Objecs of categories as complex numbers

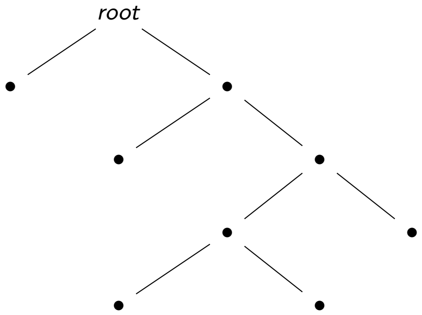
Tjitske Koster

Radboud University Nijmegen

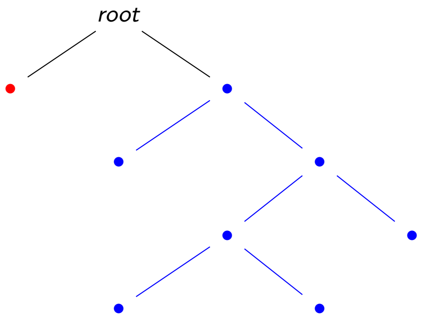
January 2023

Outline

Trees



Trees



We say that the tree over here is $[t_1, t_2]$. Where t_1 is the left subtree, and t_2 is the right subtree, attached at the root.

Bijection between trees

Lawvrere

We have a **very specific** bijection between one tree T, and a seven tuple tree T^7.

Very specific/explicit

By a very specific bijection we mean a bijection that can be calculated in “constant time". I.e. the time is independent of the trees we have.

Bijection between trees

Lawvrere

We have a **very specific** bijection between one tree T, and a seven tuple tree T^7.

First prove

Let $t = (t_1, ..., t_7)$ be a tuple of seven trees, with at least one of trees 1,2,3,4 is non empty. Tree:

$$[[[[[[t_7, t_6]t_5]t_4]t_3]t_2]t_1]$$

If 1 upto 4 are empty then ... See Reference [4].

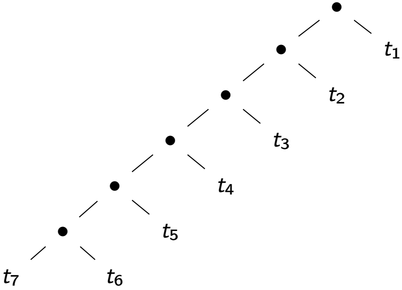
Bijection between trees

First prove

Let $t = (t_1, \ldots, t_7)$ be a tuple of seven trees, with at least one of trees 1,2,3,4 is non empty. Tree:

$$[[[[[[t_7, t_6]t_5]t_4]t_3]t_2]t_1]$$

If 1 upto 4 are empty then ... See Reference [4].



Another way of proving

One tree to two

We have a very explicit injection from one tree to a tuple of two trees.

$$T \to T^2$$

Proof.

We send tree t to the trees $(t, 0)$. □

Note

This is not a bijection and moreover there doesn't exists an explicit bijection.

Another way of proving

One tree to two

We have a very explicit injection from one tree to a tuple of two trees.

$$T \to T^2$$

Proof.

We send tree t to the trees $(t, 0)$. □

Note

This is not a bijection and moreover there doesn't exists an explicit bijection.

$T \cong 1 + T^2$

However, we can define a very explicit bijection from T to $1 + T^2$ by attaching two trees with a root, or taking the empty tree.

From $T \cong 1 + T^2$ to $T^7 \cong T$

Complex numbers

Now we assume T is a complex number and we solve $T = 1 + T^2$ implying $T = e^{\frac{i\pi}{3}}$.

From $T \cong 1 + T^2$ to $T^7 \cong T$

Complex numbers

Now we assume T is a complex number and we solve $T = 1 + T^2$ implying $T = e^{\frac{i\pi}{3}}$.
Then $T^6 = 1$ but that is not an equivalence of trees...

From $T \cong 1 + T^2$ to $T^7 \cong T$

Complex numbers

Now we assume T is a complex number and we solve $T = 1 + T^2$ implying $T = e^{\frac{i\pi}{3}}$.
Then $T^6 = 1$ but that is not an equivalence of trees...
However, we do have $T^7 = T$ as we have seen before

Proving with nuclear penny's

Let us prove the equivalence one more time, but now with a game.
First legal move:

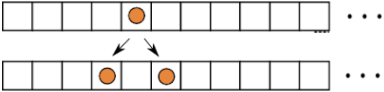


Figure: Fission

Proving with nuclear penny's

Let us prove the equivalence one more time, but now with a game.
First legal move:

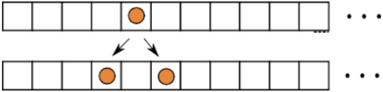


Figure: Fission

Second legal move:

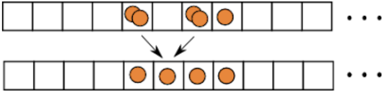


Figure: Fusion

See the blog by Sigfpe, Reference [1]

Question of nuclear penny's

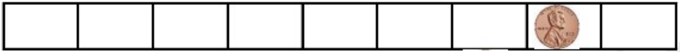
If this is the starting position:

Figure: Start

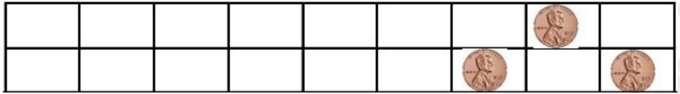
Can we reach this target position?

