Material Interpretation and Constructive Analysis of Maximal Ideals in $\mathbb{Z}[X]$

Franziskus Wiesnet

TU Wien

December 17, 2024

FWF Österreichischer Wissenschaftsfonds

Material interpretation – general concept

Given a possibly classical proof of a statement of the form $A \to B$.

Material interpretation – general concept

Given a possibly classical proof of a statement of the form $A \to B$.

Goal: A proof for a statement $\neg A \vee B$, where $\neg A$ is a constructively stronger form of the negation of A.

Material interpretation – general concept

Given a possibly classical proof of a statement of the form $A \to B$.

Goal: A proof for a statement $\neg A \vee B$, where $\neg A$ is a constructively stronger form of the negation of A.

A and B may also be slightly modified. However, the statement and the proof should remain as close as possible to their original form.

A classical proof

Theorem

Let $M \subseteq \mathbb{Z}[X]$ be a maximal ideal. Then, there exists a prime number p with $p \in M$.

FWF Österreichischer Wissenschaftsfonds

A classical proof

Theorem

Let $M \subseteq \mathbb{Z}[X]$ be a maximal ideal. Then, there exists a prime number p with $p \in M$.

Proof.

There is some non-constant $f \in M$:

A classical proof

Theorem

Let $M \subseteq \mathbb{Z}[X]$ be a maximal ideal. Then, there exists a prime number p with $p \in M$.

Proof.

There is some non-constant $f \in M$: Either $X \in M$, or $X \notin M$ and there is some $g \in \mathbb{Z}[X]$ with $gX - 1 \in M$ as M is maximal.

A classical proof

Theorem

Let $M \subseteq \mathbb{Z}[X]$ be a maximal ideal. Then, there exists a prime number p with $p \in M$.

Proof.

There is some non-constant $f \in M$: Either $X \in M$, or $X \notin M$ and there is some $g \in \mathbb{Z}[X]$ with $gX - 1 \in M$ as M is maximal. Let d be the leading coefficient of f.

A classical proof

Theorem

Let $M \subseteq \mathbb{Z}[X]$ be a maximal ideal. Then, there exists a prime number p with $p \in M$.

Proof.

There is some non-constant $f \in M$: Either $X \in M$, or $X \notin M$ and there is some $g \in \mathbb{Z}[X]$ with $gX - 1 \in M$ as M is maximal. Let d be the leading coefficient of f. Assume there is no prime number p with $p \in M$.

A classical proof

Theorem

Let $M \subseteq \mathbb{Z}[X]$ be a maximal ideal. Then, there exists a prime number p with $p \in M$.

Proof.

There is some non-constant $f \in M$: Either $X \in M$, or $X \notin M$ and there is some $g \in \mathbb{Z}[X]$ with $gX - 1 \in M$ as M is maximal. Let d be the leading coefficient of f. Assume there is no prime number p with $p \in M$. As a maximal ideal is also a prime ideal, $M \cap \mathbb{Z} = \{0\}$.

FWF Österreichischer Wissenschaftsfonds

A classical proof

Theorem

Let $M \subseteq \mathbb{Z}[X]$ be a maximal ideal. Then, there exists a prime number p with $p \in M$.

Proof.

There is some non-constant $f \in M$: Either $X \in M$, or $X \notin M$ and there is some $g \in \mathbb{Z}[X]$ with $gX - 1 \in M$ as M is maximal. Let d be the leading coefficient of f. Assume there is no prime number p with $p \in M$. As a maximal ideal is also a prime ideal, $M \cap \mathbb{Z} = \{0\}$. Hence the canonical homomorphism $\mathbb{Z} \to \mathbb{Z}[X]/M$ is injective into the field $\mathbb{Z}[X]/M$ and induces a ring extension $\mathbb{Z}[d^{-1}] \to \mathbb{Z}[X]/M$.

A classical proof

Theorem

Let $M \subseteq \mathbb{Z}[X]$ be a maximal ideal. Then, there exists a prime number p with $p \in M$.

Proof.

There is some non-constant $f \in M$: Either $X \in M$, or $X \notin M$ and there is some $g \in \mathbb{Z}[X]$ with $gX - 1 \in M$ as M is maximal. Let d be the leading coefficient of f. Assume there is no prime number p with $p \in M$. As a maximal ideal is also a prime ideal, $M \cap \mathbb{Z} = \{0\}$. Hence the canonical homomorphism $\mathbb{Z} \to \mathbb{Z}[X]/M$ is injective into the field $\mathbb{Z}[X]/M$ and induces a ring extension $\mathbb{Z}[d^{-1}] \to \mathbb{Z}[X]/M$. This is an **integral ring extension** with the integral polynomial $d^{-1}f$.

