

(Not only commutative) Gröbner bases in Magma

Magmalena Wiertel

March 3, 2026

Finitely presented algebras - one sided ideals

```
1 > K := RationalField();
2 > F<x, y, z> := FreeAlgebra(K, 3);
3 > B := [x^2 - y*z, x*y - y*z, y*x - z^2, y^3 - x*z];
4 > I := ideal<F | B>;
5 Two-sided ideal of Free associative algebra of rank 3 over Rational
  Field
6 Order: Non-commutative Graded Lexicographical
7 Variables: x, y, z
```

It is also possible to construct one-sided ideals

```
1 > Il := lideal<F | B>;
2 > Ir := rideal<F | B>;
3 Left ideal of Free associative algebra of rank 3 over Rational Field
4 Right ideal of Free associative algebra of rank 3 over Rational
  Field
5
```

Basis?

```
1 > K := RationalField();
2 > F<x, y> := FreeAlgebra(K, 2);
3 > B := [x^2 + y^2];
4 > I := ideal<F | B> ;
5 > Basis(I);
```

gives the following

```
1 [
2 x^2 + y^2
3 ]
```

Admissible orders

An admissible order on $\langle x_1, \dots, x_n \rangle$ is any relation \geq on the set of monomials such that

- ▶ \geq is linear order;
- ▶ if $q \geq p$ and $qr \geq pr$ and $sq \geq sp$ for all monomials p, q, r, s ;
- ▶ \geq is well-ordered.

Let $f = \sum_{\alpha} a_{\alpha} x^{\alpha}$ be a nonzero noncommutative polynomial in $K\langle x_1, \dots, x_n \rangle$, with $a_{\alpha} \in K^*$ and let \geq be an admissible order. **The leading term** of f is

$$LT(f) := a_{\alpha} x^{\alpha} \text{ such that } x^{\alpha} = \max\{x_{\alpha}^a \mid x_{\alpha}^a \neq 0\}.$$

Order of monomials

Magma supports only the noncommutative degree-lexicographical order on the set of monomials, which first compares degrees and then uses a lexicographical order.

```
1 >K := RationalField();
2 >F<x, y, z> := FreeAlgebra(K, 3);
3 >rels := [x^2 + y^2];
4 >I := ideal <F | rels>;
5 Two-sided ideal of Free associative algebra of rank 3 over Rational
  Field
6 Order: Non-commutative Graded Lexicographical
7 Variables: x, y, z
8 Homogeneous
```

In the above example

$$1 < z < y < x < z^2 < zy < zx < yz < y^2 < yx < xz < xy < x^2 < \dots$$

Change of the order on generators

```
1 >F<z, y, x> := FreeAlgebra(K, 3);
2 >J := ideal <F | rels>;
3 Two-sided ideal of Free associative algebra of rank 3 over Rational
  Field
4 Order: Non-commutative Graded Lexicographical
5 Variables: z, y, x
```

Noncommutative Gröbner basis

Let $A = K\langle x_1, \dots, x_n \rangle$ with admissible order \succcurlyeq .

Definition

Let $I \subset K\langle x_1, \dots, x_n \rangle$ be an ideal. We call a subset $G \subset I$ a Gröbner basis of I , if G generates I and

$$\langle LT(G) \rangle = \langle LT(I) \rangle.$$

Elements of

$$N = \{w \in \langle x_1, \dots, x_n \rangle \mid w \text{ is not the leading term of any element of } I\}$$

are called **normal words** with respect to I .

Definition

If additionally G is a minimal generating set of $LT(G)$, leading monomials have coefficient 1 and $g - LT(g) \in \text{span}N$ for all $g \in G$, then G is a **reduced Gröbner basis**.

