

# PhD Seminars 2002/2003: Dr. C. D. Wensley Semester 2

Gareth Evans

April 3, 2003

## Contents

<b>1 Seminar 1: 14th January 2003</b>	<b>3</b>
1.1 Polynomial Rings . . . . .	3
1.2 Monomial Orderings . . . . .	4
<b>2 Seminar 2: 24th January 2003</b>	<b>6</b>
2.1 Ideals . . . . .	6
2.2 Quotient Rings . . . . .	6
2.3 Definitions, Results and Examples . . . . .	6
2.4 Localisation and Local Rings . . . . .	7
2.5 Formal Power Series Rings $\mathbb{K}[[x_1, \dots, x_n]]$ . . . . .	7
<b>3 Seminar 3: 19th February 2003</b>	<b>9</b>
3.1 The Division Algorithm for $R = K[x_1, \dots, x_n]$ . . . . .	9
3.2 Monomial Ideals . . . . .	9
<b>4 Seminar 4: 5th March 2003</b>	<b>11</b>
4.1 Monomial Ideals, Part 2 . . . . .	11
4.2 Gröbner Bases: Definition . . . . .	11
4.3 Properties of Gröbner Bases . . . . .	12

<b>5 Seminar 5: 12th March 2003</b>	<b>13</b>
5.1 How to tell if the basis $\{f_1, \dots, f_s\}$ for $I \triangleleft k[x_1, \dots, x_n]$ is a Gröbner Basis? . . . . .	13
5.1.1 $S$ -polynomials . . . . .	13
<b>6 Seminar 6: 19th March 2003</b>	<b>15</b>
6.1 Buchberger's Algorithm . . . . .	15
6.2 Syzygies . . . . .	16
<b>7 Seminar 7: 26th March 2003</b>	<b>17</b>
7.1 Syzygies Part 2 . . . . .	17

# 1 Seminar 1: 14th January 2003

## 1.1 Polynomial Rings

In a polynomial ring  $A[x]$ ,  $A$  is a ring (commutative ring with identity) and  $x = \{x_1, \dots, x_n\}$  is a set of indeterminates. For the coefficients, we have  $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n$ , with  $|\alpha| = \sum \alpha_i$ . Now  $\mathbb{N}^n$  is a monoid with operation  $\alpha + \beta = (\alpha_1 + \beta_1, \dots, \alpha_n + \beta_n)$  and identity  $(0, \dots, 0)$ . It follows that  $x^\alpha = x_1^{\alpha_1} \dots x_n^{\alpha_n}$  is a monomial where the order is unimportant (the  $x_i$  commute), and  $\text{Mon}(x) = \{x^\alpha \mid \alpha \in \mathbb{N}^n\}$  is the free commutative monoid on  $x$  with identity  $1 = x^{(0, \dots, 0)}$ . Note that  $x^\alpha/x^\beta$  is read as ' $x^\alpha$  divides  $x^\beta$ ' if there exists a  $\gamma \in \mathbb{N}^n$  with  $\alpha + \gamma = \beta$ .

Now  $ax^\alpha$ ,  $a \in A$  is a term while a polynomial is a finite sum of terms

$$f = \sum_{\alpha \in \mathbb{N}^n}^{\text{finite}} a_\alpha x^\alpha = \sum a_{(\alpha_1, \dots, \alpha_n)} x_1^{\alpha_1} \dots x_n^{\alpha_n}.$$

Alternatively, we can sum over all  $\mathbb{N}^n$  with finitely many  $a_\alpha \neq 0$ .

The degree of  $f$  is  $\deg(f) = \max\{|\alpha| : a_\alpha \neq 0\}$ , with  $\deg(a_0 x^0) = 0$  ( $a_0 \neq 0$ ) and  $\deg(0x^0) = -1$  ( $-\infty$  if you can handle it). A polynomial ring  $A[x]$  is a set of polynomials with the usual addition and multiplication. We identify  $a_0 x^0 \in A[x]$  with  $a_0 \in A$ , where  $A$  is the ground ring and  $A^*$  is the group of units in  $A$  ( $A[x]^* = A^*$ ). If  $K$  is an infinite field we may identify  $f \in K[x]$  with the polynomial function  $\tilde{f} : K^n \rightarrow K$ ,  $(p_1, \dots, p_n) \mapsto f(p_1, \dots, p_n)$ .

The distributive representation of  $f$  is  $f = \sum a_\alpha x^\alpha$ ,  $a_\alpha \in A$ , and this is usually used for Groebner basis computation. On the other hand, the recursive representation of  $f$ ,  $f = \sum_{\nu \in \mathbb{N}} f_\nu x_\nu^\nu$ ,  $f_\nu \in A(x_1, \dots, x_{n-1})$ , is usually used for factorisation computations.

A morphism of rings  $\psi : A \rightarrow B$  makes  $B$  an  $A$ -algebra because there is a scalar multiplication  $a.b = (\psi a)b$  (an  $A$ -algebra is an  $A$ -module with a multiplication). For example, in the inclusion  $A \rightarrow A[x]$ , we have  $A[x] = A \oplus A^+[x]$ , where  $A^+[x]$  consists of polynomials of positive degree = an algebra without identity.