FWF Österreichischer Wissenschaftsfonds

A classical proof

Theorem

Let $M \subseteq \mathbb{Z}[X]$ be a maximal ideal. Then, there exists a prime number p with $p \in M$.

Proof.

There is some non-constant $f \in M$: Either $X \in M$, or $X \notin M$ and there is some $g \in \mathbb{Z}[X]$ with $gX - 1 \in M$ as M is maximal. Let d be the leading coefficient of f. Assume there is no prime number p with $p \in M$. As a maximal ideal is also a prime ideal, $M \cap \mathbb{Z} = \{0\}$. Hence the canonical homomorphism $\mathbb{Z} \to \mathbb{Z}[X]/M$ is injective into the field $\mathbb{Z}[X]/M$ and induces a ring extension $\mathbb{Z}[d^{-1}] \to \mathbb{Z}[X]/M$. This is an **integral ring extension** with the integral polynomial $d^{-1}f$. As $\mathbb{Z}[X]/M$ is a field, also $\mathbb{Z}[d^{-1}]$ must be a field, which is impossible. $\square$

A constructive proof

Definition

Let R be a ring. For a boolean valued function $M : R \to \mathbb{B}$ and a function $\nu : R \to R$, we say that (M, ν) is an EXPLICIT MAXIMAL IDEAL if M is an ideal, $1 \notin M$ and $a\nu(a) - 1 \in M$ for all $a \in R \setminus M$.

A constructive proof

Definition

Let R be a ring. For a boolean valued function $M : R \to \mathbb{B}$ and a function $\nu : R \to R$, we say that (M, ν) is an EXPLICIT MAXIMAL IDEAL if M is an ideal, $1 \notin M$ and $a\nu(a) - 1 \in M$ for all $a \in R \setminus M$.
Furthermore, we say that there is EVIDENCE THAT (M, ν) IS NOT AN EXPLICIT MAXIMAL IDEAL if one of the following cases holds:

- $0 \notin M$,
- there are $a, b \in M$ with $a + b \notin M$,
- there are $\lambda \in R$ and $a \in M$ with $\lambda a \notin M$,
- $1 \in M$, or
- there is $a \in R \setminus M$ with $a\nu(a) - 1 \notin M$.

FWF Österreichischer Wissenschaftsfonds

A constructive proof

Theorem

Let $M : \mathbb{Z}[X] \to \mathbb{B}$ *and* $\nu : \mathbb{Z}[X] \to \mathbb{Z}[X]$ *be given. Then, either there exists a prime number* $p \in M$*, or there is evidence that* (M, ν) *is not an explicit maximal ideal in* $\mathbb{Z}[X]$*.*

A constructive proof

Goal:
Prime number $p \in M$ or evidence that (M, ν) is not an explicit maximal ideal.
Given:
$M : \mathbb{Z}[X] \to \mathbb{B}$, $\nu : \mathbb{Z}[X] \to \mathbb{Z}[X]$

A constructive proof

Goal:
Prime number $p \in M$ or evidence that (M, ν) is not an explicit maximal ideal.
Given:
$M : \mathbb{Z}[X] \to \mathbb{B}$, $\nu : \mathbb{Z}[X] \to \mathbb{Z}[X]$

Take some non-constant $f \in M$: If $X \in M$, we are done. Otherwise, $X \notin M$ and either $X\nu(X) - 1 \in M$ or there is evidence that (M, ν) is not an explicit maximal ideal.

FWF Österreichischer Wissenschaftsfonds

A constructive proof

Goal:
Prime number $p \in M$ or evidence that (M, ν) is not an explicit maximal ideal.
Given:
$M : \mathbb{Z}[X] \to \mathbb{B}$, $\nu : \mathbb{Z}[X] \to \mathbb{Z}[X]$, $f \in M$ non-constant, $d := \mathrm{LC}(f)$, $n := \deg(f)$

A constructive proof

Goal:
Prime number $p \in M$ or evidence that (M, ν) is not an explicit maximal ideal.
Given:
$M : \mathbb{Z}[X] \to \mathbb{B}$, $\nu : \mathbb{Z}[X] \to \mathbb{Z}[X]$, $f \in M$ non-constant, $d := \mathrm{LC}(f)$, $n := \deg(f)$

Take some prime number $q \nmid d$. Check if $q \in M$ or $m := q\nu(q) - 1 \notin M$. If yes, there is evidence that (M, ν) is not an explicit maximal ideal.