Figure: Target

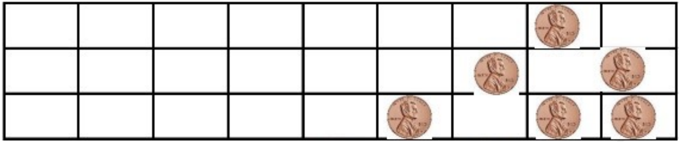
Nuclear penny's game answer



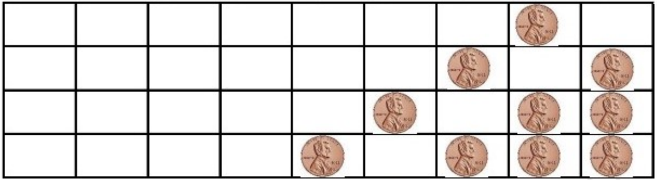
Nuclear penny's game answer



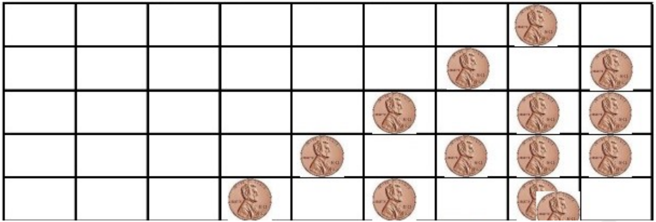
Nuclear penny's game answer



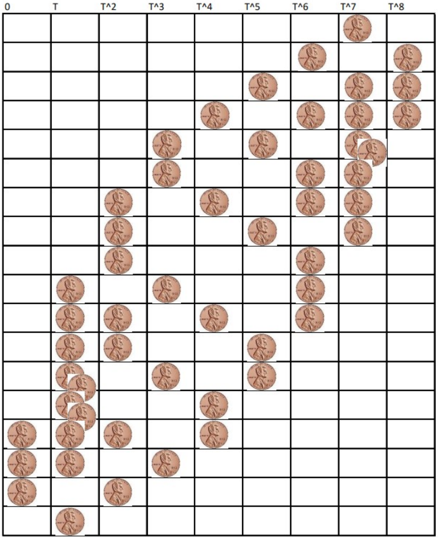
Nuclear penny's game answer



Nuclear penny's game answer



Nuclear penny's game answer



Outline

Goal

Recall

The fastest proof was to solve $T = 1 + T^2$ for complex numbers to find $T = T^7$.

Question

Can we use the complex numbers for more problems?

Goal

Recall

The fastest proof was to solve $T = 1 + T^2$ for complex numbers to find $T = T^7$.

Question

Can we use the complex numbers for more problems?

Our main result is approximately

Let p, q_1 and q_2 be polynomials over $\mathbb{N}$: If

$$t = p(t) \implies q_1(t) = q_2(t)$$

for all complex numbers t, then

$$T \cong p(T) \implies q_1(T) \cong q_2(T)$$

for all objects T of any category in which it makes sense to add and multiply objects.

The way we are gonna prove

Distributive categories/ Haskell

$\Downarrow$ $\curvearrowleft$ burnside semiring

Semirings

$\Downarrow$ $\curvearrowleft$ catalysts

Ring

Outline

Distributive categories

Distributive category

A category $\mathscr{C}$ with finite products $\times$ and coproducts $\oplus$ is called distributive if, for all $A, B, C \in \mathscr{C}$ the following morphism is an isomorphism

$$k : A \times B \oplus A \times C \to A \times (B \oplus C) \tag{1}$$

In order to get this, we have two underlying morphisms

$$j : A \times B \to A \times (B \oplus C) \tag{2}$$

$$j' : A \times C \to A \times (B \oplus C) \tag{3}$$

Distributive categories

Distributive category

A category $\mathscr{C}$ with finite products $\times$ and coproducts $\oplus$ is called distributive if, for all $A, B, C \in \mathscr{C}$ the following morphism is an isomorphism

$$k : A \times B \oplus A \times C \to A \times (B \oplus C) \tag{1}$$

In order to get this, we have two underlying morphisms

$$j : A \times B \to A \times (B \oplus C) \tag{2}$$
$$j' : A \times C \to A \times (B \oplus C) \tag{3}$$

Haskell

Let us have the objects A, B. We define the following operations:

- $A \times B$ as the Cartesian product or pair (A, B)
- $A \oplus B$ as `Either`$(A\ B)$

Haskell distributive

Lemma

Haskell is a distributive category

Proof.

We need to prove that we have an isomorphism

$$\texttt{Either}((A, B)\ (A, C)) \xrightarrow{\sim} (A, \texttt{Either}(B\ C)) \tag{4}$$

We can prove this, by showing that the two underlying morphisms are bijective.

Haskell distributive

Lemma

Haskell is a distributive category

Proof.

We need to prove that we have an isomorphism

$$\texttt{Either}((A, B)\ (A, C)) \xrightarrow{\sim} (A, \texttt{Either}(B\ C)) \tag{4}$$

We can prove this, by showing that the two underlying morphisms are bijective. We define the underlying morphisms $\texttt{left}[\texttt{Either}(a\ b)] = a$ and $\texttt{right}[\texttt{Either}(a\ b)] = b$

Haskell distributive

Lemma

Haskell is a distributive category

Proof.

We need to prove that we have an isomorphism

$$\texttt{Either}((A, B)\ (A, C)) \xrightarrow{\sim} (A, \texttt{Either}(B\ C)) \tag{4}$$

We can prove this, by showing that the two underlying morphisms are bijective. We define the underlying morphisms $\texttt{left}[\texttt{Either}(a\ b)] = a$ and $\texttt{right}[\texttt{Either}(a\ b)] = b$ such that we have:

$$\texttt{left}[\texttt{Either}((A, B)\ (A, C))] = (A, B) = (A, \texttt{left}[\texttt{Either}(B\ C)])$$
$$\texttt{right}[\texttt{Either}(A, B)\ (A, C)] = (A, C) = (A, \texttt{right}[\texttt{Either}(B\ C)])$$

Note that these maps are bijective which concludes the argument. □

Recall rings

Semiring

A semiring is a set with operations $+$ and $\cdot$, such that for all a, b, c in the set:

- $(a+b)+c = a+(b+c)$ and $a+b = b+a$
- $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
- There are neutral elements 0, 1 st $a+0 = a$ and $a \cdot 1 = a = 1 \cdot a$
- $a \cdot b + a \cdot c = a \cdot (b+c)$

Example: $(\mathbb{N}, +, \cdot)$

Recall rings

Semiring

A semiring is a set with operations $+$ and $\cdot$, such that for all a, b, c in the set:

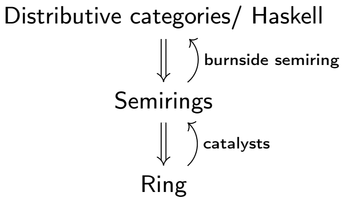
- $(a+b)+c = a+(b+c)$ and $a+b = b+a$
- $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
- There are neutral elements 0, 1 st $a+0=a$ and $a \cdot 1 = a = 1 \cdot a$
- $a \cdot b + a \cdot c = a \cdot (b+c)$

Ring

A ring is a semiring with the additional property that each element has an inverse under $+$, i.e. $a + -a = 0$.

Example: $(\mathbb{Z}, +, \cdot)$

The way we prove



Outline

Burnside semiring

Recall that in a distributive category we have the isomorphism

$$k : A \times B \oplus A \times C \xrightarrow{\sim} A \times (B \oplus C) \tag{5}$$

In semirings we have the equality

$$A \times B \oplus A \times C = A \times (B \oplus C) \tag{6}$$

Burnside semiring

Recall that in a distributive category we have the isomorphism

$$k : A \times B \oplus A \times C \xrightarrow{\sim} A \times (B \oplus C) \tag{5}$$

In semirings we have the equality

$$A \times B \oplus A \times C = A \times (B \oplus C) \tag{6}$$

Burnside semiring

$$\text{Burnside semiring} \;=\; {}^{\text{distributive category}}\big/_{\text{isomorphisms}}$$

Semiring to Haskell

Distributive categories/ Haskell

$\Downarrow$ $\curvearrowleft$ burnside semiring

Semirings

Claim

Given a statement with *equality* in a semiring, we can relate it to a similar statement, but now with *isomorphism* in the distributive category.

