# Polynomial Rings

All rings in this note are commutative.

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

If $f \in \langle f_1, f_2, \cdots, f_m\rangle$ and $f = a_1f_1 + a_2f_2 + \cdots + a_mf_m$ then

$$I' = \langle zf_1 - z_1, zf_2 - z_2, \cdots, zf_m - z_m\rangle \subset \mathbb{C}[x_1, x_2, \cdots, x_n, \underbrace{z, z_1, z_2 \cdots, z_m}_{\text{dummy variables}}]$$

reduce $_{I'}(zf) = a_1z_1 + a_2z_2 + \cdots + a_mz_m$

$$LT(a_1z_1 + a_2z_2 + \cdots + a_mz_m) < LT(zf)$$

and we have chosen our ideals so that

$$f = a_1f_1 + a_2f_2 + \cdots + a_mf_m \ .$$

There was an example last time where $f_1 = x^3y - xy^2 + 1$, $f_2 = x^2y^2 - y^3 - 1$ and we saw that reducing $x + y$ $(mod\ \langle f_1 - z_1, f_2 - z_2\rangle)$ isn't good enough to tell us how to write $x + y$ in terms of $f_1$ and $f_2$ because

$$\underset{(1,0,0,0)}{x} + \underset{(0,1,0,0)}{y} = \underset{(0,1,1,0)}{yz_1} - \underset{(1,0,0,1)}{xz_2} \ (\text{mod } I')$$

but $LT(x + y) = x$ and $LT(yz_1 - xz_2) = xz_2$ and $x < xz_1$ so $x + y$ is the smallest element of its class. However the following example fixes that.

**Example:**

Choose the lexicographic ordering $x > y$ on $F[x, y]$ and consider the ideal $I$ generated by $f_1 = x^3y - xy^2 + 1$ and $f_2 = x^2y^2 - y^3 - 1$. We know that $x + y \in \langle f_1, f_2\rangle$, but we wish to find $a_1$ and $a_2$ such that $x + y = a_1f_1 + a_2f_2$.

To find the $a_1$ and $a_2$ so that $x+y$ can be written in terms of $G = \{f_1, f_2\}$ as $x+y = a_1f_1+a_2f_2$ we reduce $z(x + y)$ modulo the ideal $\langle zf_1 - z_1, zf_2 - z_2\rangle$ and we find that it is equivalent to $yz_1 - xz_2$. In this case $LT(z(x + y)) = xz$ and $LT(yz_1 - xz_2) = xz_2$ and $xz > xz_2$ so then $yz_1 - xz_2$ is the smallest element of the class where $I' = \langle zf_1 - z_1, zf_2 - z_2\rangle$ so we have $z(x + y) + I' = yz_1 - xz_2 + I'$. This shows that $x + y = yf_1 - xf_2$. We can check this by calculating explicitly that $y(x^3y - xy^2 + 1) - x(x^2y^2 - y^3 - 1) = x + y$.

**Theorem:** Fix a monomial ordering on $R = F[x_1, \cdots, x_n]$ and suppose $\{g_1, \cdots, g_m\}$ and $\{g_{\sigma(1)}, \cdots, g_{\sigma(m)}\}$ be Gröbner basis for the nonzero ideal $I$ in $R$. Let $f_I, f_{I'} \in I$ and $r, r'$ be the quotient remainder where division algorithm with two Gröbner basis can be written uniquely in the form

$$f = f_I + r = f_{I'} + r'$$
$$r - r' = f_{I'} - f_I \in I$$

with none of the monomials in $r - r'$ are divisible by any of the leading terms $LT(g_i)$ but $LT(r - r') \in LT(\langle g_1, \cdots, g_m\rangle)$ and the only way this can happen is if $r - r' = 0$. $r$ is unique representative of the coset such that none of the monomials of $r$ are divisible by $LT(g_i)$.

**Corollary:** If $I$ is an ideal in the polynomial ring $F[x_1, x_2, \cdots, x_n]$ over a field $F$ then $I$ is finitely generated.

**Theorem:** If $g_1, g_2, \cdots, g_m$ are any set of elements of $I$ such that

$$LT(I) = \langle LT(g_1), LT(g_2), \cdots, LT(g_m)\rangle$$

then $I = \langle g_1, g_2, \cdots, g_m\rangle$.

*Sketch of proof:* Let $f \in I$, then $f = f_I + r$ where $r$ is remainder after polynomial division. $\implies f \in I$ and $f_I \in I$ then $f - f_I = r \in I \implies LT(r) \in LT(I) = \langle LT(g_1), LT(g_2), \cdots, LT(g_m)\rangle$ $\implies LT(r)$ id an alg com of the $LT(g_i)$ and a monomial but this is impossible unless $LT(r) = 0$ because none of the monomials of $r$ are divisible by $LT(g_i)$.

**Proposition:** Fix a monomial ordering on $R = F[x_1, \cdots, x_n]$ and let $I$ be a nonzero ideal in $R$. $I$ has a Gröbner basis.

*Sketch of proof:* Take $LT(I)$ and find a finite list of generators

$$LT(h_1), \cdots, LT(h_k) \text{ for some list of elements of the ring } R : h_1, \cdots, h_k.$$

This list exists because $R$ is Noetherian. The list $h_1, \cdots, h_k$ generates $I$ and is the Gröbner basis.

**Exercise:** Given $f \in \langle g_1, g_2, \cdots, g_m\rangle$ does there exist a polynomial $p(z_1, \cdots, z_m)$ with coefficient in the ring where $g_1, g_2, \cdots, g_m$ live such that $p(g_1, g_2, \cdots, g_m) = f$ if not, find $r$ in the polynomial ring such that

$$p(g_1, g_2, \cdots, g_m) = f - r.$$