Nullstellensätze

Erhard Aichinger

Institute for Algebra
Johannes Kepler University Linz
Linz, Austria

Joint work with John R. Schmitt and Henry Zhan (Middlebury College, VT, USA)

Bern, May 2026

Some questions of the form:

"Is every A a B?"

Over the reals

Is every solution of $x^2 + y^2 = 2$ also a solution of

Over the reals

Is every solution of $x^2 + y^2 = 2$ also a solution of

$$2x^2y - x^3 - x^2 - xy^2 + 2x + 2y^3 - y^2 - 4y + 2 = 0\,?$$

Over the reals

Is every solution of $x^2 + y^2 = 2$ also a solution of

$$2x^2y - x^3 - x^2 - xy^2 + 2x + 2y^3 - y^2 - 4y + 2 = 0\,?$$

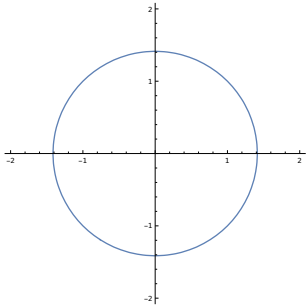
- Geometric Interpretation:

Over the reals

Is every solution of $x^2 + y^2 = 2$ also a solution of

$$2x^2y - x^3 - x^2 - xy^2 + 2x + 2y^3 - y^2 - 4y + 2 = 0\,?$$

- Geometric Interpretation:



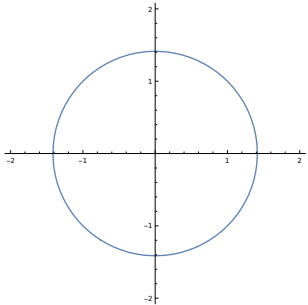
$x^2 + y^2 = 2.$

Over the reals

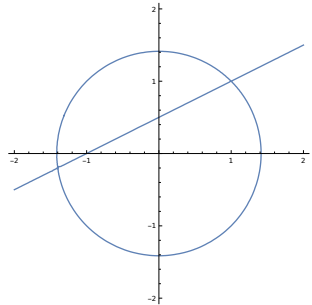
Is every solution of $x^2 + y^2 = 2$ also a solution of

$$2x^2y - x^3 - x^2 - xy^2 + 2x + 2y^3 - y^2 - 4y + 2 = 0\,?$$

- Geometric Interpretation:



$x^2 + y^2 = 2.$



$2x^2y - x^3 - x^2 - xy^2 + 2x + 2y^3 - y^2 - 4y + 2 = 0$

Over the reals

Is every solution of $x^2 + y^2 = 2$ also a solution of

$$2x^2y - x^3 - x^2 - xy^2 + 2x + 2y^3 - y^2 - 4y + 2 = 0\,?$$

- Arithmetic verification with Mathematica.

$$P = -2 + x^2 + y^2;$$

$$Q = 2 + 2x - x^2 - x^3 - 4y + 2x^2y - y^2 - xy^2 + 2y^3;$$

$$\text{GroebnerBasis}[\{P,\ Q * z - 1\}, \{x, y, z\}]$$

$$\{1\}$$

Over the reals

Is every solution of $x^2 + y^2 = 2$ also a solution of

$$2x^2y - x^3 - x^2 - xy^2 + 2x + 2y^3 - y^2 - 4y + 2 = 0\,?$$

- An arithmetic reason:

$$2x^2y - x^3 - x^2 - xy^2 + 2x + 2y^3 - y^2 - 4y + 2 = (-x + 2y - 1)(x^2 + y^2 - 2)$$

Over the reals

Is every solution of $x^2 + y^2 = 2$ also a solution of

$$2x^2y - x^3 - x^2 - xy^2 + 2x + 2y^3 - y^2 - 4y + 2 = 0\,?$$

- Ask GPT-5: The answer I got was:
  Yes.

  $$2x^2y - x^3 - x^2 - xy^2 + 2x + 2y^3 - y^2 - 4y + 2 = (-x + 2y - 1)\,(x^2 + y^2 - 2).$$

  Therefore, for any (x, y) with $x^2 + y^2 = 2$, the expression equals 0.

Over a commutative ring

Is every solution of $x^2 - y = y^2 = 0$ also a solution of

Over a commutative ring

Is every solution of $x^2 - y = y^2 = 0$ also a solution of $x = 0$?

Over a commutative ring

Is every solution of $x^2 - y = y^2 = 0$ also a solution of $x = 0$?

- Over the complex numbers:
  Yes. We obtain $x^4 = (x^2)^2 = y^2 = 0$.

Over a commutative ring

Is every solution of $x^2 - y = y^2 = 0$ also a solution of $x = 0$?

- In the commutative subring $\mathbb{R}[\begin{pmatrix} 0&1&0&0\\0&0&1&0\\0&0&0&1\\0&0&0&0 \end{pmatrix}]$ of $\mathrm{Mat}_2(\mathbb{R})$:

  No. Set

$$x := \begin{pmatrix} 0&1&0&0\\0&0&1&0\\0&0&0&1\\0&0&0&0 \end{pmatrix} \text{ and } y := \begin{pmatrix} 0&0&1&0\\0&0&0&1\\0&0&0&0\\0&0&0&0 \end{pmatrix}.$$

Over some integral domains:

Is every solution of $x^{17} + y^{17} = z^{17}$ a solution of $xyz = 0$?

- No on $\mathbb{R}$: $x = y = 1$, $z = 2^{\frac{1}{17}}$.
- Yes on $\mathbb{Q}$: By the confirmation for $n = 17$ of Fermat's Last Theorem.

Implications between identities

A question on implications:

Let R be a commutative ring with 1, and let $p_1, \ldots, p_m, q \in R[x_1, \ldots, x_n]$.
Questions:

- Is $\forall \boldsymbol{a} \in R^n : p_1(\boldsymbol{a}) = \cdots = p_m(\boldsymbol{a}) = 0 \Longrightarrow q(\boldsymbol{a}) = 0$ true?
- Is $\forall \boldsymbol{a} \in S^n : p_1(\boldsymbol{a}) = \cdots = p_m(\boldsymbol{a}) = 0 \Longrightarrow q(\boldsymbol{a}) = 0$ true in all rings S containing R?

We may ask for

- Characterization Theorems
- Effective methods / algorithms

A Strong Nullstellensatz describes when such implications (also called "quasi-identities" or "Horn clauses") are valid.