A constructive proof

Goal:

Prime number $p \in M$ or evidence that (M, ν) is not an explicit maximal ideal.

Given:

$M : \mathbb{Z}[X] \to \mathbb{B}$, $\nu : \mathbb{Z}[X] \to \mathbb{Z}[X]$, $f \in M$ non-constant, $d := \mathrm{LC}(f)$, $n := \deg(f)$, $q \nmid d$ prime, $q \notin M$, $m := q\nu(q) - 1 \in M$

A constructive proof

Goal:
Prime number $p \in M$ or evidence that (M, ν) is not an explicit maximal ideal.
Given:
$M : \mathbb{Z}[X] \to \mathbb{B}$, $\nu : \mathbb{Z}[X] \to \mathbb{Z}[X]$, $f \in M$ non-constant, $d := \mathrm{LC}(f)$, $n := \deg(f)$, $q \nmid d$ prime, $q \notin M$, $m := q\nu(q) - 1 \in M$

For each $i \in \{0, \dots, n-1\}$ we get some $k_i \in \mathbb{N}$, $h_i \in \mathbb{Z}[X]$ and $(a_{ij})_{j \in \{0,\dots,n-1\}} \in \mathbb{Z}^n$ with

$$d^{k_i} \nu(q) x^i + h_i f = \sum_{j=0}^{n-1} a_{ij} x^j. \quad (!)$$

Let A be the matrix $(d^{k_i} \nu(q) \delta_{ij} - a_{ij})_{i,j \in \{0,\dots,n-1\}}$, then

$$A \begin{pmatrix} x^0 \\ \vdots \\ x^{n-1} \end{pmatrix} = \begin{pmatrix} -h_0 f \\ \vdots \\ -h_{n-1} f \end{pmatrix}$$

A constructive proof

Goal:
Prime number $p \in M$ or evidence that (M, ν) is not an explicit maximal ideal.
Given:
$M : \mathbb{Z}[X] \to \mathbb{B}$, $\nu : \mathbb{Z}[X] \to \mathbb{Z}[X]$, $f \in M$ non-constant, $d := \mathrm{LC}(f)$,
$n := \deg(f)$, $q \nmid d$ prime, $q \notin M$, $m := q\nu(q) - 1 \in M$,
$(k_i)_{i \in \{0,\ldots,n-1\}} \in \mathbb{N}^n$, $(a_{ij})_{i,j \in \{0,\ldots,n-1\}} \in \mathbb{Z}^{n \times n}$,
$A = (d^{k_i}\nu(q)\delta_{ij} - a_{ij})_{i,j \in \{0,\ldots,n-1\}}$,
$A(x^0, \ldots, x^{n-1})^T = (-h_0 f, \ldots, -h_{n-1} f)^T$

A constructive proof

Goal:
Prime number $p \in M$ or evidence that (M, ν) is not an explicit maximal ideal.
Given:
$M : \mathbb{Z}[X] \to \mathbb{B}$, $\nu : \mathbb{Z}[X] \to \mathbb{Z}[X]$, $f \in M$ non-constant, $d := \mathrm{LC}(f)$,
$n := \deg(f)$, $q \nmid d$ prime, $q \notin M$, $m := q\nu(q) - 1 \in M$,
$(k_i)_{i \in \{0,\ldots,n-1\}} \in \mathbb{N}^n$, $(a_{ij})_{i,j \in \{0,\ldots,n-1\}} \in \mathbb{Z}^{n \times n}$,
$A = (d^{k_i}\nu(q)\delta_{ij} - a_{ij})_{i,j \in \{0,\ldots,n-1\}}$,
$A(x^0, \ldots, x^{n-1})^T = (-h_0 f, \ldots, -h_{n-1} f)^T$

Let $\hat{A}$ be the adjugate matrix of A with $\hat{A}A = \det(A)E$. Then

$$\begin{pmatrix} \det(A)x^0 \\ \vdots \\ \det(A)x^{n-1} \end{pmatrix} = \hat{A} \begin{pmatrix} -h_0 f \\ \vdots \\ -h_{n-1} f \end{pmatrix}.$$

in particular $\det(A) = -\sum_{j=0}^{n-1} \hat{A}_{0j} h_j f$ by the first line

A constructive proof

Goal:
Prime number $p \in M$ or evidence that (M, ν) is not an explicit maximal ideal.