**Lemma 1.1** *Let  $\psi : A \rightarrow B$  and  $\chi : B \rightarrow C$  be ring morphisms and  $f_1, \dots, f_n \in C$ . Then there exists a unique morphism  $\phi : A[x] \rightarrow C$  with  $\phi x_i = f_i$  and  $\phi a = (\psi a).1 \in C$ : (the usual case is when  $C = B[y]$  with  $y = \{y_1, \dots, y_m\}$ )*

$$\begin{array}{ccc}
 A & \xrightarrow{\psi} & B \\
 \downarrow & & \downarrow \chi \\
 A[x] & \xrightarrow{\phi} & C
 \end{array}
 \qquad
 \begin{array}{ccc}
 a & \xrightarrow{\quad} & \psi a \\
 \downarrow & & \downarrow \\
 a & \xrightarrow{\quad} & \phi a = \chi \psi a
 \end{array}$$

## 1.2 Monomial Orderings

Our aim here is to find a total order on  $\mathbb{N}^n$  and hence on monomials which is compatible with  $\alpha > \beta \Rightarrow \alpha + \gamma > \beta + \gamma$  for all  $\gamma$ . This allows us to write  $f \in A[x]$  in a unique ordered way:  $f = a_\alpha x^\alpha + a_\beta x^\beta + \dots + a_\gamma x^\gamma$  with  $\alpha > \beta > \dots > \gamma$ ,  $a_\alpha \neq 0$ .

$$\begin{aligned} \text{So we have } \quad \text{LM}(f) &:= \text{leadmon}(f) = x^\alpha; \\ \text{LE}(f) &:= \text{leadexp}(f) = \alpha; \\ \text{LT}(f) &:= \text{lead}(f) = a_\alpha x^\alpha; \\ \text{LC}(f) &:= \text{leadcoef}(f) = a_\alpha; \text{ and} \\ \text{tail}(f) &:= f - \text{lead}(f) = a_\beta x^\beta + \dots + a_\gamma x^\gamma. \end{aligned}$$

**Example 1.2**  $\text{lex} := >_{\text{lp}}$ :  $x^\alpha >_{\text{lp}} x^\beta \Leftrightarrow \exists! 1 \leq i \leq n$  such that  $\alpha_1 = \beta_1, \dots, \alpha_{i-1} = \beta_{i-1}, \alpha_i > \beta_i$ .

**Example 1.3**  $\text{deglex} := >_{\text{Dp}}$ :  $x^\alpha >_{\text{Dp}} x^\beta \Leftrightarrow \deg x^\alpha > \deg x^\beta$  or  $\deg x^\alpha = \deg x^\beta$  and  $\exists! 1 \leq i \leq n$  such that  $\alpha_1 = \beta_1, \dots, \alpha_{i-1} = \beta_{i-1}, \alpha_i > \beta_i$ .

**Remark 1.4** ‘deglex’ is also known as ‘length lex’.

**Example 1.5**  $\text{degrevlex} := >_{\text{dp}}$ :  $x^\alpha >_{\text{dp}} x^\beta \Leftrightarrow \deg x^\alpha > \deg x^\beta$  or  $\deg x^\alpha = \deg x^\beta$  and  $\exists! 1 \leq i \leq n$  such that  $\alpha_n = \beta_n, \dots, \alpha_{i+1} = \beta_{i+1}, \alpha_i < \beta_i$ .

In all three examples above, we have  $x^\alpha > 1$  for all  $\alpha \neq 0$ .

**Example 1.6**

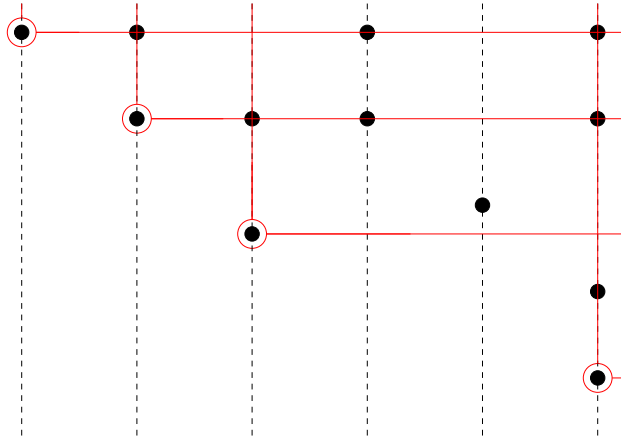
$$\begin{aligned} x_1^3 &>_{\text{lp}} x_1^2 x_2^2, \quad x_1^3 <_{\text{Dp}} x_1^2 x_2^2, \quad x_1^3 <_{\text{dp}} x_1^2 x_2^2; \\ x_1^2 x_2 x_3^2 &>_{\text{lp}} x_1 x_2^3 x_3, \quad x_1^2 x_2 x_3^2 >_{\text{Dp}} x_1 x_2^3 x_3, \quad x_1^2 x_2 x_3^2 <_{\text{dp}} x_1 x_2^3 x_3. \end{aligned}$$

**Definition 1.7** A monomial order is *global* if  $x^\alpha > 1$  for all  $\alpha \neq 0$ , *local* if  $x^\alpha < 1$  for all  $\alpha \neq 0$ , and *mixed* otherwise.

**Definition 1.8** The natural partial order  $>_{\text{nat}}$  on  $\mathbb{N}^n$  is  $\alpha \geq_{\text{nat}} \beta \Leftrightarrow a_i \geq \beta_i$  for  $1 \leq i \leq n$ .

**Lemma 1.9** (*Dickson’s Lemma*) For  $M$  any subset of  $\mathbb{N}^n$ , there is a finite subset  $B \subseteq M$  such that for all  $\alpha \in M$  there exists a  $\beta \in B$  such that  $\beta \leq_{\text{nat}} \alpha$ .

**Proof:** (Sketch) Case  $n = 1$ : Take the minimum  $B = \{\min(\alpha) \mid \alpha \in M\}$ . Case  $n = 2$ : illustrated by the following diagram, where the elements circled in red are less than anything above and to the right:



The proof is finished by induction.

