Polynomial Rings

All rings in this note are commutative.

1. Polynomials in Several Variables over a Field and Gröbner Bases

Example:

$f_1 = x^3y - xy^2 + 1$

$f_2 = x^2y^2 - y^3 - 1$

$g = x + y \in I(f_1, f_2)$

Find $a(x,y)$, $b(x,y)$ such that $a(x,y)f_1 + b(x,y)f_2 = g$

$$\left.\begin{array}{rl} y(f_1 = x^3y - xy^2 + 1) & \Longrightarrow yf_1 = x^3y^2 - xy^3 + y \\ -x(f_2 = x^2y^2 - y^3 - 1) & \Longrightarrow xf_2 = x^3y^2 - xy^3 - x \end{array}\right\} yf_1 - xf_2 = x + y$$

Definition: A *monomial ordering* on $x_1^{\alpha_1}x_2^{\alpha_2}\cdots x_n^{\alpha_n} > x_1^{\beta_1}x_2^{\beta_2}\cdots x_n^{\beta_n}$ total order that satisfies "well ordering hypothesis" $x^\alpha x^\beta$ then $\vec{x}^{\vec{\gamma}} \cdot \vec{x}^{\vec{\alpha}} > \vec{x}^{\vec{\gamma}} \cdot \vec{x}^{\vec{\beta}}$.

($\vec{x}^{\vec{\alpha}}$ = left, define ↑, $\vec{x}^{\vec{\beta}}$ = right)

Lexicographic = dictionary order on the exponents

$x_1^2x_2^3x_3^1 \underset{lex}{>} x_1^1x_2^3x_3^2$

$x_1^2x_2^2x_3^4 \underset{lex}{>} x_1^3x_2^2x_3^2x_4^2$

Looking at exponents $\vec{\alpha} = (\alpha_1, \alpha_2, \cdots, \alpha_n)$ and $\vec{\beta} = (\beta_1, \beta_2, \cdots \beta_n)$,

$$x^\alpha \underset{lex}{>} x^\beta \text{ if } \alpha_1 > \beta_1 \text{ and } (\alpha_2, \cdots, \alpha_n) \underset{lex}{>} (\beta_2, \cdots \beta_n).$$

Definition: Fix a monomial ordering on the polynomial ring $F[x_1, x_2, \cdots, x_n]$.

(1) The *leading term* of a nonzero polynomial $p(x)$ in $F[x_1, x_2, \cdots, x_n]$, denoted $LT(p(x))$, is the monomial term of maximal order in $p(x)$ and the leading term of $p(x) = 0$ is 0.
If $p(x) = \sum_\alpha c_{\vec{\alpha}}\vec{x}^{\vec{\alpha}}$ then $LT(p(x)) = \max_{\vec{\alpha}}\left(c_{\vec{\alpha}}\vec{x}^{\vec{\alpha}}\right)$.

(2) If I is an ideal in $F[x_1, x_2, \cdots, x_n]$, the *ideal of leading terms*, denoted $LT(I)$, is the ideal generated by the leading terms of all the elements in the ideal, i.e., $LT(I) = \langle LT(p(x)) : p(x) \in I\rangle$.

Example

If lexicographic, $LT(x^3y - xy^4 + 1) = x^3y$.
If graded lexicographic, $LT(x^3y - xy^4 + 1) = -xy^4$.

Definition: A *Gröbner basis* (dependent on monomial order) for an ideal I in the polynomial ring $F[x_1, x_2, \cdots, x_n]$ is a list of polynomials $f_1, \cdots, f_n$ for I whose leading terms generate the ideal of all leading terms in I, i.e., $I = \langle f_1, f_2, \cdots, f_n\rangle$ such that

$$LT(I) = \langle LT(f_1), LT(f_2), \cdots, LT(f_n)\rangle.$$

Fix a monomial ordering on $F[x_1, x_2, \cdots, x_n]$, and suppose $f_1, f_2, \cdots, f_n$ is a set of nonzero polynomials in $F[x_1, x_2, \cdots, x_n]$. If g is any polynomial in $F[x_1, x_2, \cdots, x_n]$, start with the set of quotient $q_1, q_2, \cdots, q_n$ and a remainder r, all polynomials at the end of this procedure where

$$g = q + 1f_1, +q_2 f_2 + \cdots + q_n f_n + r.$$

*Step*1: Check for smallest i such that $LT(f_i)$ divides $LT(g)$.