Theorem

If G is Gröbner basis of $I \subseteq A$, then as a vector spaces

$$A = I \oplus \text{span}N.$$

Example

Let $K\langle x, y \rangle$ with degree-lexicographical order on $K\langle x, y \rangle$ with $x > y$ and

$$I = (x^2 + y^2).$$

Then $G := \{x^2 + y^2\}$ is not a Gröbner basis of I , because

$$x(x^2 + y^2) - (x^2 + y^2)x = xy^2 - y^2x,$$

so $xy^2 \in \langle LT(I) \rangle \setminus \langle x^2 \rangle$.

$\{x^2 + y^2, xy^2 - y^2x\}$ is a Gröbner basis.

The basis of $A = K\langle x, y \rangle / I$ is given by the set of normal words

$$y^k(xy)^t, y^k(xy)^t x \text{ for } k, t = 0, 1, 2, \dots$$

Working with noncommutative polynomials

Monomials in free algebra are always ordered with respect to the graded-lexicographical order!

- ▶ `Coefficients(f)`
- ▶ `LeadingCoefficient(f)`
- ▶ `TrailingCoefficient(f)`
- ▶ `MonomialCoefficient(f, m)`
- ▶ `Monomials(f)`
- ▶ `LeadingMonomial(f)`
- ▶ `Evaluate(f, s)`
- ▶ `Terms(f)`
- ▶ `LeadingTerm(f)`
- ▶ `Length(m)`
- ▶ `m[i]`
- ▶ `TotalDegree(f)`
- ▶ `LeadingTotalDegree(f)`

```
1 >K := RationalField();
2 >F<x, y> := FreeAlgebra(K, 2);
3 >f := 10*x*y^5 - 10*y*x^5 + 6*x*y - 10*x^5;
4 >Terms(f); // [ 10*x*y^5, -10*y*x^5, -10*x^5, 6*x*y ]
5 >LeadingMonomial(f); // x*y^5
6 >LeadingTerm(f); // 10*x*y^5
7 >MonomialCoefficient(f, x*y); // 6
```

Noncommutative Gröbner basis in Magma

Gröbner basis may be constructed for any kind of ideal.

If basis is infinite - to interrupt the computation, one can press Ctrl-C.

Magma always computes **the unique (sorted) reduced Gröbner basis** of I .

```
1 >K := RationalField();
2 >F<x, y, z> := FreeAlgebra(K, 3);
3 >B := [x^2 - y*z, x*y - y*z, y*x - z^2, y^3 - x*z];
4 >I := ideal<F | B> ;
5 >Groebner(I); // I has to be an ideal!
6 >Basis(I)
```

- ▶ `Groebner(I)` constructs the basis of a given ideal I ;
- ▶ `GroebnerBasis(I)` constructs and returns the basis of a given ideal I or a set of generators of I .

On the other hand, the following gives an error

```
1 >Alg := quo<F | I> ;
2 >GroebnerBasis(Alg);
```

Noncommutative Gröbner basis in Magma

```
1 > K := RationalField();
2 > F<x, y, z> := FreeAlgebra(K, 3);
3 > B := [x^2 - y*z, x*y - y*z, y*x - z^2, y^3 - x*z];
4 > I := ideal<F | B>;
5 > IL := lideal<F | B>;
6 > GroebnerBasis(IL);
7 [
8 y^3 - x*z,
9 x^2 - y*z,
10 x*y - y*z,
11 y*x - z^2
12 ]
13 > GroebnerBasis(I);
14 [
15 y*z^2*y - y*z^2, y*z^3 - y*z^2, z*y*z^2 - y*z^2,
16 z^2*y^2 - y*z^2, z^2*y*z - y*z^2, z^3*y - y*z^2,
17 z^4 - y*z^2, x*z*x - y*z^2, x*z*y - z^3,
18 x*z^2 - y*z^2, y^3 - x*z, y^2*z - z^2*y,
19 y*z*x - y*z^2, y*z*y - y*z^2, z^2*x - z^2*y,
20 x^2 - y*z, x*y - y*z, y*x - z^2
21 ]
22
```