□

## 2 Seminar 2: 24th January 2003

### 2.1 Ideals

Let  $A$  be a commutative ring with 1. An ideal  $I$  is an additive subgroup closed under scalar multiplication.  $I$  may have a system of generators  $I = \langle f_1, f_2, \dots \rangle$ ,  $I$  may be finitely generated, and  $I$  is principal if it only has one generator, i.e.  $I = \langle f \rangle$ .

Expressing  $f \in \langle f_1, f_2 \rangle$  as  $f = a_1 f_1 + a_2 f_2$  is not in general unique because of relations between the  $f_i$ , including the trivial relation  $f_1 f_2 - f_2 f_1 = 0$ . If  $\phi : A \rightarrow B$  is a ring homomorphism and if  $J \trianglelefteq B$  then the preimage  $I = \phi^{-1} J \trianglelefteq A$ . However  $I \trianglelefteq A$  does not imply that  $\phi I \trianglelefteq B$ .  $A$  is Noetherian if every ideal is finitely generated.

**Theorem 2.1** (*Hilbert Basis Theorem*):  $A = \text{Noetherian} \Rightarrow A[x_1, \dots, x_n]$  is Noetherian. The proof uses the equivalent property: Every chain of ideals  $I_1 \trianglelefteq I_2 \trianglelefteq \dots$  becomes stationary.

### 2.2 Quotient Rings

**Definition 2.2**  $A/I = \{[a] = a + I \mid a \in A\}$ , with  $[a] + [b] = [a + b]$  and  $[a].[b] = [a.b]$ . The residue map (or quotient map or natural map) is  $\pi$  (or  $\nu$ ):  $A \rightarrow A/I$ ,  $a \mapsto [a]$ , and it is surjective with kernel  $I$ .

**Lemma 2.3**  $\{J \trianglelefteq A \mid I \trianglelefteq J\} \cong \{\text{ideals in } A/I\}$  ( $\langle i_1, \dots, i_k, j_1, \dots, j_\ell \rangle \mapsto \langle [j_1], \dots, [j_\ell] \rangle$ ).

### 2.3 Definitions, Results and Examples

*Definitions (Sketches)*

- Zero Divisor:  $ab = 0$ .
- Integral Domain: 0 is the only one.
- Principal Ideal Ring: All ideals are principal.
- Prime Ideal:  $ab \in I \Rightarrow a \in I$  or  $b \in I$ .
- Maximal Ideal.
- $\text{Max}(A)$  = the set of maximal ideals.
- $\text{Spec}(A)$  = the set of prime ideals.
- Affine Ring:  $A \cong \mathbb{K}[x_1, \dots, x_n]/I$ , where  $\mathbb{K}$  is a field.

## Results

- $I$  is a prime ideal  $\Leftrightarrow A/I$  is an integral domain.
- $I$  is a maximal ideal  $\Leftrightarrow A/I$  is a field.
- Every maximal ideal is a prime ideal.
- $\phi : A \rightarrow B$  a ring homomorphism and  $J \trianglelefteq B$  prime implies that  $\phi^{-1}J$  is prime.

## Examples

- $p$  prime:  $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$  is a field.
- $6\mathbb{Z}$  is not prime and  $\mathbb{Z}_6$  has zero divisors.
- $n\mathbb{Z} \subset m\mathbb{Z}$  iff  $m|n$  so that the maximal ideals in  $\mathbb{Z}$  are the  $p\mathbb{Z}$ 's.
- Polynomial rings over a field are integral domains.
- $I = \langle (x+1)(x^2+1) \rangle \trianglelefteq \mathbb{Q}[x]$  has zero divisors  $(x+1)$  and  $(x^2+1)$ .

## 2.4 Localisation and Local Rings

Localisation is about enlarging a ring by introducing denominators, e.g.  $\mathbb{Z} \rightarrow \mathbb{Q}$ .

**Definition 2.4**  $A$  is local if it has exactly one maximal ideal  $\mathfrak{m}$ .

**Example 2.5**  $\mathbb{K}[x]$  is not local because  $\langle x \rangle, \langle x-1 \rangle, \dots, \langle x-n \rangle$  are all maximal.

## Results

- Every ideal  $A$  contains at least one maximal ideal.
- If  $I \trianglelefteq A$  then there exists a maximal ideal  $J$  with  $I \trianglelefteq J$ .
- $A$  is local  $\Leftrightarrow$  the non units in  $A$  form an ideal, which is the required  $\mathfrak{m}$ .

## 2.5 Formal Power Series Rings $\mathbb{K}[[x_1, \dots, x_n]]$

The elements of a formal power series ring are as follows (ignoring convergence):

$$\sum_{0, \dots, 0}^{\infty, \dots, \infty} a_{i_1 i_2 \dots i_n} x_1^{i_1} \dots x_n^{i_n}$$

**Example 2.6** In the ring  $\mathbb{K}[[x]]$ ,  $x - 1$  is a unit:  $\frac{1}{x-1} = -(1 + x + x^2 + \dots + x^n + \dots)$ . Any series with non-zero constant term has an inverse, so that  $\mathfrak{m} = \langle x \rangle =$  all series with zero constant term.

**Definition 2.7** If  $A$  is an integral domain, then  $\text{Quot}(A) = \mathbb{Q}(A) = \{\frac{a}{b} \mid a, b \in A, b \neq 0\}$  is a field, with  $\frac{a}{b} + \frac{a'}{b'} = \frac{ab' + a'b}{bb'}$  and  $\frac{a}{b} \cdot \frac{a'}{b'} = \frac{a \cdot a'}{b \cdot b'}$ .

Strictly speaking, the above definition should say that  $\frac{a}{b}$  denotes the equivalence class of  $(a, b)$  under the relation  $(a, b) \sim (a', b') \Leftrightarrow ab' = a'b$ . Further,  $\frac{a}{b} = 0 \Leftrightarrow a = 0$ , and if  $a \neq 0$  then we have  $(\frac{a}{b})^{-1} = \frac{b}{a}$ .

