Gröbner Bases

Fabiana ÇULLHAJ[1], Edmond PISHA[2]

- *Department of Mathematic, University of "Aleksander Moisiu" Durres, Albania*
  Email: fabianacullhaj@hotmail.com– Phone: +355693067339
- *Department of Mathematic, Tirana University, Albania.*
  Email: pishamondi@yahoo.com– Phone: +355692532476

ABSTRACT

In this paper, we will give a leisurely introduction to the theory of Gröbner bases. First we will see how to determine whether a polynomial *f* is contained in an ideal and how an answer to this problem leads to a method to determine whether two ideals are equal. We will use Euclidian Algorithem for solving this problems. After that will be introduced what we mean by the leading term of a polynomial in *n* variables. So we will explain Gröbner bases notion and will present the algorithem due to Bruno Buchberger wich transform the abstract notion of a Gröbner basis in a fondamental tool in computational algebra. And in the end we will give some applications of Gröbner bases.

Keywords: *Variety, algorithem, term order, Gröbner bases, reduced, S-polynomial.*

1. INTRODUCTION

Let k be a field. Consider $k[x_1,\ldots,x_n]$ which is the set of all polynomials in the variables $x_1,\ldots,x_n$ with coefficients in k. Such polinomial are finite sums of *terms* of the form $ax_1^{1},\ldots,x_n^{n}$, where $a \in k$ and $_i \in \mathrm{N}, i = 1,\ldots,n$. We call $x_1^{1},\ldots,x_n^{n}$ *a power product*. Note that $k[x_1,\ldots,x_n]$ is a commutative ring with respect to polynomial addition and multiplication.

***Definition* 1.1**. *Let I ċ k[$x_1,\ldots,x_n$], I ÷ ¤. I is an ideal in k[$x_1,\ldots,x_n$] if*

1. *f; g Č I implies that f + g Č I.*
2. *f Č I and h Č k[$x_1,\ldots,x_n$] implies that hf Č I.*

It will be important for us to be able to identify all of the generators of an ideal.

One of the most important results in polynomial ideal theory is the Hilbert Basis Theorem. This result is important because it says that any ideal in $k[x_1,\dots,x_n]$ has a finite set of generators.

Theorem 1.2 *(Hilbert Basis Theorem) Every ideal in* $k[x_1,\dots,x_n]$ *is finitely generated.In other words, if I is an ideal in* $k[x_1,\dots,x_n]$*, then there exists* $f_1,\dots, f_s$ Č $k[x_1,\dots,x_n]$*such that*

$$I = \langle f_1,\dots, f_s \rangle = \left\{ \sum_{i=1}^{s} u_i f_i / u_i \in k[x_1,\dots,x_n], i = 1,\dots,n \right\}.$$

Let see the polinomials with one variable from $k[x]$. Here we will use the well known Euclidean Algorithem. First let give some notation: If $f \neq 0 \in k[x]$,

$$f = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$$

with $a_i \in$ k and $a_n \neq 0$, $i = 1,\dots,n$, then:

The *degree* of f, denoted $deg(f) = n$, is the larges exponent of x in f.

The *leading term* of f, denoted $lt(f) = a_n x^n$, is the term of f with highest degree.

The *leading coefficient* of f, denoted $lc(f) = a_n$, is the coefficient in the leading term of f.

The main tool in Euclidean Algorithem is the **Division Algorithem**:

INPUT: $f, g \in k[x]$ with $g \neq 0$

OUTPUT: q, r such that $f = qg + r$ and

$r = 0$ or $deg(r) < deg(g)$

INITIALIZATION: $q =: 0; r =: f$

WHILE $r \neq 0$ **AND** $deg(r) < deg(g)$**DO**

$$q := q + \frac{lt(r)}{lt(g)}$$

$$r := r - \frac{lt(r)}{lt(g)} g$$

Now let $I = \langle f, g \rangle$ and suppose that $f \xrightarrow{g} h$ Then since $h = f - \frac{lt(r)}{lt(g)} g$ we can replace *f* by *h* in the generating set of *I*, $I = \langle h, g \rangle$. So we can gave the nex theorem:

Theorem 1.2: *Every ideal* f Č $k[x]$ *is generated by one element*.

