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

30- Friday April 6, 2012.

Definition 30.1: For a monomial ordering on $F[x_1,\ldots,x_n]$, if $f_1,f_2\in F[x_1,\ldots,x_n]$ and M is the monic least common multiple of $LT(f_1)$ and $LT(f_2)$, then $S(f_1,f_2)=\frac{M}{LT(f_1)}\,f_1-\frac{M}{LT(f_2)}\,f_2$.[1]

Lemma 30.2: For a monomial ordering on $F[x_1,\ldots,x_n]$, if $f_1,\ldots,f_k\in F[x_1,\ldots,x_n]$ have the *same multi-degree* α and the linear combination $h=a_1f_1+\ldots+a_kf_k$ with $a_1,\ldots,a_k\in F$ has strictly smaller multi-degree, then $h=b_2S(f_1,f_2)+\ldots+b_kS(f_{k-1},f_k)$ for some $b_2,\ldots,b_k\in F$.
Proof: One writes $f_i=c_if'_i$ with $c_i\in F$ and f'_i monic, so that $h=\sum_{i=1}^k a_ic_if'_i$, which can be written as $h=a_1c_1(f'_1-f'_2)+(a_1c_1+a_2c_2)\,(f'_2-f'_3)+\ldots+(a_1c_1+\ldots+a_{k-1}c_{k-1})\,(f'_{k-1}-f'_k)+\big(\sum_{i=1}^k a_ic_i\big)\,f'_k$. Since h and each $f'_{i-1}-f'_i$ has multi-degree strictly smaller than α, one deduces that $\sum_{i=1}^k a_ic_i=0$, and then one observes that $S(f_{i-1},f_i)=f'_{i-1}-f'_i$ for $i=2,\ldots,k$.

Remark 30.3: Lemma 30.2 will be used in showing Buchberger's criterion, which is a way to check that a list $\{g_1,\ldots,g_k\}$ is a Gröbner basis of an ideal I by putting all the $S(g_i,g_j)$ through the general polynomial division algorithm; then, the criterion will be used for constructing Gröbner bases with Buchberger's algorithm.

Lemma 30.4: (*Buchberger's criterion*) For a monomial ordering on $F[x_1,\ldots,x_n]$, a non-zero ideal I of $F[x_1,\ldots,x_n]$, and a set $G=\{g_1,\ldots,g_k\}$ generating I, then G is a Gröbner basis of I if and only if $S(g_i,g_j)=0\pmod G$ for $i,j=1,\ldots,k$, where $f=0\pmod G$ means that the remainder of the general polynomial division by $g_1,\ldots,g_k$ (in this order) gives a remainder 0.
Proof: If G is a Gröbner basis of I, then the remainder of the general polynomial division of $S(g_i,g_j)$ is 0, since $S(g_i,g_j)\in I$.

One assumes that $S(g_i,g_j)=0\pmod G$ for $i,j=1,\ldots,k$, and for showing that G is a Gröbner basis one must show that for every $f\in I$ its leading term $LT(f)$ is in the ideal generated by $LT(g_1),\ldots,LT(g_k)$. Since $f\in I$ and $g_1,\ldots,g_k$ generate I, one has $f=\sum_i h_ig_i$ for some $h_1,\ldots,h_k\in F[x_1,\ldots,x_n]$, and among those representations one considers one which gives the lowest possible value to $\alpha=\max_i\partial(h_ig_i)$, the largest multi-degree of any summand (using the fact that the monomial ordering is a well order), and one has $\partial(f)\le\alpha$. One writes $f=\sum_{\partial(h_ig_i)=\alpha}LT(h_i)\,g_i+\sum_{\partial(h_ig_i)=\alpha}\big(h_i-LT(h_i)\big)\,g_i+\sum_{\partial(h_ig_i)<\alpha}h_i\,g_i$, noticing that the multi-degree of the last two sums is $<\alpha$. If one has $\partial(f)=\alpha$, then keeping only the terms of multi-degree α in the preceding equality, one finds that $LT(f)=\sum_{\partial(h_ig_i)=\alpha}LT(h_i)\,LT(g_i)$, which is the desired conclusion.