Existence of solutions

The question

$$\forall \boldsymbol{a} \in R^n : p_1(\boldsymbol{a}) = \cdots = p_m(\boldsymbol{a}) = 0 \Longrightarrow q(\boldsymbol{a}) = 0$$

becomes simpler if we set $q := 1$.

Then

$$\forall \boldsymbol{a} \in R^n : p_1(\boldsymbol{a}) = \cdots = p_m(\boldsymbol{a}) = 0 \Longrightarrow 1 = 0$$

holds iff $p_1 = \cdots = p_m = 0$ is unsolvable over R.

A theorem that guarantees the existence of solutions is called a Weak Nullstellensatz.

Weak Nullstellensätze

Universal algebraic methods.

Universal Weak Nullstellensatz (Karl Dörge 1967).

Let R be a commutative ring with 1, and let $p_1, \ldots, p_m \in R[x_1, \ldots, x_n]$.
Then $p_1 = \cdots = p_m = 0$ has a solution in some commutative ring with 1 extending $S \iff$ there is no $r \in R$ with $r \neq 0$ that can be written as $r = \sum_{i=1}^{m} h_i\, p_i$ with $h_i \in R[x_1, \ldots, x_n]$.

Universal algebraic methods.

Universal Weak Nullstellensatz (Karl Dörge 1967).

Let R be a commutative ring with 1, and let $p_1, \ldots, p_m \in R[x_1, \ldots, x_n]$.
Then $p_1 = \cdots = p_m = 0$ has a solution in some commutative ring with 1 extending $S \iff$ there is no $r \in R$ with $r \neq 0$ that can be written as $r = \sum_{i=1}^{m} h_i\, p_i$ with $h_i \in R[x_1, \ldots, x_n]$.

Why does $\Longrightarrow$ hold?

"Proof" by example: $x = xy + x - 1 = 0$ is unsolvable because

$$(y+1) \cdot x - 1 \cdot (xy + x - 1) = 1.$$

In general: Let $\boldsymbol{s}$ be a solution. Then
$\sum_{i=1}^{m} h_i(\boldsymbol{s}) p_i(\boldsymbol{s}) = \sum_{i=1}^{m} h_i(\boldsymbol{s}) \cdot 0 = 0,$ and thus $r = 0$.

Universal algebraic methods.

Universal Weak Nullstellensatz (Karl Dörge 1967).

Let R be a commutative ring with 1, and let $p_1, \ldots, p_m \in R[x_1, \ldots, x_n]$.
Then $p_1 = \cdots = p_m = 0$ has a solution in some commutative ring with 1 extending $S \iff$ there is no $r \in R$ with $r \neq 0$ that can be written as $r = \sum_{i=1}^{m} h_i\, p_i$ with $h_i \in R[x_1, \ldots, x_n]$.

The $\Longleftarrow$-direction is the deeper one.

Proof of $\Longleftarrow$:

- Let $I := \{\sum_{i=1}^{m} h_i\, p_i \mid h_i \in R[x_1, \ldots, x_n]\}$. This I is called the ideal generated by $p_1, \ldots, p_m$.
- Define the factor structure $S := R[x_1, \ldots, x_n]/I$.
- Then $(a_1, \ldots, a_n) := (x_1 + I, \ldots, x_n + I)$ is a solution of $p_1 = \cdots = p_m = 0$ in S.
- Since $I \cap R = \{0\}$, $\{r + I \mid r \in R\}$ is a subring of S isomorphic to R.

Compare with Hilbert's Theorem:

Universal Weak Nullstellensatz (Karl Dörge 1967).

Let R be a commutative ring with 1. Then $p_1 = \cdots = p_m = 0$ has a solution in some commutative ring with 1 extending $S \iff$ there is no $r \in R$ with $r \neq 0$ that can be written as $r = \sum_{i=1}^{m} h_i\, p_i$ with $h_i \in R[x_1, \ldots, x_n]$.

Hilbert's Weak Nullstellensatz (1893).

For $f_1, \ldots, f_s \in \mathbb{C}[x_1, \ldots, x_n]$, $f_1(\boldsymbol{x}) = \cdots = f_s(\boldsymbol{x}) = 0$ has a solution in $\mathbb{C}^n$ iff there are no $h_1, \ldots, h_s \in \mathbb{C}[\boldsymbol{x}]$ such that $1 = h_1 f_1 + \cdots h_s f_s$.

- Hilbert's Theorem asserts that the solutions are inside $\mathbb{C}$.
- The Universal Weak Nullstellensatz provides a solution in some extension ring $\mathbb{C}[\boldsymbol{x}]/I$ of $\mathbb{C}$.
- The "universal algebraic ideas" can be pushed to provide a solution in some extension field of $\mathbb{C}$.

Compare with Hilbert's Theorem:

Universal Weak Nullstellensatz (Karl Dörge 1967).

Let R be a commutative ring with 1. Then $p_1 = \cdots = p_m = 0$ has a solution in some commutative ring with 1 extending $S \iff$ there is no $r \in R$ with $r \neq 0$ that can be written as $r = \sum_{i=1}^{m} h_i\, p_i$ with $h_i \in R[x_1, \ldots, x_n]$.

Hilbert's Weak Nullstellensatz (1893).

For $f_1, \ldots, f_s \in \mathbb{C}[x_1, \ldots, x_n]$, $f_1(\boldsymbol{x}) = \cdots = f_s(\boldsymbol{x}) = 0$ has a solution in $\mathbb{C}^n$ iff there are no $h_1, \ldots, h_s \in \mathbb{C}[\boldsymbol{x}]$ such that $1 = h_1 f_1 + \cdots h_s f_s$.

- By "universal algebraic" ideas, we obtain a maximal ideal M such that we have a solution in $\mathbb{K} := \mathbb{C}[\boldsymbol{x}]/M$, which is a field.
- The fact that $\mathbb{C}[\boldsymbol{x}]/M$ is algebraic over $\mathbb{C}$ and hence equal to $\mathbb{C}$ needs some extra argument:

Compare with Hilbert's Theorem:

Universal Weak Nullstellensatz (Karl Dörge 1967).

Let R be a commutative ring with 1. Then $p_1 = \cdots = p_m = 0$ has a solution in some commutative ring with 1 extending $S \iff$ there is no $r \in R$ with $r \neq 0$ that can be written as $r = \sum_{i=1}^{m} h_i\, p_i$ with $h_i \in R[x_1, \ldots, x_n]$.