Proposition 1.3: *Let* $f_1, f_2 \in k[x]$, *with one of* f_1, f_2 *not zero. Then* $gcd(f_1, f_2)$ *exist and*

$$\langle f_1, f_2 \rangle = \langle \gcd(f_1, f_2) \rangle.$$

So by the **Euclidean Algorithem** we can finde gcd, and so we can finde a single generator of ideal $\langle f_1, f_2 \rangle$.

INPUT: $f_1, f_2 \in k[x]$ with one of f_1, f_2 not zero
OUTPUT: $f = gcd(f_1, f_2)$
INITIALIZATION: $f =: f_1$, $g =: f_2$
WHILE $g \neq 0$ **DO**

$f \xrightarrow{g}_+ r$ where *r* is the reminder of the division of *f* by *g*
$f := g$
$g := r$
$f := \frac{1}{lc(f)} f$

We can proceed in the same way in the case of ideals generated by more than two polynomials, $I = \langle f_1, .., f_n \rangle$ with not all f_i'zero.

2. TERM ORDERS

Recall that the set of power products is denoted by: $T^n = \{ x_1^{1}, \ldots, x_n^{n} \mid {}_i \in N, i = 1,..,n \}$. If we have $x^{\sim}$, $x \in T^n$, exactly one of the following three relations must happen:

$$x^{\sim} < x , \quad x^{\sim} = x \quad \text{or } x^{\sim} > x .$$

***Definition* 2.1**: *A term order on* T^n *is a total order* $<$ *on* T^n *such that*

1. $1 < x$ *for all* x Č T^n, $x \div 1$.

2. *If* $x^{\sim} < x$ *,then* $x^{\sim} x^{¥} < x \ x^{¥}$ *for all* $x^{¥}$ Č T^n.

Next we give some examples of term orders that are commonly used. We will assume that

$$x_1 > x_2 > ,\ldots,> x_n.$$

Definition* 2.2.** *We define the* ***lexicographical ordering *(denoted by lex) as follows:*
For $\sim = (\sim_1,..,\sim_n); \quad = (\ _1,.., \ _n)$ Č N^n *we define*

$$x^{\sim} < x \quad <=> \begin{cases} \text{the first coordinates } \sim_i \text{ and } \ _i \text{ in } \sim \text{ and } \ , \\ \text{form the left, which are different, satisfy } \sim_i < \ _i \end{cases}$$

Definition* 2.3.** *We define the* ***degree lexicographical ordering *(denoted deglex) as follows:*
For $\sim = (\sim_1,..,\sim_n); \quad = (\ _1,.., \ _n)$ Č N^n *we define*

$$x^{\sim} < x \quad <=> \begin{cases} \sum_{i=1}^{n} \sim_i < \sum_{i=1}^{n} \ _i \\ \sum_{i=1}^{n} \sim_i = \sum_{i=1}^{n} \ _i \text{ and } x^{\sim} < x \\ \text{with respect to lex with } x_1 > x_2 > \ldots > x_n \end{cases}$$

Definition* 2.4** *We define the* ***degree reverse lexicographical ordering *(denoted degrevlex) as follows: For* $\sim = (\sim_1,..,\sim_n); \quad = (\ _1,.., \ _n)$ Č N^n *we define*

$$x^{\sim} < x \quad <=> \begin{cases} \sum_{i=1}^{n} \sim_i < \sum_{i=1}^{n} \ _i \\ \sum_{i=1}^{n} \sim_i = \sum_{i=1}^{n} \ _i \text{ and the first coordinate } \sim_i \text{ and } \ _{\mathrm{i}} \\ \text{in } \sim \text{ and } \ \text{ from the right, xhich are different, satisfy } \sim_{\mathrm{i}} > \ _i \end{cases}$$

Now choose a term order on T^n. For all $f \in k[x_1,\ldots,x_n]$ we can write

$$f = a_1 x^{\sim_1} + a_2 x^{\sim_2} + \ldots + a_r x^{\sim_r}$$

where $0 \neq a_i \in k$, x^{ai} are power products, and $x^{\sim_1} > x^{\sim_2} > \ldots > x^{\sim_r}$. We definene:

(i) the leading power product of f to be $lp(f) = x^{\sim_1}$;
(ii) the leading coefficient of f to be $lc(f) = a_1$;
(*iii*) the leading term of f to be $lt(f) = a_1 x^{\sim_1}$.

