Maximal ideals in rings, constructively

– an invitation –

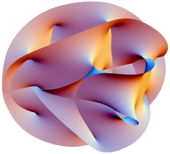
Computability in Europe 2022:
Revolutions and Revelations in Computability
11–15 July 2022, Swansea

Ingo Blechschmidt
University of Augsburg

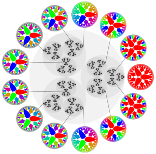
Peter Schuster
University of Verona

In this talk

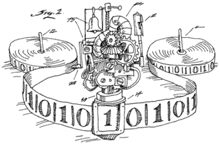
traveling the
multiverse



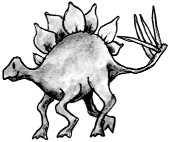
commutative
algebra



a fractal
without points



proofs as programs



monadic side effects

What others are saying

"a bad joke"

"non-informative"

Transfinite methods in algebra

Theorem. Let M be a surjective matrix with more rows than columns over a field. Then $\lightning$.

Proof. Elementary linear algebra. $\square$

Transfinite methods in algebra

Theorem. Let M be a surjective matrix with more rows than columns over a ring A. Then $1 = 0$ in A.

Transfinite methods in algebra

Theorem. Let M be a surjective matrix with more rows than columns over a ring A. Then $1 = 0$ in A.

Proof. Assume not.

Transfinite methods in algebra

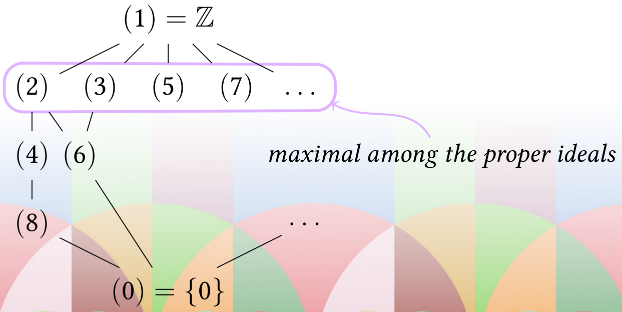
Theorem. Let M be a surjective matrix with more rows than columns over a ring A. Then $1 = 0$ in A.

Proof. Assume not. Then there is a maximal ideal $\mathfrak{m}$.

Transfinite methods in algebra

Theorem. Let M be a surjective matrix with more rows than columns over a ring A. Then $1 = 0$ in A.

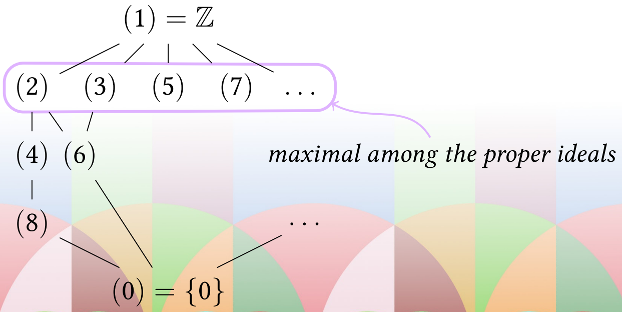
Proof. Assume not. Then there is a maximal ideal $\mathfrak{m}$.



Transfinite methods in algebra

Theorem. Let M be a surjective matrix with more rows than columns over a ring A. Then $1 = 0$ in A.

Proof. Assume not. Then there is a maximal ideal $\mathfrak{m}$. The matrix is surjective over the field $A/\mathfrak{m}$. This is a contradiction to basic linear algebra. □



Transfinite methods in algebra

Theorem. Let M be a surjective matrix with more rows than columns over a ring A. Then $1 = 0$ in A.