The denominators in  $\mathbb{Q}(A)$  form a set  $S = A \setminus \{0\}$  that satisfies

- (1)  $1 \in S$  and
- (2)  $a, b \in S \Rightarrow ab \in S$ .

Let us now consider a ring  $A$ .  $S \subset A^{\neq 0}$  is multiplicative if (1) and (2) hold above. The localisation or ring of fractions is given by

$$S^{-1}A := \{\frac{a}{b} \mid a \in A, b \in S\},$$

where  $\frac{a}{b}$  denotes the equivalence class of  $(a, b)$  under the relation  $(a, b) \sim (a', b') \Leftrightarrow \exists s \in S$  such that  $S(ab' - a'b) = 0$ , with  $+$  and  $\cdot$  as above.

**Proposition 2.8**  $S^{-1}A$  is a commutative ring with 1.

**Example 2.9** If  $A = \mathbb{Z}$  and  $S =$  the odd integers, then  $S^{-1}A = \{\frac{a}{b} \mid a \in \mathbb{Z}, b \text{ odd}\} =$  the ‘localisation of  $\mathbb{Z}$  at the prime 2’. Here,  $S^{-1}A$  is local with  $\mathfrak{m} = \{\frac{a}{b} \mid a \text{ even}, b \text{ odd}\} = 2S^{-1}A$ . Further,  $S^{-1}A \setminus \mathfrak{m} = \{\frac{a}{b} \mid a, b \text{ both odd and } (\frac{a}{b})^{-1} = \frac{b}{a}\}$ .

**Example 2.10** If  $A = \mathbb{Z}$  and  $S = \{\text{all non-negative powers of } 2\}$ , then  $S^{-1}A = \{\frac{a}{2^m} \mid a \in \mathbb{Z}, m \in \mathbb{Z}^{\geq 0}\}$ .

### 3 Seminar 3: 19th February 2003

#### 3.1 The Division Algorithm for $R = K[x_1, \dots, x_n]$

Given polynomials  $f, g_1, \dots, g_s \in R$ , the goal is to divide  $f$  by the  $g_i$  and obtain a remainder  $r$ , where  $f = q_1g_1 + \dots + q_s g_s + r$ . We write  $r = \text{rem}(f, \{g_1, \dots, g_s\})$ , where  $r = 0$  or  $r$  is a  $k$ -linear sum of monomials, none of which is divisible by  $\text{LM}(g_i)$  for  $1 \leq i \leq s$ . Further, if  $q_i g_i \neq 0$ , then  $\text{LT}(f) \geq \text{LT}(q_i g_i)$ . Assuming the  $g_i$  are ordered by decreasing lead term, here is the algorithm:

```

Set  $q_i = 0$  for  $1 \leq i \leq s$ ;
 $h := f$ ; changed := true;
while changed do
{
   $t := \text{LT}(h)$ ; changed := false;  $i := 0$ ;
  while (( $i < s$ ) and not changed) do
  {
     $i := i + 1$ ;
     $t_i := \text{LT}(g_i)$ ;
    if ( $t_i \mid t$ ) then
    {
      changed := true;
       $h := h - (t/t_i)g_i$ ;
       $q_i := q_i + (t/t_i)$ ;
    }
  }
}

```

**Example 3.1** Take  $f = x^2y^2$ ,  $g_1 = \frac{1}{2}x^2y + 3x^2 - 2xy - 4y$  and  $g_2 = \frac{1}{2}xy^2 - 2xy + 3y^2 - 4x$ , with length-lex order  $x > y$ . At  $i = 1$ ,  $t := x^2y^2$ ,  $t_i := \frac{1}{2}x^2y$  and  $\frac{t}{t_i} = 2y$ . So  $h := f - 2yg_1 = 4xy^2 - 6x^2y + 8y^2$  and  $q_1 := 2y$ . Now  $\frac{t}{t_1} = -12$ ,  $h := h + 12g_1 = 4x^2y + 36x^2 - 24xy + 8y^2 - 48y$ , and  $q_1 := 2y - 12$ . Then  $\frac{t}{t_2} = 8$  and  $h := h - 8g_2 = 36x^2 - 8xy - 16y^2 + 32x - 48y = r$ .

#### 3.2 Monomial Ideals

**Definition 3.2**  $I \trianglelefteq R$  is a monomial ideal if there is an  $A \subseteq \mathbb{N}^n$  such that  $I$  consists of all polynomials which are finite sums  $\sum_{\alpha \in A} h_\alpha x^\alpha$ , where  $h_\alpha \in R$ ,  $h_\alpha \neq 0$ , and  $x^{(\alpha_1, \dots, \alpha_n)} \equiv x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n}$ . We write  $I = \langle x^\alpha \mid \alpha \in A \rangle$ .

**Lemma 3.3**  $x^\beta \in I \iff x^\alpha \mid x^\beta$  for some  $\alpha \in A$ .

**Proof:** Let  $x^\beta = \sum c_\alpha x^\alpha$ , so that  $x^\beta$  is a multiple of at least one term in some  $c_\alpha x^\alpha$ . It follows that  $x^\beta = x^\gamma x^\alpha$ , where  $x^\gamma$  is a monomial in some  $c_\alpha$ . The other direction of the proof is obvious.  $\square$

**Lemma 3.4** *If  $f \in R$ , the following conditions are equivalent:*

- (i)  $f \in I$ ;
- (ii) Every term of  $f$  is in  $I$ ;
- (iii)  $f$  is a  $k$ -linear combination of the monomials of  $I$ .