It remains to show that the case $\partial(f)<\alpha$ contradicts the minimality assumption for α. One changes the indexing of the first sum, so that it corresponds to i varying from 1 to ℓ, with $\ell\ge1$ by the fact that $\alpha=\max_i\partial(h_ig_i)$ (since the sum cannot be empty), and $\ell\ge2$ by the assumption $\partial(f)<\alpha$ (which implies that the terms in x^α cancel). One writes $a_i\in F$ for the coefficient in $LT(h_i)$, so that $LT(h_i)=a_ih'_i$ for a monic monomial h'_i for $1\le i\le\ell$; since each term $h'_i\,g_i$ has multi-degree α, but the sum $\sum_{i=1}^\ell a_i(h'_i\,g_i)$ has multi-degree $<\alpha$, Lemma 30.2 implies that this sum can be written as $\sum_{i=2}^\ell b_iS(h'_{i-1}g_{i-1},h'_ig_i)$ for some $b_2,\ldots,b_\ell\in F$. For defining $S(g_{i-1},g_i)$, Definition 30.1 introduces the monic monomial M which is the least common multiple of $LT(g_{i-1})$ and $LT(g_i)$, but since $x^\alpha=LT(h'_{i-1}\,g_{i-1})=LT(h'_i\,g_i)$ (because $LT(h'_j\,g_j)=x^\alpha$ for $j=1,\ldots,\ell$), x^α is a multiple of both $LT(g_{i-1})$ and $LT(g_i)$, hence $x^\alpha=x^\beta M$ for a non-negative multi-degree β, and Definition 30.1 gives $S(h'_{i-1}g_{i-1},h'_ig_i)=x^\beta S(g_{i-1},g_i)$ for $i=2,\ldots,\ell$. For $i=2,\ldots,\ell$, $S(g_{i-1},g_i)=0\pmod G$ by hypothesis, i.e. the general polynomial division of $S(g_{i-1},g_i)$ by $g_1,\ldots,g_k$ produces a decomposition $S(g_{i-1},g_i)=\sum_{j=1}^k q_jg_j$ with a zero remainder, and one checks easily that the general polynomial division of $x^\beta S(g_{i-1},g_i)$ produces the decomposition $S(h'_{i-1}g_{i-1},h'_ig_i)=x^\beta S(g_{i-1},g_i)=\sum_{j=1}^k x^\beta q_jg_j$ with a zero remainder; moreover, since $\partial\big(x^\beta S(g_{i-1},g_i)\big)<\alpha$ the the general polynomial division algorithm implies that each term $x^\beta q_jg_j$ has a multi-degree $<\alpha$, contradicting the minimality assumption of α.

[1] So that if ψ_1 and ψ_2 are monic with the same multidegree, one has $S(\psi_1,\psi_2)=\psi_1-\psi_2$.

Definition 30.5: A Gröbner basis $\{g_1, \ldots, g_k\}$ for a non-zero ideal I (of $F[x_1, \ldots, x_n]$, for which one has chosen a monomial ordering) is called a *minimal Gröbner basis* if each $LT(g_i)$ is monic, and $LT(g_j)$ is not divisible by $LT(g_i)$ for $j \neq i$;[2] it is called a *reduced Gröbner basis* if each $LT(g_i)$ is monic, and no term in g_j is divisible by $LT(g_i)$ for $j \neq i$.[3]

Remark 30.6: (*Buchberger's algorithm*) One starts from a generating system $G = \{g_1, \ldots, g_k\}$ of a non-zero ideal I (of $F[x_1, \ldots, x_n]$, for which one has chosen a monomial ordering), and one computes the remainders of the general polynomial divisions of $S(g_i, g_j)$ by $g_1, \ldots, g_k$ (for $j \neq i$). If all remainders are 0, then one has found a Gröbner basis by Buchberger criterion (Lemma 30.4), but once one finds a remainder $r \neq 0$, one adds it to the list as g_{k+1}, and one restarts the process with the enlarged set G. If at one stage the general polynomial division of $S(g_i, g_j)$ has given remainder 0, one does not need to reconsider the general polynomial division later by an enlarged list, since the new elements are added *after* $g_1, \ldots, g_k$.[4] The algorithm produces a Gröbner basis after a finite number of steps (Lemma 30.7).

Once one has a Gröbner basis, it stays a Gröbner basis if one multiplies each g_i by a non-zero constant ($\in F^*$), so that one may assume that each g_i is monic. If $LT(g_j)$ is a multiple of $LT(g_i)$ for $j \neq i$, one suppresses g_j from the list without changing the ideal generated by the $LT(g_i)$, so that it still produces a Gröbner basis, and after a finite number of such reductions, one obtains a minimal Gröbner basis.