Given:
$M : \mathbb{Z}[X] \to \mathbb{B}$, $\nu : \mathbb{Z}[X] \to \mathbb{Z}[X]$, $f \in M$ non-constant, $d := \mathrm{LC}(f)$,
$n := \deg(f)$, $q \nmid d$ prime, $q \notin M$, $m := q\nu(q) - 1 \in M$,
$(k_i)_{i \in \{0,\ldots,n-1\}} \in \mathbb{N}^n$, $(a_{ij})_{i,j \in \{0,\ldots,n-1\}} \in \mathbb{Z}^{n \times n}$,
$A = (d^{k_i}\nu(q)\delta_{ij} - a_{ij})_{i,j \in \{0,\ldots,n-1\}}$,
$A(x^0, \ldots, x^{n-1})^T = (-h_0 f, \ldots, -h_{n-1} f)^T$, $\det(A) = -\sum_{j=0}^{n-1} \hat{A}_{0j} h_j f$

A constructive proof

Goal:
Prime number $p \in M$ or evidence that (M, ν) is not an explicit maximal ideal.
Given:
$M : \mathbb{Z}[X] \to \mathbb{B}$, $\nu : \mathbb{Z}[X] \to \mathbb{Z}[X]$, $f \in M$ non-constant, $d := \mathrm{LC}(f)$,
$n := \deg(f)$, $q \nmid d$ prime, $q \notin M$, $m := q\nu(q) - 1 \in M$,
$(k_i)_{i \in \{0,\dots,n-1\}} \in \mathbb{N}^n$, $(a_{ij})_{i,j \in \{0,\dots,n-1\}} \in \mathbb{Z}^{n \times n}$,
$A = (d^{k_i}\nu(q)\delta_{ij} - a_{ij})_{i,j \in \{0,\dots,n-1\}}$,
$A(x^0, \dots, x^{n-1})^T = (-h_0 f, \dots, -h_{n-1} f)^T$, $\det(A) = -\sum_{j=0}^{n-1} \hat{A}_{0j} h_j f$

Looking at the definition of A, we have
$\det(A) = d^K \nu(q)^n + b_{n-1}\nu(q)^{n-1} + \cdots + b_1\nu(q) + b_0$ for some
$b_0, \dots, b_{n-1} \in \mathbb{Z}$ and $K := \sum k_i$.

A constructive proof

Goal:
Prime number $p \in M$ or evidence that (M, ν) is not an explicit maximal ideal.
Given:
$M : \mathbb{Z}[X] \to \mathbb{B}$, $\nu : \mathbb{Z}[X] \to \mathbb{Z}[X]$, $f \in M$ non-constant, $d := \mathrm{LC}(f)$,
$n := \deg(f)$, $q \nmid d$ prime, $q \notin M$, $m := q\nu(q) - 1 \in M$,
$(k_i)_{i \in \{0,\dots,n-1\}} \in \mathbb{N}^n$, $(a_{i,j})_{i,j \in \{0,\dots,n-1\}} \in \mathbb{Z}^{n \times n}$,
$A = (d^{k_i}\nu(q)\delta_{ij} - a_{ij})_{i,j \in \{0,\dots,n-1\}}$,
$A(x^0, \dots, x^{n-1})^T = (-h_0 f, \dots, -h_{n-1} f)^T$, $b_0, \dots, b_{n-1} \in \mathbb{Z}, K := \sum k_i$,
$d^K \nu(q)^n + b_{n-1}\nu(q)^{n-1} + \cdots + b_1 \nu(q) + b_0 = -\sum_{j=0}^{n-1} \hat{A}_{0j} h_j f$

A constructive proof

Goal:
Prime number $p \in M$ or evidence that (M, ν) is not an explicit maximal ideal.
Given:
$M : \mathbb{Z}[X] \to \mathbb{B}$, $\nu : \mathbb{Z}[X] \to \mathbb{Z}[X]$, $f \in M$ non-constant, $d := \mathrm{LC}(f)$,
$n := \deg(f)$, $q \nmid d$ prime, $q \notin M$, $m := q\nu(q) - 1 \in M$,
$(k_i)_{i \in \{0,\dots,n-1\}} \in \mathbb{N}^n$, $(a_{i,j})_{i,j \in \{0,\dots,n-1\}} \in \mathbb{Z}^{n \times n}$,
$A = (d^{k_i} \nu(q) \delta_{ij} - a_{ij})_{i,j \in \{0,\dots,n-1\}}$,
$A(x^0, \dots, x^{n-1})^T = (-h_0 f, \dots, -h_{n-1} f)^T$, $b_0, \dots, b_{n-1} \in \mathbb{Z}, K := \sum k_i$,
$d^K \nu(q)^n + b_{n-1} \nu(q)^{n-1} + \dots + b_1 \nu(q) + b_0 = -\sum_{j=0}^{n-1} \hat{A}_{0j} h_j f$

