21-238, Math Studies Algebra 2, Department of Mathematical Sciences, Carnegie Mellon University
Spring 2012: Monday, Wednesday, Friday, 10:30 am, Doherty Hall 1211.
Luc TARTAR, University Professor of Mathematics, Wean Hall 6212, tartar@cmu.edu

29- Friday March 30, 2012.

Definition 29.1: Given a monomial ordering on the polynomial ring $F[x_1,\ldots,x_n]$, the *leading term* $LT(P)$ of a non-zero polynomial $P=\sum_m r_m m$ (with $r_m\in F$ and only a finite number of coefficients $r_m\neq 0$), is the term $r_m m$ for the maximum among the monic monomials m satisfying $r_m\neq 0$, and the *multi-degree* of P, denoted $\partial(P)$ is the multi-index of m; by convention, one also uses $LT(0)=0$.

For an ideal I in $F[x_1,\ldots,x_n]$, the *ideal of leading terms*, denoted $LT(I)$, is the ideal generated by the leading terms of all the elements of the ideal, i.e. $LT(I)=(LT(P)\mid P\in I)$, so that this definition is different from that used inside Lemma 28.2.

Remark 29.2: One has $LT(P\,Q)=LT(P)\,LT(Q)$ and $\partial(P\,Q)=\partial(P)+\partial(Q)$ for non-zero polynomials $P,Q\in F[x_1,\ldots,x_n]$, but the definitions of $LT(P)$ and $\partial(P)$ depend upon the monomial ordering used.

Example 29.3: A *lexicographic* ordering consists in giving a total order among the variables $x_1,\ldots,x_n$, and deducing the corresponding monomial ordering. For example, if $x_1>\ldots>x_n$, then for multi-indices $\alpha\neq\beta$ one has $x^\alpha\geq x^\beta$ if and only if the smallest $i\in\{1,\ldots,n\}$ for which $\alpha_i\neq\beta_i$ has $\alpha_i>\beta_i$.

Remark 29.4: For $n=2$ and $x_1>x_2$, the lexicographic order is $1<x_2<x_2^2<\ldots<x_1<x_1x_2<x_1x_2^2<\ldots<x_1^2<x_1^2x_2<x_1^2x_2^2<\ldots$, so that there are infinitely many different monomials between x_2 and x_1 for example. For avoiding this effect, it is natural then to invent the notion of grading of Example 29.5.

Example 29.5: The *grading* of a monomial ordering $\leq$, denoted $\leq_g$ consists in saying that $m_1\geq_g m_2$ if and only if either $deg(m_1)>deg(m_2)$ or $deg(m_1)=deg(m_2)$ and $m_1\geq m_2$; by Lemma 28.7, it is a monomial ordering. The grading of a lexicographic ordering as $x_1>\ldots>x_n$ is called the *grlex* monomial ordering.

Remark 29.6: The grlex monomial ordering associated to $x_1>x_2>x_3$ is then $1<x_3<x_2<x_1<x_3^2<x_2x_3<x_2^2<x_1x_3<x_1x_2<x_1^2<x_3^3<\ldots$.

Example 29.7: The *grevlex* monomial ordering is defined by first choosing a total ordering of the variables, like $x_1>\ldots>x_n$, and then defining $m_1\geq m_2$ if and only if either $deg(m_1)>deg(m_2)$ or $deg(m_1)=deg(m_2)$ and the first exponent of $x_n,\ldots,x_1$ (in that order) where m_1 and m_2 differ is *smaller* in m_1. Using Lemma 28.7, one checks easily that it is a monomial ordering.

Remark 29.8: If $n=2$, the grevlex monomial ordering is the same as the grlex monomial ordering, but for $n\geq 3$ it is not the grading of any lexicographic ordering: indeed, the grevlex monomial ordering associated to $x_1>x_2>x_3$ is $1<x_3<x_2<x_1<x_3^2<x_2x_3<x_1x_3<x_2^2<x_1x_2<x_1^2<x_3^3<\ldots$.

