection from $\mathbb{N}_n$ to $\mathbb{N}_n$:

$$p \text{ is permutation of length } n :\Leftrightarrow p : \mathbb{N}_n \xrightarrow{\text{bijective}} \mathbb{N}_n.$$

Example: Take the sequence $s = [a, b, c, d, e]$ and the permutation $p = [1, 0, 4, 3, 2]$. Then we have

$$p \circ s = [b, a, e, d, c].$$

Further results: see lecture notes.

Example: Sorting Problem

- **Input**:
  - $n \in \mathbb{N}$ . . . the length of the sequence,
  - $s : \mathbb{N}_n \to \mathbb{R}$ . . . a sequence of length n on $\mathbb{R}$.
- **Output**: $t : \mathbb{N}_n \to \mathbb{R}$ such that
  - t is permutation of s,
  - t is sorted with respect to $\leq$.

$$\begin{array}{l} t \text{ is permutation of } s :\Leftrightarrow \\ \quad \textbf{let } n = \text{length}(t) : \\ \qquad n = \text{length}(s) \wedge \\ \qquad \exists p : p \text{ is permutation of length } n \wedge p \circ s = t; \end{array}$$

$$\begin{array}{l} t \text{ is sorted with respect to } \leq :\Leftrightarrow \\ \quad \forall 0 \leq i < \text{length}(t) - 1 : t_i \leq t_{i+1}. \end{array}$$

Embedding Sets

Homomorphism

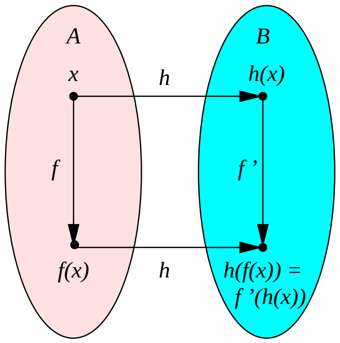
Definition: Let $f : A^n \to A$ and $f' : B^n \to B$. We call h a homomorphism from A to B (with respect to f and f') if we have:

$$\begin{array}{l} h : A \xrightarrow{\text{hom}(f,f')} B :\Leftrightarrow \\ \quad h : A \to B \wedge \\ \quad (\exists n \in \mathbb{N} : \\ \qquad f : A^n \to A \wedge f' : B^n \to B \wedge \\ \qquad (\forall x \in A^n : h(f(x_0, \ldots, x_{n-1})) = f'(h(x_0), \ldots, h(x_{n-1})))). \end{array}$$

An isomorphism is a bijective homomorphism.

$$h : A \xrightarrow{\text{iso}(f,f')} B :\Leftrightarrow h : A \xrightarrow{\text{hom}(f,f')} B \wedge h : A \xrightarrow{\text{bijective}} B.$$

Illustration



We may compute with f in A or with f' in B.

Example

Take $h : \mathbb{N} \to \mathbb{Z}$ defined as

$$h(x) := \langle x, 0 \rangle.$$

Then we have, for all $x \in \mathbb{N}$ and $y \in \mathbb{N}$,

$$\begin{aligned} h(x +_{\mathbb{N}} y) &= h(x) +_{\mathbb{Z}} h(y); \\ h(x *_{\mathbb{N}} y) &= h(x) *_{\mathbb{Z}} h(y) \end{aligned}$$

i.e., h is a homomorphism from $\mathbb{N}$ to $\mathbb{Z}$ (for the operations $+$ and $*$).

Example

Take $h : \mathbb{Z} \to \mathbb{Q}$ defined as

$$h(x) := \frac{x}{1_{\mathbb{Z}}}.$$

Then we have, for all $x \in \mathbb{Z}$ and $y \in \mathbb{Z}$,

$$\begin{aligned} h(x +_{\mathbb{Z}} y) &= h(x) +_{\mathbb{Q}} h(y); \\ h(x -_{\mathbb{Z}} y) &= h(x) -_{\mathbb{Q}} h(y); \\ h(x *_{\mathbb{Z}} y) &= h(x) *_{\mathbb{Q}} h(y) \end{aligned}$$

i.e., h is a homomorphism from $\mathbb{Z}$ to $\mathbb{Q}$ (for operations $+$, $-$, $*$).

Example

Take the domain "List(T)" with functions "length" and "append".

We have for all $x \in \text{List}(T)$ and $y \in \text{List}(T)$

$$\text{length}(\text{append}(x, y)) = \text{length}(x) + \text{length}(y)$$

i.e., "length" is a homomorphism from "List(T)" to $\mathbb{N}$ with respect to "append" and $+$.

Example

Take the set of polynomials Poly.

We have, for all polynomials x and y and $a \in \mathbb{R}$,

$$\begin{aligned}(x+y)[a] &= x[a] +_{\mathbb{R}} y[a] \\ (x-y)[a] &= x[a] -_{\mathbb{R}} y[a] \\ (-x)[a] &= -_{\mathbb{R}} x[a] \\ (x*y)[a] &= x[a] *_{\mathbb{R}} y[a]\end{aligned}$$

i.e., polynomial evaluation is a homomorphism from Poly to $\mathbb{R}$ (for operations $+$, $-$, $*$).