**Corollary 3.5** *If  $I = \langle x^\alpha \mid \alpha \in A \rangle$  and  $J = \langle x^\beta \mid \beta \in B \rangle$ , then  $I = J \iff A = B$ .*

**Corollary 3.6** *Let  $>$  be a relation on  $\mathbb{N}^n$  such that (i)  $>$  is a total order and (ii)  $\alpha > \beta$  and  $\gamma \in \mathbb{N}^n \Rightarrow \alpha + \gamma > \beta + \gamma$ . Then  $>$  is a well-ordering  $\iff 0$  is a least element.*

**Definition 3.7** A basis  $\{x^{\alpha_1}, \dots, x^{\alpha_s}\}$  for  $I$  is minimal if no  $x^{\alpha_i}$  divides  $x^{\alpha_j}$  for  $i \neq j$ .

**Lemma 3.8** *Every monomial ideal has a unique minimal basis.*

## 4 Seminar 4: 5th March 2003

### 4.1 Monomial Ideals, Part 2

**Proposition 4.1** Let  $I \triangleleft k[x_1, \dots, x_n]$ . Then (i)  $\langle LT(I) \rangle$  is a monomial ideal and (ii) there are  $g_1, \dots, g_t \in I$  such that  $\langle LT(I) \rangle = \langle LT(g_1), \dots, LT(g_t) \rangle$ .

**Proof:** (Notation:  $LT(I) = \{\text{the set of leading terms of } f \in I\}$ ,  $LM(I) = \{\text{the set of leading monomials of } f \in I\}$ ,  $\langle LT(I) \rangle = \text{the ideal generated by } LT(I)$ , and  $\langle LM(I) \rangle = \text{the ideal generated by } LM(I)$ ). (i) Since  $k$  is a field, we have  $\langle LT(I) \rangle = \langle LM(I) \rangle$ . (ii) By Dickson's Lemma, there is a finite monomial basis for  $\langle LM(I) \rangle$ ,  $\langle LM(I) \rangle = \langle LM(g_1), \dots, LM(g_t) \rangle$  for some  $g_1, \dots, g_t \in I$ , because  $\{LM(g_1), \dots, LM(g_t)\}$  is a subset of  $LM(I)$ .  $\square$

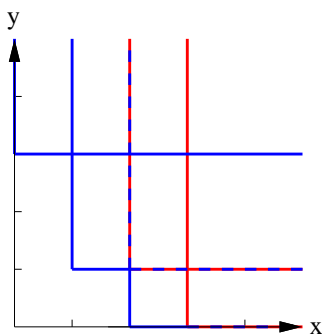
**Theorem 4.2** (The Hilbert Basis Theorem (HBT)) Every  $I \triangleleft k[x_1, \dots, x_n]$  has a finite generating set.

**Proof:** Assume that  $I \neq \{0\}$  ( $I = \{0\} \dots \{0\}$  is a generating set). It follows that  $\langle LT(I) \rangle = \langle LT(g_1), \dots, LT(g_t) \rangle$  by the above proposition. *Claim:*  $I = \langle g_1, \dots, g_t \rangle$ . Now it is clear that  $\langle g_1, \dots, g_t \rangle \triangleleft I$ . For the other direction, let  $f \in I$  and divide by  $g_1, \dots, g_t$  to obtain  $f = a_1g_1 + \dots + a_tg_t + r$ , where no term in  $r$  is divisible by a  $LM(g_i)$ . Therefore,  $r = f - a_1g_1 - \dots - a_tg_t$  and so if  $r \neq 0$  then (by the Lemma)  $LM(r)$  is divisible by some  $LM(g_i)$ , which gives a contradiction so that we must have  $r = 0$ .  $\square$

### 4.2 Gröbner Bases: Definition

**Definition 4.3** Fix a monomial order. A finite subset  $\{g_1, \dots, g_t\}$  of an ideal  $I$  is a Gröbner Basis if  $\langle LT(g_1), \dots, LT(g_t) \rangle = \langle LT(I) \rangle$ . Equivalently, by the Lemma,  $G$  is a Gröbner Basis for  $I \iff \{f \in I \Rightarrow LT(g_i) \mid LT(f) \text{ for some } i\}$ .

**Example 4.4** If  $f_1 = x^3 - 2xy$ ,  $f_2 = x^2y - 2y^2 + x$  and the order is deglex, then the Gröbner Basis is  $g_1 = x^2, g_2 = xy$  and  $g_3 = y^2 - \frac{1}{2}x$  (so that  $f_1 = xg_1 - 2g_2$  and  $f_2 = yg_1 - 2g_3$ ), and the situation is summarised by the following diagram:



**Example 4.5** If  $I = \langle f_1, \dots, f_s \rangle$  and all the  $f_i$  are linear, for the lexicographic order a Gröbner Basis is obtained by Gaussian Elimination. Therefore, if  $I = \langle w + x + y + z, w + x - y - z, w - x + y - z \rangle$ , it follows that we do the following elimination to obtain  $G = \{w - z, x + z, y + z\}$ :

$$\begin{aligned} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \end{bmatrix} &\sim \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & -2 & -2 \\ 0 & -2 & 0 & -2 \end{bmatrix} \sim \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix} \\ &\sim \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 0 & -1 \\ & 1 & 0 & 1 \\ & & 1 & 1 \end{bmatrix}. \end{aligned}$$

**Definition 4.6** An ascending chain of ideals is a nested sequence  $I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$

**Theorem 4.7** If  $I_1 \subseteq I_2 \subseteq \dots$  is an ascending chain in  $I$ , then for some  $N$  we have  $I_N = I_{N+1} = \dots$

**Proof:** Form  $\bigcup_{i=1}^{\infty} I_i = I$ , another ideal. By the Hilbert Basis Theorem,  $I = \langle g_1, \dots, g_s \rangle$ . But each  $g_j$  is in some  $I_j$  so we consider  $\max(j)$ , etc. □

### 4.3 Properties of Gröbner Bases

**Proposition 4.8** Let  $I \triangleleft k[x_1, \dots, x_n]$ ,  $G = \{g_1, \dots, g_t\}$  and  $f \in k[x_1, \dots, x_n]$ . Then there is a unique  $r \in k[x_1, \dots, x_n]$  satisfying (i) no term of  $r$  is divisible by any of the  $LT(g_i)$ ; and (ii) there is a  $g \in I$  such that  $f = g + r$ . In particular,  $r$  is the remainder on division of  $f$  by  $G$  whatever the order of the  $g_i$  in  $G$ .

