LECTURE 5-24

We now sketch a few of the main ideas in Chapter 15. We work throughout with the polynomial ring $S = k[x_1, \ldots, x_n], k$ a field. We begin with the simple observation that ideals of S generated by monomials (*monomial ideals*) are much easier to compute with than general ones; for example, it is quite easy to compute the greatest common divisor or least common multiple of any pair of monomials. More generally, if F is a free S-module with basis $\{e_i\}$, then submodules of T generated by monomials times basis vectors (called *monomials in* F are easier to work with than general submodules. We need a systematic way to pick out particular monomial terms from elements of F, To this end, we introduce a *monomial order* on the monomials of any finitely generated free module F over S; this is a total order $>$ such that if m_1, m_2 are monomials of F and if $n \neq 1$ is a monomial of S, then $m_1 > m_2$ implies $nm_1 > nm_2 > m_2$. We give three examples; in all of them the variables are ordered so that $x_1 > \cdots > x_n$. The first is *lexicographic order*, in which $m = x_1^{a_1} \ldots x_n^{a_n} < m' = x_1^{b_1} \ldots x_n^{b_n}$ if $a_i < b_i$ for the first index i for which $a_i \neq b_i$; the next is *homogeneous lexicographic order*, in which the condition for $m < m'$ is that either $\deg m < \deg m'$ or $\deg m = \deg m'$ and $m < m'$ in the lexicographic order. Finally, we have *reverse lexicographic (revlex) order*, in which the condition for $m < m'$ is that $\deg m < \deg m'$ or $\deg m = \deg m'$ and $a_i > b_i$ for the *last* index i for which they differ. Note that so far we have ordered only the monomials in S, not those of F; we supplement the order by totally ordering the basis vectors as well, and then taking the lexicographic product of these orders to totally order terms in F. Any monomial order on F is *Artinian* in the sense that every nonempty set of monomials has a least element. We extend the notation to terms (scalar multiples of monomials): if um, vn are terms with u, v nonzero elements of k, then we decree that $um > vn$ whenever $m > n$ and similarly for $\geq$. Then any $f \in F$ has an *initial term* $\text{in}(f)$ (with respect to $>$), which is the $>$-largest term occurring in f; likewise any submodule M of F has an *initial submodule* $\text{in}(M)$ generated by the initial terms of all of its elements. Then an important result of Macaulay asserts that *if F is a free S-module with basis, M a submodule of F, and if $>$ is a monomial order, then the set B of monomials not in $\text{in}(M)$ forms a basis for F/M.* Indeed, to show that B is linearly independent, note that if there were a dependence relation $p = \sum_i u_i m_i \in M$ with the $m_i \in B$ and the u_i nonzero elements of k, then $\text{in}(p)$ would lie in $\text{in}(M)$. But $\text{in}(p)$ is one of the $u_i m_i$ and m_i is in B, this is a contradiction. Now if B did not span F/M, then among the elements of F not in the span of M and B we could take f to be one with minimal initial term $\text{in}(f)$. If $\text{in}(f)$ were in B, we could subtract it from f, getting a polynomial not in the span with a smaller initial term, a contradiction, so we may assume that $\text{in}(f) \in \text{in}(M)$. Subtracting an element of M with the same initial term as f results in a similar contradiction.

A *Gröbner basis* of a submodule M of a free module F with basis is a set of elements $g_1, \ldots, g_t$ of M such that $\text{in}(g_1), \ldots, \text{in}(g_t)$ generates $\text{in}(M)$. Note that if $N \subset M$ are submodules with $\text{in}(N) = \text{in}(M)$ with respect to a monomial order, then $N = M$, for otherwise there would be $f \in M$ not in N whose initial term is smallest among initial terms of elements not in N, and then $\text{in}(f) = \text{in}(g)$ for some $g \in N$. But then $f - g \in M, f - g \notin N$, and $f - g$ has smaller initial term than f, a contradiction. Hence any Gröbner basis is automatically a set of generators (though it may not be minimal as such). Such bases always exist for any submodule M, as given any set of generators we may enlarge it to another set whose initial elements generate $\text{in}(M)$. A Gröbner basis $g_1, \ldots, g_t$ is said to be *minimal* if no initial term of any g_i divides the initial term of another; clearly any Gröbner basis can be shrunk to a minimal one. Now if F is a free S-module with basis, we have a fixed monomial order $<$, and we are given $g_1, \ldots, g_t, f \in F$, then we can perform the following construction. Supposing inductively that monomials $m_1, \ldots, m_p$ in S and elements $g_{s_1}, \ldots, g_{s_p}$ have been chosen, set $f' = f - \sum_u m_u g_{s_u}$; if $f' \neq 0$ and some $\text{in}(g_i)$ divides a monomial term of f, let m be the greatest such term, set $s_{p+1} = i, m_{p+1} = m/\text{in}(g_i), f" = f' - m_{p+1} g_i$, and continue inductively, relabelling $f"$ as f'. The process ends after finitely many steps, either with $f' = 0$ or with no monomial term of f' divisible by $\text{in}(g_i)$ for any i; we call f' the *remainder* of f (with respect to the g_i) and the expression $f = \sum m_i g_i + f'$ *standard* (note however that it is not uniquely determined by f and the g_i, though we can modify the algorithm to make it unique). Given a free module F with basis and $g_1, \ldots, g_t \in F$, let g'_i be the initial term of g_i. For each pair of indices i, j for which g'_i, g'_j involve the same basis element e_k, there are monomials $m_{ij}, m_{ji} \in S$ such that $g_{ij} = m_{ji} g_i - m_{ij} g_j$ has a lower initial term than either $m_{ji} g_i$ or $m_{ij} g_j$; let h_{ij} be the remainder of g_{ij} with respect to the g_i, setting $h_{ij} = 0$ if g_i, g_j do not involve the same basis element. Then *Buchberger's Criterion* asserts that *$g_1, \ldots, g_t$ form a Gröbner basis for the submodule they generate if and only if $h_{ij} = 0$ for all i and j.* As an example, take $g_1 = x^2, g_2 = xy + y^2$ in $k[x, y]$, and order the monomials lexicographically, taking $x > y$. The initial terms are x^2, xy, whose gcd is x. Applying the division algorithm to g_1, g_2, we get $yg_1 - xg_2 = -xy^2$, whose remainder with respect to g_1, g_2 is y^3, which is not divisible by either of the initial terms we have, so we add y^3 to the basis. Then $g_1 = x^2, g_2 = xy + y^2, g_3 = y^3$ is a Gröbner basis. As a bonus, we obtain all syzygies (relations) among the elements of this basis (Theorem 15.10 in Eisenbud): these relations are generated by the single one $x^2 g_2 - (xy + y^2) g_1$, together with the formula $g_3 = yg_1 + (y - x) g_2$ that arose from the construction of g_3. In fact, *every finitely generated S-module has a resolution by free modules of length at most n* (Hilbert's chain-of-syzygies theorem).