3. MULTIVARIABLE DIVISION ALGORITHM

Definition* 3.1.** *Let f; g; h* $\in k[x_1,\ldots,x_n]$ *with g ÷ 0. We say that f* ***reduces *to h modulo g in one step, denoted* $f \xrightarrow{g} h,$

if and only if lp(g) divides a non-zero term $ax^{\sim}$ *that appears in f and*

$$f = f - \frac{\sim x^{\sim}}{lt(g)} g.$$

***Definition* 3.2.** *Let f, h and* $f_1,\ldots,f_s$ *be the polinomials in* $k[x_1,\ldots,x_n]$ *with* f_i *÷ 0 for* $i=1,\ldots,s$.
Let F ={ $f_1,\ldots,f_s$ }*. We say that f* ***reduces*** *to h modulo F, denoted*

$$f \xrightarrow{F}_{+} h,$$

if and only if there exist a sequence of indices $i_1, i_2,..,i_t \in \{ 1,\ldots,s \}$ *and a sequence of polynomials* $h_1,\ldots, h_{t-1} \in k[x_1,\ldots,x_n]$ *such that*

$$f \xrightarrow{f_{i_1}} h_1 \xrightarrow{f_{i_2}} h_2 \xrightarrow{f_{i_3}} \ldots \xrightarrow{f_{i_{t-1}}} h_{t-1} \xrightarrow{f_{i_t}} h.$$

Definition* 3.3**. *A polynomial r is called* ***reduced *with respect to a set of non-zero polynomials*
F ={ $f_1,\ldots,f_s$ } *if r = 0 or no power product that appears in r is divisible by any one of the* $lp(f_i)$*, i = 1,…, s. In other words, r cannot be reduced modulo F.*

Definition* 3.4.** *If* $f \xrightarrow{F}_{+} r$ *and r is reduced with respect to F, then we call r a* ***remainder *for f with respect to F.*

The reduction process allows the formulation of the following ***division algorithm for multivariate polynomials*** which mirrors the univariate division algorithm:

INPUT: $f_1, f_2,\ldots,f_s \in k[x_1,\ldots,x_n]$ *with* f_i ÷ 0
OUTPUT: $u_1,\ldots,u_s$*, r such that* $f = u_1f_1+\ldots+u_sf_s+r$ *and r is reduced with respect to*
{ $f_1,\ldots,f_s$} *and* $\max(lp(u_1)lp(f_1),\ldots, lp(u_s)lp(f_s),lp(f_r))=lp(f)$
INITIALIZATION: $u_1:= 0,\ldots,u_s:= 0, r: = 0, h: = f$
WHILE $h \neq 0$ **DO**
If there exists *i* such that lp(f_i) divides lp(*h*) **Then**

Choose i least such that lp(f_i) divides lp(h)

$$u_i := u_i + \frac{\mathrm{lt(h)}}{lt(f_i)}$$

$$h_i := h_i - \frac{\mathrm{lt(h)}}{lt(f_i)} f$$

ELSE

$$r := r + lt(h)$$

$$h := h - lt(h)$$

4 . GRÖBNER BASES AND BUCHBERGER'S ALGORITHM

***Definition* 4.1**. *A set of non-zero polynomials G ={ $g_1,\ldots,g_t$ }, contained in an ideal I, is called a* **<u>Gröbner basis</u>** *for I if and only if for all f Č I such that f ÷ 0, there exists iČ {1,…,t} such that lp(g_i) divides lp(f).*

***Definition* 4.2:** *For a subset S of k[$x_1,\ldots, x_n$], the leading term ideal of S is the ideal*

Lt(S)= $\langle lt(s) / s \in S \rangle$.

Theorem 4.3 . *Let I be a non-zero ideal of k[$x_1,\ldots, x_n$]. The following statements are equivalent for a set of non-zero polynomials G ={ $g_1,\ldots,g_t$ }$\subseteq$ I.*

(i) G is a Gröbner basis for I.

(ii) f Č I if and only if $f \xrightarrow{G}_+ 0$.

(iii) f Č I if and only if $f = \sum_{i=1}^{t} h_i g_i$ *with* lp(*f*)= $\max_{1 \le i \le t}(\mathrm{lp}(h_i)\mathrm{lp}(\mathrm{g_i}))$

(iv) Lt(G)=Lt(I).

As a consequence of the preceding theorem, we have the important result, pointed out earlier, that a Gröbner basis G = {$g_1,\ldots,g_t$}for I is a set of generators for I,that is, I = $\langle g_1,\ldots, g_t \rangle$.