Noncommutative Gröbner basis - parameters

- ▶ Magma by default uses the noncommutative Faugère F_4 algorithm, which works for two-sided ideals defined over a finite fields and \mathbb{Q}
- ▶ The Buchberger's algorithm can be used for ideals over any field

This can be controlled by Faugere parameter (true by default).

```
1 > k<e> := CyclotomicField(3);
2 > F <b, a> := FreeAlgebra(k, 2);
3 > rels := [a^2*b - e^2*a*b^2 - e^2*b*a^2 + b^2*a,
4 > a^3 + a*b*a - e*a*b^2 - e*b*a^2 + b*a*b + b^3,
5 > a^6,
6 > a^5*b + a^4*b*a + a^3*b*a^2 + a^2*b*a^3 + a*b*a^4 + b*a^5];
7 > I := ideal<F | rels>;
8 > time GroebnerBasis(I);
9 > time GroebnerBasis(I: Faugere:=false);
10 Time: 0.030
11 Time: 0.000
```

Access the basis

If the Gröbner basis was already computed, `BasisElement(I, i)` (the same as `Basis(I)[i]`) gives i -th element of the basis.

```
1 > k<e> := CyclotomicField(3);
2 > F <b, a> := FreeAlgebra(k, 2);
3 > rels := [a^2*b - e^2*a*b^2 - e^2*b*a^2 + b^2*a,
4 > a^3 + a*b*a - e*a*b^2 - e*b*a^2 + b*a*b + b^3,
5 > a^6,
6 > a^5*b + a^4*b*a + a^3*b*a^2 + a^2*b*a^3 + a*b*a^4 + b*a^5];
7 > I := ideal<F | rels>;
8 > GroebnerBasis(I);
9 > BasisElement(I, 13);
10 b*a*b*a^2 + (e + 1)*b*a^2*b*a + (e + 1)*b*a^4 + a*b*a^2*b + (e + 1)*
    a^2*b*a*b + a^4*b + (-e - 2)*a^5
```

Noncommutative Gröbner basis - order matters!

Gröbner basis can be finite or infinite depending on the chosen order. For example, let us consider the algebra $A = K\langle x, y \rangle / \langle x^2 + xy \rangle$ and deg-lex order on $\langle x, y \rangle$

- ▶ if $y > x$ the set $\{x^2 + xy\}$ is a Gröbner basis
- ▶ when $x > y$, the set $\{x^2 + xy\}$ is not a Gröbner basis. For example $x(x^2 + xy) - (x^2 + xy)x = -xyx + x^2y \in I$, so

$$xyx = LT((x^2 + xy)y - x^2y + xyx) \in \langle LT(I) \rangle.$$

It can be checked that then $\{xy^n x + xy^{n+1} \mid n \geq 0\}$ is (an infinite) Gröbner basis.

```
1 > K := RationalField();
2 > F<y, x> := FreeAlgebra(K, 2);
3 > B := [x^2 + x*y];
4 > I := ideal<F | B>;
5 > GroebnerBasis(I);
6 [
7 x*y + x^2
8 ]
9 > F<x, y> := FreeAlgebra(K, 2);
10 > B := [x^2 + x*y];
11 > I := ideal<F | B>;
12 > GroebnerBasis(B); // does not stop!
```

Truncated Gröbner basis

- ▶ `GroebnerBasis(S, d)` returns the degree- d Gröbner basis of the ideal generated by a set S of polynomials;
- ▶ If the ideal is homogeneous, the result is equal to the set of all polynomials in the full Gröbner basis of this ideal, whose total degree is less than or equal to d .

```
1 > K := Rationals();
2 > F<c,b,a> := FreeAlgebra(K, 3);
3 > rels := [ a^2 - a, b^2 - b, c^2 - c,
4 > b*a*b - a*b*a, c*b*c - b*c*b, c*a*c - a*c*a];
5 > I := ideal< F | rels >;
6 > A := quo< F | rels>;
7 > GroebnerBasis(rels, 7);
8 c*a*b*c*a*b*a - a*c*a*b*c*a*b
```

Normal forms

For given ideal I and $f \in K\langle x_1, \dots, x_n \rangle$ it is possible to find the normal form of f with respect to I (Magma will compute the Gröbner basis).

