# Introduction to Gröbner Bases

*W. Windsteiger, April 28, 2006*

**Introduction to the Theory / Applications**

**An Algorithm to Compute Gröbner Bases (GB)**

**Improvements in the GB-Algorithm**

**Applications**

**Further Reading**

## Introduction to the Theory / Applications

- Gröbner Bases: central algorithmic method in computational *polynomial ideal theory* (commutative algebra, algebraic geometry).
  - Introduced by Bruno Buchberger in his PhD thesis 1965.
  - Further developed mainly by BB himself in the 1970's.
  - Since the 1980's: Development of the theory, generalization of the theory, and applications of the theory by various authors.
  - Became own entry in the AMS subject classification index.

## Introduction to the Theory / Applications

- Gröbner Bases: central algorithmic method in computational polynomial ideal theory (commutative alge−bra, algebraic geometry).
- Gröbner Bases: can be *effectively computed* for any finite set of *multivariate polynomials*.
  - — Notions such as "Ideal basis" or similar existed earlier, but Bruno Buchberger invented the first *algo−rithm for computing a GB* in his PhD thesis 1965.
  - — Original algorithm improved in various ways ("sugar cube strategy", "Gröbner walk", etc.), but *all improvements are still based on the original Buchberger Algorithm*.
  - — Now, many implementations: *Mathematica*, MAPLE, Singular, MAGMA, TI-92 (!), etc.

```
In[1]:= GroebnerBasis[{3 x^4 + 2 x y^2 + y^3, x^2 y - 5 x y + 2 x^3}, {x, y}]

Out[1]= {5625 y^4 + 1340 y^5 + 150 y^6 + 3 y^7, 23709375 x y^2 - 623560 y^4 - 369975 y^5 - 8952 y^6,
   355640625 x^2 y + 47418750 y^3 - 10774085 y^4 - 1134600 y^5 - 20532 y^6,
   711281250 x^3 - 1778203125 x y - 47418750 y^3 + 10774085 y^4 + 1134600 y^5 + 20532 y^6}
```

# Introduction to the Theory / Applications

- Gröbner Bases: central algorithmic method in computational polynomial ideal theory (commutative algebra, algebraic geometry).
- Gröbner Bases: can be effectively computed for any finite set of multivariate polynomials.
- Gröbner Bases: often allow *easy answers* to questions involving sets of *multivariate polynomials* (by transforming the set into a Gröbner basis).

## 2 Examples

### Systems of Algebraic Equations

- From the above GB we can immediately tell that the set of polynomial equations

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

$$x^2 y - 5xy + 2x^3 = 0$$

— *has* solutions

— has only *finitely many* solutions.

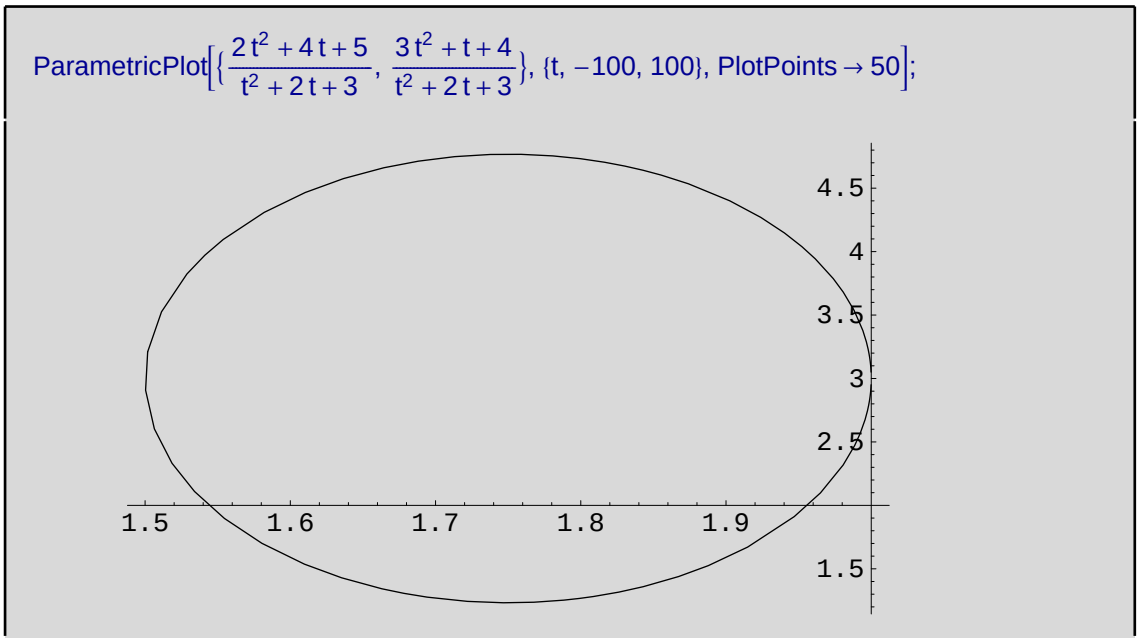
### Algebraic Geometry

- Take the 2D-curve in parametric description

$$x = \frac{2t^2 + 4t + 5}{t^2 + 2t + 3}$$

$$y = \frac{3t^2 + t + 4}{t^2 + 2t + 3}.$$

```
In[2]:= ParametricPlot[{(2t^2 + 4t + 5)/(t^2 + 2t + 3), (3t^2 + t + 4)/(t^2 + 2t + 3)}, {t, -100, 100}, PlotPoints → 50];
```




Find an implicit representation of the same curve (this is, in general, called the *implicitization* of a geometrical object). For this we just compute