Multiplying both sides with q^n leads to

$$d^K (q\nu(q))^n + \sum_{j=0}^{n-1} b_j q^{j+1} (q\nu(q))^{n-j-1} = \sum_{j=0}^{n-1} (-q^n \hat{A}_{0j} h_j) f$$

A constructive proof

Goal:
Prime number $p \in M$ or evidence that (M, ν) is not an explicit maximal ideal.
Given:
$M : \mathbb{Z}[X] \to \mathbb{B}$, $\nu : \mathbb{Z}[X] \to \mathbb{Z}[X]$, $f \in M$ non-constant, $d := \mathrm{LC}(f)$,
$n := \deg(f)$, $q \nmid d$ prime, $q \notin M$, $m := q\nu(q) - 1 \in M$,
$(k_i)_{i \in \{0,\dots,n-1\}} \in \mathbb{N}^n$, $(a_{i,j})_{i,j \in \{0,\dots,n-1\}} \in \mathbb{Z}^{n \times n}$,
$A = (d^{k_i} \nu(q) \delta_{ij} - a_{ij})_{i,j \in \{0,\dots,n-1\}}$,
$A(x^0, \dots, x^{n-1})^T = (-h_0 f, \dots, -h_{n-1} f)^T$, $b_0, \dots, b_{n-1} \in \mathbb{Z}, K := \sum k_i$,
$d^K (q\nu(q))^n + \sum_{j=0}^{n-1} b_j q^{j+1} (q\nu(q))^{n-j-1} = \sum_{j=0}^{n-1} (-q^n \hat{A}_{0j} h_j) f$

A constructive proof

Goal:
Prime number $p \in M$ or evidence that (M, ν) is not an explicit maximal ideal.
Given:
$M : \mathbb{Z}[X] \to \mathbb{B}$, $\nu : \mathbb{Z}[X] \to \mathbb{Z}[X]$, $f \in M$ non-constant, $d := \mathrm{LC}(f)$,
$n := \deg(f)$, $q \nmid d$ prime, $q \notin M$, $m := q\nu(q) - 1 \in M$,
$(k_i)_{i \in \{0,\ldots,n-1\}} \in \mathbb{N}^n$, $(a_{i,j})_{i,j \in \{0,\ldots,n-1\}} \in \mathbb{Z}^{n \times n}$,
$A = (d^{k_i}\nu(q)\delta_{ij} - a_{ij})_{i,j \in \{0,\ldots,n-1\}}$,
$A(x^0, \ldots, x^{n-1})^T = (-h_0 f, \ldots, -h_{n-1} f)^T$, $b_0, \ldots, b_{n-1} \in \mathbb{Z}, K := \sum k_i$,
$d^K(q\nu(q))^n + \sum_{j=0}^{n-1} b_j q^{j+1}(q\nu(q))^{n-j-1} = \sum_{j=0}^{n-1}(-q^n \hat{A}_{0j} h_j) f$

For each $i \in \{1, \ldots, n\}$ one can easily compute some polynomial g_i with $(m+1)^i = 1 + mg_i$. This leads to
$d^K + \sum_{j=0}^{n-1} b_j q^{n-j} = \sum_{j=0}^{n-1}(-q^n \hat{A}_{0j} h_j) f - (d^K g_n + \sum_{j=1}^{n-1} b_j q^{n-j} g_j) m$

A constructive proof

Goal:
Prime number $p \in M$ or evidence that (M, ν) is not an explicit maximal ideal.
Given:
$M : \mathbb{Z}[X] \to \mathbb{B}$, $\nu : \mathbb{Z}[X] \to \mathbb{Z}[X]$, $f \in M$ non-constant, $d := \mathrm{LC}(f)$,
$n := \deg(f)$, $q \nmid d$ prime, $q \notin M$, $m := q\nu(q) - 1 \in M$,
$(k_i)_{i \in \{0,\ldots,n-1\}} \in \mathbb{N}^n$,$K := \sum k_i$, $(a_{i,j})_{i,j \in \{0,\ldots,n-1\}} \in \mathbb{Z}^{n \times n}$,
$A = (d^{k_i}\nu(q)\delta_{ij} - a_{ij})_{i,j \in \{0,\ldots,n-1\}}$,
$A(x^0, \ldots, x^{n-1})^T = (-h_0 f, \ldots, -h_{n-1} f)^T$, $b_0, \ldots, b_{n-1} \in \mathbb{Z}$,
$d^K + \sum_{j=0}^{n-1} b_j q^{n-j} = \sum_{j=0}^{n-1}(-q^n \hat{A}_{0j} h_j) f + (-d^K g_n - \sum_{j=1}^{n-1} b_j q^{n-j} g_j) m$