- ▶ `NormalForm(f, I)` - does not finish if basis is infinite!

```
1 > K := RationalField();
2 > F<x, y> := FreeAlgebra(K, 2);
3 > B := [x^2 + y^2];
4 > I := ideal<F | B>; // Groebner(I): [x*y^2 - y^2*x, x^2 + y^2]
5 > NormalForm(y^2*x - x*y^2, I);
6 0
```

- ▶ `NormalForm(f, S)`, where S is a set of polynomials - does not compute the basis!

```
1 NormalForm(y^2*x - x*y^2, B);
2 -x*y^2 + y^2*x
```

- ▶ check whether f is in an ideal I (equivalent to `NormalForm(f, I)` being 0)

```
1 > y^2*x - x*y^2 in I
2 true
```

How to get basis consisting of normal words?

If a graded algebra $K\langle x_1, \dots, x_n \rangle / I$ is finite dimensional, it is possible to compute its dimension and a set of normal words.

```
1 > K := RationalField();
2 > F<x, y, z> := FreeAlgebra(K, 3);
3 > B := [x^2 - y*z, x*y - y*z, y*x - z^2, y^3 - x*z];
4 > I := ideal<F | B>;
5 > A := quo<F | B>;
6 > Dimension(A);
7 > MonomialBasis(A);
8 16
9 {@
10 1, z, y, x, z^2, z*y, z*x, y*z, y^2, x*z, z^3,
11 z^2*y, z*y*z, z*y^2, z*x*z, y*z^2
12 @}
```

Function `HilbertSeries(A, d)` works only for the graded commutative rings!

How to find normal words up to dimension d in infinite dimensional case?

```
1 MonomialBasis := function(F, B, d)
2   rels := [LeadingMonomial(f) : f in GroebnerBasis(B)];
3   AssociatedMon := quo<F | rels> ;
4   S := {};
5   for m in MonomialsOfDegree(F,d) do
6     nf := NormalForm(m, rels);
7     if not nf eq 0 then
8       Include(~S, nf);
9     end if;
10  end for;
11  return S;
12 end function;
```

For example

```
1 > K := RationalField();
2 > F<x, y> := FreeAlgebra(K, 2);
3 > B := [x^2 + y^2];
4 > MonomialBasis(F, B, 8);
5 { y^5*x*y*x, x*y*x*y*x*y*x*y, y^4*x*y*x*y, y^3*x*y*x*y*x,
6   y*x*y*x*y*x*y*x, y^7*x, y^8, y^2*x*y*x*y*x*y, y^6*x*y}
```

Commutative Gröbner bases

Monomial order

A monomial order on $K[x_1, \dots, x_n]$ is any relation \geq on $\mathbb{Z}_{\geq 0}^n$ (or equivalently on the set of monomials) which is

- ▶ \geq is linear order;
- ▶ if $\alpha \geq \beta$ and $\gamma \in \mathbb{Z}_{\geq 0}^n$, then $\alpha + \gamma \geq \beta + \gamma$;
- ▶ $>$ is a well order on $\mathbb{Z}_{\geq 0}^n$

Let $f = \sum_{\alpha} a_{\alpha} x^{\alpha}$ be a nonzero polynomial in $K[x_1, \dots, x_n]$ and let \geq be a monomial order. **The leading term** of f is

$$LT(f) := a_{\alpha} x^{\alpha} \text{ such that } \alpha = \max\{\alpha \in \mathbb{Z}_{\geq 0}^n \mid a_{\alpha} \neq 0\}.$$

Commutative Gröbner basis

Definition

Fix a monomial order on $K[x_1, \dots, x_n]$. A finite subset $G = \{g_1, \dots, g_t\}$ of an ideal I is a Gröbner basis of I if

$$\langle LT(g_1), \dots, LT(g_t) \rangle = \langle LT(I) \rangle.$$

Gröbner basis G is reduced if

- ▶ leading coefficients of $p \in G$ are 1,
- ▶ for all $p \in G$, no monomial of p lies in $\langle LT(G \setminus \{p\}) \rangle$.