Example

$$\mathbb{N} \subseteq' \mathbb{Z} \subseteq' \mathbb{Q} \subseteq' \mathbb{R} \subseteq' \mathbb{C}$$

where

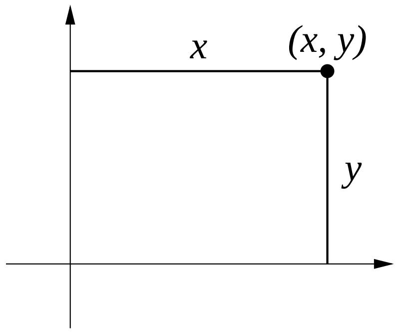
$$A \subseteq' B :\Leftrightarrow \exists h, B' \subseteq B : h : A \overset{\mathrm{iso}(O_A, O'_B)}{\longrightarrow} B'.$$

and O_A denotes the considered operations on A, O'_B denotes the corresponding operations on B' and $h : A \overset{\mathrm{iso}(O_A, O'_B)}{\longrightarrow} B'$ states that h is an isomorphism between A and B for each operation pair.

Every number domain is isomorphic to some subset of its "successor".

Complex Numbers

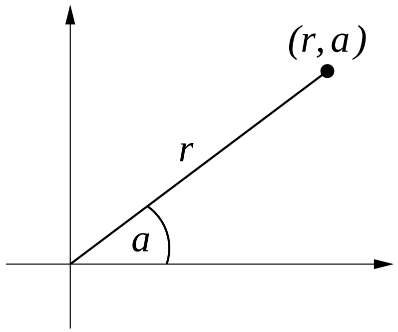
Cartesian Coordinates:



Complex number $x + y\mathrm{i}$ represented by point with coordinates $\langle x, y\rangle$.

Complex Numbers

Polar Coordinates:



Complex number $x + y\mathrm{i}$ represented by point with coordinates $\langle r, \alpha\rangle$.

Polar Representation of Complex Numbers

Definition:

$$\mathbb{C}' := (\mathbb{R}_{>0} \times [0, 2\pi[) \cup \{\langle 0, 3\pi/2 \rangle\}$$

- Angles expressed in "radians" (i.e., $\pi = 180^\circ$).
- Zero point is assigned unique (but arbitrary) angle $3\pi/2$.

$$\begin{array}{l} \text{cartesian} : \mathbb{C}' \to \mathbb{C} \\ \text{cartesian}(z) = z_0 * \cos(z_1) + z_0 * \sin(z_1)\text{i}. \end{array}$$

Translation from new domain into original domain.

Translation

$$\begin{array}{l} \text{polar} : \mathbb{C} \to \mathbb{C}' \\ \text{polar}(z) = (\sqrt{z_0^2 + z_1^2}, \alpha) \\ \quad \textbf{where } \alpha = \\ \quad\quad \textbf{if } z_0 = 0 \textbf{ then} \\ \quad\quad\quad \textbf{if } z_1 > 0 \textbf{ then } \pi/2 \textbf{ else } 3\pi/2 \\ \quad\quad \textbf{else} \\ \quad\quad\quad \textbf{let } a = \arctan(z_1/z_0) : \\ \quad\quad\quad \text{shift}(\textbf{if } z_0 \geq 0 \textbf{ then } a \textbf{ else } \pi - a) \end{array}$$

$$\begin{array}{l} \text{shift} : \mathbb{R} \to [0, 2\pi[\\ \text{shift}(a) := (\textbf{such } b : b \in [0, 2\pi[\wedge \exists i \in \mathbb{Z} : a - b = 2\pi i) \end{array}$$

Translation from original domain into new domain.

Relationship

Proposition: cartesian and polar are bijections.

$$\begin{array}{l} \text{cartesian} \circ \text{polar} = 1_{\mathbb{C}}, \\ \text{polar} \circ \text{cartesian} = 1_{\mathbb{C}'} \end{array}$$

Definition:

$$x *_{\mathbb{C}'} y := \langle x_0 * y_0, \text{shift}(x_1 + y_1) \rangle$$

Proposition: $\mathbb{C}$ and $\mathbb{C}'$ are isomorphic with respect to multiplication.

$$\begin{array}{l} \text{polar} : \mathbb{C} \xrightarrow{\text{iso}(*_{\mathbb{C}}, *_{\mathbb{C}'})} \mathbb{C}' \\ \text{cartesian} : \mathbb{C}' \xrightarrow{\text{iso}(*_{\mathbb{C}'}, *_{\mathbb{C}})} \mathbb{C} \end{array}$$

Proof

$$\forall x \in \mathbb{C}', y \in \mathbb{C}' : \text{cartesian}(x *_{\mathbb{C}'} y) = \text{cartesian}(x) *_{\mathbb{C}} \text{cartesian}(y).$$