Semiring to Haskell

Distributive categories/ Haskell

$\Downarrow$ $\uparrow$ burnside semiring

Semirings

Claim

Given a statement with *equality* in a semiring, we can relate it to a similar statement, but now with *isomorphism* in the distributive category.

Example

$$\forall \text{ semirings } A \text{ and all } a \in A; \text{ if } p_1(a) = p_2(a) \text{ then } q_1(a) = q_2(a)$$

Is equivalent with:

$$\forall \text{ distr. categories } \mathcal{A} \text{ and all } T \in \mathcal{A}; \text{ if } p_1(T) \cong p_2(T) \text{ then } q_1(T) \cong q_2(T).$$

The way we prove

Distributive categories/ Haskell

$\Downarrow$ $\curvearrowleft$ burnside semiring

Semirings

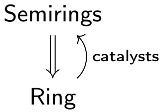
$\Downarrow$ $\curvearrowleft$ catalysts

Ring

Outline

From rings to semirings

Note that the difference between rings and semirings is, that rings have subtraction.



From rings to semirings

Note that the difference between rings and semirings is, that rings have subtraction.

$$\begin{array}{c} \text{Semirings} \\ \Downarrow \quad \curvearrowleft \text{ catalysts} \\ \text{Ring} \end{array}$$

Proposition 7: Catalysts

Let $p_1; p_2; q_1; q_2 \in \mathbb{N}[x]$ and suppose that

$$p_1(x) = p_2(x) \Rightarrow q_1(x) = q_2(x) \text{ ring-theoretically:}$$

Then there exists $s \in \mathbb{N}[x]$ such that

$$p_1(x) = p_2(x) \Rightarrow q_1(x) + s(x) = q_2(x) + s(x) \text{ semiring-theoretically:}$$

Rings

Definition

Let $p_1; p_2; q_1; q_2 \in \mathbb{Z}[x]$: We say that

$$p_1(x) = p_2(x) \Rightarrow q_1(x) = q_2(x) \text{ ring-theoretically:}$$

if the following equivalent conditions hold:

a) For all rings A and all $a \in A$ if $p_1(a) = p_2(a)$ then $q_1(a) = q_2(a)$
b) as a), but restricted to commutative rings
c) q_1 and q_2 represent the same element of the quotient ring $\mathbb{Z}[x]/(p_1 - p_2)$
d) $p_1 - p_2$ divides $q_1 - q_2$ in the ring $\mathbb{Z}[x]$.

Rings

Definition

Let $p_1; p_2; q_1; q_2 \in \mathbb{Z}[x]$: We say that

$$p_1(x) = p_2(x) \Rightarrow q_1(x) = q_2(x) \text{ ring-theoretically:}$$

if the following equivalent conditions hold:

a) For all rings A and all $a \in A$ if $p_1(a) = p_2(a)$ then $q_1(a) = q_2(a)$
b) as a), but restricted to commutative rings
c) q_1 and q_2 represent the same element of the quotient ring $\mathbb{Z}[x]/(p_1 - p_2)$
d) $p_1 - p_2$ divides $q_1 - q_2$ in the ring $\mathbb{Z}[x]$.

Note

We have $q_1 - q_2 = r(p_1 - p_2)$ for $r \in \mathbb{Z}[x]$

Proof Proposition catalysts

Proposition 7: Catalysts

Let $p_1; p_2; q_1; q_2 \in \mathbb{N}[x]$ and suppose that

$$p_1(x) = p_2(x) \Rightarrow q_1(x) = q_2(x) \text{ ring-theoretically:}$$

Then there exists $s \in \mathbb{N}[x]$ such that

$$p_1(x) = p_2(x) \Rightarrow q_1(x) + s(x) = q_2(x) + s(x) \text{ semiring-theoretically:}$$

Proposition 7: Catalysts

Let $p_1; p_2; q_1; q_2 \in \mathbb{N}[x]$ and suppose that $q_1 - q_2 = r(p_1 - p_2)$ for $r \in \mathbb{Z}[x]$.
Then there exists $s \in \mathbb{N}[x]$ such that
$p_1(x) = p_2(x) \Rightarrow q_1(x) + s(x) = q_2(x) + s(x)$ hold semiring-theoretically

Proof Proposition catalysts

Proposition 7: Catalysts

Let $p_1; p_2; q_1; q_2 \in \mathbb{N}[x]$ and suppose that $q_1 - q_2 = r(p_1 - p_2)$ for $r \in \mathbb{Z}[x]$. Then there exists $s \in \mathbb{N}[x]$ such that $p_1(x) = p_2(x) \Rightarrow q_1(x) + s(x) = q_2(x) + s(x)$ hold semiring-theoretically

Proof.

We write $r = r_1 - r_2$ for some $r_1, r_2 \in \mathbb{N}[x]$, so $q_1 - q_2 = (r_1 - r_2)(p_1 - p_2)$ and then

$$q_1 + r_1 p_2 + r_2 p_1 = q_2 + r_1 p_1 + r_2 p_2 \text{ in } \mathbb{N}[x]$$

Proof Proposition catalysts

Proposition 7: Catalysts

Let $p_1; p_2; q_1; q_2 \in \mathbb{N}[x]$ and suppose that $q_1 - q_2 = r(p_1 - p_2)$ for $r \in \mathbb{Z}[x]$. Then there exists $s \in \mathbb{N}[x]$ such that $p_1(x) = p_2(x) \Rightarrow q_1(x) + s(x) = q_2(x) + s(x)$ hold semiring-theoretically

Proof.

We write $r = r_1 - r_2$ for some $r_1, r_2 \in \mathbb{N}[x]$, so $q_1 - q_2 = (r_1 - r_2)(p_1 - p_2)$ and then

$$q_1 + r_1 p_2 + r_2 p_1 = q_2 + r_1 p_1 + r_2 p_2 \text{ in } \mathbb{N}[x]$$

set $s = r_1 p_1 + r_2 p_2$ in $\mathbb{N}[x]$, so $s = r_1 p_1 + r_2 p_1$ in $\mathbb{N}[x]/(p_1 = p_2)$ then:

Proof Proposition catalysts

Proposition 7: Catalysts

Let $p_1; p_2; q_1; q_2 \in \mathbb{N}[x]$ and suppose that $q_1 - q_2 = r(p_1 - p_2)$ for $r \in \mathbb{Z}[x]$. Then there exists $s \in \mathbb{N}[x]$ such that $p_1(x) = p_2(x) \Rightarrow q_1(x) + s(x) = q_2(x) + s(x)$ hold semiring-theoretically

Proof.