Another important consequence of the preceding theorem is the fact that every nonzero ideal I $\subseteq$ k[$x_1,\ldots, x_n$] has a Gröbner basis.

Given a set of generators $f_1,\ldots,f_s$ of an ideal I $\subseteq$ k[$x_1,\ldots, x_n$], Buchberger's Algorithm produces a Gröbnerbasis for I. We recall that such a finite set of generators for I always exists by Hilbert's Basis Theorem.

Definition* 4.5**. *Let L = lcm(lp(f), lp(g)). The* ***S-polynomial *of f and g is defined to be*

$$S(f,g)=\frac{L}{lt(f)}f-\frac{L}{lt(g)}g.$$

BUCHBERGER'S ALGORITHM

INPUT: F ={$f_1,\ldots,f_s$ } $\subseteq k[x_1,\ldots,x_n]$ *with* f_i ÷ 0 (1≤ i ≤ s)
OUTPUT: G ={ $g_1,\ldots,g_t$ }, a Gröbner basis for $\langle f_1,\ldots,f_s\rangle$
INITIALIZATION: *G:= F,G :=* {{f_i; f_j} | f_i ÷ f_j Č *G*}
WHILE $G \neq 0$ **DO**

Choose *any* {*f, g*}$\in$ *G*
G: = G – {{*f, g*}}
$S(f,g \xrightarrow{G}_+ h$ where *h* is reduced with respect to G
IF $h \neq 0$**THEN**

G: = G $\cup$ {{*u, h*}|for all *u*Č *G* }
G: = G $\cup$ {*h*}

<u>*Example.*</u> ([1], Problem 1.7.3(b))
Let $f_1 = x^2y + z$; $f_2 = xz + y$ Č $Q[x; y; z]$ *and lex,* $z > y > x$, *be the term order. We want to find a Gröbner basis for* $\langle f_1, f_2\rangle$.

INITIALIZATION: G := {f_1; f_2}, *G =* {{f_1; f_2}}
Step 1.

Choose {f_1; f_2}*:*
G := Ą
$S(f_1,f_2)=\frac{xz}{z}\left(z+x^2y\right)-\frac{xz}{xz}(xz+y)=x^3y-y=h$ *which is reduced with respect*
to G since lp(f₁) = z, lp(f₂) = xz
Since h ÷ *0, let* $f_3 := x^3y$ J y
G := {{f_1; f_3},{{f_2; f_3}}
G := {f_1; f_2; f_3}*;*

Step 2.

Choose {f_1; f_3}.
G := {f_2; f_3}
$S(f_1,f_3)=\frac{x^3yz}{z}\left(x^2y+z\right)-\frac{x^3yz}{xz}(x^3y-y)=x^5y^2+yz$
Note that $yz + x^5y^2 = y\,(z + x^2y) + (x^5y^2 - x^2y^2)$

$x^5y^2 - x^2y^2 = x^2y\,(x^3y - y)$

Therefore, since $S(f_1, f_3) = yf_1 + x^2yf_3,\ S(f_1, f_3) \xrightarrow{G}_+ 0 = h$

Step 3.

Choose {$f_2; f_3$}.

G := Ą;

$$S(f_2, f_3) = \frac{x^3yz}{xz}(xz + y) - \frac{x^3yz}{x^3y}(x^3y - y) = x^2y^2 + yz = yf_1$$

Thus, $S(f_2, f_3) \xrightarrow{G}_+ 0 = h$

The algorithm ends, G = {$f_1; f_2; f_3$} is our desired Gröbner basis.

The following example shows that the algorithm is sensitive to the term order chosen. That is, for the same input of generators { $f_1,\ldots, f_s$ }, we may get different Gröbner basis outputs, depending on the term order.

<u>*Example*</u> ([1], Problem 1.7.3(a))

Let $f_1; f_2$ be as above but let the term order be deglex, $x > y > z$:

INITIALIZATION: G := {$f_1; f_2$}, G := {{$f_1; f_2$}}

Step 1.