Hilbert's Weak Nullstellensatz (1893).

For $f_1, \ldots, f_s \in \mathbb{C}[x_1, \ldots, x_n]$, $f_1(\boldsymbol{x}) = \cdots = f_s(\boldsymbol{x}) = 0$ has a solution in $\mathbb{C}^n$ iff there are no $h_1, \ldots, h_s \in \mathbb{C}[\boldsymbol{x}]$ such that $1 = h_1 f_1 + \cdots h_s f_s$.

- By "universal algebraic" ideas, we obtain a maximal ideal M such that we have a solution in $\mathbb{K} := \mathbb{C}[\boldsymbol{x}]/M$, which is a field.
- The fact that $\mathbb{C}[\boldsymbol{x}]/M$ is algebraic over $\mathbb{C}$ needs some extra argument:
- For $\mathbb{C}$, there is an "ad hoc"-argument: If x_1 is not algebraic, then $(\frac{1}{x_1 - \alpha})_{\alpha \in \mathbb{C}}$ is linear independent in $\mathbb{K}$ of cardinality $2^{\aleph_0}$.

Compare with Hilbert's Theorem:

Universal Weak Nullstellensatz (Karl Dörge 1967).

Let R be a commutative ring with 1. Then $p_1 = \cdots = p_m = 0$ has a solution in some commutative ring with 1 extending $S \iff$ there is no $r \in R$ with $r \neq 0$ that can be written as $r = \sum_{i=1}^{m} h_i\, p_i$ with $h_i \in R[x_1, \ldots, x_n]$.

Hilbert's Weak Nullstellensatz (1893).

For $f_1, \ldots, f_s \in \mathbb{C}[x_1, \ldots, x_n]$, $f_1(\boldsymbol{x}) = \cdots = f_s(\boldsymbol{x}) = 0$ has a solution in $\mathbb{C}^n$ iff there are no $h_1, \ldots, h_s \in \mathbb{C}[\boldsymbol{x}]$ such that $1 = h_1 f_1 + \cdots h_s f_s$.

- By "universal algebraic" ideas, we obtain a maximal ideal M such that we have a solution in $\mathbb{K} := \mathbb{C}[\boldsymbol{x}]/M$, which is a field.
- The fact that $\mathbb{C}[\boldsymbol{x}]/M$ is algebraic over $\mathbb{C}$ needs some extra argument:
- Over arbitrary fields, we need to speak about Noether normalization and integral extensions.

Strong Nullstellensätze

Universal algebraic methods

Universal Strong Nullstellensatz.

Let R be a commutative ring with 1. Then the following are equivalent:

1. For all commutative rings S with 1 that contain a homomorphic image of R as a subring, we have

$$\forall \boldsymbol{a} \in S^n : p_1(\boldsymbol{a}) = \cdots = p_m(\boldsymbol{a}) = 0 \Longrightarrow q(\boldsymbol{a}) = 0.$$

2. There are $h_1, \ldots, h_m \in R[\boldsymbol{x}]$ such that $q = \sum_{i=1}^{m} h_i p_i$.

Proof of (1)⇒(2):

- Let $S := R[x_1, \ldots, x_n]/\langle p_1, \ldots, p_m \rangle = R[\boldsymbol{x}]/I$.
- Then set $a_i := x_i + I$.
- Then $p_i(a_1, \ldots, a_n) = p(x_i + I, \ldots, x_n + I) = p(x_1, \ldots, x_n) + I = 0 + I$.
- Hence $0 = q(a_1, \ldots, a_n)$, and thus $q(x_1, \ldots, x_n) \in I$.

Universal algebraic methods

Universal Strong Nullstellensatz.

Let R be a commutative ring with 1. Then the following are equivalent:

1. For all commutative rings S with 1 that contain a homomorphic image of R as a subring, we have

$$\forall \boldsymbol{a} \in S^n : p_1(\boldsymbol{a}) = \cdots = p_m(\boldsymbol{a}) = 0 \Longrightarrow q(\boldsymbol{a}) = 0.$$

2. There are $h_1, \ldots, h_m \in R[\boldsymbol{x}]$ such that $q = \sum_{i=1}^{m} h_i p_i$.

Proof of (1)⇒(2) for logicians:

- Let $\mathcal{V}$ be the variety of commutative rings with 1.
- Adjoin a constant symbol $\bar{r}$ for every $r \in R$ and $\bar{x}_i$ for all $i \in \{1, \ldots, n\}$, and let $\mathcal{V}_R$ be the variety of these augmented algebras.
- Consider the subvariety $\mathrm{Mod}(\{p_i(\bar{x}_1, \ldots, \bar{x}_n) \approx 0 \mid i \in \underline{n}\})$.

Universal algebraic methods

Universal Strong Nullstellensatz.

Let R be a commutative ring with 1. Then the following are equivalent:

1. For all commutative rings S with 1 that contain a homomorphic image of R as a subring, we have

$$\forall \boldsymbol{a} \in S^n : p_1(\boldsymbol{a}) = \cdots = p_m(\boldsymbol{a}) = 0 \Longrightarrow q(\boldsymbol{a}) = 0.$$

2. There are $h_1, \ldots, h_m \in R[\boldsymbol{x}]$ such that $q = \sum_{i=1}^{m} h_i p_i$.

Proof of (1)⇒(2) for logicians:

- By the assumption, $q(\bar{x}_1, \ldots, \bar{x}_n) \approx 0 \in \mathrm{Th}(\mathrm{Mod}(\{p_i(\bar{x}_1, \ldots, \bar{x}_n) \approx 0 \mid i \in \underline{n}\}))$.
- By [Birkhoff 1935], $(q, 0)$ lies in the fully invariant congruence generated by $(p_1, 0), \ldots, (p_n, 0)$ in the free algebra in $\mathcal{V}_R$ over the empty set.

Universal algebraic methods

Universal Strong Nullstellensatz.

