1 More on Polynomial Rings

We now continue our discussion on polynomial rings.

1.1 Zeros

Theorem 1.1

A polynomial of degree n with coefficients in a field F has at most n zeros, counted with multiplicity.

Proof. We use induction on n, the degree of the polynomial.

- Base Case: Suppose $n = 0$. This means that the polynomial has degree zero, which clearly doesn't have any zeros.
- Inductive Step: Suppose this theorem is true for all polynomials of degree less than or equal to $n - 1$. Then, let $f(x)$ be a polynomial of degree n.
  1. Case 1: Suppose $f(x)$ has no roots[a]. Then, we have 0 roots which is clearly less than n roots, so we are done by $0 \leq n$.
  2. Case 2: Suppose a is a root of $f(x)$ of multiplicity $k \geq 1$. By definition, $f(x) = (x - a)^k g(x)$, where $g(a) \neq 0$ by k being maximal (or else we could add one more to k). If $b \neq a$ is a root of $f(x)$, then $0 = f(b) = (b - a)^k g(b)$, where $b - a$ is non-zero. Since F is a field, it is an integral domain so
  $$b - a \neq 0 \implies (b - a)^k \neq 0$$
  and
  $$0 = (b - a)^k g(b) \implies g(b) = 0$$
  In other words, every other root must come from $g(x)$. Note that $\deg g(x) = n - k \leq n - 1$. So, by the inductive hypothesis, $g(x)$ has at most $n - k$ roots with multiplicity, so $f(x)$ has less than or equal to $k + n - k = n$ roots (where k is the number of a roots with multiplicity; and $n - k$, which are the roots of g with multiplicity).

This completes the proof. □

[a] For example, consider $x^2 + 1 \in \mathbb{R}[x]$. This doesn't have any *real* roots.

1.1.1 Example: Integers Modulo 6

Consider $x^2 - x \in \mathbb{Z}/6\mathbb{Z}$. This is *not* a field because it is not an integral domain. This polynomial has roots 0, 1, 3, and 4.

Note that this particular polynomial has *4* zeros. The theorem we discussed above states that if the polynomial has coefficients in a *field*, then we should not expect this to happen.

1.2 Principal Ideal Domain

Definition 1.1: Principal Ideal Domain

A **principal ideal domain** (PID) is an integral domain R in which every ideal has the form $\langle a \rangle$ for some $a \in R$.

1.2.1 Example: The Integers

$\mathbb{Z}$ is a PID with

$$n\mathbb{Z} = \langle n \rangle$$

1.3 PIDs and Polynomial Rings

Theorem 1.2

Let F be a field. Then, $F[x]$ is a PID.

Proof. We know $F[x]$ is an integral domain. Let $I \subseteq F[x]$ be an ideal.

1. Case 1: Consider $I = \{0\}$. This is a principal ideal since $I = \{0\} = \langle 0 \rangle$.
2. Case 2: Suppose $I \neq \{0\}$. Choose some $g(x) \in I \subseteq \{0\}$ of minimal degree. Clearly, $\langle g(x) \rangle = \{g(x) \cdot f(x) \mid f(x) \in F[x]\} \subseteq I$ by property of an ideal. Now, take any element $f(x) \in I$. Write $f(x) = g(x)q(x) + r(x)$ where $\deg r(x) < \deg g(x)$ by the division theorem. This implies that $r(x) = f(x) - g(x)q(x)$. Now, $f(x) \in I$ and $g(x) \in I$, and since ideals are closed it follows that $g(x)q(x) \in I$. Additionally, since ideals are closed under addition, $f(x) - g(x)q(x) \in I$ and thus $r(x) \in I$. Note that $r(x) \in I$ with $\deg r(x) < \deg g(x)$, so by $g(x) \in I \setminus \{0\}$ of minimal degree, $r(x) \notin I \setminus \{0\}$. This implies that $r(x) = 0$ so $f(x) = g(x)q(x) \in \langle g(x) \rangle$ and thus $I \subseteq \langle g(x) \rangle$.

This concludes the proof. $\square$

Corollary 1.1

Let F be a field and $I \subseteq F[x]$ a non-zero ideal. Then, $I = \langle g(x) \rangle$ if and only if $g(x) \in I \setminus \{0\}$ of minimal degree.

1.3.1 Example: Homomorphism

Consider the homomorphism

$$\varphi : \mathbb{R}[x] \mapsto \mathbb{C}$$

defined by the evaluation map

$$f(x) \mapsto f(i)$$

By the first isomorphism theorem,

$$\mathbb{R}[x] / \ker \varphi \cong \varphi(\mathbb{R}[x])$$

Note that

$$\varphi(\mathbb{R}[x]) = \mathbb{C}$$

because

$$\varphi(a + bx) = a + bi \in \mathbb{C} \text{ for all } a + bi \in \mathbb{C}$$

Additionally, note that

$$x^2 + 1 \in \ker \varphi$$

because

$$\varphi(x^2 + 1) = i^2 + 1 = -1 + 1 = 0$$

And so $\ker \varphi = \langle x^2 + 1 \rangle$. This is specifically due to us trying every lower degree (from the proof above); that is:

- $0 \neq a \implies \varphi(2) = 2 \neq 0$, so degree 0 is not possible.
- $a + bx$, $b \neq 0 \implies \varphi(a + bx) = a + bi \neq 0$, so degree 1 is not possible.
- But, we have a quadratic polynomial that works.