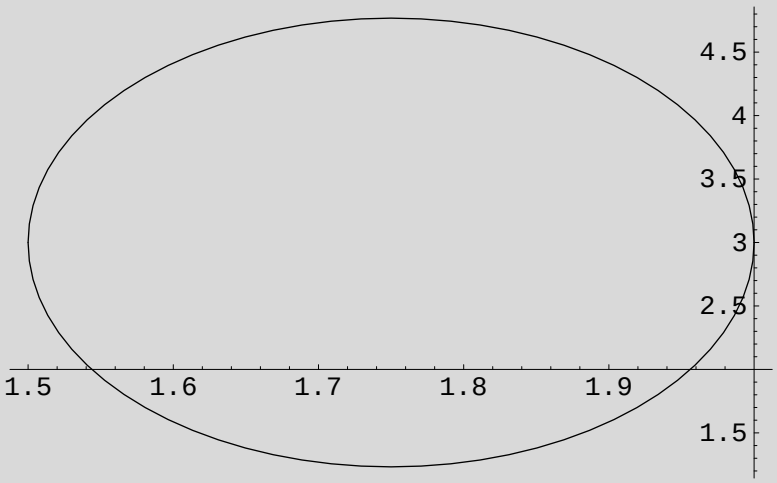
In[3]:=
```
GroebnerBasis[{x (t^2 + 2 t + 3) - (2 t^2 + 4 t + 5), y (t^2 + 2 t + 3) - (3 t^2 + t + 4)}, {t, x, y}]
```

Out[3]=
$$\{159 - 175\,x + 50\,x^2 - 6\,y + y^2,\ -18 - 3\,t + 10\,x + y + t\,y,\ -7 - 10\,t + 5\,x + 5\,t\,x - y\}$$

The polynomial *not containing* the parameter is an implicit representation of the curve!

In[4]:=
```
Needs["Graphics`ImplicitPlot`"]
```

In[5]:=
```
ImplicitPlot[159 - 175 x + 50 x^2 - 6 y + y^2 == 0, {x, 1.5, 2}, AspectRatio → 1 / GoldenRatio];
```



# What is a Gröbner Basis?

## Ingredients

- $K[x_1, \ldots, x_n]$ … the (commutative) ring of polynomials in $n$ indeterminates over the coefficient field $K$ (with addition and multiplication).
- $F \subset K[x_1, \ldots, x_n]$ … finite set of polynomials (say $F = \{F_1, \ldots, F_m\}$).
- Ideal$[F]$ … the ideal generated by $F$, i.e.

$$\Big\{\sum_{i=1}^{m} h_i \; F_i \; : h_i \in K[x_1, \ldots, x_n]\Big\}$$

  Ideals play an important role when studying the *common roots* of the polynomials in $F$. A common root of $F$ is also a root of any other polynomial in Ideal$[F]$, in other words, Ideal$[F]$ preserves the common roots of $F$.

- An ideal $\mathcal{I}$ in a ring $R$ always induces a *congruence relation*:

$$f \sim_{\mathcal{I}} g \;\Leftrightarrow\; f - g \in \mathcal{I}$$

- The *residue class ring (factor ring)* $R/\mathcal{I}$ consists of the residue classes w.r.t. $\sim_{\mathcal{I}}$, addition and multiplication are well-defined.
  (An ideal in a ring plays a similar role like a normal subgroup in a group …)

# What is a Gröbner Basis?

## How to Arrive at the Notion of a ‘‘Gröbner Basis’’

- GB are a generalization of GCD (univariate case) and triangluar matrices (linear case), in other words the GB algorithm specializes
  - to the *Euclidean algorithm* in the univariate case and
  - to the *Gaussian algorithm* in the linear case.

# What is a Gröbner Basis?

## How to Arrive at the Notion of a "Gröbner Basis" by Generalization of the GCD Concept

- Consider the case of univariate polynomials, i.e. $n = 1$. Let $\mathcal{I} = \text{Ideal}[F_1, \ldots, F_m]$. Given two polynomials $f$ and $g$, decide whether $f \sim_{\mathcal{I}} g$.
  Every ideal in $K[x]$ is generated by a single generator, namely $\text{GCD}[F_1, \ldots, F_m]$ (the greatest common divisor of the $F_i$). Then

$$f \sim_{\mathcal{I}} g \Leftrightarrow f - g \in \text{Ideal}[\text{GCD}[F_1, \ldots, F_m]] \Leftrightarrow f - g = h * \text{GCD}[F_1, \ldots, F_m] \Leftrightarrow (f - g) \bmod \text{GCD}[F_1, \ldots, F_m] = 0.$$

```
In[6]:= Needs["Algebra`PolynomialExtendedGCD`"]

In[7]:= {F1, F2} = {x^2 - 1, x^2 + 2 x + 1};

In[8]:= f = x^5 - 3 x^3 + 2 x;
        g = 3 x^7 + 26 x^4 + 19 x - 5;

In[10]:= {G, {c1, c2}} = PolynomialExtendedGCD[F1, F2]

Out[10]= {1 + x, {-1/2, 1/2}}

In[11]:= PolynomialRemainder[f - g, G, x]

Out[11]= 1

In[12]:= h = PolynomialQuotient[f - g, G, x]

Out[12]= 4 - 21 x + 21 x^2 - 24 x^3 - 2 x^4 + 3 x^5 - 3 x^6
```

In fact,

```
In[13]:= f - g

Out[13]= 5 - 17 x - 3 x^3 - 26 x^4 + x^5 - 3 x^7

In[14]:= Expand[h * G]

Out[14]= 4 - 17 x - 3 x^3 - 26 x^4 + x^5 - 3 x^7
```

On the other hand:

In[15]:=
```
f = x^5 + 3 x^2 + 2 x – 3;
g = x^5 – 3 x^3 – 5;
```

In[17]:=
```
PolynomialRemainder[f – g, G, x]
```

Out[17]=
```
0
```

In[18]:=
```
h = PolynomialQuotient[f – g, G, x]
```

Out[18]=
```
2 + 3 x^2
```

In fact,

In[19]:=
```
f – g
```

Out[19]=
```
2 + 2 x + 3 x^2 + 3 x^3
```

*f* - *g* is a multiple of the GCD:

In[20]:=
```
Expand[h * G]
```

Out[20]=
```
2 + 2 x + 3 x^2 + 3 x^3
```

*f* - *g* is a linear combination of the original generators:

In[21]:=
```
(c1 h) F1 + (c2 h) F2    // Expand
```

Out[21]=
```
2 + 2 x + 3 x^2 + 3 x^3
```

# What is a Gröbner Basis?

## How to Arrive at the Notion of a "Gröbner Basis" by Generalization of the GCD Concept

### Multivariate Polynomials

- Every multivariate polynomial consists of a sum of *monomials*, every monomial consists of a *coefficient* and a *power product*, a power product is a product of powers of individual variables.

$$\underbrace{\overbrace{3}^{\text{coef}}\ \overbrace{x^4}^{\text{pp}}}_{\text{monomials}} + \underbrace{\overbrace{2}^{\text{coef}}\ \overbrace{x\,y^2}^{\text{pp}}}_{\text{monomials}} + \underbrace{\overbrace{y^3}^{\text{pp}}}_{\text{monomials}}$$

- For reduction, we need an *admissible ordering* $\prec$ on the power products, i.e.

| | | |
|---|---|---|
| $1 \prec p$ | for all power products $p \neq 1$ | (well-foundedness) |
| $p_1 \prec p_2 \Rightarrow s * p_1 \prec s * p_2$ | for all power products $p_1, p_2, s$ | (compatibility with $*$) |

- Typical admissible orderings based on an ordering of the individual variables $x_1 > \ldots > x_n$:
  - lexicographic: first sort by powers of $x_1$, then by $x_2$, etc. (like names in a telephone book).
  - total degree lexicographic: first sort by total degree, within same degree sort lexicographically.
- *Leading monomial* (lm) of a polynomial $p$: the greatest monomial in $p$ w.r.t. $\prec$.

# What is a Gröbner Basis?

## How to Arrive at the Notion of a ‘‘Gröbner Basis’’ by Generalization of the GCD Concept

### Polynomial Reduction

- For multivariate polynomials we need a *generalized division* of a polynomial by a set of polynomials: *polynomial reduction*.
- Like *polynomial division*: ‘‘iterated subtraction of multiples of the divisor in order to cancel power products’’.
- We call $f$ *reducible by* $g$ *to* $f_1$ if there is a monomial in $f$, which is a multiple of the leading monomial of $g$, and we get $f_1$ by subtracting an appropriate multiple of $g$ from $f$ such that this monomial cancels, otherwise we say $f$ is not reducible by $g$.

  We write: $f \rightarrow_g f_1$.
- We call $h$ *a normal form of* $f$ *w.r.t* $F$ if there is a sequence of reductions

  $f \rightarrow_{g_1} f_1 \rightarrow_{g_2} f_2 \rightarrow_{g_3} \ldots \rightarrow_{g_k} h$

  such that

  — $g_i \in F$ for all $1 \leq i \leq k$

  — $h$ is not reducible by any polynomial in $F$.

  We write: $f \rightarrow_F^\star h$.
- We write *NormalForm*$[f, F]$ for such an $h$ with $f \rightarrow_F^\star h$.

**Example**

Lexikographic ordering based on $x > y$: Try to always eliminate the leading monomial.

```
In[22]:= f = x^4 + y^4;
         {F1, F2} = {x + y - 1, x y - 3}; h = f;

In[24]:= h = h - x^3 F1 // Expand
Out[24]= x^3 - x^3 y + y^4

In[25]:= h = h - (-1) x^2 F2 // Expand
Out[25]= -3 x^2 + x^3 + y^4

In[26]:= h = h - x^2 F1 // Expand
Out[26]= -2 x^2 - x^2 y + y^4

In[27]:= h = h - (-1) x F2 // Expand
Out[27]= -3 x - 2 x^2 + y^4

In[28]:= h = h - (-2) x F1 // Expand
Out[28]= -5 x + 2 x y + y^4

In[29]:= h = h - 2 F2 // Expand
Out[29]= 6 - 5 x + y^4

In[30]:= h = h - (-5) F1 // Expand
Out[30]= 1 + 5 y + y^4
```

The original polynomial as a *linear combination* of the *normal form* and the *generators of the ideal*:

In[31]:=
$$(1+5y+y^4)+(x^3+x^2-2x-5)*F_1+(-x^2-x+2)*F_2 \text{ // Expand}$$

Out[31]=
$$x^4+y^4$$

Alternatively: Try to use $F_1$ as much as possible.

In[32]:=
$$f=x^4+y^4;$$
$$\{F_1, F_2\}=\{x+y-1, xy-3\}; h=f;$$

In[34]:=
$$h=h-x^3 F_1 \text{ // Expand}$$

Out[34]=
$$x^3-x^3 y+y^4$$

In[35]:=
$$h=h-(-1)x^2 y F_1 \text{ // Expand}$$

Out[35]=
$$x^3-x^2 y+x^2 y^2+y^4$$

In[36]:=
$$h=h-x^2 F_1 \text{ // Expand}$$

Out[36]=
$$x^2-2x^2 y+x^2 y^2+y^4$$

In[37]:=
$$h=h-x y^2 F_1 \text{ // Expand}$$

Out[37]=
$$x^2-2x^2 y+x y^2-x y^3+y^4$$

In[38]:=
$$h=h-(-2)x y F_1 \text{ // Expand}$$

Out[38]=
$$x^2-2xy+3x y^2-x y^3+y^4$$

In[39]:=
$$h=h-x F_1 \text{ // Expand}$$

Out[39]=
$$x-3xy+3x y^2-x y^3+y^4$$

In[40]:=
$$h=h-(-1)y^3 F_1 \text{ // Expand}$$

Out[40]=
$$x-3xy+3x y^2-y^3+2y^4$$

In[41]:=
```
h = h − 3 y^2 F1 // Expand
```
Out[41]=
$$x - 3xy + 3y^2 - 4y^3 + 2y^4$$

In[42]:=
```
h = h − (−3) y F1 // Expand
```
Out[42]=
$$x - 3y + 6y^2 - 4y^3 + 2y^4$$

In[43]:=
```
h = h − F1 // Expand
```
Out[43]=
$$1 - 4y + 6y^2 - 4y^3 + 2y^4$$

Available in *Mathematica*:

In[44]:=
```
PolynomialReduce[f, {F1, F2}, {x, y}]
```
Out[44]=
$$\left\{\left\{1 + x + x^2 + x^3 - 3y - 2xy - x^2 y + 3y^2 + xy^2 - y^3, 0\right\}, 1 - 4y + 6y^2 - 4y^3 + 2y^4\right\}$$

In[45]:=
```
(1 − 4 y + 6 y^2 − 4 y^3 + 2 y^4) +
    (1 + x + x^2 + x^3 − 3 y − 2 x y − x^2 y + 3 y^2 + x y^2 − y^3) * F1 + 0 F2 // Expand
```
Out[45]=
$$x^4 + y^4$$

## Observation

*Reduction w.r.t. an arbitrary set of polynomial is not necessarily unique!*

## Gröbner Bases Allow Unique Normal Forms!

$F$ is a Gröbner basis iff for all $f \in K[x_1, \ldots, x_n]$ : $f \to_F^\star h_1 \wedge f \to_F^\star h_2 \Rightarrow h_1 = h_2$ .

### Some Facts about GB

— $F$ is a Gröbner basis iff for all $f \in \text{Ideal}[F]$ : $f \to_F^\star 0$.

— if $F$ is a Gröbner basis: $f \in \text{Ideal}[F] \Leftrightarrow f \to_F^\star 0$ .

— $\to_F^\star$ is a canonical simplifier for $\sim_{\text{Ideal}[F]}$, i.e. GB allow arithmetic in the residue class ring.

— If $F$ is a GB w.r.t. the lexicographic term ordering induced by $x_n > \ldots > x_1$ then
$F$ has the *elimination property*, i.e. $\text{Ideal}[F] \bigcap K[x_1, \ldots, x_i] = \text{Ideal}[F \bigcap K[x_1, \ldots, x_i]]$,

i.e. the $i$-th elimination ideal can easily be determined −−− just take the polynomials that depend only on the first $i$ variables! This is the key to solving systems of algebraic equations, see later.

## An Algorithm to Compute Gröbner Bases

- Given: $F \subset K[x_1, \ldots, x_n]$ finite, term ordering $\prec$
- Find: $G$, s.t.
  - Ideal[$G$] = Ideal[$F$]
  - $G$ is a Gröbner basis.

# An Algorithm to Compute Gröbner Bases

## Main Theorem of Gröbner Bases Theory

— $F$ is a Gröbner basis iff for all $f_1, f_2 \in F$ : S-Polynomial$[f_1, f_2] \to_F^\star 0$.

## S-Polynomials

◆ Multiply two polynomials in such a way that, after subtraction, the leading monomial vanishes! Formally,

$$\text{S-Polynomial}[f_1, f_2] := \frac{\text{lcm}[\text{lm}[f_1], \text{lm}[f_2]]}{\text{lm}[f_1]}\ f_1 \ - \ \frac{\text{lcm}[\text{lm}[f_1], \text{lm}[f_2]]}{\text{lm}[f_2]}\ f_2$$

# An Algorithm to Compute Gröbner Bases

## Main Idea

- Reduce all S-Polynomials w.r.t. to $F$.
- If all reductions yield 0 then $F$ is a Gröbner basis (by the main theorem).
- If a reduction yields an $h \neq 0$ then
  - — adjoin $h$ to $F$ (in order to make $h$ reduce to 0 w.r.t. the new $F$) and
  - — inspect all new S-Polynomials that can now be formed.

## The Basic Algorithm

```
GB[F_] :=
  Module[{G = F, P = {{f1, f2} : fi ∈ F, f1 ≠ f2}, p, h},
    While[P ≠ ∅,
      {p1, p2} = any pair from P;
      P = P − {{p1, p2}};
      h = NormalForm[S-Polynomial[p1, p2], G];
      If[h ≠ 0,
        P = P ⋃ {{h, g} : g ∈ G};
        G = G ⋃ {h}]]]
```

**The algorithm …**

- is *correct*, because of the main theorem (upon termination, all S-Polynomials reduce to 0) and
- *terminates*, due to Dickson's Lemma (the sequence $(l_i)_{i\in\mathbb{N}}$ of leading monomials of the new $h$'s has the property that every $l_i$ is *not a multiple* of any $l_j$ with $j < i$, hence the sequence *must be finite*.).

# An Algorithm to Compute Gröbner Bases

## Refinements

- A Gröbner basis $F$ is called a *reduced Gröbner basis* iff for all $f \in F$: $f$ is not reducible by any $g \in F - \{f\}$ and $\mathrm{lm}[f] = 1$.
- For every $F$ there is a *uniquely determined* reduced Gröbner basis that generates the same ideal as $F$, we will refer to it as $\mathrm{GB}[F]$.

## Illustration of the Algorithm

We use total degree lexicographic ordering w.r.t. $y > x$.

In[46]:=
```
G = {3 x^4 + 2 x y^2 + y^3, x^2 y - 5 x y + 2 x^3}; P = {{G[[1]], G[[2]]}};
```

First pair:

In[47]:=
```
{p1, p2} = P[[1]]; Print[{p1, p2}]; P = Rest[P];
```
$\{3 x^4 + 2 x y^2 + y^3, 2 x^3 - 5 x y + x^2 y\}$

In[48]:=
```
sp = y p1 - 3 x^2 p2 // Expand
```
Out[48]=
$$-6 x^5 + 15 x^3 y + 2 x y^3 + y^4$$

In[49]:=
```
{c, h} = PolynomialReduce[sp, G, {y, x}, MonomialOrder → DegreeLexicographic]
```
Out[49]=
$$\left\{\left\{-\frac{14}{3} - 2 x, 35 + 7 x + 4 y\right\}, -70 x^3 + 175 x y + \frac{88 x y^2}{3} + \frac{14 y^3}{3} + 4 x y^3 + y^4\right\}$$

In[50]:=
```
P = Join[P, Table[{h, G[[i]]}, {i, 1, Length[G]}]]; PrependTo[G, h];
```