Let R be a commutative ring with 1. Then the following are equivalent:

1. For all commutative rings S with 1 that contain a homomorphic image of R as a subring, we have

$$\forall \boldsymbol{a} \in S^n : p_1(\boldsymbol{a}) = \cdots = p_m(\boldsymbol{a}) = 0 \Longrightarrow q(\boldsymbol{a}) = 0.$$

2. There are $h_1, \ldots, h_m \in R[\boldsymbol{x}]$ such that $q = \sum_{i=1}^{m} h_i p_i$.

Proof of (1)⇒(2) for logicians:

- By the assumption, $q(\bar{x}_1, \ldots, \bar{x}_n) \approx 0 \in \mathrm{Th}(\mathrm{Mod}(\{p_i(\bar{x}_1, \ldots, \bar{x}_n) \approx 0 \mid i \in \underline{n}\}))$.
- By [Birkhoff 1935], $(q, 0)$ lies in the ~~fully invariant~~ congruence generated by $(p_1, 0), \ldots, (p_n, 0)$ in the free algebra in $\mathcal{V}_R$ over the empty set.

Classical Strong Nullstellensätze

Hilbert's Strong Nullstellensatz (Hilbert 1893).

Let $f_1, \ldots, f_s, g \in \mathbb{C}[x_1, \ldots, x_n]$. The following are equivalent:

1. $\forall \boldsymbol{a} \in \mathbb{C}^n \ : \ f_1(\boldsymbol{a}) = \cdots = f_s(\boldsymbol{a}) = 0 \Longrightarrow g(\boldsymbol{a}) = 0.$
2. $\neg \exists \boldsymbol{a} \in \mathbb{C}^n, v \in \mathbb{C} \ : \ f_1(\boldsymbol{a}) = \cdots = f_s(\boldsymbol{a}) = g(\boldsymbol{a}) \cdot v - 1 = 0.$
3. there are $h_1, \ldots, h_s \in \mathbb{C}[\boldsymbol{x}]$ and $r \in \mathbb{N}$ such that $g^r = h_1 f_1 + \cdots h_s f_s$.

Classical Nullstellensätze

Hilbert's Strong Nullstellensatz for arbitrary fields.

Let $\mathbb{F}$ be a field, and let $f_1, \ldots, f_s, g \in \mathbb{F}[x_1, \ldots, x_n]$. If there are no $h_1, \ldots, h_s \in \mathbb{F}[\boldsymbol{x}]$ and $r \in \mathbb{N}$ such that $g^r = h_1 f_1 + \cdots h_s f_s$, then there is an algebraic extension field $\mathbb{K}$ of $\mathbb{F}$ and $\boldsymbol{a} \in \mathbb{K}^n$ such that

$$f_1(\boldsymbol{a}) = \cdots = f_s(\boldsymbol{a}) = 0 \text{ and } g(\boldsymbol{a}) \neq 0.$$

"Perfect Nullstellensatz" (Salomon, Shalit, Shamovich 2018.)

Let $\mathbb{F}$ be a field, and let $f_1, \ldots, f_s, g \in \mathbb{F}[x_1, \ldots, x_n]$. If there are no $h_1, \ldots, h_s \in \mathbb{F}[\boldsymbol{x}]$ such that $g = h_1 f_1 + \cdots h_s f_s$, then there is a commutative ring $\mathbb{K}$ extending $\mathbb{F}$ such that $\dim_{\mathbb{F}}(\mathbb{K})$ is finite and there is $\boldsymbol{a} \in \mathbb{K}^n$ such that

$$f_1(\boldsymbol{a}) = \cdots = f_s(\boldsymbol{a}) = 0 \text{ and } g(\boldsymbol{a}) \neq 0.$$

Effectiveness

Are there algorithms to decide the validity of quasi-identities?

- $\mathbb{Z}$:
- $\mathbb{R}, \mathbb{C}$:
- Finite commutative ring R:

Effectiveness

Are there algorithms to decide the validity of quasi-identities?

- $\mathbb{Z}$:
  - $\forall \boldsymbol{a} \in \mathbb{Z}^n : p_1(\boldsymbol{a}) = \cdots = p_m(\boldsymbol{a}) = 0 \Longrightarrow q(\boldsymbol{a}) = 0$:
    Undecidable (Matiyasevich 1970).
  - *For all commutative rings R with 1 containing $\mathbb{Z}$ and* $\forall \boldsymbol{a} \in R^n : p_1(\boldsymbol{a}) = \cdots = p_m(\boldsymbol{a}) = 0 \Longrightarrow q(\boldsymbol{a}) = 0$:
    Decidable. Use Gröbner bases in $\mathbb{Z}[x_1, \ldots, x_n]$ to determine whether $\langle p_1, \ldots, p_m \rangle \cap \mathbb{Z} \neq \{0\}$ or $q \in \langle p_1, \ldots, p_m \rangle$. (Kandri-Rody and Kapur 1988; Aichinger 2024).
  - $\forall \boldsymbol{a} \in \mathbb{Q}^n : p_1(\boldsymbol{a}) = \cdots = p_m(\boldsymbol{a}) = 0 \Longrightarrow q(\boldsymbol{a}) = 0$: Unknown.
- $\mathbb{R}, \mathbb{C}$:
- Finite commutative ring R:

Effectiveness

Are there algorithms to decide the validity of quasi-identities?

- $\mathbb{Z}$:
- $\mathbb{R}, \mathbb{C}$:
  - $\forall \boldsymbol{a} \in \mathbb{R}^n : p_1(\boldsymbol{a}) = \cdots = p_m(\boldsymbol{a}) = 0 \Longrightarrow q(\boldsymbol{a}) = 0$: Decidable. The first order theory of the reals is decidable (Tarski 1948, Collins 1975).
  - $\forall \boldsymbol{a} \in \mathbb{C}^n : p_1(\boldsymbol{a}) = \cdots = p_m(\boldsymbol{a}) = 0 \Longrightarrow q(\boldsymbol{a}) = 0$: Decidable. Use Hilbert + Gröbner bases (Buchberger 1965) or Hilbert + (Herrmann 1926).
- Finite commutative ring R:

Effectiveness

Are there algorithms to decide the validity of quasi-identities?

- $\mathbb{Z}$:
- $\mathbb{R}, \mathbb{C}$:
- Finite commutative ring R:
  $\forall \boldsymbol{a} \in R^n : p_1(\boldsymbol{a}) = \cdots = p_m(\boldsymbol{a}) = 0 \Longrightarrow q(\boldsymbol{a}) = 0$:

Effectiveness

Are there algorithms to decide the validity of quasi-identities?