Choose {$f_2; f_1$}*:*

G := Ą

$S(f_2, f_1) = \frac{x^2yz}{xz}(xz + y) - \frac{x^2yz}{x^2y}(x^2y + z) = xy^2 - z^2 = h$, *which is reduced with respect to G since lp(f_1) = x^2y, lp(f_2) = xz*

Since h ÷ 0, let f_3 := xy^2 J *z^2 (Note that lp(f_3) = xy^2)*

G := {{$f_1; f_3$},{$f_2; f_3$}}

G := {$f_1; f_2; f_3$}

Step 2.

Choose {$f_1; f_3$}*:*

G := {{$f_2; f_3$}}

$$S(f_1, f_3) = \frac{x^2y^2}{x^2y}(x^2y + z) - \frac{x^2y^2}{xy^2}(xy^2 + z^2) = xz^2 + yz = z\ f_2$$

So, $S(f_1, f_3) \xrightarrow{G}_+ 0 = h$

Step 3.

Choose {$f_2; f_3$}*:*

G := Ą

$S(f_2, f_3) = \frac{xy^2z}{xz}(xz + z) - \frac{xy^2z}{xy^2}(xy^2 - z^2) = y^3 - z^2 = h$, *which is reduced with*

respect to G.

Since h ÷ 0, let $f_4 := y^3 + z^3$ *(Note that* $lp(f_4) = y_3$*)*

$G := \{\{f_1; f_4\}; \{f_2; f_4\}; \{f_3; f_4\}\}$

$G := \{f_1; f_2; f_3; f_4\}$

Step 4.

Choose $\{f_4; f_1\}$:

$G := \{\{f_2; f_4\}; \{f_3; f_4\}\}$

$$S(f_4, f_1) = \frac{x^2y^3}{y^3}(y^3 + z^3) - \frac{x^2y^3}{x^2y}(x^2y + z) = x^2z^3 - y^2z = (xz^2 - yz) f_2$$

So $S(f_4, f_1) \xrightarrow{G}_+ 0 = h$

Step 5.

Choose $\{f_4; f_2\}$:

$G := \{\{f_3; f_4\}\}$

$$S(f_4, f_2) = \frac{xy^3z}{y^3}(y^3 + z^3) - \frac{xy^3z}{xz}(xz + y) = xz^4 - y^4$$

Note that $xz^4 - y^4 = z^3(xz + y) = (-y^4 - yz^3) - y^4 - yz^3 =$

$= -y(y^3 + z^3)$

Therefore, since $S(f_4; f_2) = z^3 f_2$ J $y f_4$, $S(f_4, f_2) \xrightarrow{G}_+ 0 = h$

Step 5.

Choose $\{f_4; f_3\}$:

$G := \varnothing$

$$S(f_4, f_3) = \frac{xy^3}{y^3}(y^3 + z^3) - \frac{xy^3}{xy^2}(xy^2 - z^2) = xz^3 + yz^2 = z^2 f_2$$

So $S(f_4, f_3) \xrightarrow{G}_+ 0 = h$

The algorithm ends, $G = \{f_1; f_2; f_3; f_4\}$ *is our desired Gröbner basis.*

Moreover, we point out that even in the event that the term order is fixed, uniqueness of Gröbner bases is not guaranteed. Buchberger's Algorithm can produce different Gröbner bases if different f_i are chosen at a given step. In order to achieve uniqueness, one needs to restrict Gröbner bases as follows (see [1]):

***Definition* 4.6**. *A Gröbner basis G = {g_1,…,g_t} is called* **minimal** *if for all i, lc(g_i)=1 and for all i ÷ j, lp(g_i) does not divide lp(g_j).*

***Definition* 4.7**. *A Gröbner basis G = {g_1,…,g_t}is called a* **reduced** *Gröbner basis if, for all i, lc(g_i)=1 and g_i is reduced with respect to G – {g_i} That is, for all i, nonon-zero term in g_i is divisible by any lp(g_j) for any j ÷ i.*

Theorem 4.8: *Fix a term order. Then every non-zero ideal I has a unique reduced Gröbner basis with respect to this term order.*

5. Applications of Gröbner basis

Proposition 5.1: *Let I, J be ideals in k[x_1,…,x_n] and let w be a new variable. Consider the ideal* $\langle wI,(1-w)J\rangle$ *in k[x_1,…,x_n, w]. Then* I ∩ J = $\langle wI,(1-w)J\rangle$ ∩*k*[x_1,…,x_n, *w*].

<u>*Example:*</u> Consider the following ideals in Q[*x*, *y*]: $I=\langle x^2+y^3-1, x-yx+3\rangle$ and $J=\langle x^2y-1\rangle$.