Proof. Assume not. Then there is a maximal ideal $\mathfrak{m}$. The matrix is surjective over the field $A/\mathfrak{m}$. This is a contradiction to basic linear algebra. $\square$

Proof. Write $M = \binom{x}{y}$. By surjectivity, have $u, v \in A$ with

$$u \binom{x}{y} = \binom{1}{0} \quad \text{and} \quad v \binom{x}{y} = \binom{0}{1}.$$

Hence $1 = -\underbrace{(vy-1)}_{=0} - vy\underbrace{(ux-1)}_{=0} + vx\underbrace{(uy-0)}_{=0} = 0.$ $\square$

Transfinite methods in algebra

Theorem. Let M be a surjective matrix with more rows than columns over a ring A. Then $1 = 0$ in A.

Proof. Assume not. Then there is a maximal ideal $\mathfrak{m}$. The matrix is surjective over the field $A/\mathfrak{m}$. This is a contradiction to basic linear algebra. $\square$

Proof. Write $M = \binom{x}{y}$. By surjectivity, have $u, v \in A$ with

$$u \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \text{and} \quad v \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

Hence $1 = -\underbrace{(vy-1)}_{=0} - vy\underbrace{(ux-1)}_{=0} + vx\underbrace{(uy-0)}_{=0} = 0.$ $\square$

Abstract proofs should be blueprints for concrete ones.

The status of maximal ideals

- In classical mathematics, every ring has a maximal ideal.
  – *Zorn's lemma*

The status of maximal ideals

- In classical mathematics, every ring has a maximal ideal.
  – *Zorn's lemma*

- Without Zorn, every countable ring has a maximal ideal.
  – *Iterative construction given enumeration* $x_0, x_1, \ldots$ *[Krull 1929]:*

$$\mathfrak{m}_0 = \{0\}, \qquad \mathfrak{m}_{n+1} = \begin{cases} \mathfrak{m}_n + (x_n), & \text{if } 1 \notin \mathfrak{m}_n + (x_n), \\ \mathfrak{m}_n, & \text{else.} \end{cases}$$

The status of maximal ideals

- In classical mathematics, every ring has a maximal ideal.
  – *Zorn's lemma*

- Without Zorn, every countable ring has a maximal ideal.
  – *Iterative construction given enumeration* $x_0, x_1, \ldots$ *[Krull 1929]:*

$$\mathfrak{m}_0 = \{0\}, \qquad \mathfrak{m}_{n+1} = \begin{cases} \mathfrak{m}_n + (x_n), & \text{if } 1 \notin \mathfrak{m}_n + (x_n), \\ \mathfrak{m}_n, & \text{else.} \end{cases}$$

  – *Also constructively! [Krivine 1996], [Berardi–Valentini 2004]*

$$\mathfrak{m}_0 = \{0\}, \qquad \mathfrak{m}_{n+1} = \mathfrak{m}_n + (\underbrace{\{x_n \mid 1 \notin \mathfrak{m}_n + (x_n)\}}_{\text{a certain subsingleton set}})$$

The status of maximal ideals

- In classical mathematics, every ring has a maximal ideal.
  – *Zorn's lemma*

- Without Zorn, every countable ring has a maximal ideal.
  – *Iterative construction given enumeration $x_0, x_1, \ldots$ [Krull 1929]:*

$$\mathfrak{m}_0 = \{0\}, \qquad \mathfrak{m}_{n+1} = \begin{cases} \mathfrak{m}_n + (x_n), & \text{if } 1 \not\in \mathfrak{m}_n + (x_n), \\ \mathfrak{m}_n, & \text{else.} \end{cases}$$

  – *Also constructively! [Krivine 1996], [Berardi–Valentini 2004]*

$$\mathfrak{m}_0 = \{0\}, \qquad \mathfrak{m}_{n+1} = \mathfrak{m}_n + (\underbrace{\{x_n \mid 1 \not\in \mathfrak{m}_n + (x_n)\}}_{\text{a certain subsingleton set}})$$

$A/\mathfrak{m}$ is a residue field: noninvertible implies zero.