**Proof:** The division algorithm gives  $r$  satisfying (i), and we can then define  $g = f - r$ . For uniqueness, suppose that  $f = g'_1 + r_1 = g'_2 + r_2$ , so that  $r_2 - r_1 = g'_1 - g'_2 \in I$ . But if  $r_2 \neq r_1$  then  $LT(r_2 - r_1) \in \langle LT(I) \rangle$  and so  $LT(r_2 - r_1)$  is divisible by some  $LT(g_i)$ . But this is a contradiction, so we must have  $r_1 = r_2$  and  $g'_1 = g'_2$ . □

**Corollary 4.9**  $f \in I \iff r = 0$ .

## 5 Seminar 5: 12th March 2003

### 5.1 How to tell if the basis $\{f_1, \dots, f_s\}$ for $I \triangleleft k[x_1, \dots, x_n]$ is a Gröbner Basis?

A possible obstruction in answering the above question is the occurrence of  $\sum a_i f_i$  with a leading term *not* in  $\langle LT(f_1), \dots, LT(f_s) \rangle$ . One way this might occur is if leading terms in  $p = ax^\alpha f_i - bx^\beta f_j$  ( $a, b \in k$ ) cancel, where  $p \in I$  and  $LT(p) \in \langle LT(I) \rangle$ .

#### 5.1.1 $S$ -polynomials

Let  $f, g \in k[x_1, \dots, x_n]$ ,  $\alpha = \text{multideg}(f)$ ,  $\beta = \text{multideg}(g)$ , and  $\gamma = (\gamma_1, \dots, \gamma_n)$ , where  $\gamma_i = \max(\alpha_i, \beta_i)$ . Then  $x^\gamma = LCM(LM(f), LM(g))$ .

**Definition 5.1** The  $S$ -polynomial of  $f$  and  $g$  is defined as follows:

$$S(f, g) = \frac{x^\gamma}{LT(f)} f - \frac{x^\gamma}{LT(g)} g.$$

**Example 5.2** Let  $g_1 = 3x^3y^2z - z$ ,  $g_2 = 5xy^3z^2 - x$ , and  $g_3 = 7x^2yz^3 - y$ . Then we have  $\alpha(1) = (3, 2, 1)$ ,  $\beta(1) = (0, 1, 2)$ ,  $\alpha(2) = (1, 3, 2)$ ,  $\beta(2) = (2, 0, 1)$ ,  $\alpha(3) = (2, 1, 3)$ , and  $\beta(3) = (1, 2, 0)$ , where  $\alpha(i) + \beta(i) = (3, 3, 3)$ . By inspection,  $yz^2g_1 - 2x^2zg_2 + xy^2g_3 = 2x^3z - xy^3 - yz^3$ . Can we express this as a sum of  $S$ -polynomials? Well,

$$\begin{aligned} S(g_1, g_2) &= \frac{x^{(3,3,2)}}{3x^{(3,2,1)}}(3x^3y^2z - z) - \frac{x^{(3,3,2)}}{5x^{(1,3,2)}}(5xy^3z^2 - x) \\ &= -\frac{1}{3}yz^2 + \frac{1}{5}x^3; \\ S(g_2, g_3) &= -\frac{1}{5}x^2z + \frac{1}{7}y^3; \text{ and} \\ S(g_3, g_1) &= -\frac{1}{7}xy^2 + \frac{1}{3}z^3, \end{aligned}$$

so we can deduce that  $2x^3z - xy^3 - yz^3 = 10zS(g_1, g_2) + \frac{7}{3}yz^3 - xy^3 = 10zS(g_1, g_2) + 7yS(g_3, g_1)$ .

**Lemma 5.3** Suppose that  $p = \sum_{i=1}^s c_i x^{\beta(i)} g_i$ , where we have  $c_i \in k$  and  $\beta(i) + \text{multideg}(g_i) = \delta$  if  $c_i \neq 0$ . If  $\text{multideg}(p) < \delta$  then there exists constants  $b_{jk}$  such that  $p = \sum_{j,k} b_{jk} x^{\delta - \gamma_{jk}} S(g_j, g_k)$ , where  $\gamma_{jk} = LCM(LM(g_j), LM(g_k))$ . (In the above example,  $\gamma_{12} = (3, 3, 2)$ ,  $\gamma_{23} = (2, 3, 3)$ ,  $\gamma_{31} = (3, 2, 3)$ ,  $\delta - \gamma_{12} = (0, 0, 1)$ ,  $\delta - \gamma_{23} = (1, 0, 0)$ , and  $\delta - \gamma_{31} = (0, 1, 0)$ ).

