1 Polynomial Rings

Definition 1.1: Polynomial Ring

Let R be a commutative ring. The **polynomial ring** over R in the indeterminate x is defined by

$$R[x] = \{a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \mid a_0, a_1, \ldots, a_n \in R, n \in \mathbb{Z}_{\geq 0}\}$$

Remark: We say that the set represented by $R[x]$ is a set of "formal symbols." In other words, these are things we can write down, not functions.

Definition 1.2

We say that

$$a_0 + a_1x + a_2x^2 + \cdots + a_nx^n = b_0 + b_1x + b_2x^2 + \cdots + b_mx^m$$

are equal if $a_i = b_i$ for all $i = 0, 1, 2, \ldots$. Here, we define $a_i = 0$ if $i > n$, and $b_i = 0$ if $i > m$.

Consider $\mathbb{F}_2[x]$. Here, polynomials determine functions. Consider $f(x) = x$ and $g(x) = x^2$. Then, this determines a function:

$f(x)$	$g(x)$
$\varphi_f : \mathbb{F}_2 \mapsto \mathbb{F}_2$ defined by: • $\varphi_f(0) = 0$ • $\varphi_f(1) = 1$	$\varphi_g : \mathbb{F}_2 \mapsto \mathbb{F}_2$ defined by: • $\varphi_g(0) = 0^2 = 0$ • $\varphi_g(1) = 1^2 = 1$

Here, $f(x) \neq g(x)$ but they determine the same function $\mathbb{F}_2 \mapsto \mathbb{F}_2$

Definition 1.3

In $R[x]$, if

$$f(x) = a_0 + a_1x + \cdots + a_nx^n$$
$$g(x) = b_0 + b_1x + \cdots + b_mx^m$$

then

$$f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_s + b_s)x^s$$

for $s = \max\{n, m\}$. Additionally,

$$f(x)g(x) = c_0 + c_1x + \cdots + c_{n+m}x^{n+m}$$

where

$$c_0 = a_0b_0$$
$$c_1 = a_1b_0 + a_0b_1$$
$$c_2 = a_2b_0 + a_1b_1 + a_0b_2$$
$$c_k = a_kb_0 + a_{k-1}b_1 + \cdots + a_1b_{k-1} + a_0b_k$$

Remark: In practice, we use distributive law for multiplication.

Definition 1.4

When $f(x) = a_0 + a_1x + \cdots + a_nx^n$ with $a_n \neq 0$, we say that:

- $f(x)$ has **degree** n, written $\deg f(x) = n$. However[a], if $f(x) = 0$, then we say that $f(x)$ has *no* degree *or* $f(x)$ has degree $-\infty$.
- a_n is the **leading coefficient** of $f(x)$.
- $f(x) = a_0$ is a **constant** polynomial.
- If $a_n = 1$, we say that $f(x)$ is a **monic** polynomial.

[a] If $f(x)$ is degree 0, then $f(x) = a_0x^0 = a_0$ for $a_0 \neq 0$.

Remarks:

- We omit terms like $0x^k$. For example, if our polynomial is $1 + 0x + 1x^2$, then we write $1 + 1x^2$.
- We write $1x^k$ as just x^k. So, for example, we write $1 + 1x^2$ as $1 + x^2$.
- We write $\cdots + (-a_k)x^k + \ldots$ as $\cdots - a_kx^k + \ldots$. For example, $1 + (-1)x^2 = 1 - x^2$.

1.1 Properties of Polynomial Rings

Proposition. *Let R be a commutative ring and $r \in R$. Then, the evaluation map*

$$\varphi_r : R[X] \mapsto R$$

$$f(x) \mapsto f(r) = a_0 + a_1r + a_2r^2 + \cdots + a_nr^n$$

is a homomorphism.

Proof. The proof is straightforward.

- Addition:

$$\begin{aligned} \varphi_r(f(x) + g(x)) &= \varphi_r((a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_s + b_s)x^s) \\ &= (a_0 + b_0) + (a_1 + b_1)r + \cdots + (a_s + b_s)r^s \\ &= a_0 + a_1r + \cdots + a_nr^n + b_0 + b_1r + \cdots + b_mr^m \\ &= \varphi_r(f(x)) + \varphi_r(g(x)) \end{aligned}$$

- Multiplication:

$$\begin{aligned} \varphi_r(f(x)g(x)) &= \varphi_r(c_0 + c_1x + \cdots + c_{n+m}x^{n+m}) \\ &= c_0 + c_1r + \cdots + c_{n+m}r^{n+m} \\ &= (a_0 + a_1r + \cdots + a_nr^n)(b_0 + b_1r + \cdots + b_mr^m) \\ &= \varphi_r(f(x))\varphi_r(g(x)) \end{aligned}$$

This proves that this is a homomorphism. □

Remark: This is not an injective homomorphism, but it **is** a surjective homomorphism.

Theorem 1.1

If D is an integral domain, then $D[x]$ is an integral domain.

Proof. $D[x]$ is commutative by definition. We know that $1 \in D$ so $f(x) = 1$ is the unity of $D[x]$. Suppose $f(x), g(x) \in D[x] \setminus \{0\}$ so that

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n$$

$$g(x) = b_0 + b_1 x + \cdots + b_m x^m$$

for $a_n \neq 0$ and $b_m \neq 0$. Then,

$$f(x)g(x) = a_0 b_0 + (a_1 b_0 + a_1 b_0)x + \cdots + a_n b_m x^{n+m}$$

but, $a_n \neq 0$ and $b_m \neq 0$ which implies that $a_n b_m \neq 0$ by D being an integral domain. Thus, $f(x)g(x) \neq 0$, so there are no zero-divisors and $D[x]$ is an integral domain. $\square$