We write $r = r_1 - r_2$ for some $r_1, r_2 \in \mathbb{N}[x]$, so $q_1 - q_2 = (r_1 - r_2)(p_1 - p_2)$ and then

$$q_1 + r_1 p_2 + r_2 p_1 = q_2 + r_1 p_1 + r_2 p_2 \text{ in } \mathbb{N}[x]$$

set $s = r_1 p_1 + r_2 p_2$ in $\mathbb{N}[x]$, so $s = r_1 p_1 + r_2 p_1$ in $\mathbb{N}[x]/(p_1 = p_2)$ then:

$$\begin{aligned} q_1 + r_1 p_2 + r_2 p_1 &= q_2 + r_1 p_1 + r_2 p_2 && \text{in } \mathbb{N}[x] \\ q_1 + r_1 p_1 + r_2 p_1 &= q_2 + r_1 p_1 + r_2 p_1 && \text{in } \mathbb{N}[x]/(p_1 = p_2) \\ q_1 + s &= q_2 + s && \text{in } \mathbb{N}[x]/(p_1 = p_2) \end{aligned}$$

Proof Proposition catalysts

Proposition 7: Catalysts

Let $p_1; p_2; q_1; q_2 \in \mathbb{N}[x]$ and suppose that $q_1 - q_2 = r(p_1 - p_2)$ for $r \in \mathbb{Z}[x]$. Then there exists $s \in \mathbb{N}[x]$ such that $p_1(x) = p_2(x) \Rightarrow q_1(x) + s(x) = q_2(x) + s(x)$ hold semiring-theoretically

Proof.

We write $r = r_1 - r_2$ for some $r_1, r_2 \in \mathbb{N}[x]$, so $q_1 - q_2 = (r_1 - r_2)(p_1 - p_2)$ and then

$$q_1 + r_1 p_2 + r_2 p_1 = q_2 + r_1 p_1 + r_2 p_2 \text{ in } \mathbb{N}[x]$$

set $s = r_1 p_1 + r_2 p_2$ in $\mathbb{N}[x]$, so $s = r_1 p_1 + r_2 p_1$ in $\mathbb{N}[x]/(p_1 = p_2)$ then:

$$\begin{aligned} q_1 + r_1 p_2 + r_2 p_1 &= q_2 + r_1 p_1 + r_2 p_2 && \text{in } \mathbb{N}[x] \\ q_1 + r_1 p_1 + r_2 p_1 &= q_2 + r_1 p_1 + r_2 p_1 && \text{in } \mathbb{N}[x]/(p_1 = p_2) \\ q_1 + s &= q_2 + s && \text{in } \mathbb{N}[x]/(p_1 = p_2) \end{aligned}$$

thus $q_1 + s$ and $q_2 + s$ represent the same element of the quotient semiring $\mathbb{N}[x]/(p_1 = p_2)$ as required. □

The way we prove

Distributive categories/ Haskell

$\Downarrow$ $\circlearrowleft$ burnside semiring

Semirings

$\Downarrow$ $\circlearrowleft$ catalysts

Ring

Outline

Goal

Theorem 17

First set of requirements. Second set of requirements. Then

$$x = p(x) \Rightarrow q_1(x) = q_2(x) \text{ semiring-theoretically}$$

Goal

Theorem 17

First set of requirements. Second set of requirements. Then

$$x = p(x) \Rightarrow q_1(x) = q_2(x) \text{ semiring-theoretically}$$

Proposition 2

Set of requirements implies:

$$x = p(x) \Rightarrow q_1(x) = q_2(x) \text{ ring-theoretically}$$

Theorem 16

Set of requirements if:

$$x = p(x) \Rightarrow q_1(x) = q_2(x) \text{ ring-theoretically}$$

then it also holds semring-theoretically.

Proof of Proposition 2

Proposition 2

Let $p, q_1, q_2 \in \mathbb{Z}[x]$ Suppose that the polynomial $p(x) - x \in \mathbb{Z}[x]$ is primitive (the coefficients are co-prime) and has no repeated complex roots, and that each complex root t satisfies $q_1(t) = q_2(t)$: Then

$$x = p(x) \Rightarrow q_1(x) = q_2(x) \text{ ring-theoretically}$$

Proof.

This proof uses the division algorithm and Gauss lemma which can only be done in rings, not semirings. □

Proof of Proposition 2

Proposition 2

Let $p, q_1, q_2 \in \mathbb{Z}[x]$ Suppose that the polynomial $p(x) - x \ \in \mathbb{Z}[x]$ is primitive (the coefficients are co-prime) and has no repeated complex roots, and that each complex root t satisfies $q_1(t) = q_2(t)$: Then

$$x = p(x) \Rightarrow q_1(x) = q_2(x) \text{ ring-theoretically}$$

Example

Take $p(x) = 1 + x^2$ then we have $p(x) - x = 1 - x + x^2$. We see that $(1, -1, 1)$ are co-prime.

Proof of Proposition 2

Proposition 2

Let $p, q_1, q_2 \in \mathbb{Z}[x]$ Suppose that the polynomial $p(x) - x \ \in \mathbb{Z}[x]$ is primitive (the coefficients are co-prime) and has no repeated complex roots, and that each complex root t satisfies $q_1(t) = q_2(t)$: Then

$$x = p(x) \Rightarrow q_1(x) = q_2(x) \text{ ring-theoretically}$$

Example

Take $p(x) = 1 + x^2$ then we have $p(x) - x = 1 - x + x^2$. We see that $(1, -1, 1)$ are co-prime. The two complex roots are $e^{\pm i\pi/3}$