In[51]:=
```
P
```
Out[51]=
$$\left\{\left\{-70 x^3 + 175 x y + \frac{88 x y^2}{3} + \frac{14 y^3}{3} + 4 x y^3 + y^4, 3 x^4 + 2 x y^2 + y^3\right\},\right.$$
$$\left.\left\{-70 x^3 + 175 x y + \frac{88 x y^2}{3} + \frac{14 y^3}{3} + 4 x y^3 + y^4, 2 x^3 - 5 x y + x^2 y\right\}\right\}$$

In[52]:=
```
G
```
Out[52]=
$$\left\{-70 x^3 + 175 x y + \frac{88 x y^2}{3} + \frac{14 y^3}{3} + 4 x y^3 + y^4, 3 x^4 + 2 x y^2 + y^3, 2 x^3 - 5 x y + x^2 y\right\}$$

Next pair:

In[53]:=
```
{p1, p2} = P[[1]]; Print[{p1, p2}]; P = Rest[P];
```

$$\left\{-70\,x^3+175\,x\,y+\frac{88\,x\,y^2}{3}+\frac{14\,y^3}{3}+4\,x\,y^3+y^4,\ 3\,x^4+2\,x\,y^2+y^3\right\}$$

In[54]:=
```
sp = 3 x^4 p1 − y^4 p2 // Expand
```

Out[54]=
$$-210\,x^7+525\,x^5\,y+88\,x^5\,y^2+14\,x^4\,y^3+12\,x^5\,y^3-2\,x\,y^6-y^7$$

In[55]:=
```
{c, h} = PolynomialReduce[sp, G, {y, x}, MonomialOrder → DegreeLexicographic]
```

Out[55]=
$$\left\{\left\{-\frac{2\,x\,y^2}{3}-\frac{y^3}{3},\ -70\,x^3+175\,x\,y+\frac{88\,x\,y^2}{3}+\frac{14\,y^3}{3}+4\,x\,y^3,\ 0\right\},\ 0\right\}$$

Next pair:

In[56]:=
```
{p1, p2} = P[[1]]; Print[{p1, p2}]; P = Rest[P];
```

$$\left\{-70\,x^3+175\,x\,y+\frac{88\,x\,y^2}{3}+\frac{14\,y^3}{3}+4\,x\,y^3+y^4,\ 2\,x^3-5\,x\,y+x^2\,y\right\}$$

In[57]:=
```
sp = x^2 p1 − y^3 p2 // Expand
```

Out[57]=
$$-70\,x^5+175\,x^3\,y+\frac{88\,x^3\,y^2}{3}+\frac{14\,x^2\,y^3}{3}+2\,x^3\,y^3+5\,x\,y^4$$

In[58]:=
```
{c, h} = PolynomialReduce[sp, G, {y, x}, MonomialOrder → DegreeLexicographic]
```

Out[58]=
$$\left\{\left\{\frac{56}{9}+\frac{7\,x}{3}+\frac{4\,y}{3},\ \frac{1}{3}\left(-\frac{784}{9}-70\,x-\frac{112\,y}{3}-4\,y^2\right),\right.\right.$$
$$\left.\left.\frac{1}{3}\left(\frac{1960}{3}+\frac{1127\,x}{3}+\frac{644\,y}{3}+56\,x\,y+16\,y^2+6\,x\,y^2\right)\right\},\ 0\right\}$$

In[59]:=
```
P
```

Out[59]=
$$\{\}$$

In[60]:=
```
G
```

Out[60]=
$$\left\{-70\,x^3+175\,x\,y+\frac{88\,x\,y^2}{3}+\frac{14\,y^3}{3}+4\,x\,y^3+y^4,\ 3\,x^4+2\,x\,y^2+y^3,\ 2\,x^3-5\,x\,y+x^2\,y\right\}$$

Reduced GB:

```
In[61]:= MapAt[Expand[#/3] &, G, 2]
```

$$\text{Out[61]}= \left\{-70\,x^3+175\,x\,y+\frac{88\,x\,y^2}{3}+\frac{14\,y^3}{3}+4\,x\,y^3+y^4,\ x^4+\frac{2\,x\,y^2}{3}+\frac{y^3}{3},\ 2\,x^3-5\,x\,y+x^2\,y\right\}$$

Compare to *Mathematica*: basically the same module a constant factor (*Mathematica*'s polynomials are not normalized, but have interger coefficients).

```
In[62]:= GroebnerBasis[G, {y, x}, MonomialOrder → DegreeLexicographic]
```

$$\text{Out[62]}= \left\{2\,x^3-5\,x\,y+x^2\,y,\ 3\,x^4+2\,x\,y^2+y^3,\ -210\,x^3+525\,x\,y+88\,x\,y^2+14\,y^3+12\,x\,y^3+3\,y^4\right\}$$

## Improvements in the GB-Algorithm

- Costly operation: reductions to 0. AND: These add no new information! Thus, try to avoid!
  There are *two criteria [Buchberger]*.
  - if lcm[lm[$f_1$], lm[$f_2$]] = lm[$f_1$]·lm[$f_2$] then S-Polynomial[$f_1$, $f_2$] $\to_F^\star$ 0.
    (would prevent first 0-reduction in example.)
  - more complicated, does *not prevent* to the second 0-reduction above.
- The sequence, in which pairs are considered, has drastical influence on the complexity. (Take pairs with small lcm of their lm's first.)
- Ordering of the power products has drastical influence: Total degree faster than lexicographic! (Note: the GB depends on the ordering!)
- Many improvements can be found in the literature (by Buchberger himself in the Bose-paper 1985, "sugar cube strategy", FGLM, "Gröbner walk", etc.),

# Applications

## Solving Systems of Algebraic Equations

We write $\overline{F}$ for $\{f = 0 : f \in F\}$. Some facts:

- GB[$F$] = {1} iff $\overline{F}$ has no solutions.
- for all $x_i$: GB[$F$] contains an $f$ s.t. lm[$f$] = $x_i^j$ iff $\overline{F}$ has finitely many solutions (Ideal[$F$] is called 0-dimensional in that case).
- For lexicographic ordering induced by $x_n > \ldots > x_1$ we have the elimination property, which means, that GB[$F$] is *triangularized* (if Ideal[$F$] is 0-dimensional) in the following sense:
  - GB[$F$] contains one univariate polynomial in $x_1$.
  - GB[$F$] contains at least one polynomial in $x_1$ and $x_2$.
  - etc.