Theorem

If $G = \{g_1, \dots, g_t\}$ is Gröbner basis of I , then for every $f \in K[x_1, \dots, x_n]$ there exist unique g and r such that

1. $f = g + r$ for some $g \in I$,
2. no term of r is divisible by any $LT(g_1), \dots, LT(g_t)$.

r is then called **the normal form of f** .

Commutative Gröbner basis

It is possible to compute Gröbner basis of rings over fields or Euclidean rings.

- ▶ `Groebner(I: parameters)` allows to change the parameters
- ▶ `GroebnerBasis(I: parameters)` returns the reduced Gröbner basis, can be used with both ideals and set of generators;
- ▶ `GroebnerBasisUnreduced(S: parameters)` returns unreduced basis;
- ▶ `GroebnerBasis(S, d)` - Gröbner basis up to degree d

Parameters

- ▶ `Faugere`
- ▶ `HomogeneousWeights`
- ▶ `Homogenize`
- ▶ `DegreeStart` - if it is equal to d , ignore S -polynomial pairs of degree less than d
- ▶ `IdealWithFixedBasis(S)`

Monomial orders

PolynomialRing(K, n, order) allows to choose monomial order

- ▶ "lex" - lexicographical - default!

Definition

We say that $\alpha \geq_{lex} \beta$ if, in $\alpha - \beta \in \mathbb{Z}^n$, the leftmost nonzero entry is positive.

- ▶ "glex" - graded lexicographical
- ▶ "grevlex" - graded reverse lexicographical
- ▶ "weight" - weight - based on linearly independent vectors of weights $[w_1, \dots, w_n]$, $w_i \in \mathbb{Q}^n$, it first compares the dot product with w_1 , in case of a tie uses the second weight, etc.
- ▶ "grevlexw", "elim", "univ", ...

To check the order MonomialOrder(P)

```
1 > P<x, y> := PolynomialRing(RationalField(), 2, "glex");
2 > I := ideal<P | x^2 + y^2 > ;
3 > MonomialOrder(I);
4 > Q<x, y> := PolynomialRing(RationalField(), 2, "weight", [1, 0, 0,
    1]);
5 > J := ideal<Q | x^2 + y^2 > ;
6 > MonomialOrder(J);
7 <"glex">
8 <"weight", [ 1, 0, 0, 1 ]>
```

Monomial orders

Sequence of weights `MonomialOrderWeightVectors(P)`

```
1 > P<x, y> := PolynomialRing(RationalField(), 2, "lex");
2 > I := ideal<P | x^2 + y^2 > ;
3 > MonomialOrderWeightVectors(I);
4 [
5 [ 1, 0 ],
6 [ 0, 1 ]
7 ]
```

Change of order: `ChangeOrder(P, order)` or `ChangeOrder(I, Q)` return an ideal J and the isomorphism from P to the algebra Q with other order. Makes computation of Gröbner basis of J faster using Gröbner basis of I .

```
1 > J:= ChangeOrder(I, "weight", [1, 1, 1, 0]);
2 > _,f := ChangeOrder(I, "weight", [1, 1, 0, 1]);
3 > MonomialOrder(J);
4 > I eq J;
5 <"weight", [ 1, 1, 1, 0 ]>
6 >> I eq J;
7 ^
8 Runtime error in 'eq': Arguments are not compatible
9 Argument types given: RngMPol, RngMPol
```

Commutative Gröbner basis - related functions

If $G = \{g_1, \dots, g_t\}$ is a Gröbner basis of I , then for every $f \in K[x_1, \dots, x_n]$ there exist unique g and r such that

1. $f = g + r$ for some $g \in I$,
2. no term of r is divisible by any $LT(g_1), \dots, LT(g_t)$.