Take arbitrary $x \in \mathbb{C}'$ and $y \in \mathbb{C}'$. We then have

$$\begin{aligned} \text{cartesian}(x *_{\mathbb{C}'} y) &= \\ \text{cartesian}(x_0 y_0, \text{shift}(x_1 + y_1)) &= \\ x_0 y_0 \cos(\text{shift}(x_1 + y_1)) + (x_0 y_0 \sin(\text{shift}(x_1 + y_1)))\text{i} &= (*) \\ x_0 y_0 \cos(x_1 + y_1) + (x_0 y_0 \sin(x_1 + y_1))\text{i}. & \end{aligned}$$

(*) holds because of the definition "shift" and for every $x \in \mathbb{R}$,

$$\begin{aligned} \sin(x + 2\pi) &= \sin(x), \\ \cos(x + 2\pi) &= \cos(x) \end{aligned}$$

Proof (Continued)

We also have

$$\begin{aligned}
\text{cartesian}(x) *_{\mathbb{C}} \text{cartesian}(y) &= \\
(x_0\cos(x_1) + x_0\sin(x_1)\mathrm{i}) *_{\mathbb{C}} (y_0\cos(y_1) + y_0\sin(y_1)\mathrm{i}) &= \\
(x_0y_0\cos(x_1)\cos(y_1) - x_0y_0\sin(x_1)\sin(y_1)) + \\
(x_0y_0\cos(x_1)\sin(y_1) + x_0y_0\sin(x_1)\cos(y_1))\mathrm{i} &= \\
x_0y_0(\cos(x_1)\cos(y_1) - \sin(x_1)\sin(y_1)) + \\
x_0y_0(\cos(x_1)\sin(y_1) + x_0y_0\sin(x_1)\cos(y_1))\mathrm{i}
\end{aligned}$$

We assume the knowledge

$$\begin{aligned}
\cos(x_1 + y_1) &= \cos(x_1)\cos(y_1) - \sin(x_1)\sin(y_1) \\
\sin(x_1 + y_1) &= \cos(x_1)\sin(y_1) + \sin(x_1)\cos(y_1)
\end{aligned}$$

as granted and are therefore done.

Complex Root

Definition:

$$\begin{aligned}
&\sqrt{\ } : (\mathbb{N} \times \mathbb{C}') \to \mathbb{C}' \\
&\sqrt[n]{z} := \langle \sqrt[n]{z_0}, z_1/n \rangle.
\end{aligned}$$

Proposition: For every $n \in \mathbb{N}_{>0}$ and $z \in \mathbb{C}'$, the n-th roots of z are $\sqrt[n]{z}$ and the n-1 values that have the same distance from the origin and their angle shifted by multiples of $2\pi/n$:

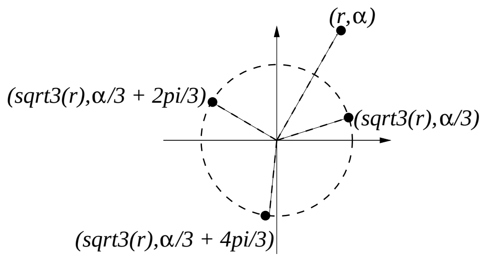
$$\begin{aligned}
&\forall n \in \mathbb{N}_{>0}, z \in \mathbb{C}' : \\
&\quad \textbf{let } r = \sqrt[n]{z} : \\
&\quad (\forall s \in \mathbb{C}' : z = s^n \Leftrightarrow \exists i \in \mathbb{N} : s = \langle r_0, \text{shift}(r_1 + 2\pi i/n)\rangle).
\end{aligned}$$

Relationship

- $\mathbb{C}$ and $\mathbb{C}'$ are isomorphic.
  - $+, *, -, /$.
- Application for computing.
  - Operate in one domain.
  - Translate results into other domain.

An operation is typically easier to compute in one of the domains.

Illustration



All roots are on same circle and have equal distance.

Translation

Definition:

$$\sqrt{\ } : (\mathbb{N}_{>0} \times \mathbb{C}) \to \mathbb{C}$$
$$\sqrt[n]{z} := \text{cartesian}(\sqrt[n]{\text{polar}(z)}).$$

$$+_{\mathbb{C}'} : (\mathbb{C}' \times \mathbb{C}') \to \mathbb{C}'$$
$$x +_{\mathbb{C}'} y := \text{polar}(\text{cartesian}(x) +_{\mathbb{C}} \text{cartesian}(y));$$
$$-_{\mathbb{C}'} : (\mathbb{C}' \times \mathbb{C}') \to \mathbb{C}'$$
$$x -_{\mathbb{C}'} y := \text{polar}(\text{cartesian}(x) +_{\mathbb{C}} \text{cartesian}(y)).$$

Compute $\sqrt{\ }$ in $\mathbb{C}$', but $+$ and $-$ in $\mathbb{C}$.

Summary

- Function notions:
  - Image, injective, surjective, bijective.
  - Properties.
- Counting set elements:
  - Size of a finite set.
  - Countable sets, enumerations.
  - Comparing infinite sets.
  - Permutations.
- Embedding sets:
  - Homomorphisms, isomorphisms.
  - Examples, application for computing.