  This allows to compute all solutions "componentwise" using "backsubstitution" (like in the Gaussian algorithm!).

**Example**

```
In[63]:= F = {3 x^4 + 2 x y^2 + y^3, x^2 y - 5 x y + 2 x^3};
```

- Go for sulutions for $x$ primarily? ⟶ Choose $y > x$.

```
In[64]:= G = GroebnerBasis[F, {y, x}]

Out[64]= {-375 x^5 + 185 x^6 - 45 x^7 + 3 x^8,
   -1000 x^3 - 200 x^4 + 35 x^5 - 30 x^6 + 3 x^7 + 2500 x y, 375 x^4 - 110 x^5 + 45 x^6 - 3 x^7 + 125 y^3}
```

```
In[65]:= G[[1]] // Factor

Out[65]= x^5 (-375 + 185 x - 45 x^2 + 3 x^3)
```

- Compare to the manual computation above w.r.t. total degree ordering: there we had *no univariate polynomial*.
- Go for sulutions for $y$ primarily? ⟶ Choose $x > y$.

```
In[66]:= G = GroebnerBasis[F, {x, y}]

Out[66]= {5625 y^4 + 1340 y^5 + 150 y^6 + 3 y^7, 23709375 x y^2 - 623560 y^4 - 369975 y^5 - 8952 y^6,
   355640625 x^2 y + 47418750 y^3 - 10774085 y^4 - 1134600 y^5 - 20532 y^6,
   711281250 x^3 - 1778203125 x y - 47418750 y^3 + 10774085 y^4 + 1134600 y^5 + 20532 y^6}
```

In[67]:=
```
gy = G[[1]] // Factor
```

Out[67]=
$$y^4 \left(5625 + 1340\, y + 150\, y^2 + 3\, y^3\right)$$

In[68]:=
```
sy = Solve[gy == 0, y]
```

Out[68]=
$$\{\{y \to 0\}, \{y \to 0\}, \{y \to 0\}, \{y \to 0\},$$
$$\left\{y \to \frac{1}{3}\left(-50 - 232\, 5^{2/3}\left(\frac{2}{19925 - 281\sqrt{1865}}\right)^{1/3} - \left(\frac{5}{2}\left(19925 - 281\sqrt{1865}\right)\right)^{1/3}\right)\right\},$$
$$\left\{y \to -\frac{50}{3} + \frac{116}{3}\, 5^{2/3}\left(1 + i\sqrt{3}\right)\left(\frac{2}{19925 - 281\sqrt{1865}}\right)^{1/3} + \right.$$
$$\left.\frac{1}{6}\left(1 - i\sqrt{3}\right)\left(\frac{5}{2}\left(19925 - 281\sqrt{1865}\right)\right)^{1/3}\right\},$$
$$\left\{y \to -\frac{50}{3} + \frac{116}{3}\, 5^{2/3}\left(1 - i\sqrt{3}\right)\left(\frac{2}{19925 - 281\sqrt{1865}}\right)^{1/3} + \right.$$
$$\left.\frac{1}{6}\left(1 + i\sqrt{3}\right)\left(\frac{5}{2}\left(19925 - 281\sqrt{1865}\right)\right)^{1/3}\right\}\}$$

Now: substitute the solutions for $y$ into the polynomials depending only on $x$, $y$.

In[69]:=
```
Gx = Rest[G] /. sy; Short[Gx, 2]
```

Out[69]//Short=
$$\{\{0, 0, 711281250\, x^3\}, \ll 5 \gg, \{-623560$$
$$\left(-\frac{50}{3} + \frac{116}{3}\, 5^{\ll 1 \gg}\, (\ll 1 \gg)\left(\frac{2}{\ll 1 \gg}\right)^{1/3} + \frac{1}{6}\left(1 + i\sqrt{3}\right)\left(\frac{5}{2}\left(19925 - 281 \ll 1 \gg\right)\right)^{1/3}\right)^4 -$$
$$369975\, (\ll 1 \gg)^5 - 8952\, (\ll 1 \gg \ll 1 \gg^6 +$$
$$23709375\left(-\frac{50}{3} + \ll 1 \gg + \frac{1}{6}\,(1 + \ll 1 \gg)\,(\ll 1 \gg)^{1/3}\right)^2 x, \ll 1 \gg, \ll 1 \gg\}\}$$

Each of those is a system of equations *only depending on x* ⟶ take their GCD and solve!

The first four are easy, we get $x = 0$, thus we have $\langle 0, 0\rangle$ as a solution with multiplicity 4.

Now consider the fifth:

In[70]:=
```
Gx5 = Gx[[5]]; Map[Exponent[#, x] &, Gx5]
```

Out[70]=
```
{1, 2, 3}
```

In[71]:=
```
PolynomialRemainder[Gx5[[2]], Gx5[[1]], x] // Simplify
```

Out[71]=
```
0
```

```
In[72]:= PolynomialRemainder[Gx5[[3]], Gx5[[1]], x] // Simplify
Out[72]= 0
```

Thus the GCD of the 3 polynomials is the *first* one, the one with lowest degree! This is not by chance!