**Proof:** Let  $g_i = d_i x^{\alpha(i)} + \text{other terms}$  ( $1 \leq i \leq j$ ), so that  $c_i x^{\beta(i)} g_i = (c_i d_i) x^{\alpha(i) + \beta(i)} + \text{other terms}$ . By assumption,  $\alpha(i) + \beta(i) = \delta$  and  $\sum_{i=1}^s c_i d_i = 0$  (in the example  $3 - 10 + 7 = 0$ ). Let us define

$$p_i = \frac{x^{\beta(i)} g_i}{d_i} = x^\delta + \text{other terms.}$$

Then

$$\begin{aligned}
\sum c_i x^{\beta(i)} g_i &= \sum_{i=1}^s c_i d_i p_i \\
&= c_1 d_1 (p_1 - p_2) + (c_1 d_1 + c_2 d_2) (p_2 - p_3) \\
&\quad + (c_1 d_1 + c_2 d_2 + c_3 d_3) (p_3 - p_4) + \dots + \left(\sum c_i d_i\right) p_s.
\end{aligned}$$

It is easy to check that  $x^{\delta-\gamma_{jk}} S(g_j, g_k) = p_j - p_k$  so that  $\sum c_i x^{\beta(i)} g_i = c_1 d_1 x^{\delta-\gamma_{12}} S(g_1, g_2) + (c_1 d_1 + c_2 d_2) x^{\delta-\gamma_{23}} S(g_2, g_3) + \dots$ . In particular, this shows that  $S(g_j, g_k)$  is a combination of the  $S(g_\ell, g_m)$ , where  $|j - k| \neq 1$  and  $m = \ell + 1$ .  $\square$

**Theorem 5.4** *A basis  $G = \{g_1, \dots, g_t\}$  for  $I$  is a Gröbner Basis if for all pairs  $i \neq j$  the remainder when  $S(g_i, g_j)$  is divided by  $G$  is zero.*

## 6 Seminar 6: 19th March 2003

### 6.1 Buchberger's Algorithm

The algorithm used to construct a Gröbner Basis is known as Buchberger's algorithm, and we shall now consider a primitive version of this algorithm:

*Input:* A basis  $F = \langle f_1, \dots, f_s \rangle$  for  $I$ .

*Algorithm:*

$G := F$ ;

REPEAT

{

$G' := G$ ;

for each pair  $\{p, q\} \in G'$  do

{

$S := \overline{S\text{-poly}(p, q)}^{G'}$  (i.e. reduce using  $G'$ );

if  $S \neq 0$  then  $G := G \cup \{S\}$ ; fi;

}

}

UNTIL  $(G == G')$

*Output:*  $G$

**Theorem 6.1** *The above algorithm terminates in a finite number of steps (the proof uses the ascending chain condition on successive  $\langle LT(G) \rangle$ 's).*

**Lemma 6.2** *Let  $p \in G$  be such that  $LT(p) \in \langle LT(G \setminus \{p\}) \rangle$ . Then  $G \setminus \{p\}$  is also a Gröbner Basis.*

**Definition 6.3** A Gröbner Basis is *minimal* if every  $g \in G$  is monic and for all  $p \in G$ ,  $LT(p) \notin \langle LT(G \setminus \{p\}) \rangle$ .

**Definition 6.4** A Gröbner Basis is *reduced* if every  $g \in G$  is monic and for all  $p \in G$  no monomial of  $p$  lies in  $\langle LT(G \setminus \{p\}) \rangle$ .

**Proposition 6.5**  *$I$  has a unique reduced Gröbner Basis.*

**Proof:** Assume that  $G$  is minimal. Given  $g \in G$ , let  $g' = \bar{g}^{G \setminus \{g\}}$  and set  $G' = (G \setminus \{g\}) \cup \{g'\}$ . Claim:  $G'$  is also minimal. To see this, note that  $\langle LT(G) \rangle = \langle LT(G') \rangle$  and iterate the procedure — when a  $g$  is reduced it stays reduced and we end up with a reduced Gröbner Basis.

To prove uniqueness, suppose that  $G$  and  $\tilde{G}$  are both reduced Gröbner Bases. Because of this, both bases must also be minimal, and so this implies that (as sets)  $LT(G) = LT(\tilde{G})$ . Therefore, given a  $g \in G$  there is a  $\tilde{g} \in \tilde{G}$  with  $LT(g) = LT(\tilde{g})$  (take  $g \in G$  and reduce modulo  $\tilde{G}$  to 0: for some  $\tilde{g} \in \tilde{G}$  we have  $LT(\tilde{g}) \mid LT(g)$ ). Now reduce  $\tilde{g}$  modulo  $G$  to 0: there exists a  $\bar{g} \in G$  with  $LT(\bar{g}) \mid LT(\tilde{g}) \mid LT(g)$  so that the minimal condition implies that  $LT(\bar{g}) = LT(g) = LT(\tilde{g})$ . Now consider  $g - \tilde{g} \in I$ . We can deduce that  $\overline{g - \tilde{g}}^G = 0$ : each term in  $g - \tilde{g}$  is not divisible by any  $LT(p)$  (for any  $p \in G$ ) or by any  $LT(\tilde{p})$  (for any  $\tilde{p} \in \tilde{G}$ ), so there must be no remaining terms, i.e. we must have  $g = \tilde{g}$ .  $\square$

## 6.2 Syzygies

**Definition 6.6** Given a finite set of polynomials  $G$  in  $k[x_1, \dots, x_n]$  and  $f \in k[x_1, \dots, x_n]$ , we say that ‘ $f$  reduces to 0 mod  $G$ ’ and write  $f \rightarrow_G 0$  if we can write  $f = a_1g_1 + \dots + a_tg_t$  so that, whenever  $a_i g_i \neq 0$ ,  $\text{multideg}(f) \geq \text{multideg}(a_i g_i)$ .