Proof of Proposition 2

Proposition 2

Let $p, q_1, q_2 \in \mathbb{Z}[x]$ Suppose that the polynomial $p(x) - x \in \mathbb{Z}[x]$ is primitive (the coefficients are co-prime) and has no repeated complex roots, and that each complex root t satisfies $q_1(t) = q_2(t)$: Then

$$x = p(x) \Rightarrow q_1(x) = q_2(x) \text{ ring-theoretically}$$

Example

Take $p(x) = 1 + x^2$ then we have $p(x) - x = 1 - x + x^2$. We see that $(1, -1, 1)$ are co-prime. The two complex roots are $e^{\pm i\pi/3}$, for both complex roots we have

$$(e^{\pm i\pi/3})^7 = e^{\pm i\pi/3}$$

Then now it should hold that $x = 1 + x^2 \Rightarrow x^7 = x$,

Proof of Proposition 2

Proposition 2

Let $p, q_1, q_2 \in \mathbb{Z}[x]$ Suppose that the polynomial $p(x) - x \ \in \mathbb{Z}[x]$ is primitive (the coefficients are co-prime) and has no repeated complex roots, and that each complex root t satisfies $q_1(t) = q_2(t)$: Then

$$x = p(x) \Rightarrow q_1(x) = q_2(x) \text{ ring-theoretically}$$

Example

Take $p(x) = 1 + x^2$ then we have $p(x) - x = 1 - x + x^2$. We see that $(1, -1, 1)$ are co-prime. The two complex roots are $e^{\pm i\pi/3}$, for both complex roots we have

$$(e^{\pm i\pi/3})^7 = e^{\pm i\pi/3}$$

Then now it should hold that $x = 1 + x^2 \Rightarrow x^7 = x$,so we should find an $r \in \mathbb{Z}[x]$ such that $x^7 - x = r(1 - x + x^2)$.

Proof of Proposition 2

Proposition 2

Let $p, q_1, q_2 \in \mathbb{Z}[x]$ Suppose that the polynomial $p(x) - x \ \in \mathbb{Z}[x]$ is primitive (the coefficients are co-prime) and has no repeated complex roots, and that each complex root t satisfies $q_1(t) = q_2(t)$: Then

$$x = p(x) \Rightarrow q_1(x) = q_2(x) \text{ ring-theoretically}$$

Example

Take $p(x) = 1 + x^2$ then we have $p(x) - x = 1 - x + x^2$. We see that $(1, -1, 1)$ are co-prime. The two complex roots are $e^{\pm i\pi/3}$, for both complex roots we have

$$(e^{\pm i\pi/3})^7 = e^{\pm i\pi/3}$$

Then now it should hold that $x = 1 + x^2 \Rightarrow x^7 = x$,so we should find an $r \in \mathbb{Z}[x]$ such that $x^7 - x = r(1 - x + x^2)$.Take $r = x^5 + x^4 - x^2 - x$.

$$\begin{aligned} x^7 - x &= (x^5 + x^4 - x^2 - x)(1 - x + x^2) \\ &= x^5 + x^4 - x^2 - x - x^6 - x^5 + x^3 + x^2 + x^7 + -x^6 - x^4 - x^3 \\ &= x^7 - x \end{aligned}$$

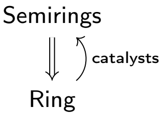
Catalysts

Recall Theorem 16

Let p, q_1, q_2 be polynomials such that p has non-zero constant term and degree at least two, and q_1 and q_2 have degree at least one. If

$$x = p(x) \Rightarrow q_1(x) = q_2(x) \text{ ring-theoretically}$$

then it also holds semiring-theoretically.



Catalysts

Recall Theorem 16

Let p, q_1, q_2 be polynomials such that p has non-zero constant term and degree at least two, and q_1 and q_2 have degree at least one. If

$$x = p(x) \Rightarrow q_1(x) = q_2(x) \text{ ring-theoretically}$$

then it also holds semiring-theoretically.

Recall Proposition 7: Catalysts

Let $p_1; p_2; q_1; q_2 \in \mathbb{N}[x]$ and suppose that

$$p_1(x) = p_2(x) \Rightarrow q_1(x) = q_2(x) \text{ ring-theoretically:}$$

Then there exists $s \in \mathbb{N}[x]$ such that

$$p_1(x) = p_2(x) \Rightarrow q_1(x) + s(x) = q_2(x) + s(x) \text{ semiring-theoretically:}$$

Outline

High elements

Definition

Given a set A with operation $*$, we say $b \leq a$

$$\exists c \in A \text{ such that } b * c = a$$

An element $a \in A$ is called High if **for all** $b \in A$ we have $b \leq a$. The High elements of A are denoted by $\mathrm{H}(A)$.

High elements

Definition

Given a set A with operation $*$, we say $b \leq a$

$$\exists c \in A \text{ such that } b * c = a$$

An element $a \in A$ is called High if **for all** $b \in A$ we have $b \leq a$. The High elements of A are denoted by $\mathrm{H}(A)$.

Properties of High elements

- If a is High and $a \leq b$, then b is high.
- If a is High then for all b we have $a * b$ is high (since $a \leq a * b$).

High elements

Definition

Given a set A with operation $*$, we say $b \leq a$

$$\exists c \in A \text{ such that } b * c = a$$

An element $a \in A$ is called High if **for all** $b \in A$ we have $b \leq a$. The High elements of A are denoted by $\mathrm{H}(A)$.

Properties of High elements

- If a is High and $a \leq b$, then b is high.
- If a is High then for all b we have $a * b$ is high (since $a \leq a * b$).

Example: all elements of $(\mathbb{Z}, +)$ are high, for all a, b there exists a c such that $b + c = a$ (take $c = a - b$).

High elements

Definition

Given a set A with operation $*$, we say $b \leq a$

$$\exists c \in A \text{ such that } b * c = a$$

An element $a \in A$ is called High if **for all** $b \in A$ we have $b \leq a$. The High elements of A are denoted by $\mathrm{H}(A)$.

Properties of High elements

- If a is High and $a \leq b$, then b is high.
- If a is High then for all b we have $a * b$ is high (since $a \leq a * b$).

Example: all elements of $(\mathbb{Z}, +)$ are high, for all a, b there exists a c such that $b + c = a$ (take $c = a - b$).
Non example: $(\mathbb{N}, +)$ has no high element, since for all n we have that for $n + 1$ we cannot find a c such that $n + 1 + c = n$.

Group of High elements

Lemma

The High elements of a commutative semigroup A form a group.

Group of High elements

Lemma

The High elements of a commutative semigroup A form a group.

Proof.

Take $d \in \mathrm{H}(A)$, since it is High $\exists z \in \mathrm{H}(A)$ such that $d * z = d$.

Group of High elements

Lemma

The High elements of a commutative semigroup A form a group.

Proof.

Take $d \in \mathrm{H}(A)$, since it is High $\exists z \in \mathrm{H}(A)$ such that $d * z = d$.
Claim: z is the unit. This is because $\forall b \in \mathrm{H}(A)$ $\exists c$ such that

$$d * c = b$$
$$z * d * c = b$$
$$z * b = b.$$

So we conclude that z is indeed the unit.

Group of High elements

Lemma

The High elements of a commutative semigroup A form a group.

Proof.