- $\mathbb{Z}$:
- $\mathbb{R}, \mathbb{C}$:
- Finite commutative ring R:
  $\forall \boldsymbol{a} \in R^n : p_1(\boldsymbol{a}) = \cdots = p_m(\boldsymbol{a}) = 0 \Longrightarrow q(\boldsymbol{a}) = 0$: clearly decidable.

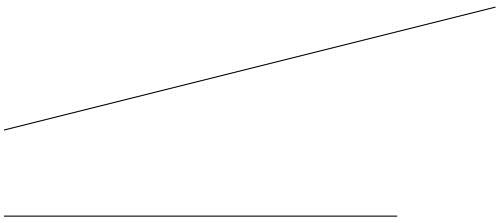
Effectiveness

Are there algorithms to decide the validity of quasi-identities?

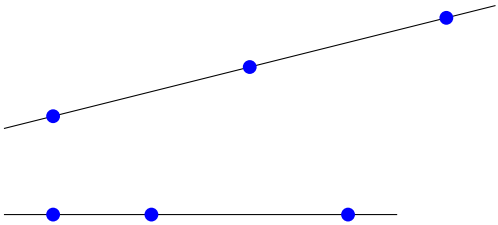
- $\mathbb{Z}$:
- $\mathbb{R}, \mathbb{C}$:
- Finite ~~commuatative~~ ring R:
  $\forall \boldsymbol{a} \in R^n : p_1(\boldsymbol{a}) = \cdots = p_m(\boldsymbol{a}) = 0 \Longrightarrow q(\boldsymbol{a}) = 0$: clearly decidable.
  Complexity: **P** for rings with $R \cdot R = 0$, **NP**-complete for all other rings (Aichinger and Grünbacher 2023).

Automated Geometrical Theorem Proving

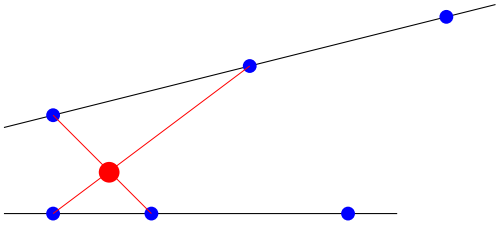
Geometrical Theorem Proving



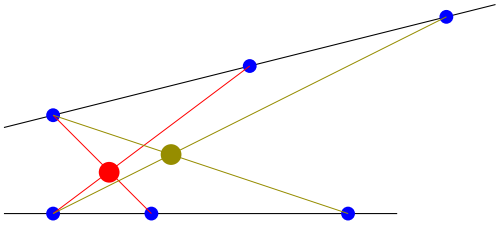
Geometrical Theorem Proving



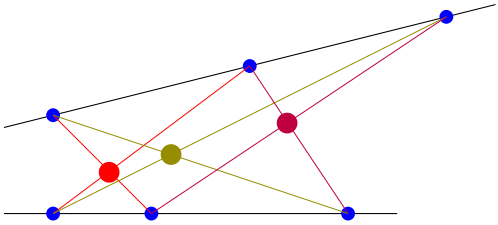
Geometrical Theorem Proving



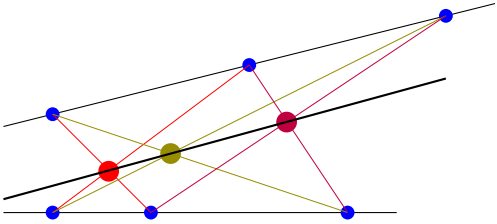
Geometrical Theorem Proving



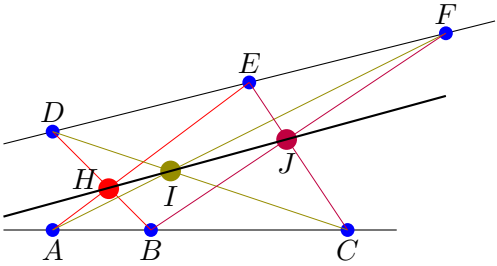
Geometrical Theorem Proving



Geometrical Theorem Proving



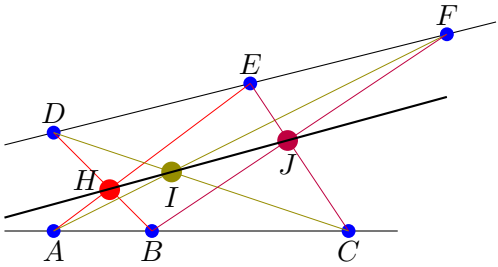
Geometrical Theorem Proving



Theorem (Pappus of Alexandria, ∼320) Let $A, B, C, D, E, F, H, I, J$ points in the plane such that each of the following triples is collinear:
(A, B, C), (D, E, F), (A, H, E), (D, H, B), (D, I, C), (A, I, F), (E, J, C), (B, J, F).

Then (H, I, J) are collinear.

Geometrical Theorem Proving



Theorem (Pappus of Alexandria, ∼320)
Let $A, B, C, D, E, F, H, I, J$ points in the plane such that each of the following triples is collinear:
(A, B, C), (D, E, F), (A, H, E), (D, H, B), (D, I, C), (A, I, F), (E, J, C), (B, J, F).
Assume that (A, B, D) and (A, B, E) are not collinear.

Then (H, I, J) are collinear.

Geometrical Theorem Proving

Theorem. Suppose that (A, B, C), (D, E, F), (A, H, E), (D, H, B), (D, I, C), (A, I, F), (E, J, C), (B, J, F) are collinear, and that (A, B, D) and (A, B, E) are not collinear.
Then (H, I, J) is collinear.

Proof:

- We try to construct a counterexample.
- We coordinatize points with pairs of real numbers:
  $A = (a_1, a_2), \ldots, J = (j_1, j_2)$.
- $C(u_1, u_2, v_1, v_2, w_1, w_2) := \det(\begin{pmatrix} u_1 & u_2 & 1 \\ v_1 & v_2 & 1 \\ w_1 & w_2 & 1 \end{pmatrix}) =$
  $-u_2v_1 + u_1v_2 + u_2w_1 - v_2w_1 - u_1w_2 + v_1w_2$ has the property:
  $C(u_1, u_2, v_1, v_2, w_1, w_2) = 0$ iff $(\binom{u_1}{u_2}, \binom{v_1}{v_2}, \binom{w_1}{w_2})$ is collinear.