If no i exists (all $LT(f_i)$ do not divide $LT(g)$) then $r = g$ and $q_1 = q_2 = \cdots = q_n = 0$ *STOP*!
If $LT(f_i)$ divides $LT(g)$ then add $\frac{LT(g)}{LT(f_i)}$ to q_i and $g' = g - \frac{LT(g)}{LT(f_i)} f_i$.

*Step*2: Repeat with g' until *STOP*!

Example:

$g = x^3y^3 + 3x^2y^4$
$f_1 = xy^4$

If lexicographic, $g = 0 \cdot f_1 + x^3y^3 + 3x^2y^4$
If reverse lexicographic, $g = 3x(x^2y^4) + x^3y^3$

$g = x^2 + x - y^2 + y$
$f_1 = xy + 1$
$f_2 = x + y$

$$g' = -x(x+y) + x^2 + x - y^2 + y = -xy + x - y^2 + y$$
$$g'' = (xy+1) - xy + x - y^2 + y = x - y^2 + y + 1$$
$$g''' = -(x+y) + x - y^2 + y + 1 = -y^2 + 1$$
$$g = -1 \cdot (xy+1) + (x+y) + (-y^2+1)$$

Exercise: Try the example above with $f_1 = x + y$, $f_2 = xy + 1$, and $g = x^2 + x - y^2 + y$

For a Gröbner basis the result is unique $\Longrightarrow g \in I(= \langle f_1, \cdots, f_n \rangle,\ f_1, \cdots f_n$ is Gröbner basis) $\Longleftrightarrow$ division algorithm reduces g to 0 remainder.
Gröbner basis always exists for a polynomial ring over a field.

Examples *on Sage*

(1) Does $x + y$ lie in the ideal generated by

$$f_1 = x^3 \cdot y - x \cdot y^2 + 1$$
$$f_2 = x^2 \cdot y^2 - y^3 - 1$$

```
sage: P = PolynomialRing(QQ,['x','y'])
sage: (x,y)=P.gens()
sage: f1 = x^3*y-x*y^2+1
sage: f2 = x^2*y^2-y^3-1
sage: P.ideal([f1,f2]).reduce(x+y)
0
```

Computer says "yes" to question (1).
Lets look at the Grobner basis:

```
sage: P.ideal([f1,f2]).groebner_basis()
[y^4 - y^3 - 1, x + y]
```

(2) How can we express $x + y$ as an algebraic combination of the generators f_1 and f_2?
Answer: Reduce $z(x + y)$ in the ideal $\langle z \cdot f_1 - z_1, z \cdot f_2 - z_2 \rangle$ where z, z_1, z_2 are all 'dummy' variables and x, y and z are all higher weight than z_1 and z_2.

```
sage: P = PolynomialRing(QQ,['x','y','z','z1','z2'])
sage: (x,y,z,z1,z2)=P.gens()
sage: f1 = x^3*y-x*y^2+1
sage: f2 = x^2*y^2-y^3-1
sage: P.ideal([z*f1-z1,z*f2-z2]).reduce(z*(x+y))
y*z1 - x*z2
```

The computer says: $x + y = y \cdot f_1 - x \cdot f_2$.
Lets look at the Grobner basis:

```
sage: P.ideal([z*f1-z1,z*f2-z2]).groebner_basis()
[y^4*z + x*y^3*z1 - y^4*z1 - x^2*y^2*z2 + x*y^3*z2 - y^3*z - z - z2,
 x^2*y^2*z1 - x^3*y*z2 - y^3*z1 + x*y^2*z2 - z1 - z2, x*z + y*z - y*z1 + x*z2]
```

