Lecture 3

Polynomial Rings

Fix a commutative ring R with 1 (e.g. $R = \mathbb{Z}, R = \mathbb{Q}$, etc) Let X be an indeterminate

Definition 3.1: Polynomial Ring

A **polynomial** in X with coefficients in R is a formal, finite sum

$$a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0, \quad a_i \in R, i \in \{0, \ldots, n\}$$

Note: If $a_n \neq 0$ and $a_m = 0, \quad \forall m > n$. Then we say the **degree** of the polynomial is n. If $a_k = 1$, we often omit it from the notation, e.g

$$X^2 + 2$$

has a 1 "missing" infront of X^2.
If $a_n = 1$, we say the polynomial is **monic**

Definition 3.2: Constant Polynomial

The set of polynomials in X w/ coefficients in R is denoted

$$R[X] \coloneqq \{a_n X^n + \cdots + a_0 | a_i \in R\}$$

If the degree of $p \in R[X]$ is zero, we say p is a **constant** polynomial.

Observe that there is an obvious inclusion map from a ring into the ring of polynomials, by taking each element $a \in R$ to the constant polynomial $a \in R[X]$.

$$\begin{aligned} R &\to R[X] \\ a &\mapsto a \end{aligned}$$

Claim: $R[X]$ is a ring.

Proof. We check the ring properties
(i) Closure under addition

$$\begin{aligned} &(a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0) + (b_n X^n + b_{n-1} X^{n-1} + \cdots + b_1 X + b_0) \\ =&(a_n + b_n) X^n + (a_{n-1} + b_{n-1}) X^{n_1} + \cdots + (a_1 + b_1) X + (a_0 + b_0) \end{aligned}$$

(ii) Closure under multiplication

$$\begin{aligned} &(a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0) \cdot (b_n X^n + b_{n-1} X^{n-1} + \cdots + b_1 X + b_0) \\ &= (a_0 \cdot b_0) + (a_1 \cdot b_0 + a_0 \cdot b_1) X + (a_2 \cdot b_0 + a_1 \cdot b_1 + a_0 \cdot b_2) X^2 \\ &\qquad + \cdots + \sum_{k=0}^{l} a_k \cdot b_{l-k} X^l + \cdots + (a_n \cdot b_m) X^{n+m} \end{aligned}$$

■

Example 3.1 $\mathbb{Z}[X], \mathbb{Q}[X], \mathbb{Z}/3\mathbb{Z}[X]$. In particular, we may write

$$X+2, X^3+2X^2+1 \in \mathbb{Z}/3\mathbb{Z}[X]$$

Factoring polynomials depends on the coefficient ring. For example

$$X^2-2 \in \mathbb{Z}[X]$$
$$X^2-2 = (X+\sqrt{2}) \cdot (X-\sqrt{2}) \in \mathbb{R}[X]$$

Similarly, $X^2+1 \in \mathbb{Z}[X], X^2+1 \in \mathbb{R}[X]$. These polynomials doesn't factor in either ring, but it does factor in $\mathbb{C}[X]$

$$X^2+1 = (X+i)(X-i)$$

it also factors in $\mathbb{Z}/2\mathbb{Z}[X]$

$$X^2+1 = (X+1)(X+1) \pmod 2$$

Because $X^2+2X+1 \equiv X^2+1 \pmod 2$

Proposition 3.1

Let R be an integral domain and $p(X), q(X) \in R[X]$

(i) $\deg(p(X) \cdot q(X)) = \deg p(X) + \deg q(X)$.

(ii) $R[X]^\times = R^\times$

(iii) $R[X]$ is an integral domain

Proof.

(i) The leading term is

$$(a_n \cdot b_m) X^{n+m}$$

Since R is an integral domain and $a_n, b_m \neq 0$. Then $a_n \cdot b_m \neq 0$ (This also proves (iii))

(ii) Suppose $p(X) \in R[X]^\times$, say $p(X) \cdot q(X) = 1$.

Then

$$\deg(p \cdot q) = \deg(1) = 0 \implies \deg(p) = \deg(q) = 0 \implies p \in R$$

■

Example 3.2 $\mathbb{Z}/4\mathbb{Z}[X]$

Consider $2X^2+1, 2X^5+3X$,

$$(2X^2+1) \cdot (2X^5+3X) = 2 \cdot 2X^7 + \text{ lower terms} = 0 \cdot X^7 + \text{ lower terms}$$

This implies

$$\deg\left((2X^2+1) \cdot (2X^5+3X)\right) < \deg(2X^2+1) + \deg(2X^5+3x)$$

Ring Homomorphisms

Definition 3.3: Ring homomorphism and isomorphism

Let R, S be rings. A **ring homomorphism** is a map $f : R \to S$ such that

(i) $f(a +_R b) = f(a) +_S f(b)$ (**Group homomorphism**)

(ii) $f(a \cdot_R b) = f(a) \cdot_S f(b)$

If f is a bijective ring homomorphism, we say it is a **ring isomorphism**.
We say, in this case R is **isomorphic** to S as rings and write

$$R \cong S$$

Definition 3.4

The **kernel** of a ring homomorphism $f : R \to S$ is the subset

$$\operatorname{Ker} f := f^{-1}(0_S) \subset R$$

Proposition 3.2

Let R, S be rings and $f : R \to S$ a homomorphism

(i) $\operatorname{Im} f \subset S$ is a subring

(ii) $\operatorname{Ker} f \subset R$ is a subring

Moreover, if $r \in R$, $a \in \operatorname{Ker} f$ then $r \cdot a \in \operatorname{Ker} f$

Proof.
(i)
Claim: $f(0_R) = 0_S$ and in particular $\operatorname{Im} f \neq \emptyset$.