Geometrical Theorem Proving

Theorem. Suppose that (A, B, C), (D, E, F), (A, H, E), (D, H, B), (D, I, C), (A, I, F), (E, J, C), (B, J, F) are collinear, and that (A, B, D) and (A, B, E) are not collinear.
Then (H, I, J) is collinear.

Proof:

- A counterexample has to satisfy

$$C(a_1, a_2, b_1, b_2, c_1, c_2) = \cdots = C(b_1, b_2, j_1, j_2, f_1, f_2) = 0,$$
$$C(a_1, a_2, b_1, b_2, d_1, d_2) \neq 0,\ C(a_1, a_2, b_1, b_2, e_1, e_2) \neq 0,$$
$$C(h_1, h_2, i_1, i_2, j_1, j_2) \neq 0.$$

Geometrical Theorem Proving

Theorem. Suppose that (A, B, C), (D, E, F), (A, H, E), (D, H, B), (D, I, C), (A, I, F), (E, J, C), (B, J, F) are collinear, and that (A, B, D) and (A, B, E) are not collinear.
Then (H, I, J) is collinear.

Proof:

- A counterexample has to satisfy

$$C(a_1, a_2, b_1, b_2, c_1, c_2) = \cdots = C(b_1, b_2, j_1, j_2, f_1, f_2) = 0,$$
$$C(a_1, a_2, b_1, b_2, d_1, d_2) \cdot z_1 = 1,\ C(a_1, a_2, b_1, b_2, e_1, e_2) \neq 0,$$
$$C(h_1, h_2, i_1, i_2, j_1, j_2) \neq 0.$$

Geometrical Theorem Proving

Theorem. Suppose that (A, B, C), (D, E, F), (A, H, E), (D, H, B), (D, I, C), (A, I, F), (E, J, C), (B, J, F) are collinear, and that (A, B, D) and (A, B, E) are not collinear.
Then (H, I, J) is collinear.

Proof:

- A counterexample has to satisfy

$$C(a_1, a_2, b_1, b_2, c_1, c_2) = \cdots = C(b_1, b_2, j_1, j_2, f_1, f_2) = 0,$$
$$C(a_1, a_2, b_1, b_2, d_1, d_2) \cdot z_1 = 1,\ C(a_1, a_2, b_1, b_2, e_1, e_2) \cdot z_2 = 1,$$
$$C(h_1, h_2, i_1, i_2, j_1, j_2) \cdot z_3 = 1.$$

- The theorem holds if and only if this **system of equations** has no solution in the real numbers.

Geometrical Theorem Proving

We use the computer algebra system “Mathematica”.

pappus.nb * - Wolfram Mathematica 12.0

File Edit Insert Format Cell Graphics Evaluation Palettes Window Help

In[40]:=
```
Collinear[P1_, P2_, P3_] := Det[{P1, P2, P3}];
AA = {a1, a2, 1}; BB = {b1, b2, 1}; CC = {c1, c2, 1};
DD = {d1, d2, 1}; EE = {e1, e2, 1}; FF = {f1, f2, 1};
HH = {h1, h2, 1}; II = {i1, i2, 1}; JJ = {j1, j2, 1};
TheSystem = {Collinear[AA, BB, CC], Collinear[DD, EE, FF], Collinear[AA, HH, EE], Collinear[DD, HH, BB],
  Collinear[DD, II, CC], Collinear[AA, II, FF], Collinear[EE, JJ, CC], Collinear[BB, JJ, FF],
  (*Non degenerate*)
  Collinear[AA, BB, DD] * z1 - 1, Collinear[AA, BB, EE] * z2 - 1,
  (*Conclusion*)
  Collinear[HH, II, JJ] * z3 - 1}
```

Out[44]=
```
{-a2 b1 + a1 b2 + a2 c1 - b2 c1 - a1 c2 + b1 c2,
 -d2 e1 + d1 e2 + d2 f1 - e2 f1 - d1 f2 + e1 f2, a2 e1 - a1 e2 - a2 h1 + e2 h1 + a1 h2 - e1 h2,
 -b2 d1 + b1 d2 + b2 h1 - d2 h1 - b1 h2 + d1 h2, -c2 d1 + c1 d2 + c2 i1 - d2 i1 - c1 i2 + d1 i2,
 a2 f1 - a1 f2 - a2 i1 + f2 i1 + a1 i2 - f1 i2, -c2 e1 + c1 e2 + c2 j1 - e2 j1 - c1 j2 + e1 j2,
 b2 f1 - b1 f2 - b2 j1 + f2 j1 + b1 j2 - f1 j2, -1 + (-a2 b1 + a1 b2 + a2 d1 - b2 d1 - a1 d2 + b1 d2) z1,
 -1 + (-a2 b1 + a1 b2 + a2 e1 - b2 e1 - a1 e2 + b1 e2) z2, -1 + (-h2 i1 + h1 i2 + h2 j1 - i2 j1 - h1 j2 + i1 j2) z3}
```

In[45]:=
```
GroebnerBasis[TheSystem] // Timing
```

Out[45]=
```
{2.02533, {1}}
```

absolute timing | extract time | extract result | clear cache first

200%

Geometrical Theorem Proving

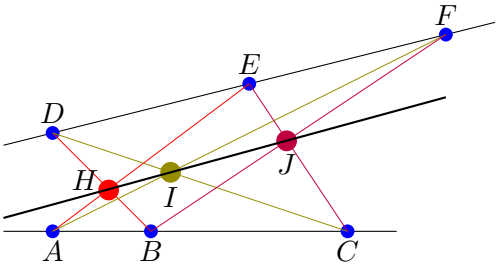
Conclusions

- There is no counterexample to Pappus's Theorem, not even in the complex plane $\mathbb{C}^2$.
- Hence (this version) of Pappus's Theorem holds.
- Similar proofs for: Desargues, Ceva, Menelaus, ...
- **Algebraic** way to decide which first order formulae hold in the relational structure

$$\mathbf{L} = (\mathbb{C}^2, \mathrm{IsCollinearTriple}(x, y, z))$$

by **solving systems of polynomial equations**.
What about **other axiomatizations** or **calculi** for this structure $\mathbf{L}$?