Take $d \in \mathrm{H}(A)$, since it is High $\exists z \in \mathrm{H}(A)$ such that $d * z = d$.
Claim: z is the unit. This is because $\forall b \in \mathrm{H}(A)$ $\exists c$ such that

$$d * c = b$$
$$z * d * c = b$$
$$z * b = b.$$

So we conclude that z is indeed the unit.
Also each element has an inverse, since $z \in \mathrm{H}(A)$ and so $\forall b \in \mathrm{H}(A) \exists c$ such that $b * c = z$, we say c is the inverse of b. □

High elements continued

Corollary 11

If a_1, a_2 are High elements of a commutative semi-group $(A, *)$ and if there exists an $b \in A$ such that $a_1 * b = a_2 * b$ then $a_1 = a_2$.

High elements continued

Corollary 11

If a_1, a_2 are High elements of a commutative semi-group $(A, *)$ and if there exists an $b \in A$ such that $a_1 * b = a_2 * b$ then $a_1 = a_2$.

Proof.

Take any High element $\tilde{a}$. Then we write

$$a_1 * b * \tilde{a} = a_2 * b * \tilde{a}$$
$$a_1 * (b * \tilde{a}) = a_2 * (b * \tilde{a})$$

Note that $b * \tilde{a}$ is an High element since $\tilde{a}$ is.

High elements continued

Corollary 11

If a_1, a_2 are High elements of a commutative semi-group $(A, *)$ and if there exists an $b \in A$ such that $a_1 * b = a_2 * b$ then $a_1 = a_2$.

Proof.

Take any High element $\tilde{a}$. Then we write

$$a_1 * b * \tilde{a} = a_2 * b * \tilde{a}$$
$$a_1 * (b * \tilde{a}) = a_2 * (b * \tilde{a})$$

Note that $b * \tilde{a}$ is an High element since $\tilde{a}$ is.
Now since the high elements form a group with inverses, there is an inverse of $b * \tilde{a}$ so we can conclude $a_1 = a_2$. □

High polynomials

Fix a polynomial $p \in (\mathbb{N}[x], \cdot)$ and form the quotient $\mathbb{N}[x]/(x = p(x))$.
We will write $f \leq g$ to say that $f \leq g \in \mathbb{N}[x]/(x = p(x))$

Lemma 13

If p has non-zero constant term then $1 \leq x \leq x^2 \leq \ldots$

High polynomials

Fix a polynomial $p \in (\mathbb{N}[x], \cdot)$ and form the quotient $\mathbb{N}[x]/(x = p(x))$.
We will write $f \leq g$ to say that $f \leq g \in \mathbb{N}[x]/(x = p(x))$

Lemma 13

If p has non-zero constant term then $1 \leq x \leq x^2 \leq \ldots$

Proof.

By assumption $1 \leq p$, so $1 \leq x$,

High polynomials

Fix a polynomial $p \in (\mathbb{N}[x], \cdot)$ and form the quotient $\mathbb{N}[x]/(x = p(x))$.
We will write $f \leq g$ to say that $f \leq g \in \mathbb{N}[x]/(x = p(x))$

Lemma 13

If p has non-zero constant term then $1 \leq x \leq x^2 \leq \ldots$

Proof.

By assumption $1 \leq p$, so $1 \leq x$,then iteratively multiply both sides with x to make the sequence $1 \leq x \leq x^2 \leq \ldots$ □

High polynomials continued

Lemma 14

If p has non-zero constant term and degree ≥ 2 then we have:

- $x \geq nx$
- $x \geq x^n$

High polynomials continued

Lemma 14

If p has non-zero constant term and degree ≥ 2 then we have:

- $x \geq nx$
- $x \geq x^n$

Proof.

We prove by induction. We show only the case $n = 2$, then we can multiply to see it holds for all n.

High polynomials continued

Lemma 14

If p has non-zero constant term and degree ≥ 2 then we have:

- $x \geq nx$
- $x \geq x^n$

Proof.

We prove by induction. We show only the case $n = 2$, then we can multiply to see it holds for all n.
By assumption $p(x) \geq 1 + x^d$, for $d \geq 2$ so $x \geq 1 + x^d$.

$$x \geq x^d$$

For the second bullet, we see $x \geq x^d$ and since $d \geq 2$ we have $x \geq x^2$. □

High polynomials continued

Lemma 14

If p has non-zero constant term and degree ≥ 2 then we have:

- $x \geq nx$
- $x \geq x^n$

Proof.

We prove by induction. We show only the case $n = 2$, then we can multiply to see it holds for all n.
By assumption $p(x) \geq 1 + x^d$, for $d \geq 2$ so $x \geq 1 + x^d$.

$$\begin{aligned} x &\geq x^d \\ &= x^{d-1}x \end{aligned}$$

For the second bullet, we see $x \geq x^d$ and since $d \geq 2$ we have $x \geq x^2$. □

High polynomials continued

Lemma 14

If p has non-zero constant term and degree ≥ 2 then we have:

- $x \geq nx$
- $x \geq x^n$

Proof.

We prove by induction. We show only the case $n = 2$, then we can multiply to see it holds for all n.
By assumption $p(x) \geq 1 + x^d$, for $d \geq 2$ so $x \geq 1 + x^d$.

$$\begin{aligned} x &\geq x^d \\ &= x^{d-1}x \\ &\geq x^{d-1}(1 + x^d) \end{aligned}$$

For the second bullet, we see $x \geq x^d$ and since $d \geq 2$ we have $x \geq x^2$. □

High polynomials continued

Lemma 14

If p has non-zero constant term and degree ≥ 2 then we have:

- $x \geq nx$
- $x \geq x^n$

Proof.

We prove by induction. We show only the case $n = 2$, then we can multiply to see it holds for all n.
By assumption $p(x) \geq 1 + x^d$, for $d \geq 2$ so $x \geq 1 + x^d$.

$$\begin{aligned} x &\geq x^d \\ &= x^{d-1}x \\ &\geq x^{d-1}(1 + x^d) \\ &= x^{d-1} + x^{2d-1} \end{aligned}$$

For the second bullet, we see $x \geq x^d$ and since $d \geq 2$ we have $x \geq x^2$. □

High polynomials continued

Lemma 14

If p has non-zero constant term and degree ≥ 2 then we have:

- $x \geq nx$
- $x \geq x^n$

Proof.