Starting with a minimal Gröbner basis G, if for some $j \neq i$ a term in g_j is a multiple of $LT(g_i)$ (and this term cannot be the leading term $LT(g_j)$), one replaces it by the remainder in its general polynomial division by G, and no term in the remainder is a multiple of one of the $LT(g_i)$ by construction; of course, it amounts to adding to g_j an element of I without changing the leading term. After a finite number of such reductions, one obtains a reduced Gröbner basis.

Lemma 30.7: Given a generating set $G = \{g_1, \ldots, g_k\}$ of a non-zero ideal I of $F[x_1, \ldots, x_n]$ (for which one has chosen a monomial ordering), Buchberger's algorithm for producing a reduced Gröbner basis of I (Remark 30.6) terminates in a finite number of steps.

Proof: By definition of the algorithm, when one adds an element g_{k+1} to G, it is not divisible by any $LT(g_i)$ for $i = 1, \ldots, k$, so that the ideal generated by $\{LT(g_1), \ldots, LT(g_{k+1})\}$ is strictly larger than the ideal generated by $\{LT(g_1), \ldots, LT(g_k)\}$,[5] so that the algorithm creates an increasing sequence of ideals, which must become constant by Hilbert's basis theorem (Lemma 28.3), hence one can only add a finite number of terms to G. Of course, the existence of a finite generating set G for the ideal also follows from Hilbert's basis theorem.

Remark 30.8: For $f_1, \ldots, f_k \in F[x_1, \ldots, x_n]$, one denotes $Z(f_1, \ldots, f_k)$ the set of their common zeros, i.e. $\{a \in F^n \mid f_1(a) = \ldots = f_k(a) = 0\}$. Then if f belongs to the ideal $I = (f_1, \ldots, f_k)$, one has $f = \sum_i q_i f_i$, so that $f(a) = 0$. If $h_1, \ldots, h_\ell$ is another set of generators of I, then the set of their common zeros $Z(h_1, \ldots, h_\ell)$ coincides with $Z(f_1, \ldots, f_k)$.[6]

Gröbner bases help studying the question of common zeros by describing a way to choose a monomial ordering for eliminating variables.

---

[2] It can be shown that two minimal Gröbner bases have the same number of elements and the same set of leading terms.

[3] It can be shown that there is a unique reduced Gröbner basis.

[4] If the general polynomial division of $S(g_i, g_j)$ has given remainder $r \neq 0$ (which belongs to I), then one must divide r by g_{k+1} (or any element added after), and that may change the remainder of the general polynomial division and add some quotients for the added elements.

[5] It is a simple property of a *monomial ideal*, i.e. an ideal J generated by a set of monic monomials $m_\alpha, \alpha \in A$, that a monomial x^β belongs to J if and only if x^β is a multiple of one of the m_α: if there is an identity $x^\beta = \sum_\alpha P_\alpha m_\alpha$ for a finite list of non-zero polynomials P_α, one keeps only the terms proportional to x^β in each product $P_\alpha m_\alpha$, i.e. a term $c_\alpha x^\beta$, and since one obtains $1 = \sum_\alpha c_\alpha$, there exists $\alpha \in A$ with $c_\alpha \neq 0$, and it implies that x^β is a multiple of m_α. Similarly, a polynomial P belongs to J if and only if each of its terms is a multiple of one of the m_α.

[6] If all the h_j were vanishing at a supplementary point b, then all elements of I would vanish at b, so that the f_i would have b as a common zero.

Definition 30.9: If I is an ideal in $F[x_1, \ldots, x_n]$, then $I_i = I \cap F[x_{i+1}, \ldots, x_n]$ is called the i^{th} *elimination ideal* of I with respect to the ordering $x_1 > \cdots > x_n$.