A constructive proof

Goal:
Prime number $p \in M$ or evidence that (M, ν) is not an explicit maximal ideal.
Given:
$M : \mathbb{Z}[X] \to \mathbb{B}$, $\nu : \mathbb{Z}[X] \to \mathbb{Z}[X]$, $f \in M$ non-constant, $d := \mathrm{LC}(f)$,
$n := \deg(f)$, $q \nmid d$ prime, $q \notin M$, $m := q\nu(q) - 1 \in M$,
$(k_i)_{i \in \{0,\dots,n-1\}} \in \mathbb{N}^n$,$K := \sum k_i$, $(a_{i,j})_{i,j \in \{0,\dots,n-1\}} \in \mathbb{Z}^{n \times n}$,
$A = (d^{k_i}\nu(q)\delta_{ij} - a_{ij})_{i,j \in \{0,\dots,n-1\}}$,
$A(x^0, \dots, x^{n-1})^T = (-h_0 f, \dots, -h_{n-1} f)^T$, $b_0, \dots, b_{n-1} \in \mathbb{Z}$,
$d^K + \sum_{j=0}^{n-1} b_j q^{n-j} = \sum_{j=0}^{n-1}(-q^n \hat{A}_{0j} h_j) f + (-d^K g_n - \sum_{j=1}^{n-1} b_j q^{n-j} g_j) m$

$D := d^K + \sum_{j=0}^{n-1} b_j q^{n-j} \in \mathbb{Z}$ and $d^K + \sum_{j=0}^{n-1} b_j q^{n-j} \neq 0$ as otherwise $q \mid d$.

A constructive proof

Goal:
Prime number $p \in M$ or evidence that (M, ν) is not an explicit maximal ideal.
Given:
$M : \mathbb{Z}[X] \to \mathbb{B}$, $\nu : \mathbb{Z}[X] \to \mathbb{Z}[X]$, $f \in M$ non-constant, $d := \mathrm{LC}(f)$,
$n := \deg(f)$, $q \nmid d$ prime, $q \notin M$, $m := q\nu(q) - 1 \in M$,
$(k_i)_{i \in \{0,\ldots,n-1\}} \in \mathbb{N}^n$, $K := \sum k_i$, $(a_{i,j})_{i,j \in \{0,\ldots,n-1\}} \in \mathbb{Z}^{n \times n}$,
$A = (d^{k_i}\nu(q)\delta_{ij} - a_{ij})_{i,j \in \{0,\ldots,n-1\}}$,
$A(x^0, \ldots, x^{n-1})^T = (-h_0 f, \ldots, -h_{n-1} f)^T$, $b_0, \ldots, b_{n-1} \in \mathbb{Z}$,
$D = \sum_{j=0}^{n-1}(-q^n \hat{A}_{0j} h_j) f + (-d^K g_n - \sum_{j=1}^{n-1} b_j q^{n-j} g_j) m \in \mathbb{Z} \setminus \{0\}$

A constructive proof

Goal:
Prime number $p \in M$ or evidence that (M, ν) is not an explicit maximal ideal.
Given:
$M : \mathbb{Z}[X] \to \mathbb{B}$, $\nu : \mathbb{Z}[X] \to \mathbb{Z}[X]$, $f \in M$ non-constant, $d := \mathrm{LC}(f)$,
$n := \deg(f)$, $q \nmid d$ prime, $q \notin M$, $m := q\nu(q) - 1 \in M$,
$(k_i)_{i \in \{0,\ldots,n-1\}} \in \mathbb{N}^n$,$K := \sum k_i$, $(a_{i,j})_{i,j \in \{0,\ldots,n-1\}} \in \mathbb{Z}^{n \times n}$,
$A = (d^{k_i}\nu(q)\delta_{ij} - a_{ij})_{i,j \in \{0,\ldots,n-1\}}$,
$A(x^0, \ldots, x^{n-1})^T = (-h_0 f, \ldots, -h_{n-1} f)^T$, $b_0, \ldots, b_{n-1} \in \mathbb{Z}$,
$D = \sum_{j=0}^{n-1}(-q^n \hat{A}_{0j} h_j)f + (-d^K g_n - \sum_{j=1}^{n-1} b_j q^{n-j} g_j)m \in \mathbb{Z} \setminus \{0\}$

As $m, f \in M$ either $D \in M$ or there is evidence that (M, ν) is not an explicit maximal ideal.

