21-237: Math Studies Algebra I November 18, 2022

Lecture 31 : Hilbert's Basis Theorem

Lecturer: James Cummings
Scribe: Rajeev Godse

1 Free modules

Notation: In general, infinite sums/products aren't defined over algebraic structures, because they do not admit notions of convergence. However, we define them by convention when the support of a sum is finite. That is, if we have some infinite family $(r_i)_{i\in I}$ drawn from an abelian group but $W_I = \{i \in I : r_i \neq 0\}$ is finite, then we define $\sum_{i\in I} r_i = \sum_{i\in W_I} r_i$. If $W_I = \emptyset$, define the sum to be 0.

Suppose an R-module M is free with basis X. Then, for each $m \in M$, there is a unique sequence $(r_x)_{x\in X}$ such that $\{x \in X : r_x \neq 0\}$ is finite and $m = \sum_{x\in X} r_x x$. That X is spanning gives us existence and that X is independent gives us uniqueness, an easy exercise.

M is also isomorphic to an R-module whose elements are $(r_x)_{x\in X}$ with $\{x \in X : x \neq 0\}$ finite, with pointwise addition and multiplication, which we might refer to as the direct sum of $|X|$ copies of R.

2 Closure under polynomial-ization

Facts:

(1) R is a Noetherian ring $\implies R[x]$ is a Noetherian ring, sometimes called Hilbert's basis theorem.

(2) R is a UFD $\implies R[x]$ is a UFD.

Proof of (1): Let I be an ideal of $R[x]$.

For each n, let $J_n = \{r \in R : \exists a_0, \dots, a_{n-1} \in R, \sum_{i=0}^{n-1} a_i x^i + rx^n \in I\}$.

Claim (A): J_n is an ideal of R. *Proof*: $0 = 0 + 0x + \dots 0x^n \in I$, so $0 \in J_n$. J_n is closed under linear combinations with coefficients from R since the polynomials witnessing membership in J_n are in ideal I which is closed under linear combinations and the witness for a linear combination of elements in J_n is the corresponding linear combination of witnessing polynomials for constituent elements. □

Claim (B): $J_n \subseteq J_{n+1}$. *Proof*: $p \in I \implies px \in I$. □

As R is Noetherian, the ascending chain (J_n) eventually stabilizes, i.e. there is $m \in \mathbb{N}$ such that $n \geq m \implies J_n = J_m$. As R Noetherian, for each i with $0 \leq i \leq m$, J_i is a finitely generated ideal of R, so choose $F_i \subseteq I$, a finite set of polynomials of degree i such that their leading coefficients generate J_i.

Let $F = \bigcup_{i=0}^{m} F_i$. We claim F generates I.

Claim: For all $h \in I$, h is an $R[x]$-linear combination of elements of F.

Proof: $h = 0$ works. If $h \neq 0$, let's induct on degree.

In particular, suppose that for all polynomials in I of smaller degree than h, the claim holds.

Case 1: $\deg(h) = t \leq m$. The leading coefficient of h is $c \in J_t$.

c is R-linear in the leading coefficients of the polynomials in F_t from our setup.

Then subtracting that R-linear combination of those polynomials from h eliminates the leading term and yields a lower degree polynomial. By the induction hypothesis that polynomial is in I, so by closure of I under linear combinations, $h \in I$.

Case 2: $\deg(h) = t > m$. The leading coefficient of $h = c \in J_t = J_m$.

As before, c is an R-linear combination of leading coefficients of polynomials in F_m.

Subtracting $x^{t-m}\times$ the same R-linear combination of polynomials eliminates the leading term, giving a polynomial of lower degree. Then, entirely as before, $h \in I$. □

As any ideal is finitely generated, $R[x]$ is Noetherian. □