Definition 29.9: Given a monomial ordering on the polynomial ring $F[x_1,\ldots,x_n]$, a *Gröbner basis* for an ideal I in the polynomial ring $F[x_1,\ldots,x_n]$ is a finite set of generators $\{g_1,\ldots,g_k\}$ for I whose leading terms generate the ideal $LT(I)$.[1]

Remark 29.10: Gröbner bases were named by BUCHBERGER in honour of his advisor,[2] and they are useful for the *general polynomial division* by an arbitrary set $\{g_1,\ldots,g_k\}$ of non-zero polynomials $F[x_1,\ldots,x_n]$, and for doing this one uses a monomial ordering.

Given a polynomial $f\in F[x_1,\ldots,x_n]$, the goal is to write $f=q_1g_1+\ldots+q_kg_k+r$, and one starts with $q_1=\ldots=q_k=r=0$, and one checks if the leading term of $LT(f)$ is divisible by the leading terms $LT(g_1),\ldots,LT(g_k)$, in this order:[3] if the current $LT(f)$ is divisible by $LT(g_i)$ for some $i\in\{1,\ldots,k\}$, i.e. $LT(f)=a\,m\,LT(g_i)$ for some $a\in F$ and some monic monomial m, one adds $a\,m$ to q_i, one replaces f by

[1] Wolfgang GRÖBNER, Austrian mathematician, 1899–1980. He worked in Innsbruck, Austria. Gröbner bases were named after him by his student BUCHBERGER.

[2] Bruno BUCHBERGER, Austrian mathematician, born in 1942. He worked at Johannes Kepler University in Linz, Austria. The Buchberger algorithm for constructing Gröbner bases is named after him (and he coined the term Gröbner bases after his advisor's name).

[3] If $n=m=1$, this is how the Euclidean division algorithm goes for writing $f=q\,g+r$.

$f - a\,m\,g_i$, and one restarts; since $LT(f) = LT(a\,m\,g_i)$, the monic monomial in the leading term $LT(f - a\,m\,g_i)$ is $<$ the monic monomial in $LT(f)$; if the current $LT(f)$ is not divisible by $LT(g_1), \ldots, LT(g_k)$, one adds $LT(f)$ to r, one replaces f by $f - LT(f)$, and one restarts; the monic monomial in the leading term $LT\big(f - LT(f)\big)$ is $<$ the monic monomial in $LT(f)$, so that after finitely many operations it stops, and all the terms in r (whose monic monomial terms are decreasing) are divisible by none of the $LT(g_i)$.

Example 29.11: Let $f = x^2 + x - y^2 + y$, with $g_1 = x\,y + 1$ and $g_2 = x + y$, using the order $x > y$. Since $LT(f) = x^2 = x\,LT(g_2)$, one adds x to q_2, and one changes f into $f = -x\,y + x - y^2 + y$; since $LT(f) = -x\,y = -LT(g_1)$, one adds -1 to q_1 and one changes f into $f = x - y^2 + y + 1$; since $LT(f) = x = LT(g_2)$, one adds 1 to q_2 and one changes f into $f = -y^2 + 1$, which one finally adds to r; one has obtained $f = -g_1 + (x + 1)\,g_2 - y^2 + 1$.

With the same monomial order, one uses $g_1 = x + y$ and $g_2 = x\,y + 1$. Since $LT(f) = x^2 = x\,LT(g_1)$, one adds x to q_1, and one changes f into $f = -x\,y + x - y^2 + y$; since $LT(f) = -x\,y = -y\,LT(g_1)$, one adds $-y$ to q_1 and one changes f into $f = x + y$; since $LT(f) = x = LT(g_1)$ so that one adds 1 to q_1 and one changes f into $f = 0$, and one has found that $f = q_1 g_1$ with $q_1 = x - y + 1$.