Lemma 30.10: If $G = \{g_1, \ldots, g_k\}$ is a Gröbner basis for the non-zero ideal I in $F[x_1, \ldots, x_n]$ with respect to the lexicographic ordering $x_1 > \cdots > x_n$, then $G_i = G \cap F[x_{i+1}, \ldots, x_n]$ is a Gröbner basis of the i^{th} elimination ideal $I_i = I \cap F[x_{i+1}, \ldots, x_n]$ of I; in particular, $I \cap F[x_{i+1}, \ldots, x_n] = \{0\}$ if and only if $G_i = \emptyset$.
Proof: One has $G_i \subset I_i$, and for showing that G_i is a Gröbner basis of I_i it suffices to show that $LT(G_i)$, the set of leading terms of elements in G_i, generates $LT(I_i)$ (as an ideal in $F[x_{i+1}, \ldots, x_n]$). One has $\big(LT(G_i)\big) \subset \big(LT(I_i)\big)$, and one wants to show that for every $f \in I_i$ its leading term $LT(f)$ is a combination of elements in $LT(G_i)$. Since $f \in I$ and G is a Gröbner basis, one has $LT(f) = a_1 LT(g_1) + \ldots + a_k LT(g_k)$ with $a_1, \ldots, a_k \in F[x_1, \ldots, x_n]$, and one writes each a_i as a sum of monomials $m_{i,j}$, and since $LT(f)$ is a monomial which does not contain the variables $x_1, \ldots, x_i$, one deduces an equality by suppressing all the terms $m_{i,j} LT(g_i)$ which contain the variables $x_1, \ldots, x_i$, and one obtains $LT(f)$ as a $F[x_{i+1}, \ldots, x_n]$-linear combination of those $LT(g_i)$ which do not contain the variables $x_1, \ldots, x_i$, and one observes that by the choice of ordering of the monomials, once the leading term $LT(g_i)$ does not contain the variables $x_1, \ldots, x_i$, then no other term of g_i does, hence $g_i \in G_i$.

Remark 30.11: If $I = (f_1, \ldots, f_k)$ and $J = (g_1, \ldots, g_\ell)$ are two ideals in $F[x_1, \ldots, x_n]$, then $I + J = (I \cup J) = (f_1, \ldots, f_k, g_1, \ldots, g_\ell)$, and $I\,J = (f_i g_j \mid i = 1, \ldots, k, j = 1, \ldots, \ell)$,[7] and Lemma 30.12 gives a procedure for computing what $I \cap J$ is.

Lemma 30.12: If $I = (f_1, \ldots, f_k)$ and $J = (g_1, \ldots, g_\ell)$ are two ideals in $F[x_1, \ldots, x_n]$, and K is the ideal generated by $\{t\,f_1, \ldots, t\,f_k, (1-t)\,g_1, \ldots, (1-t)\,g_\ell\}$ in $F[t, x_1, \ldots, x_n]$ (i.e. in one more variable t), then, $I \cap J = K \cap F[x_1, \ldots, x_n]$, so that $I \cap J$ is the first elimination ideal of K with respect to the ordering $t > x_1 > \cdots > x_n$.[8]
Proof: If $h \in I \cap J \subset F[x_1, \ldots, x_n]$, then $h = t\,h + (1-t)\,h \in K$, so that $I \cap J \subset K \cap F[x_1, \ldots, x_n]$. Conversely, let $h \in F[x_1, \ldots, x_n]$ which belongs to K, i.e. it can be written as $h = \sum_{i=1}^k a_i t\, f_i + \sum_{j=1}^\ell b_j (1-t)\, g_j$, with $a_1, \ldots, a_k, b_1, \ldots, b_\ell \in F[t, x_1, \ldots, x_n]$. Then one divides both sides by $t\,(t-1)$ and one writes the equality between the remainders: it consists in keeping the remainder of the division of each a_i by $t-1$, and keeping the remainder of the division of each b_j by $-t$, which is equivalent to considering that the a_i and the b_j belong to $F[x_1, \ldots, x_n]$, and then the coefficient of t gives $0 = \sum_{i=1}^k a_i\, f_i - \sum_{j=1}^\ell b_j\, g_j$, and the constant coefficient gives $h = \sum_{j=1}^\ell b_j\, g_j$, which implies $h \in J$, but combining the two equations gives $h = \sum_{i=1}^k a_i\, f_i \in I$.

Remark 30.13: The technique of elimination goes back to BÉZOUT,[9] to whom one owes Bézout's theorem, which restricted to two plane algebraic curves, $P(x,y) = 0$ for a polynomial of total degree p and $Q(x,y) = 0$ for a polynomial of total degree q, states that eliminating one of the variables gives a polynomial of degree $(\leq)\ p\,q$, if the two curves do not share a component.

---

[7] Recall that for two ideals I, J in a commutative ring R, the notation of the product $I\,J$ is the set of finite sums $\sum_\alpha r_\alpha i_\alpha j_\alpha$ with $r_\alpha \in R$, $i_\alpha \in I$, $j_\alpha \in J$ (i.e. the ideal generated by all the products $i\,j$ for $i \in I$ and $j \in J$).

[8] Of course, from a practical point of view, one first finds a Gröbner basis for K, for which one uses Buchberger's algorithm (Remark 30.6), and then one uses Lemma 30.10.

[9] Étienne BÉZOUT, French mathematician, 1730–1783. He worked in Paris, France. Bézout's theorem is named after him.