

Definition 1 (Complex of R -modules 1.10). A **complex of R -Modules** is a sequence of modules F_i

and maps $F_i \rightarrow F_{i-1}$ such that the compositions $F_{i+1} \rightarrow F_i \rightarrow F_{i-1}$ are all zero. The homology of this complex at F_i is the module

$$\ker (F_i \rightarrow F_{i-1}) / \operatorname{im} (F_{i+1} \rightarrow F_i)$$

A free resolution of an R -module M is a complex

$$\mathcal{F} : \dots \rightarrow F_n \xrightarrow{\phi_n} \dots \rightarrow F_1 \xrightarrow{\phi_1} F_0$$

of free R -Modules such that $\operatorname{coker} \phi_1 = M$ and \mathcal{F} is exact (sometimes we add “ $\rightarrow 0$ ” to the right of \mathcal{F} and then insist that \mathcal{F} be exact except at F_0). We shall sometimes abuse this notation and say that an exact sequence

$$\mathcal{F} : \dots \rightarrow F_n \xrightarrow{\phi_n} \dots \rightarrow F_1 \xrightarrow{\phi_1} F_0 \rightarrow M \rightarrow 0$$

is a resolution of M . The image of the map ϕ_i is called the i th syzygy module of M . A resolution \mathcal{F} is a graded free resolution if R is a graded ring, the F_i are graded free modules, and the maps are homogeneous maps of degree 0. Of course only graded modules can have graded free resolutions. If for some $n < \infty$ we have $F_{n+1} = 0$, but $F_i \neq 0 \forall 0 \leq i \leq n$, then we shall say that \mathcal{F} is a finite resolution of length n .

Theorem 1 (Hilberts syzygy theorem 1.13). If $R = k[x_1, \dots, x_r]$, then every finitely generated graded R -Module has a finite graded free resolution of length $\leq r$.

Theorem 2 (Buchberger’s Criterion 15.8). The elements g_1, \dots, g_t form a Gröbner basis $\iff h_{ij} = 0$ for all i and j

Definition 2 (initial term 325). If $>$ is a monomial order, then for any $f \in F$ we define the **initial term** of f , written $\operatorname{in}_>(f)$ to be the greatest term of f with respect to the order $>$, and if M is a submodule of F we define $\operatorname{in}_>(M)$ to be the monomial submodule generated by the elements $\operatorname{in}_>(f)$ for all $f \in M$. When there is no danger of confusion we will simply write in in place of $\operatorname{in}_>$.

Definition 3 (Groebnerbasis 328). A **Gröbner basis with respect to an order $>$ on a free module with basis F** is a set of elements $g_1, \dots, g_t \in F$ such that if M is the submodule of F generated by g_1, \dots, g_t , then $\operatorname{in}_>(g_1), \dots, \operatorname{in}_>(g_t)$ generate $\operatorname{in}_>(M)$. We then say, that g_1, \dots, g_t is a **Gröbner basis for M**

Proposition-Definition 3 (15.6). Let F be a free S -module with basis and monomial order $>$. If $f, g_1, \dots, g_t \in F$ then there is an expression

$$f = \sum f_i g_i + f' \text{ with } f' \in F, f_i \in S_i,$$

where none of the monomials of f' is in $(\operatorname{in}(g_1), \dots, \operatorname{in}(g_t))$ and

$$\operatorname{in}(f) \geq \operatorname{in}(f_i g_i)$$

for every i . Any such f' is called a **remainder of f with respect to g_1, \dots, g_t** , and an expression $f = \sum f_i g_i + f'$ satisfying the condition of the proposition is called a **standard expression for f in terms of g_i** .

Algorithmus 1 (Division Algorithm 328). Let F be a free S -module with basis and a fixed monomial order. If $f, g_1, \dots, g_t \in F$, then we may produce a standard expression

$$f = \sum m_u g_{s_u} + f'$$

for f with respect to g_1, \dots, g_t by defining the indices s_u and the terms m_u inductively. Having chosen s_1, \dots, s_p and m_1, \dots, m_p , if

$$f'_p := f - \sum_{u=1}^p m_u g_{s_u} \neq 0$$

and m is the maximal term of f'_p that is divisible by some $\text{in}(g_i)$, then we choose

$$s_{p+1} = i, m_{p+1} = m / \text{in}(g_i)$$

This process terminates when either $f'_p = 0$ or no $\text{in}(g_i)$ divides a monomial of f'_p ; the remainder f' is then the last f'_p produced.

Algorithmus 2 (Buchberger's Algorithm 333). In the situation of Theorem 15.8, suppose that M is a submodule of F , and let $g_1, \dots, g_t \in M$ be a set of generators of M . Compute the remainders h_{ij} . If all of the $h_{ij} = 0$, then the g_i form a Gröbner basis for M . If some $h_{ij} \neq 0$, then replace g_1, \dots, g_t with g_1, \dots, g_t, h_{ij} , and repeat the process. As the submodule generated by the initial forms of g_1, \dots, g_t, h_{ij} is strictly larger than that generated by the initial forms of g_1, \dots, g_t , this process must terminate after finitely many steps. The upperbound

$$b = ((r+1)(d+1)+1)^{2^{(s+1)}(r+1)}$$

, where

r = number of variables, d = maximum degree of the polynomials g_i , and s = the degree of the Hilbert polynomial (this

Definition 4 (334).

$$\tau_{ij} := m_{ji}\epsilon_i - m_{ij}\epsilon_j - \sum_u f_u^{(ij)}\epsilon_u$$

, for $i < j$ such that $\text{in}(g_i)$ and $\text{in}(g_j)$ involve the same basis element of F .

Literatur

- [1] David Eisenbud. *Commutative Algebra*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, 1995.