Lemma 29.12: For a monomial ordering on $F[x_1, \ldots, x_n]$, let $\{g_1, \ldots, g_k\}$ be a Gröbner basis for a non-zero ideal I in $F[x_1, \ldots, x_n]$. Then

i) Every $f \in F[x_1, \ldots, x_n]$ can be written in a unique way in the form $f = f_I + r$ with $f_I \in I$, and no non-zero term in the remainder r is divisible by any of the leading terms $LT(g_1), \ldots, LT(g_k)$.

ii) Both f_I and r can be computed by the general polynomial division (Remark 29.10) by $\{g_1, \ldots, g_k\}$ and are independent of the order in which the polynomials g_i are used in the division.[4]

iii) The remainder r provides a unique representative for the coset of f in the quotient $F[x_1, \ldots, x_n]/I$, and in particular $f \in I$ if and only if $r = 0$.

Proof: Whatever the set $\{g_1, \ldots, g_k\} \subset I$, the general division produces an element $f_I = \sum_{i=1}^k q_i g_i \in I$ and a remainder having the required properties, and the uniqueness comes from the fact that the ideal generated by $LT(g_1), \ldots, LT(g_k)$ is $LT(I)$ (so that this condition implies that $g_1, \ldots, g_k$ generate I).

If $f = f_I + r = f'_I + r'$, then $f_I - f'_I = r' - r$, so that $LT(r' - r) \in LT(I)$, hence it is a combination of $LT(g_1), \ldots, LT(g_k)$, but this cannot happens if $r' \neq r$, since no (non-zero) term in $r' - r$ is a multiple of one of the $LT(g_i)$, in particular $LT(r' - r)$.[5] The uniqueness implies that whatever the order of operations in the general division, one ends up with the same r and the same f_I (but possibly different coefficients q_i).

If $r = 0$, then $f = f_I \in I$, while if $f \in I$ it can be written as $f + 0$ and the uniqueness implies $r = 0$.

Lemma 29.13: For a monomial ordering on $F[x_1, \ldots, x_n]$, if $g_1, \ldots, g_k$ are elements of a non-zero ideal I such that $LT(g_1), \ldots, LT(g_k)$ generate $LT(I)$, then $\{g_1, \ldots, g_k\}$ is a Gröbner basis for I. Every non-zero ideal I possesses a Gröbner basis.[6]

Proof: The first part was noticed in the proof of Lemma 29.12, since the only property used for proving uniqueness was that $LT(g_1), \ldots, LT(g_k)$ generate $LT(I)$, and then since r must be 0 for any element $f \in I$, the division must provide that result, and write f as a combination of the g_i. The existence follows from Hilbert's basis theorem (Lemma 28.3) that $LT(I)$ is finitely generated, by $f_1, \ldots, f_\ell \in LT(I)$, and then each f_i is a finite combination of $LT(f_{i,j})$ with $f_{i,j} \in I$ for $j = 1, \ldots, n_i$, and the union of all the $f_{i,j}$ gives a desired list $\{g_1, \ldots, g_k\}$.

Additional footnotes: KEPLER.[7]

[4] For $k \geq 2$, it is f_I which is defined in a unique way, and not the list $q_1, \ldots, q_k$, since $g_1 g_2 = q_1 g_1 = q_2 g_2$ with $q_1 = g_2$ and $q_2 = g_1$.

[5] If a monic monomial m can be written as $\sum_{i=1}^k P_i m_i$ for some monic monomials $m_1, \ldots, m_k$ and some polynomials $P_1, \ldots, P_k$, then it remains true if one only keeps in each P_i the term $r_i m'_i$ with $r_i \in R$ and m'_i the monic monomial such that $m_i m'_i = m$, showing it can only happen when m is a multiple of *one* of the m_j.

[6] At this point, the existence of a Gröbner basis is proved in a non-constructive way, by invoking Hilbert's basis theorem, but later Buchberger's algorithm will provide an explicit way to construct Gröbner bases.

[7] Johannes KEPLER, German-born mathematician, 1571–1630. He worked in Graz, Austria, in Prague, now capital of the Czech republic, and in Linz, Austria, where the Johannes Kepler University is now named after him.