A constructive proof

Goal:
Prime number $p \in M$ or evidence that (M, ν) is not an explicit maximal ideal.
Given:
$M : \mathbb{Z}[X] \to \mathbb{B}$, $\nu : \mathbb{Z}[X] \to \mathbb{Z}[X]$, $f \in M$ non-constant, $d := \mathrm{LC}(f)$,
$n := \deg(f)$, $q \nmid d$ prime, $q \notin M$, $m := q\nu(q) - 1 \in M$,
$(k_i)_{i \in \{0,\ldots,n-1\}} \in \mathbb{N}^n$,$K := \sum k_i$, $(a_{i,j})_{i,j \in \{0,\ldots,n-1\}} \in \mathbb{Z}^{n \times n}$,
$A = (d^{k_i}\nu(q)\delta_{ij} - a_{ij})_{i,j \in \{0,\ldots,n-1\}}$,
$A(x^0, \ldots, x^{n-1})^T = (-h_0 f, \ldots, -h_{n-1} f)^T$, $b_0, \ldots, b_{n-1} \in \mathbb{Z}$,
$D = \sum_{j=0}^{n-1}(-q^n \hat{A}_{0j} h_j) f + (-d^K g_n - \sum_{j=1}^{n-1} b_j q^{n-j} g_j) m \in \mathbb{Z} \setminus \{0\} \cap M$

A constructive proof

Goal:
Prime number $p \in M$ or evidence that (M, ν) is not an explicit maximal ideal.
Given:
$M : \mathbb{Z}[X] \to \mathbb{B}$, $\nu : \mathbb{Z}[X] \to \mathbb{Z}[X]$, $f \in M$ non-constant, $d := \mathrm{LC}(f)$,
$n := \deg(f)$, $q \nmid d$ prime, $q \notin M$, $m := q\nu(q) - 1 \in M$,
$(k_i)_{i \in \{0,\ldots,n-1\}} \in \mathbb{N}^n$,$K := \sum k_i$, $(a_{i,j})_{i,j \in \{0,\ldots,n-1\}} \in \mathbb{Z}^{n \times n}$,
$A = (d^{k_i} \nu(q) \delta_{ij} - a_{ij})_{i,j \in \{0,\ldots,n-1\}}$,
$A(x^0, \ldots, x^{n-1})^T = (-h_0 f, \ldots, -h_{n-1} f)^T$, $b_0, \ldots, b_{n-1} \in \mathbb{Z}$,
$D = \sum_{j=0}^{n-1} (-q^n \hat{A}_{0j} h_j) f + (-d^K g_n - \sum_{j=1}^{n-1} b_j q^{n-j} g_j) m \in \mathbb{Z} \setminus \{0\} \cap M$

Let $D = \prod_{i=1}^{m} p_i$ be the prime factorization of D, then there is some p_i with $p_i \in M$ or there is evidence that (M, ν) is not an explicit maximal ideal (!).

Notes

- At first glance, the constructive proof may seem more complex; however, it is actually very elementary.

Notes

- At first glance, the constructive proof may seem more complex; however, it is actually very elementary.
- A few “non-constructive” principles remain. In particular, membership to M must be decidable.

FWF Österreichischer Wissenschaftsfonds

Notes

- At first glance, the constructive proof may seem more complex; however, it is actually very elementary.
- A few "non-constructive" principles remain. In particular, membership to M must be decidable.
- Instead of applying Modus Ponens, there is often a case distinction if a certain element is in M or not.

FWF Österreichischer Wissenschaftsfonds

Notes

- At first glance, the constructive proof may seem more complex; however, it is actually very elementary.
- A few "non-constructive" principles remain. In particular, membership to M must be decidable.
- Instead of applying Modus Ponens, there is often a case distinction if a certain element is in M or not.
- An implementation already exists as a Python program using **SymPy**.

FWF Österreichischer Wissenschaftsfonds

An Agda implementation

Work in progress, supported by **Felix Cherubini**

- The implementation is based on the Agda Cubical library, as it provides polynomials and matrices.
- As part of the project, Cubical has already been extended by the determinant and the adjugate matrix.