We wish to compute I ∩ J. We compute a Gröbner basis G for the ideal $\langle w(x^2+y^3-1), w(x-yx+3), (1-w)(x^2y-1)\rangle \subseteq \mathrm{Q}[x,y,w]$ using the deglex term ordering on the variables *x* and *y* with *x* > *y* and an elemination order with *w* greater than *x, y*. We get

$$G=\{x^3y^2-x^3y-3x^2y-xy+x+3, x^2y^4+x^4y-x^2y-y^3-x^2+1,$$
$$12853w+118x^4y+9x^2y^3-357x^3y-972x^2y^2+215x^2y-118x^2-9y^2+35x+97y-215,$$
$$x^5y+3x^2y^3+3x^2y^2-x^3+3x^2y-3y^2-3y-3\}.$$

So a Gröbner basis G for the ideal I ∩ J is

$$\{x^3y^2-x^3y-3x^2y-xy+x+3, x^2y^4+x^4y-x^2y-y^3-x^2+1, x^5y+3x^2y^3+3x^2y^2-x^3+3x^2y-3y^2-$$

Definition* 5.2*: *Let I, J be ideals in k [x_1,…, x_n]. The ideal quotient J : I is definited to be*

J : I = {*g*Č *k*[x_1,…,x_n]| gI ⊆ J }.

Lemma 5.3: *Let I=*$\langle f_1,\dots, f_s\rangle$ *be ideals in k*[x_1,…,x_n]. *Then* $J:I=\bigcap_{I=1}^{n} J:\langle f_i\rangle$.

Example: Let $g_1 = x(x+y)^2, g_2 = y, \ f_1 = x^2$ and $f_2 = x + y$ in$Q[x, y]$. Consider the ideals $I = \langle f_1, f_2 \rangle$ and $J = \langle g_1, g_2 \rangle$. We wish to compute I : J. By Lemma we have

$$J : I = (J : \langle f_1 \rangle) \cap (J : \langle f_2 \rangle) = \frac{1}{f_1}(J \cap \langle f_1 \rangle) \bigcap \frac{1}{f_2}(J : \langle f_2 \rangle).$$

First we compute $J \cap \langle f_1 \rangle$ by computing Gröbner basis G_1 for the ideal $\langle wg_1, wg_2, (1-w) f_1 \rangle \subseteq Q[x, y, w]$ with respect to the lex term ordering with $w > x > y$ to obtain $G_1 = \{x^2w - x^2, wy, x^3, x^2y\}$ so that $\frac{1}{f_1}(J \cap \langle f_1 \rangle) = \langle x, y \rangle$. Second we compute $J \cap \langle f_2 \rangle$ by computing Gröbner basis G_2 for the ideal $\langle wg_1, wg_2, (1-w) f_2 \rangle \subseteq Q[x, y, w]$ using the same order as above, and we obtain $G_1 = \{wx - x - y, wy, x^3 + y^3, xy + y^2\}$ so that $\frac{1}{f_2}(J \cap \langle f_2 \rangle) = \langle x^2 - xy + y^2, y \rangle$. Finally we compute $\langle x, y \rangle \bigcap \langle x^2 - xy + y^2, y \rangle$ by computing Gröbner basis G for the ideal $\langle wx, wy, (1-w)(x^2 - xy + y^2), (1-w) y \rangle \subseteq Q[x, y, w]$ with respect to the lex term ordering with $w > x > y$ to obtain $G = \{wx, x^2, y\}$. Therefore $J : I = \langle x^2, y \rangle$.

REFERENCES

[1] William W. Adams and Philippe Loustaunau. *An Introduction to Gröbner Bases*.
American Mathematical Society, Providence, RI, 1994.

[2] Stephen R. Czapor. *Gröbner Basis Methods for Solving Algebraic Equations*.
Ph.D. Thesis. University of Waterloo, Canada, 1988

[3] David S. Dummit and Richard M. Foote. *Abstract Algebra*, Third Edition. John Wiley and Sons, Inc., Hoboken, NJ, 2004.

[4] Franz Winkler. *Polynomial Algorithms in Computer Algebra*. Springer-Verlag Wien, New York, 1996.

[5] Rekha R. Thomas. Applications to Integer Programming *Proceedings of Symposia in*
Applied Mathematics 53 (1998):119-141.