(3) Given a list of polynomials:

$$g_1 = x^2 \cdot y - x^3 \cdot y^2 + 2 \cdot x^2 + y^2 - 1$$
$$g_2 = x \cdot y - x^2 + y^3 - 2$$
$$g_3 = x \cdot y^2 + x^3 + y^3 - x - 1$$

find what algebraic combination gives the polynomial:
$x^6*y^7-x^8*y^4+x^7*y^5-2*x^5*y^6+2*x^7*y^3-4*x^6*y^4-4*x^5*y^5-2*x^3*y^7-x^9+x^7*y^2-7*x^6*y^3$
$-x^5*y^4-7*x^4*y^5-4*x^3*y^6-3*x^2*y^7-3*x*y^8-y^9-2*x^6*y^2+5*x^5*y^3+3*x^4*y^4+x^3*y^5$
$+2*x^2*y^6+3*x^7-4*x^6*y+16*x^5*y^2+10*x^4*y^3+9*x^3*y^4+10*x^2*y^5+3*x*y^6+y^7-x^6$
$+5*x^5*y+x^4*y^2+10*x^3*y^3+x^2*y^4+6*x*y^5+2*y^6-7*x^4*y-4*x^3*y^2-9*x^2*y^3-y^5$
$-10*x^4-5*x^3*y-12*x^2*y^2-7*x*y^3-2*y^4-4*x^3+4*x^2*y-3*x*y^2+7*x^2$
$+2*x*y+3*y^2+2*x-2$

```
sage: P = PolynomialRing(QQ,['x','y','z1','z2','z3'])
sage: (x,y,z1,z2,z3) = P.gens()
sage: g1 = x^2*y-x^3*y^2+2*x^2+y^2-1
sage: g2 = x*y-x^2+y^3-2
sage: g3 = x*y^2+x^3+y^3-x-1
sage: f = x^6*y^7 - x^8*y^4 + x^7*y^5 - 2*x^5*y^6 + 2*x^7*y^3 - 4*x^6*y^4
- 4*x^5*y^5 - 2*x^3*y^7 - x^9 + x^7*y^2 - 7*x^6*y^3 - x^5*y^4 - 7*x^4*y^5
- 4*x^3*y^6 - 3*x^2*y^7 - 3*x*y^8 - y^9 - 2*x^6*y^2 + 5*x^5*y^3 + 3*x^4*y^4
+ x^3*y^5 + 2*x^2*y^6 + 3*x^7 - 4*x^6*y + 16*x^5*y^2 + 10*x^4*y^3 + 9*x^3*y^4
+ 10*x^2*y^5 + 3*x*y^6 + y^7 - x^6 + 5*x^5*y + x^4*y^2 + 10*x^3*y^3 + x^2*y^4
+ 6*x*y^5 + 2*y^6 - 7*x^4*y - 4*x^3*y^2 - 9*x^2*y^3 - y^5 - 10*x^4 - 5*x^3*y
- 12*x^2*y^2 - 7*x*y^3 - 2*y^4 - 4*x^3 + 4*x^2*y - 3*x*y^2 + 7*x^2 + 2*x*y
+ 3*y^2 + 2*x - 2
sage: P.ideal([g1-z1,g2-z2,g3-z3]).reduce(f)
z1^2*z2 - z3^3 + z1*z3 - z2*z3
```

The computer says:

$$f = g_1^2 \cdot g_2 - g_3^3 + g_1 \cdot g_3 - g_2 \cdot g_3$$

lets check:

```
sage: f == g1^2*g2 - g3^3 + g1*g3 - g2*g3
True
```

For next time:

(1) Gröbner basis exists,

(2) the quotient and remainder is unique with a Gröbner basis.