We prove by induction. We show only the case $n = 2$, then we can multiply to see it holds for all n.
By assumption $p(x) \geq 1 + x^d$, for $d \geq 2$ so $x \geq 1 + x^d$.

$$\begin{aligned} x &\geq x^d \\ &= x^{d-1}x \\ &\geq x^{d-1}(1 + x^d) \\ &= x^{d-1} + x^{2d-1} \\ &\geq x + x = 2x \end{aligned}$$

For the second bullet, we see $x \geq x^d$ and since $d \geq 2$ we have $x \geq x^2$. □

High polynomials continued 2

Lemma 13

If p has non-zero constant term then $1 \leq x \leq x^2 \leq \ldots$

Lemma 14

If p has non-zero constant term and degree ≥ 2 then we have:

- $x \geq nx$
- $x \geq x^n$

Proposition 15

If p has non-zero constant term and degree at least two then every nonconstant polynomial is high.

High polynomials continued 2

Lemma 13

If p has non-zero constant term then $1 \leq x \leq x^2 \leq \dots$

Lemma 14

If p has non-zero constant term and degree ≥ 2 then we have:

- $x \geq nx$
- $x \geq x^n$

Proposition 15

If p has non-zero constant term and degree at least two then every nonconstant polynomial is high.

Proof.

By lemma 13 we see that if we prove that x is high, then all others are to. By lemma 14 we see that x is high, so we are done. □

Outline

Proof of Theorem 16

Theorem 16

Let p, q_1, q_2 be polynomials such that p has non-zero constant term and degree at least two, and q_1 and q_2 have degree at least one. If

$$x = p(x) \Rightarrow q_1(x) = q_2(x) \text{ ring-theoretically}$$

then it also holds semring-theoretically.

Proof of Theorem 16

Theorem 16

Let p, q_1, q_2 be polynomials such that p has non-zero constant term and degree at least two, and q_1 and q_2 have degree at least one. If

$$x = p(x) \Rightarrow q_1(x) = q_2(x) \text{ ring-theoretically}$$

then it also holds semring-theoretically.

Proposition 15

If p has non-zero constant term and degree at least two then every non-constant polynomial is high.

Note

Since q_1 and q_2 are non-constant, they are high.

Proof continued

Corollary 11

If a_1, a_2 are High elements of a commutative semi-group $(A, *)$ and if there exists an $b \in A$ such that $a_1 * b = a_2 * b$ then $a_1 = a_2$.

Note

Since q_1, q_2 are High elements of $(\mathbb{N}, +)$, if there is an $s \in \mathrm{N}[x]$ such that $q_1(x) + s(x) = q_2(x) + s(x)$ then $q_1 = q_2$

Proof continued

Corollary 11

If a_1, a_2 are High elements of a commutative semi-group $(A, *)$ and if there exists an $b \in A$ such that $a_1 * b = a_2 * b$ then $a_1 = a_2$.

Note

Since q_1, q_2 are High elements of $(\mathbb{N}, +)$, if there is an $s \in \mathrm{N}[x]$ such that $q_1(x) + s(x) = q_2(x) + s(x)$ then $q_1 = q_2$

Proposition 7: Catalysts

Let $p_1; p_2; q_1; q_2 \in \mathbb{N}[x]$ and suppose that

$$p_1(x) = p_2(x) \Rightarrow q_1(x) = q_2(x) \text{ ring-theoretically:}$$

Then there exists $s \in \mathbb{N}[x]$ such that

$$p_1(x) = p_2(x) \Rightarrow q_1(x) + s(x) = q_2(x) + s(x) \text{ semiring-theoretically:}$$

Proof of Theorem 16

Theorem 16

Let p, q_1, q_2 be polynomials such that p has non-zero constant term and degree at least two, and q_1 and q_2 have degree at least one. If

$$x = p(x) \Rightarrow q_1(x) = q_2(x) \text{ ring-theoretically}$$

then it also holds semring-theoretically.

Proof.

Since q_1 and q_2 are high, and there exists a catalyst such that $q_1(x) + s(x) = q_2(x) + s(x)$ holds semiring theoretically, we conclude that $q_1 = q_2$ holds semiring theoretically. □

Recall

Proposition 2

Let $p, q_1, q_2 \in \mathbb{Z}[x]$ Suppose that the polynomial $p(x) - x \ \in \mathbb{Z}[x]$ is primitive and has no repeated complex roots, and that each complex root t satisfies $q_1(t) = q_2(t)$: Then

$$x = p(x) \Rightarrow q_1(x) = q_2(x) \text{ ring-theoretically}$$

Theorem 16

Let p, q_1, q_2 be polynomials such that p has non-zero constant term and degree at least two, and q_1 and q_2 have degree at least one. If

$$x = p(x) \Rightarrow q_1(x) = q_2(x) \text{ ring-theoretically}$$

then it also holds semring-theoretically.

Goal

Theorem 17

Let p, q_1, q_2 be polynomials such that p has non-zero constant term and degree at least two, and q_1 and q_2 have degree at least one. Suppose that the polynomial $p(x) - x \in \mathbb{Z}[x]$ is primitive and has no repeated complex roots, and that each complex root t satisfies $q_1(t) = q_2(t)$: Then

$$x = p(x) \Rightarrow q_1(x) = q_2(x) \text{ semiring-theoretically}$$

Distributive categories/ Haskell

$\Downarrow$ burnside semiring

Semirings

Goal

Theorem 17

Let p, q_1, q_2 be polynomials such that p has non-zero constant term and degree at least two, and q_1 and q_2 have degree at least one. Suppose that the polynomial $p(x) - x \in \mathbb{Z}[x]$ is primitive and has no repeated complex roots, and that each complex root t satisfies $q_1(t) = q_2(t)$: Then

$$x = p(x) \Rightarrow q_1(x) = q_2(x) \text{ semiring-theoretically}$$

Use of the burnside semiring

$$\forall \text{ semirings } A \text{ and all } a \in A; \text{ if } p_1(a) = p_2(a) \text{ then } q_1(a) = q_2(a)$$

Is equivalent with:

$$\forall \text{ distr. categories } \mathcal{A} \text{ and all } T \in \mathcal{A}; \text{ if } p_1(T) \cong p_2(T) \text{ then } q_1(T) \cong q_2(T).$$

Example

So if $c = c^2 + 1$ implies $c = c^7$ for all complex number c, then $T \cong T^2 + 1$ implies $T \cong T^7$ for all trees T.

Outline

Gaussian integers

Definition

Gaussian integers are complex numbers $z = ai + b$ for which $a, b \in \mathbb{Z}$.

Gaussian integers

Definition

Gaussian integers are complex numbers $z = ai + b$ for which $a, b \in \mathbb{Z}$.

Theorem

$\mathbb{N}[x]/(x = 1 + x + x^2)$ is isomorphic to the ring of Gaussian integers ($\mathscr{R}$).

Gaussian integers

Definition

Gaussian integers are complex numbers $z = ai + b$ for which $a, b \in \mathbb{Z}$.