The status of maximal ideals

- In classical mathematics, every ring has a maximal ideal.
  – *Zorn's lemma*

- Without Zorn, every countable ring has a maximal ideal.
  – *Iterative construction [Krull 1929]*
  – *Also constructively! [Krivine 1996], [Berardi–Valentini 2004]*
  $A/\mathfrak{m}$ is a residue field: noninvertible implies zero.

The status of maximal ideals

- In classical mathematics, every ring has a maximal ideal.
  – *Zorn's lemma*

- Without Zorn, every countable ring has a maximal ideal.
  – *Iterative construction [Krull 1929]*
  – *Also constructively! [Krivine 1996], [Berardi–Valentini 2004]*
  $A/\mathfrak{m}$ is a residue field: noninvertible implies zero.

- Constructively, every ring has a maximal ideal in some extension of the base universe.
  – *First-order consequences of its existence pass down to the base.*
  – *Obtained by applying K/B–V to the generic surjection* $\mathbb{N} \twoheadrightarrow A$ *[Joyal–Tierney 1984].*

The generic surjection

Let A be a (perhaps uncountable) set.

- Idea: Approximate the generic surjection $f : \mathbb{N} \twoheadrightarrow A$ by dynamically growing partial functions $[x_0, \ldots, x_n]$.
  – *As a proof runs its course and requires that some element $a \in A$ is contained in the image of f, refine $[x_0, \ldots, x_n]$ to $[x_0, \ldots, x_n, a]$.*

The generic surjection

Let A be a (perhaps uncountable) set.

- Idea: Approximate the generic surjection $f : \mathbb{N} \twoheadrightarrow A$ by dynamically growing partial functions $[x_0, \ldots, x_n]$.
  – *As a proof runs its course and requires that some element $a \in A$ is contained in the image of f, refine $[x_0, \ldots, x_n]$ to $[x_0, \ldots, x_n, a]$.*

- The finite approximations serve as the generating opens of a pointfree space.
  – *There is no fact of the matter whether "$f(0) = x \wedge f(1) = y$". Instead, this statement has the truth value $[x, y]$.*

The generic surjection

Let A be a (perhaps uncountable) set.

- Idea: Approximate the generic surjection $f : \mathbb{N} \twoheadrightarrow A$ by dynamically growing partial functions $[x_0, \ldots, x_n]$.
  – *As a proof runs its course and requires that some element $a \in A$ is contained in the image of f, refine $[x_0, \ldots, x_n]$ to $[x_0, \ldots, x_n, a]$.*
- The finite approximations serve as the generating opens of a pointfree space.
  – *There is no fact of the matter whether "$f(0) = x \wedge f(1) = y$". Instead, this statement has the truth value $[x, y]$.*
- Boils down to parametrizing everything by the current approximation and computing in the Eventually monad or its coarser cousin, the State monad.

Applications

Conceptual:

- Case study for proofs in algebra with minimal logic
- New constructive proof of formal substitute for existence:
  If the theory of maximal ideals of A is inconsistent, then $1 = 0$ in A.
- Strengthening of the position of maximal ideals as useful fictions
- Reification of dynamical algebra

Concrete: New constructive proofs of …

- Krull's lemma and its corollaries
- basic results of linear algebra over rings
- Suslin's lemma (key to the solution of Serre's problem)

```agda
module _ (A : Set) where

open import Data.List
open import Data.List.Membership.Propositional
open import Data.Product

data Eventually (P : List A → Set) : List A → Set where
  now
    : {σ : List A}
    → P σ
    → Eventually P σ
  later
    : {σ : List A} {a : A}
    → ((τ : List A) → a ∈ (σ ++ τ) → Eventually P (σ ++ τ))
    → Eventually P σ

State : (List A → Set) → (List A → Set)
State P σ = ((τ : List A) → Σ[ υ ∈ List A ] P (σ ++ τ ++ υ))
```

```
U:**-  Countable.agda   All L1    <N>   (Agda:Checked +5 Undo-Tree)

U:%*-  *All Done*   All L1    <M>   (AgdaInfo Undo-Tree)
```

Agda formalization available.