- In the process of backsubstitution, the GCD of the univariate polynomials in question is *always* the one with lowest degree [Gianni, Kalkbrener, 1987].

```
In[73]:= sx5 = Solve[Gx5[[1]] == 0, x]
```

$$\left\{\left\{x \to \frac{623560}{81}\left(-50-232\,5^{2/3}\left(\frac{2}{19925-281\sqrt{1865}}\right)^{1/3}-\left(\frac{5}{2}\left(19925-281\sqrt{1865}\right)\right)^{1/3}\right)^4+\frac{123325}{81}\left(-50-232\,5^{2/3}\left(\frac{2}{19925-281\sqrt{1865}}\right)^{1/3}-\left(\frac{5}{2}\left(19925-281\sqrt{1865}\right)\right)^{1/3}\right)^5+\frac{2984}{243}\left(-50-232\,5^{2/3}\left(\frac{2}{19925-281\sqrt{1865}}\right)^{1/3}-\left(\frac{5}{2}\left(19925-281\sqrt{1865}\right)\right)^{1/3}\right)^6\right)\Big/\left(2634375\left(-50-232\,5^{2/3}\left(\frac{2}{19925-281\sqrt{1865}}\right)^{1/3}-\left(\frac{5}{2}\left(19925-281\sqrt{1865}\right)\right)^{1/3}\right)^2\right)\right\}\right\}$$

```
In[74]:= s5 = Join[sy[[5]], sx5[[1]]]; N[s5]
Out[74]= {y → −40.0067, x → 10.1309}
```

Believe me, this is a solution …

```
In[75]:= F /. s5 // N
Out[75]= {−3.81988×10^−10, 4.54747×10^−13}
```

```
In[76]:= F /. s5 // Simplify
Out[76]= {0, 0}
```

Remaining solutions analogously …

*Mathematica* (e.g.) uses Gröbner bases in its internal Solve …

```
In[77]:= Solve[Thread[F == 0], {x, y}]
```

### Example (with parameters)

```
In[78]:= F = {A x^4 + B x y^2 + C y^3, x^2 y - 5 x y + 2 x^3};

In[79]:= G = GroebnerBasis[F, {x, y}, CoefficientDomain → RationalFunctions] // Short[#, 2] &
Out[79]//Short=
{-625 A^2 y^4 + (-150 A B + 40 B^2 - 200 A C) y^5 + (-5 A B - 40 A C + 8 B C - 16 C^2) y^6 - A C y^7,
  <<1>>, <<1>>, (-781250 A^6 + 625000 A^5 B - 2500000 A^5 C + 1000000 A^4 B C) x^3 +
   <<4>> + (-125 A^4 B C + <<12>> + 320 A^2 B C^3) y^6}

In[80]:= G = GroebnerBasis[F, {x, y, A, B, C}] // Short[#, 2] &
Out[80]//Short=
{625 A^2 C y^4 + 150 A B C y^5 - 40 B^2 C y^5 + 200 A C^2 y^5 + 5 A B C y^6 +
   40 A C^2 y^6 - 8 B C^2 y^6 + 16 C^3 y^6 + A C^2 y^7, <<19>>, 2 x^3 - 5 x y + x^2 y}
```

Care needs to be taken when doing symbolic computation with parameters:

- Taking the parameters to the coefficient domain considers them as belonging to a *field*, i.e. divisions etc. are performed, which, for particular values of the parameters, may be invalid. In the example: $C = 0$.
- Taking the parameters as polynomial variables considers them belonging to a *ring*. But more variables usually make the computation more expensive …

## Automated Theorem Proving

Gröbner bases have been applied successfully to automated theorem proving when statements about multivariate polynomials need to be proven. This is the case, for example, in theorems in geometry, when coordinates are introduced and geometrical properties are formulated by polynomial equations (points being on a line/curve, etc.).

### Example: Associativity of the Group Law on Elliptic Curves

- Let $\mathrm{E}$ be an elliptic curve be given by the Weierstrass equation $y^2 = x^3 + a\,x + b$ (we assume char[$K$] $\notin \{2, 3\}$, e.g. $K = \mathbb{Q}$).

```
In[81]:= ⟨x_, y_⟩ ∈ E  ^:=  -y^2 + x^3 + a x + b
```

- On $\mathrm{E}$ one can define the sum of two points $P = \langle p_1, p_2 \rangle$ and $Q = \langle q_1, q_2 \rangle$ as

$$P + Q := \begin{cases} O & \text{if } p_1 = q_1 \text{ and } p_2 = -q_2 \\ S\left[p_1, p_2, q_1, \frac{3p_1^2 + a}{2p_2}\right] & \text{if } p_1 = q_1 \text{ and } p_2 = q_2 \\ S\left[p_1, p_2, q_1, \frac{p_2 - q_2}{p_1 - q_1}\right] & \text{else} \end{cases}$$

$S[p_1, p_2, q_1, s] := \langle x_1, -p_2 + s\,(p_1 - x_1) \rangle$ where $x_1 = s^2 - p_1 - q_1$

```
In[82]:= ⟨p1_, p2_⟩ + ⟨q1_, q2_⟩  ^:=  S[p1, p2, q1, (p2 - q2)/(p1 - q1)]
```

In[83]:=
```
S[p1_, p2_, q1_, s_] := Module[{x1},
    x1 = s^2 − p1 − q1;
    ⟨x1, −p2 + s (p1 − x1)⟩]
```

◆ Associativity:

$\forall_{P,Q,R\in \mathrm{E}} : (P+Q)+R = P+(Q+R)$

Inspect *all cases* according to the definition by cases for +.
We show only *one of these cases*, namely where all sums go through the "default branch" in the definition.

$\forall_{p_1,p_2,q_1,q_2,r_1,r_2\in\mathbb{Q}} : \langle p_1, p_2\rangle, \langle q_1, q_2\rangle,$
$\langle r_1, r_2\rangle \in \mathrm{E} \Rightarrow (\langle p_1, p_2\rangle + \langle q_1, q_2\rangle) + \langle r_1, r_2\rangle = \langle p_1, p_2\rangle + (\langle q_1, q_2\rangle + \langle r_1, r_2\rangle)$

We split first and second component (and look only at the first now!), then we have the following structure:

$\forall_{p_1,p_2,q_1,q_2,r_1,r_2\in\mathbb{Q}} : \mathcal{A} = 0 \wedge \mathcal{B} = 0 \wedge C = 0 \Rightarrow \mathcal{D} - \mathcal{E} = 0$

$\neg\, \exists_{p_1,p_2,q_1,q_2,r_1,r_2\in\mathbb{Q}} : \mathcal{A} = 0 \wedge \mathcal{B} = 0 \wedge C = 0 \wedge \mathcal{D} - \mathcal{E} \neq 0$

Now the trick (Rabinovich-Trick):

$\neg\, \exists_{p_1,p_2,q_1,q_2,r_1,r_2,\xi\in\mathbb{Q}} : \mathcal{A} = 0 \wedge \mathcal{B} = 0 \wedge C = 0 \wedge (\mathcal{D} - \mathcal{E})\,\xi - 1 = 0$

In other words: The system of polynomial equations … has no solution!