- ▶ `EasyIdeal(I)`, `EasyBasis(I)` - return the ideal E equal to I and the basis whose basis is the Gröbner basis with respect to "easy" monomial order
- ▶ `IsGroebner(S)`
- ▶ `Coordinates(I, f)` for $f \in I$ returns $[g_1, \dots, g_k]$ such that $f = g_1 b_1 + \dots + g_k b_k$ for the reduced Gröbner basis $\{b_1, \dots, b_k\}$ of I
- ▶ `NormalForm(f, I)` return the unique normal form of f with respect to (the Gröbner basis of) I
- ▶ `SPolynomial(f, g)`

Commutative Gröbner basis - Buchberger's algorithm

1. For every pair $f, g \in G$, compute the S -polynomial

$$S(f, g) = \frac{\text{lcm}(\text{LM}(f), \text{LM}(g))}{\text{LT}(f)} f - \frac{\text{lcm}(\text{LM}(f), \text{LM}(g))}{\text{LT}(g)} g.$$

2. Reduce $S(f, g)$ modulo $G = \{g_1, \dots, g_k\}$, namely write

$$S(f, g) = a_1 g_1 + \dots + a_k g_k + r,$$

where a_i are polynomials and r is either 0 or is a linear combination of monomials not divisible by $\text{LT}(g_1), \dots, \text{LT}(g_k)$.

3. If $r \neq 0$, set

$$G := G \cup \{r\}$$

and repeat Step 1.

4. If all S -polynomials reduce to zero, output G .

Parameters of Buchberger's algorithm

- ▶ ReduceInitial
- ▶ RemoveRedundant

Commutative Gröbner basis over fields

```
1 > P<x, y, z> := PolynomialRing(RationalField(), 3);
2 > I := ideal<P | y - x^2, z-x^3> ;
3 > GroebnerBasis(I);
4 > S<y, z, x> := PolynomialRing(RationalField(), 3);
5 > J := ideal<S | y - x^2, z-x^3> ;
6 > GroebnerBasis(J);
7 [x^2 - y, x*y - z, x*z - y^2, y^3 - z^2 ]
8 [y - x^2, z - x^3 ]
```

```
1 > P<x, y, z> := PolynomialRing(RationalField(), 3);
2 > T := [ y - x^2, z - x^3 ];
3 > IsGroebner(T);
4 > SPolynomial(y - x^2, z - x^3);
5 > Coordinates(J, -x*y + z);
6 false
7 -x*y + z
8 [-x, 1]
```

Commutative Gröbner basis over other rings

Euclidean rings supported in Magma: \mathbb{Z} , \mathbb{Z}_m , $K[x]$, Galois rings, p -adic quotient rings, and discrete valuation rings.

It is possible to compute basis over $\mathbb{Z}[\sqrt{-5}]$ using basis over \mathbb{Z} . Variable S represents $\sqrt{-5}$, where S is less than all variables in the monomial order.

```
1 > P<x, y, S> := PolynomialRing(IntegerRing(), 3);
2 > f1 := 2*x*y + S*y;
3 > f2 := (1 + S)*x^2 - x*y;
4 > I := ideal<P | f1, f2, S^2 + 5> ;
5 > GroebnerBasis(I);
6 [
7 x^2*S + x^2 + 5*y^3 + 13*y*S - 25*y,
8 6*x^2 + 5*y^2 + 3*y*S - 10*y,
9 x*y + 5*y^3 + 13*y*S - 25*y,
10 y^2*S + 5*y^2 - 15*y,
11 10*y^2 + 5*y*S - 25*y,
12 S^2 + 5]
```

Application: elimination

The elimination theorem

If G is a Gröbner basis of an ideal I of $K[x_1, \dots, x_n]$ with respect to lex order, where $x_1 > \dots > x_n$. Then $G \cap K[x_{k+1}, \dots, x_n]$ is a Gröbner basis of the ideal $I_k = I \cap K[x_{k+1}, \dots, x_n]$.

