Jonathan Lin

1 Preliminaries

First we will recall the definition of a ring:

Definition 1. A ring is a set R along with two operations $+$ and $\cdot$ with the following properties:

- $(R, +)$ is an abelian group.
- $\cdot$ is distributive over $+$, so that $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(a + b) \cdot c = a \cdot c + b \cdot c$ for all $a, b, c \in R$.
- $\cdot$ is associative.

If $\cdot$ is commutative we call R a *commutative* ring. If R has a multiplicative identity 1 (that is, an element such that $1 \cdot r = r \cdot 1 = r$ for all $r \in R$), we say that R is a *unital* ring.

From now on we will assume that our rings are commutative (and unital?) unless otherwise stated.

Definition 2. Suppose R is a ring. Then $I \subset R$ is an **ideal** if $RI \subseteq I$ or $IR \subseteq I$ (where the terms RI and IR are the usual notation). I is called *finitely generated* if

$$I = \langle a_1, \dots, a_n \rangle = \{a_1 r_1 + \cdots + a_n r_n \mid r_i \in R\}.$$

Here are some basic examples of rings.

Example 1. The ring of integers $\mathbb{Z}$ with usual integer addition and multiplication is a commutative ring with unity. Same with $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$.

Example 2. Let R be a ring. Then the polynomial ring $R[x]$ with coefficients in R with the usual multiplication and addition is a ring.

Example 3. The sets $\mathbb{Z}/n\mathbb{Z}$ can be made into rings with addition and multiplication modulo n.

2 Hilbert's Basis Theorem

Definition 3. Let R be a ring. Then R is **Noetherian** (after Emmy Noether) if every ideal of R is finitely generated.

Proposition 1. *R is Noetherian if and only if it satisfies the ascending chain condition: For every sequence of ideals*

$$I_1 \subset I_2 \subset I_3 \subset \cdots$$

there exists some $n \in \mathbb{N}$ such that

$$I_n = I_{n+1} = I_{n+2} = \cdots .$$

Example 4. Any PID is Noetherian, and so is any field F.

Example 5. Consider the field $R = F[x_1, x_2, \dots]$ of infinitely many indeterminates where F is a field. Then we have an increasing sequence of ideals

$$\langle x_1 \rangle \subset \langle x_1, x_2 \rangle \subset \langle x_1, x_2, x_3 \rangle \subset \cdots$$

where none of the ideals in the chain are equal to one another.

We are ready to state Hilbert's Basis Theorem.

Theorem 1. *If R is a Noetherian ring, then $R[x]$ is a Noetherian Ring. It also follows that $R[x_1, \dots, x_n]$ is a Noetherian ring by induction.*

Proof. Suppose that I is an ideal in $R[x]$. Denote $LC(I)$ to be the leading coefficients of elements in I. It is straightforward to check that $LC(I)$ is an ideal in R. Since R is Noetherian, $LC(I)$ is finitely generated. This means

$$LC(I) = \langle a_1, \dots, a_n \rangle.$$

By definition, a_i is the leading coefficient of some polynomial $f_i(x) = a_i x_i^n + \cdots$. Let N be the maximum degree of the f_i. Now define $LC(I_d)$ to be the leading coefficients of elements in I that have degree d (and 0). It is easy to show that $LC(I_d)$ is also an ideal of R. So

$$LC(I_d) = \langle b_{d,1}, \dots, b_{d,n_d} \rangle$$

and we can let $f_{d,i}(x)$ be the polynomials with the $b_{d,i}$ as leading coefficient.

We claim that

$$I = \langle f_i, f_{d,j} \rangle$$

where i rangles from 1 to n, d ranges from 1 to n, and j ranges from 1 to n_d (depending on d). This will show that I is finitely generated.

Suppose not. Then take a polynomial $f \in \langle f_i, f_{d,j} \rangle$ of minimal degree. If $\deg f \geq N$, then we can find polynomials $q_i(x)$ such that $\sum_{i=1}^n q_i f_i(x)$ has the same leading term as f. Subtracting we use the minimal degree assumption and we deduce that f is in $\langle f_i \rangle$. Otherwise, if $\deg f = d < n$ then we can do the same thing but with the $f_{d,i}$ instead. This shows that I is in fact $\langle f_i, f_{d,j} \rangle$ as desired. ■