This now can "easily" be decided by inspecting the Gröbner basis of $\{\mathcal{A}, \mathcal{B}, C, (\mathcal{D}-\mathcal{E})\,\xi - 1\}$:

In[84]:=
```
Clear[Subscript, p]
```

In[85]:=
```
𝒜 = ⟨p1, p2⟩ ∈ E
```

Out[85]=
$$b + a\,p_1 + p_1^3 - p_2^2$$

In[86]:=
```
ℬ = ⟨q1, q2⟩ ∈ E
```

Out[86]=
$$b + a\,q_1 + q_1^3 - q_2^2$$

In[87]:=
```
C = ⟨r1, r2⟩ ∈ E
```

Out[87]=
$$b + a\,r_1 + r_1^3 - r_2^2$$

In[88]:=
```
𝒟 = First[(⟨p1, p2⟩ + ⟨q1, q2⟩) + ⟨r1, r2⟩]
```

Out[88]=
$$p_1 + q_1 - \frac{(p_2-q_2)^2}{(p_1-q_1)^2} - r_1 + \frac{\left(-p_2 + \frac{\left(2\,p_1+q_1-\frac{(p_2-q_2)^2}{(p_1-q_1)^2}\right)(p_2-q_2)}{p_1-q_1} - r_2\right)^2}{\left(-p_1-q_1+\frac{(p_2-q_2)^2}{(p_1-q_1)^2} - r_1\right)^2}$$

In[89]:=
$$\mathcal{E} = \text{First}[\langle p_1, p_2\rangle + (\langle q_1, q_2\rangle + \langle r_1, r_2\rangle)]$$

Out[89]=
$$-p_1 + q_1 + r_1 + \frac{\left(p_2 + q_2 - \frac{\left(2q_1 + r_1 - \frac{(q_2 - r_2)^2}{(q_1 - r_1)^2}\right)(q_2 - r_2)}{q_1 - r_1}\right)^2}{\left(p_1 + q_1 + r_1 - \frac{(q_2 - r_2)^2}{(q_1 - r_1)^2}\right)^2} - \frac{(q_2 - r_2)^2}{(q_1 - r_1)^2}$$

In[90]:=
$$\text{Conclusion} = \text{Numerator}[\text{Together}[\mathcal{D} - \mathcal{E}]]\,\xi - 1;\ \text{Short}[\text{Conclusion}]$$

Out[90]//Short=
$$-1 + \xi\left(2\,p_1^9\,q_1^4 - 5\,p_1^6\,p_2^2\,q_1^4 + \text{≪1616≫} + 6\,p_1^2\,q_1^2\,r_2^6 - 4\,p_1\,q_1^3\,r_2^6 + q_1^4\,r_2^6\right)$$

In[91]:=
$$\text{GroebnerBasis}[\{\mathcal{A}, \mathcal{B}, \mathcal{C}, \text{Conclusion}\}, \{a, b, p_1, p_2, q_1, q_2, r_1, r_2, \xi\}]$$

Out[91]=
$$\{1\}$$

*BINGO!*

Second component & all other cases: analogously. The Gröbner basis is {1} in all cases!

# Further Reading

There is extensive literature on Gröbner basis! Just ‘‘googleing’’ for ‘‘Gröbner bases’’ will probably bring you ≈123.000 matches (as of April 18, 2006). Therefore some hints on where to start:

## Articles & Original Material (all by Buchberger)


- [1] Bruno Buchberger’s Phd Thesis: *Ein Algorithmus zum Auffinden der Basiselemente des Restklassen−rings nach einem nulldimensionalen Polynomideal* (An algorithm for finding the basis elements of the residue class ring of a zerodimensional polynomial ideal). Doctoral Thesis, Mathematical Institute, Univer−sity of Innsbruck, 1965. Originally in german. *English version available in JSC Volume 41, Issues 3−4, 2006*.
- [2] The 1970 article: *Ein algorithmisches Kriterium für die Lösbarkeit eines algebraischen Gleichungssys−tems* (An algorithmic criterion for the solvability of algebraic systems of equations). Aequationes Math.4 (3),374-383. Originally in german. *English version available in [5]*.
- [3] The 1985 article (aka the ‘‘Bose paper’’): *Gröbner Bases: An Algorithmic Method in Polynomial Ideal Theory*. In: N.K.Bose. Multidimensional Systems Theory, Reidel Publishing, 1985. *Very good survey!!! Rich Literature, also to all earlier papers by Buchberger!!!*
- [4] *Introduction to Gröbner Bases*. In [5].


## Books


- [5] Buchberger, Winkler (Eds.): Gröbner Bases and Applications. Proceedings of the International Confer−ence ‘‘33 Years of Groebner Bases’’. 1998, RISC, Austria. In: London Mathematical Society Lecture Note Series, Volume 251. Cambridge University Press.
- [6] Becker, Weispfenning: Gröbner Bases: A Computational Approach to Commutative Algebra. New York: Springer−Verlag, 1993.
- [7] Cox, Little, O’Shea: Ideals, Varieties, and Algorithms: An Introduction to Algebraic Geometry and Commutative Algebra, 2nd ed. New York: Springer−Verlag, 1996.


## Web

- *Gröbner bases bibliographic database*: organized by Buchberger in the frame of the Special Semester on Gröbner bases, 2006. Searchable by categories, downloadable versions of papers, etc. Very nice! http://www.ricam.oeaw.ac.at/Groebner−Bases−Bibliography/index.php
- Bruno Buchberger’s page about Gröbner bases: www.risc.uni−linz.ac.at/people/buchberg/groebner_bases.html

## Thanks …

**… I have my plane at 4 p.m.**