Elimination ideal:

- ▶ `EliminationIdeal(I, k)` for $0 \leq k \leq n$ returns I_k
- ▶ `EliminationIdeal(I, S)` for subset S of variables "eliminates" variables from S

```
1 > P<x, y, z> := PolynomialRing(Rationals(), 3);
2 > I := ideal<P | x^2 + y^2 + z^2 - 1, x+y^2+z-1, x+y+z^2-1> ;
3 > Ez := EliminationIdeal(I, 2);
4 > GroebnerBasis(Ez);
5 > Eyz := EliminationIdeal(I, 1);
6 > GroebnerBasis(Eyz);
7 > GroebnerBasis(I);
8 [ z^7 + 3*z^3 - 8*z^2 + 4*z]
9 [y^2 - y - z^2 + z,
10 y*z + 1/4*z^6 + 1/2*z^3 + 3/4*z^2 - 3/2*z,
11 z^7 + 3*z^3 - 8*z^2 + 4*z]
12 [x + y + z^2 - 1,
13 y^2 - y - z^2 + z,
14 y*z + 1/4*z^6 + 1/2*z^3 + 3/4*z^2 - 3/2*z,
15 z^7 + 3*z^3 - 8*z^2 + 4*z]
```

Application: elimination

Aim: Solve the system of polynomial equations

$$xy = 1, \quad xz = 1.$$

```
1 > P<x, y, z> := PolynomialRing(Rationals(), 3);
2 > I := ideal<P | x*y -1, x*z-1> ;
3 > Ez := EliminationIdeal(I, 2);
4 > GroebnerBasis(Ez);
5 > Eyz := EliminationIdeal(I, 1);
6 > GroebnerBasis(Eyz);
7 > GroebnerBasis(I);
8 []
9 [y - z]
10 [x*z - 1,
11 y - z]
```

But for $z = 0$ we don't get the solution!

Application: relations ideal

Problem

For a parametrization $F : K^m \rightarrow K^n$ given by polynomials $f_1, \dots, f_n \in K[t_1, \dots, t_m]$, describe the equations defining the smallest variety V containing $F(K^m)$.

Theorem

If K is an infinite field, let $F : K^m \rightarrow K^n$ be the function determined by the polynomials parametrization $f_1, \dots, f_n \in K[t_1, \dots, t_m]$. Let I be the ideal

$$I = (x_1 - f_1, \dots, x_n - f_n) \subseteq K[t_1, \dots, t_m, x_1, \dots, x_n].$$

Then $V(I_m)$, where

$$I_m = I \cap K[x_1, \dots, x_n]$$

is the smallest variety in K^n containing $F(K^m)$.

Application: relations ideal

Example: Find the smallest variety containing $\{(t^4, t^3, t^2) \mid t \in \mathbb{Q}\} \subseteq \mathbb{Q}^4$.

- ▶ "eliminate" parameters using `EliminationIdeal`

```
1 > P<t, x, y, z> := PolynomialRing(Rationals(), 4);
2 > I := ideal<P | t^4 - x, t^3 - y, t^2 - z >;
3 > EliminationIdeal(I, 1);
4 [ x - z^2, y^2 - z^3]
```

- ▶ `RelationIdeal(F, T)` where F is a list of n polynomials and T is polynomial ring of rank n

```
1 > P<t> := PolynomialRing(Rationals(), 1);
2 > T<x, y, z> := PolynomialRing(Rationals(), 3);
3 > Q := [t^4, t^3, t^2];
4 > RelationIdeal(Q, T);
5 [ x*z - y^2, x - z^2]
```