Advanced Coding Theory and Cryptography

Notes by: Alex Pellegrini

Contents

Chapter 1

An introduction to Gröbner bases

Theorem 2.1.10 (Hilbert's Basis Theorem)

Proof. We proceed by induction on the number of variables. Let $I \subset A[X]$ be an ideal not finitely generated, we may assume it can be constructed by an infinite sequence $(f_i)_{i \in \mathbb{N}}$ of independent polynomials of minimal degree. "Independent" means that $f_i \in I \setminus J_i$ where we set $J_i :=< f_0, \ldots, f_{i-1} >$. Now let $a_i := lc(f_i)$ be the leading coefficient of f_i and consider $J := a_0, a_1, \ldots \subset A$. We know that J can be a basis for an ideal in A but since A is a Noetherian ring we have that there exists a finite basis for such ideal, say $J =< a_1, \ldots, a_N >$. We claim that $I =< f_1, \ldots, f_N >=: I'$.
Suppose by contrary that this is not true then take a polynomial $f_{N+1} \ni$, we want to show that it is a linear combination of elements of I':

$$a_{N+1} = u_1 a_1 + u_2 a_2 + \cdots + u_N a_N$$

Consider

$$g := \sum_{i=1}^{N} u_i f_i x^{deg(f_{N+1}) - deg(f_i)} \in I'$$

it has the same degree and same leading coefficient as f_{N+1}. Now $f_{N+1} - g \notin I'$ and has degree strictly less than f_{N+1} contraddicting its minimality. Therefore $f_{N+1} - g$ must be 0 and $f_{N+1} \in I'$.

The induction follows since we can consider $A[X_1, \ldots, X_m] = A'[X_m]$ where $A' := [X_1, \ldots, X_{m-1}]$ which we know is a Noetherian ring. $\square$