Geometrical Theorem Proving : degenerated cases

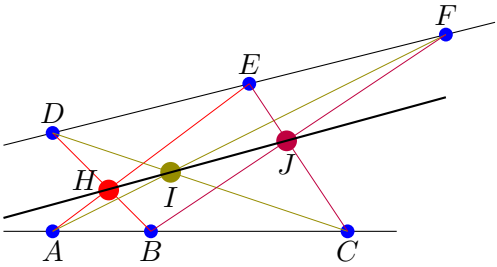


Conjecture

Let $A, B, C, D, E, F, H, I, J$ points in the plane such that each of the following triples is collinear:
(A, B, C), (D, E, F), (A, H, E), (D, H, B), (D, I, C), (A, I, F), (E, J, C), (B, J, F).

Then (H, I, J) are collinear.

Geometrical Theorem Proving : degenerated cases

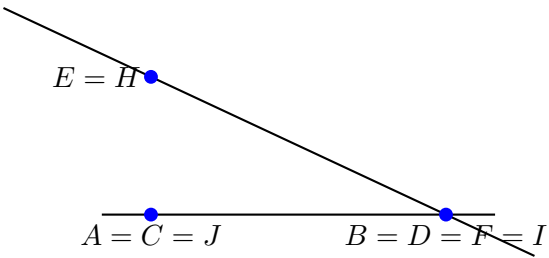


Conjecture

Let $A, B, C, D, E, F, H, I, J$ points in the plane such that each of the following triples is collinear:
(A, B, C), (D, E, F), (A, H, E), (D, H, B), (D, I, C), (A, I, F), (E, J, C), (B, J, F).
Assume that ~~(A, B, D) and~~ (A, B, E) are is not collinear.

Then (H, I, J) are collinear.

Geometrical Theorem Proving : degenerated cases



Conjecture

Let $A, B, C, D, E, F, H, I, J$ points in the plane such that each of the following triples is collinear:
(A, B, C), (D, E, F), (A, H, E), (D, H, B), (D, I, C), (A, I, F), (E, J, C), (B, J, F).
Assume that ~~(A, B, D) and~~ (A, B, E) are is not collinear.

Then (H, I, J) are collinear.

This conjecture is wrong.

Finite structures

A Nullstellensatz for finite fields

Theorem (Terjanian 1966).

For $f_1, \ldots, f_r, g \in \mathbb{F}_q[x_1, \ldots, x_n]$, the quasi-identity

$$\forall \boldsymbol{x} \in {\mathbb{F}_q}^n \ : \ f_1(\boldsymbol{x}) = \cdots = f_s(\boldsymbol{x}) = 0 \Longrightarrow g(\boldsymbol{x}) = 0$$

holds in $\mathbb{F}_q$ iff there are $h_1, \ldots, h_r, b_1, \ldots, b_n \in \mathbb{F}_q[\boldsymbol{x}]$ such that

$$g = h_1 f_1 + \cdots h_r f_r + b_1 \cdot (x_1^q - x_1) + \cdots + b_n \cdot (x_n^q - x_n).$$

Theorem (Finitesatz, P. Clark 2014).

Let $\mathbb{F}$ be a field, let $f_1, \ldots, f_r, g \in \mathbb{F}[x_1, \ldots, x_n]$, and let $X \subseteq_{\text{fin}} \mathbb{F}^n$. Then g vanishes on all common zeros of $f_1, \ldots, f_n$ in X iff there are $h_1, \ldots, h_s, h \in \mathbb{F}[\boldsymbol{x}]$ such that

$$g = h_1 f_1 + \cdots h_r f_r + h \text{ and } h \text{ vanishes on } X.$$

Combinatorial Nullstellensätze

Alon's Combinatorial Nullstellensatz I

Theorem (Alon's Nullstellensatz I).

Let $\mathbb{K}$ be a field, $S = \bigtimes_{i=1}^{n} S_i$ with $S_i \subseteq_{\text{fin}} \mathbb{K}$. Then $f \in \mathbb{K}[\boldsymbol{x}]$ vanishes on S iff there are $h_1, \ldots, h_s \in \mathbb{K}[\boldsymbol{x}]$ such that

$$f = h_1 g_1 + \cdots + h_r g_r,$$

where $g_i = \prod_{a \in S_i} (x_i - a)$ and $\deg(h_i g_i) \leq \deg(f)$ for all i.

Alon's Combinatorial Nullstellensatz II

Noga Alon's Combinatorial Nullstellensatz II 1999

Let $\mathbb{K}$ be a field, $S = \bigtimes_{i=1}^{n} S_i$ with $S_i \subseteq_{\text{fin}} \mathbb{K}$.
Let $f \in \mathbb{K}[\boldsymbol{x}]$ be such that f contains a monomial $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ with $\alpha_i < |S_i|$ for all i.
If for all monomials $x_1^{\gamma_1} \cdots x_n^{\gamma_n}$ of f with $\alpha \neq \gamma$ we have

$$\sum_{i=1}^{n} \gamma_i \leq \sum_{i=1}^{n} \alpha_i, \qquad \text{(Alon's Condition)}$$

then there is $\boldsymbol{s} \in S$ with $f(\boldsymbol{s}) \neq 0$.

Application: Let $H_1, \ldots, H_m$ be hyperplanes in $\mathbb{R}^n$ with $\{0,1\}^n \setminus \{\mathbf{0}\} \subseteq H_1 \cup \cdots \cup H_m$ and $\mathbf{0} \notin H_1 \cup \cdots \cup H_m$. Then $m \geq n$.

Alon's Combinatorial Nullstellensatz II

Noga Alon's Combinatorial Nullstellensatz II 1999

Let $\mathbb{K}$ be a field, $S = \bigtimes_{i=1}^{n} S_i$ with $S_i \subseteq_{\text{fin}} \mathbb{K}$.
Let $f \in \mathbb{K}[\boldsymbol{x}]$ be such that f contains a monomial $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ with $\alpha_i < |S_i|$ for all i.
If for all monomials $x_1^{\gamma_1} \cdots x_n^{\gamma_n}$ of f with $\alpha \neq \gamma$ we have

$$\sum_{i=1}^{n} \gamma_i \leq \sum_{i=1}^{n} \alpha_i, \qquad \text{(Alon's Condition)}$$

then there is $\boldsymbol{s} \in S$ with $f(\boldsymbol{s}) \neq 0$.

Improvements: Replace (Alon's Condition) with weaker conditions.