FWF Österreichischer Wissenschaftsfonds

Suitability of Agda for the material interpretation

Work in progress

+ Proof interpretations are fundamentally straightforward to implement in Agda
- Agda is more intended for implementing everything from scratch.
- Agda has few tactics
- The Agda library is small compared to proof assistants such as Lean or Coq.

$\Rightarrow$ At present, Agda is somewhat unsuitable for material interpretation, as several additions to the library are required.

Suitability of Lean for the material interpretation

In the early stages

- \+ The Lean library is very advanced.
- \+ Lean has many tactics.
- – Implementing proof interpretations in Lean may present some challenges.
- – The Lean library supports only classical logic.

Application

Theorem (Hilbert's 17th Problem)

Let $f \in \mathbb{Q}[X_1, \ldots, X_n]$ be given with $f(\vec{x}) \geq 0$ for all $\vec{x} \in \mathbb{Q}^n$. Then f is a sum of squares in $\mathbb{Q}(X_1, \ldots, X_n)$.

Application

Theorem (Hilbert's 17th Problem)

Let $f \in \mathbb{Q}[X_1, \ldots, X_n]$ be given with $f(\vec{x}) \geq 0$ for all $\vec{x} \in \mathbb{Q}^n$. Then f is a sum of squares in $\mathbb{Q}(X_1, \ldots, X_n)$.

The problem was classically solved in 1927 by Emil Artin using several lemmas, including Sturm's theorem and the **Artin-Schreier Theorem**:

Application

Theorem (Hilbert's 17th Problem)

Let $f \in \mathbb{Q}[X_1, \ldots, X_n]$ be given with $f(\vec{x}) \geq 0$ for all $\vec{x} \in \mathbb{Q}^n$. Then f is a sum of squares in $\mathbb{Q}(X_1, \ldots, X_n)$.

The problem was classically solved in 1927 by Emil Artin using several lemmas, including Sturm's theorem and the **Artin-Schreier Theorem**:

Theorem

Let K be an field, then

$$\bigcap \{U \subseteq K \mid U \textit{ is an order of } K\} = \left\{ \sum_{i=0}^{n} x_i^2 \;\middle|\; n \in \mathbb{N},\ x_0, \ldots, x_n \in K \right\}.$$

Application

Theorem (Hilbert's 17th Problem)

Let $f \in \mathbb{Q}[X_1, \ldots, X_n]$ be given with $f(\vec{x}) \geq 0$ for all $\vec{x} \in \mathbb{Q}^n$. Then f is a sum of squares in $\mathbb{Q}(X_1, \ldots, X_n)$.

The problem was classically solved in 1927 by Emil Artin using several lemmas, including Sturm's theorem and the **Artin-Schreier Theorem**:

Theorem

Let K be an field, then

$$\bigcap \{U \subseteq K \mid U \text{ is an order of } K\} = \left\{ \sum_{i=0}^{n} x_i^2 \;\middle|\; n \in \mathbb{N},\ x_0, \ldots, x_n \in K \right\}.$$

Hilbert's 17th Problem was constructively considered by Charles N. Delzell in 1984.

Application

Theorem (Zariski's Lemma)

Let K be a field and R an K-algebra, which is also a field. Suppose that $R = K[x_1, \ldots, x_n]$ for some $x_1, \ldots, x_n \in R$. Then R is algebraic over K, i.e. there are non-zero $f_1, \ldots, f_n \in K[X]$ such that $f_i(x_i) = 0$ for all i.

Application

Theorem (Zariski's Lemma)

Let K be a field and R an K-algebra, which is also a field. Suppose that $R = K[x_1, \ldots, x_n]$ for some $x_1, \ldots, x_n \in R$. Then R is algebraic over K, i.e. there are non-zero $f_1, \ldots, f_n \in K[X]$ such that $f_i(x_i) = 0$ for all i.

This theorem could also be used to prove the statement in the case study above. In 1947 Zariski used it to prove Hilbert's Nullstellensatz.

Theorem (Hilbert's Nullstellensatz)

Let K be an algebraically closed field, $\vec{X} := X_1, \ldots, X_n$ and $f_1, \ldots, f_m \in K[\vec{X}]$ be given. Then, either there are $g_1, \ldots, g_m \in K[\vec{X}]$ with $g_1 f_1 + \cdots + g_m f_m = 1$ or there are $x_1, \ldots, x_n \in K$ with $f_i(x_1, \ldots, x_n) = 0$ for all i.

An algorithmic version of Zariski's Lemma was already developed, which can be used to develop a material interpretation of Zariski's Lemma. This can lead to a material interpretation of Hilbert's Nullstellensatz.

FWF Österreichischer Wissenschaftsfonds