Theorem

$\mathbb{N}[x]/(x = 1 + x + x^2)$ is isomorphic to the ring of Gaussian integers ($\mathscr{R}$).

Proof.

We see

$$\mathbb{N}[x]/(x = 1 + x + x^2) \cong \mathbb{Z}[x]/(1 + x + x^2 - x) = \mathbb{Z}[x]/(1 + x^2)$$

We see the ring of Gaussian integers ($\mathscr{R}$) consists of elements $m + ni$ with $m, n \in \mathbb{Z}$. If we take the mapping $m + nx^2 \Leftrightarrow m + ni$ we see $\mathbb{Z}[x]/(1 + x^2) \cong \mathscr{R}$. □

Gaussian ring

Note

Note moreover that if $x = i$ we have $\mathcal{R} \cong \mathbb{Z}[i]/(1 + i^2) \cong \mathbb{Z}[i]$.

Gaussian integers applied

Result from before

If $x = 1 + x + x^2$ implies $x = x^5$ as before, then

$$\forall \text{ distr. categories } \mathscr{A} \text{ and all } T \in \mathscr{A}; \text{ if } T \cong 1 + T + T^2 \text{ then } T \cong T^5.$$

Gaussian integers applied

Result from before

If $x = 1 + x + x^2$ implies $x = x^5$ as before, then

$$\forall \text{ distr. categories } \mathcal{A} \text{ and all } T \in \mathcal{A}; \text{ if } T \cong 1 + T + T^2 \text{ then } T \cong T^5.$$

Note

Take $p(x) = 1 + x + x^2$. Then $x = 1 + x + x^2$ implies $x = \pm i$. So we have $x = x^5$.
Then we can conclude that if $T \cong 1 + T + T^2$ then $T \cong T^5$.

Motzkin trees

Definition

A Motzkin tree is tree where every node has either 0 1 or 2 children.

Motzkin trees

Definition

A Motzkin tree is tree where every node has either 0 1 or 2 children.

Lemma

For Motzkin trees we have $T \cong 1 + T + T^2$.

Motzkin trees

Definition

A Motzkin tree is tree where every node has either 0 1 or 2 children.

Lemma

For Motzkin trees we have $T \cong 1 + T + T^2$.

Proof.

Take a node in a tree there are 3 possibilities:

- Either the node has 0 children, this corresponds to 1.
- Or it has one child, there is a tree attached to it, this corresponds to T.
- Or it has two children, both with a tree attached, this corresponds to T^2.

□

Conclusion

Motzkin trees

Before we had $x = 1 + x + x^2$ implies $x = x^5$.
Since we have proven that for Motzkin trees $T \cong 1 + T + T^2$, we can conclude that $T \cong T^5$ for all Motzkin trees.

Gaussian penny's

Recall we have $x = 1 + x + x^2$ First legal move:

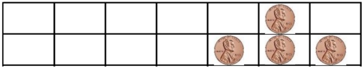


Figure: Fission

Gaussian penny's

Recall we have $x = 1 + x + x^2$ First legal move:

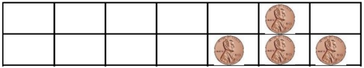


Figure: Fission

Second legal move:

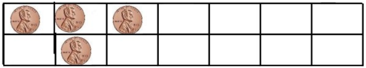


Figure: Fusion

Question of nuclear penny's

If this is the starting position:

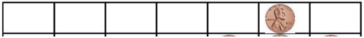


Figure: Start

Can we reach this target position?

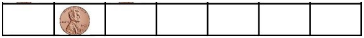
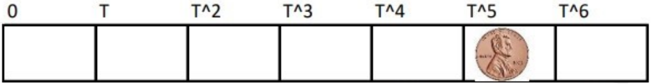
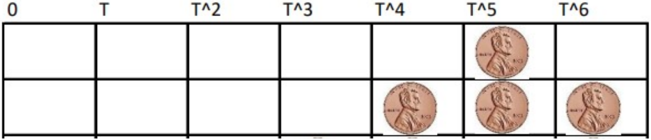


Figure: Target

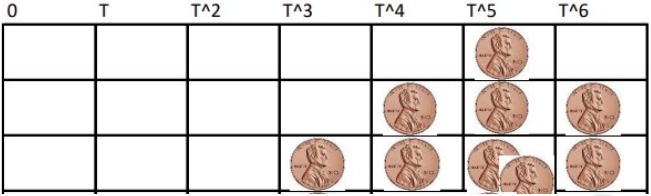
Nuclear penny's game answer



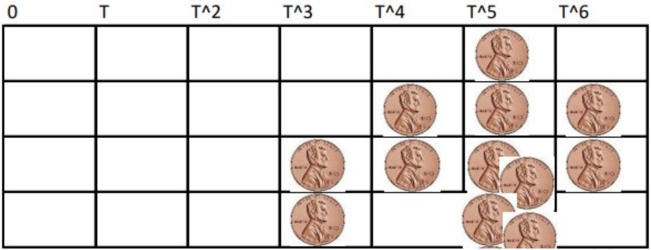
Nuclear penny's game answer



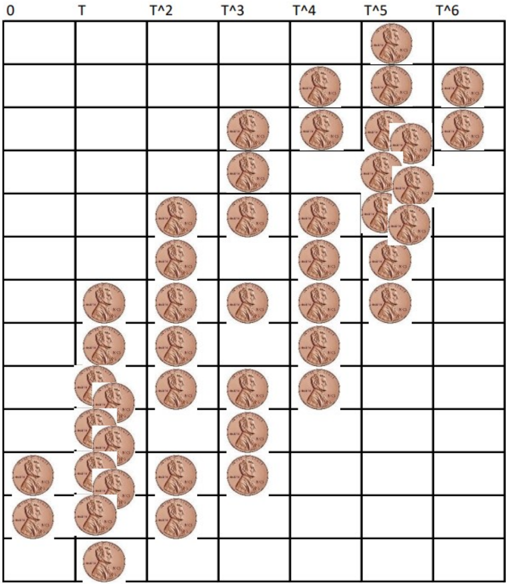
Nuclear penny's game answer



Nuclear penny's game answer



Nuclear penny's game answer



Outline

Reference

Reference

- Blog by Sigfpe at http://blog.sigfpe.com/2007/09/arboreal-isomorphisms-from-nuclear.html
- M. Fiore and T. Leinster.*Objects of categories as complex numbers*. E-print arXiv:math.CT/0212377, 2002. Also Advances in Mathematics, in press
- M. Fiore, T. Leinster, *An objective representation of the Gaussian integers*, J. Symbolic Comput., in press.
- A. Blass, *Seven trees in one*, J. Pure Appl. Algebra 103 (1995) 1–21.

Questions

Are there any questions?