Improved Combinatorial Nullstellensatz II

Noga Alon's Combinatorial Nullstellensatz II 1999

Suppose that $f \in \mathbb{K}[\boldsymbol{x}]$ contains a monomial $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ with $\alpha_i < |S_i|$ for all i.
If for all monomials $x_1^{\gamma_1} \cdots x_n^{\gamma_n}$ of f with $\alpha \neq \gamma$ we have

$$\sum_{i=1}^{n} \gamma_i \leq \sum_{i=1}^{n} \alpha_i, \qquad \text{(Alon's Condition)}$$

then there is $\boldsymbol{s} \in S$ with $f(\boldsymbol{s}) \neq 0$.

Improvements: Replace (Alon's Condition) with the following weaker conditions.

1. (Tao-Vu-Lasoń's Condition 2006) $\exists i \in \underline{n} : \gamma_i \in [0, \alpha_i - 1]$.
2. (Schauz's Condition 2008) $\exists i \in \underline{n} : \gamma_i \in [0, \alpha_i - 1] \cup [\alpha_i + 1, |S_i| - 1]$.

Structured Grids

Structured Grids

Definition (Nica 2023).
$S \subseteq_{\text{fin}} \mathbb{K}$ is λ-null $:\Leftrightarrow$ in $\prod_{a \in S}(x-a)$, the coefficients of $x^{|S|-1}, \ldots, x^{|S|-\lambda}$ are zero.

Examples

- Every finite S is 0-null.
- $\{x \in \mathbb{C} \mid x^n = 1\}$ is $n-1$-null.
- $\{0\}$, $\varnothing$ are μ-null for all $\mu \in \mathbb{N}$.
- S is 1-null if $\sum_{a \in S} a = 0$.

Nica's Combinatorial Nullstellensatz II 2023

Let $\mathbb{K}$ be a field, $S = \bigtimes_{i=1}^{n} S_i$ such that $S_i \subseteq_{\text{fin}} \mathbb{K}$ and S_i **is λ_i-null.**
Let $f \in \mathbb{K}[\boldsymbol{x}]$ be such that f contains a monomial $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ with $\alpha_i < |S_i|$ for all i.
If for all monomials $x_1^{\gamma_1} \cdots x_n^{\gamma_n}$ of f with $\alpha \neq \gamma$ we have

$$\sum_{i=1}^{n} \gamma_i \leq \min(\lambda_1, \ldots, \lambda_n) + \sum_{i=1}^{n} \alpha_i, \qquad \text{(Nica's Condition)}$$

then there is $\boldsymbol{s} \in S$ with $f(\boldsymbol{s}) \neq 0$.

Improvements:

- (Aichinger-Schmitt-Zhan's Condition)
  $\exists i \in \underline{n} : \gamma_i \in [0, \alpha_i - 1] \cup [\alpha_i + 1, \max(|S_i| - 1, \alpha_i + \lambda_i)]$.

Comparison of the Nullstellensätze

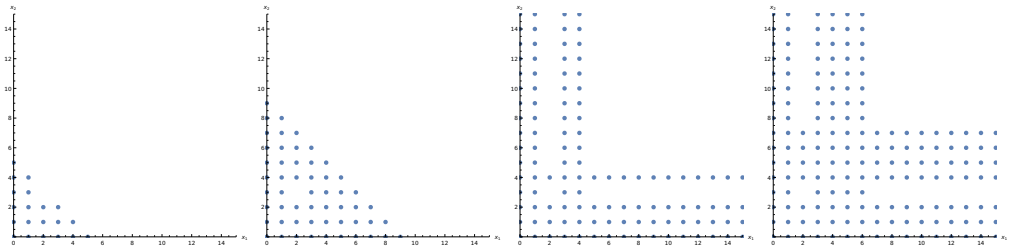
These theorems have in common:

- they guarantee a nonzero in a grid.
- the condition ensuring this is:
  1. there is a monomial $\boldsymbol{x}^{\alpha}$ in f with $\alpha_i < |S_i|$ for all i.
  2. all other monomials $\boldsymbol{x}^{\gamma}$ of f are innocuous.

The more monomials one can declare innocuous, the better.

Comparison of the Nullstellensätze

Example. $S = \{(a, b) \in \mathbb{C}^2 \mid a^5 = b^5 = 1\}$, $\lambda_1 = \lambda_2 = 4$. Suppose f contains the monomial $x_1^2 x_2^3$. Then the following monomials are declared innocuous:



Alon Nica Schauz EA-Schmitt-Zhan

Figure: $x_1^2 x_2^3$ + any linear combinations of the dotted monomials does not vanish on $S = \{(x_1, x_2) \in \mathbb{C}^2 \mid x_1^5 = x_2^5 = 1\}$.

Improved Nullstellensätze

Generalisations and Improvements:

- Multiplicity: $\boldsymbol{c}$ is a t-fold zero of f if all monomials of $f' := f(c_1 + x_1, \ldots, c_n + x_n)$ have total degree at least t. Ball and Serra (2009) provide theorems with bottom line:
  "Then there is $\boldsymbol{s} \in S$ such that $\boldsymbol{s}$ is not a t-fold zero of f."
- Multisets (Kós and Rónyai 2012).
- Beyond grids: Punctured Grids $X \setminus Y$, where X, Y are grids. (Ball and Serra 2009)
- Structured grids: Use the property that an edge of the grid is λ-null. (Nica 2023)

Our recent manuscript provides combinations of these, for example a

Structured Nullstellensatz for **punctured** grids.

Manuscript: E.Aichinger, J.R.Schmitt, H.Zhan, *Structured and punctured Nullstellensätze*, arxiv 2025.

Proofs

Proof Ideas

- Given $S \subseteq_{\text{fin}} \mathbb{F}^n$, find generators G of the ideal $\mathbb{I}(S) = \{f \in \mathbb{K}[\boldsymbol{x}] \mid f(\boldsymbol{a}) = 0 \text{ for all } \boldsymbol{a} \in S\}$.
- We want to show that $f \notin \mathbb{I}(S)$.
- Show that $\boldsymbol{x}^\alpha$ cannot disappear during multivariate polynomial division by G because
  - $\boldsymbol{x}^\alpha$ cannot be reduced by G.
  - All other monomials $\boldsymbol{x}^\gamma$ cannot produce $\boldsymbol{x}^\alpha$ in the course of the division – not in the first and not in any further step.
- f has nonzero remainder by G: Then $f \notin \langle G \rangle$ if G is a Gröbner basis.
- Use the S-Polynomial Theorem (Buchberger 1965) to show that G is indeed a Gröbner basis.