# MATH 499: Notes

October 15, 2009

Last time we found that

$$\{x^2y + y^2z, xy^2 + z^2, y^3z - xz^2, x^3z^2 + xyz^3, x^2z^2 + yz^3\}$$

was a Gröbner basis for $I = \langle x^2y + y^2z, xy^2 + z^2\rangle \subset \mathbf{R}[x, y, z]$ in grlex order with $x > y > z$.

Of course, we'd like to be able to say our Gröbner bases are unique. As a first step, we noticed last time that one element of the Gröbner basis was redundant: $x^3z^2 + xyz^3 = x(x^2z^2 + yz^)$, so we could remove it and still have a Gröbner basis

$$\{x^2y + y^2z, xy^2 + z^2, y^3z - xz^2, x^2z^2 + yz^3\}.$$

More generally, if $G$ is a Gröbner basis with $f, g \in G$ and $LT(f)$ is a multiple of $LT(g)$, then $f$ will be redundant and can be removed, i.e. the set $G - \{f\}$ is still a Gröbner basis for the same ideal. (Why?)

Of course, multiplying any element of a Gröbner basis by a scalar will give a different Gröbner basis, so if we want uniqueness, we should require that each leading coefficient be 1. Since a monomial ideal certainly has a unique minimal monomial generating set, we might hope that forcing constant leading coefficients and removing redundant elements would be enough to get a Gröbner basis which is unique, but that is not quite the case. The problem is that we could still add a multiple of one generator to another. For example, for any $a, b \in \mathbf{R}$

$$\{x^2y + axy^2 + y^2z + az^2, xy^2 + z^2, y^3z - xz^2, x^2z^2 + by^3z + yz^3 - bxz^2\}$$

is another Gröbner basis for the same ideal as above. To avoid non-uniqueness arising in this way, we say that a *reduced* Gröbner basis $G$ is a Gröbner basis where the leading coefficient of every $f \in G$ is 1 and no term of any $f \in G$ is divisible by the leading term of any $g \in G$ with $g \neq f$.

Starting with a Gröbner basis, we can get a reduced Gröbner basis by multiplying by constants to clear any leading coefficients, throwing away any elements whose leading term is a proper multiple of another leading term, and then replacing each polynomial by the remainder upon dividing it by the rest (to clear out any terms divisible by any of the other leading terms). Moreover, reduced is all we need to impose to make our Gröbner bases unique:

**Theorem.** *Fix a term order on $\mathbf{R}[x_1, \ldots, x_n]$. Then every ideal $I \subseteq \mathbf{R}[x_1, \ldots, x_n]$ has a unique reduced Gröbner basis.*

*Proof.* To prove uniqueness, suppose that $G$ and $\tilde{G}$ are two different reduced Gröbner bases for $I$. The set of leading terms of both $G$ and $\tilde{G}$ must simply by the minimal set of monomial generators of $\langle LT(I)\rangle$, so if $G \neq G'$, it is because there is some $f \in G$ and $\tilde{f} \in \tilde{G}$ with $LT(f) = LT(\tilde{f})$ but $f \neq \tilde{f}$. Then $f - \tilde{f} \in I$, so the remainder of $f - \tilde{f}$ upon division by $G$ is zero, since $G$ is a Gröbner basis. However, since $G$ and $\tilde{G}$ are both reduced Gröbner bases, no non-leading term of $f$ or $\tilde{f}$ is divisible by any leading term in $G$. Since the leading terms of $f$ and $\tilde{f}$ cancel in $f - \tilde{f}$, no term of $f - \tilde{f}$ is divisible by a leading term of $G$, so we see that no actual division occurs, and the remainder is $f - \tilde{f}$, so $f - \tilde{f} = 0$, a contradiction.

□