**Remark 6.7** This is the ‘good’ notion — better than  $\tilde{f}^G = 0$ .

**Example 6.8** Taking our total order to be *deglex*, let  $G = (e = yz + y, f = x^3 + y, g = z^4)$ . Then  $S(f, g) = z^4 f - x^3 g = yz^4 = (yz + y)(z^3 - z^2 + z - 1) + y \neq 0$ , but  $yz^4 = 0e + 0f + yg$ .

**Proposition 6.9** Let  $F$  be a finite set of polynomials in  $k[x_1, \dots, x_n]$ , and let  $f, g \in F$  be polynomials such that  $\text{LCM}(LM(f), LM(g)) = LM(f) \times LM(g)$ . Then  $S(f, g) \rightarrow_F 0$ .

**Proof:** Writing  $f = LT(f) + p$  and  $g = LT(g) + q$ , in this case  $S(f, g) = (g - q)f - (f - p)g = (-q)f + p(g)$ , so that  $S(f, g) \rightarrow_F 0$  as required (we still have to check the multidegrees though).  $\square$

## 7 Seminar 7: 26th March 2003

### 7.1 Syzygies Part 2

Let  $F = (f_1, \dots, f_s)$  be an ordered basis so that  $LT(F) = (LT(f_1), \dots, LT(f_s))$ . A syzygy on  $LT(F)$  is a vector  $H = (h_1, \dots, h_s) \in k[x_1, \dots, x_n]^s$  so that  $H \cdot L(F) = 0$ . The set of syzygies for  $L(F)$  is denoted by  $S(F)$  and is a  $k[x_1, \dots, x_n]$ -module.

In the example considered in the previous seminar, we had  $LT(F) = (3x^3y^2z, 5xy^3z^2, 7x^2yz^3)$  and  $H = (yz^2, -2x^2z, xy^2)$  ( $\alpha = (3, 3, 3)$ ). If the syzygy associated to the  $S$ -polynomial  $S(f_i, f_j)$  is given by

$$H(f_i, f_j) = \frac{x^\gamma}{LT(f_i)} \mathbf{e}_i - \frac{x^\gamma}{LT(f_j)} \mathbf{e}_j,$$

where  $\mathbf{e}_i$  and  $\mathbf{e}_j$  are unit vectors, it follows that  $H(f_1, f_2) = (\frac{1}{3}yx, -\frac{1}{5}x^2, 0)$  ( $\gamma = (3, 3, 2)$ ),  $H(f_1, f_3) = (\frac{1}{3}z^2, 0, -\frac{1}{7}xy)$  ( $\gamma = (3, 2, 3)$ ), and  $H(f_2, f_3) = (0, \frac{1}{5}xz, -\frac{1}{7}y^2)$  ( $\gamma = (2, 3, 3)$ ).

**Definition 7.1**  $H \in S(F)$  is homogeneous of multidegree  $\alpha$  if  $H = (c_1x^{\alpha(1)}, \dots, c_sx^{\alpha(s)})$  ( $c_i \in k$ ) and  $\alpha(i) + \text{multideg}(f_i) = \alpha$  whenever  $c_i \neq 0$ .

**Lemma 7.2** Every  $H$  can be written as a sum of homogeneous syzygies.

**Proposition 7.3** Every  $H \in S(F)$  can be written in the form  $H = \sum_{i < j} u_{ij}H(f_i, f_j)$ , where  $u_{ij} \in k[x_1, \dots, x_n]$ .

**Proof:** Assume that  $H$  is homogeneous of type  $\alpha$ . We know that  $H$  must have at least two non-zero components, say  $c_ix^{\alpha(i)}$  and  $c_jx^{\alpha(j)}$ , with  $\alpha(i) + \text{multideg}(f_i) = \alpha(j) + \text{multideg}(f_j) = \alpha$ . Then  $x^\gamma = \text{LCM}(LM(f_i), LM(f_j))$  divides  $x^\alpha$  and  $H - c_iLC(f_i)x^{\alpha-\gamma}H(f_i, f_j)$  has 0 in the  $i$ -th position. But the only other component affected is the  $j$ -th, and so we therefore obtain a new  $H$  with fewer non-zero terms.  $\square$

**Remark 7.4** In the example, we have  $H - c_1LC(f_1)x^{\alpha-\gamma_{12}}H(f_1, f_2) = (yz^2, -2x^2z, xy^2) - 1 \times 3z(\frac{1}{3}yz, -\frac{1}{5}x^2, 0) = (0, -\frac{7}{5}x^2z, xy^2) = -7xH(f_2, f_3)$ .

**Theorem 7.5** A basis  $G = (g_1, \dots, g_t)$  for an ideal  $I$  is a Gröbner Basis iff for every element  $H = (h_1, \dots, h_t)$  in a homogeneous spanning set for  $S(G)$  we have  $H \cdot G = \sum_{i=1}^t h_i g_i \rightarrow_G 0$ .

**Proposition 7.6** (A version of Buchberger's 2nd criterion): Given  $G = (g_1, \dots, g_t)$ , suppose we have a subset  $U \subseteq \{H(f_i, f_j) \mid 1 \leq i < j \leq t\}$  which is a basis for  $S(G)$ . In addition, suppose we have distinct elements  $g_i, g_j, g_k \in G$  such that  $LT(g_k)$  divides  $\text{LCM}(LT(g_i), LT(g_j))$ . If we have  $H(f_i, f_k) \in U$  and  $H(f_j, f_k) \in U$ , then  $U \setminus \{H(f_i, f_j)\}$  is also a basis for  $S(G)$ .

**Proof:** Follows from  $H(f_i, f_j) = \frac{x^{\gamma_{ij}}}{x^{\gamma_{ik}}}H(f_i, f_k) - \frac{x^{\gamma_{ij}}}{x^{\gamma_{jk}}}H(f_j, f_k)$ .  $\square$