Proof. By definition of ring homomorphism

$$f(0_R) = f(0_R + 0_R) = f(0_R) + f(0_R) \implies 0_s = f(0_R)$$

Where we have subtracted (in S) $f(0_R)$ from both sides. ■

Suppose now $f(a), f(b) \in \operatorname{Im} f$, then

$$f(a) \cdot f(b) = f(a \cdot b) \in \operatorname{Im} f$$

To see $f(a) - f(b) \in \operatorname{Im} f$, it suffices to see that $-f(b) = f(-b)$.
Claim: $-f(b) = f(-b)$

Proof. Again using the ring homomorphism definition

$$0 = f(0_R) = f(b + (-b)) = f(b) + f(-b) \implies f(-b) = -f(b)$$

■

(ii)
Since $f(0_R) = 0_S \implies 0_R \in \operatorname{Ker} f$, hence $\operatorname{Ker} f$ is nonempty.
Suppose $a, b \in \operatorname{Ker} f$, then

$$f(a-b) = f(a) - f(b) = 0 - 0 = 0 \implies a - b \in \operatorname{Ker} f$$

and

$$f(a \cdot b) = f(a) \cdot f(b) = 0 \cdot 0 = 0 \implies a \cdot b \in \operatorname{Ker} f$$

Now suppose $r \in R$

$$f(r \cdot a) = f(r) \cdot f(a) = f(r) \cdot 0 = 0$$

■

Example 3.3 Consider

$$\begin{aligned} f : \mathbb{Z} &\to \mathbb{Z}/2\mathbb{Z} \\ a &\mapsto a \pmod 2 \end{aligned}$$

Check the possible situations

$$\text{Addition} \left| \begin{array}{ll} \bar{0} + \bar{0} = \bar{0} & \text{even} + \text{even} = \text{even} \\ \bar{0} + \bar{1} = \bar{1} & \text{even} + \text{odd} = \text{odd} \\ \bar{1} + \bar{1} = \bar{0} & \text{odd} + \text{odd} = \text{even} \end{array} \right.$$

$$\text{Multiplication} \left| \begin{array}{ll} \bar{0} \cdot \bar{0} = \bar{0} & \text{even} \cdot \text{even} = \text{even} \\ \bar{0} \cdot \bar{1} = \bar{0} & \text{even} \cdot \text{odd} = \text{even} \\ \bar{1} \cdot \bar{1} = \bar{1} & \text{odd} \cdot \text{odd} = \text{odd} \end{array} \right.$$

Therefore $\operatorname{Ker} f = \{\text{evens}\} = 2\mathbb{Z}$ and observe that

$$f^{-1}(\bar{1}) = \{\text{odds}\} = 1 + 2\mathbb{Z} = \{1 + 2n | n \in Z\} = 1 + \operatorname{Ker} f$$

Example 3.4 The following is a non-example. Consider

$$\begin{aligned} f_n \ : \mathbb{Z} &\to \mathbb{Z} \\ a &\mapsto n \cdot a \end{aligned}$$

Then

$$f_n(a+b) = n \cdot (a+b) = n \cdot a + n \cdot b = f_n(a) + f_n(b)$$

But

$$f_n(a \cdot b) = n(a \cdot b) \stackrel{?}{=} n^2(a \cdot b) = (n \cdot a) \cdot (n \cdot b) = f_n(a) \cdot f_n(b)$$

So f_n is a ring homomorphism if and only if $n^2 = n$ (i.e $n = 0, 1$). f_0 is the constant map zero and f_1 is the identity
Therefore $f_2, f_3, \ldots$ are **NOT** ring homomorphisms

Example 3.5 Here is a polynomial homomorphism which maps a polynomial to its own constant term

$$\begin{aligned} \phi : \mathbb{R}[X] &\to \mathbb{R} \\ p(X) &\mapsto p(0) \end{aligned}$$

This can easily be checked

$$\begin{aligned}\phi(p+q) &= (p+q)(0) = p(0)+q(0) = \phi(p)\phi(q)\\ \phi(p \bullet q) &= (p \bullet q)(0) = p(0) \bullet q(0) = \phi(p) \bullet \phi(q)\end{aligned}$$

Its kernel can also be stated

$$\text{Ker}\{p \in \mathbb{R}[X] \,|\, p(0)=0\} = \{p \in R[X] \,|\, p(x) = x \bullet p'(x) \text{for some} p' \in \mathbb{R}[X]\}$$

Question: What about

$$\begin{aligned}\phi_1 \ :&\mathbb{R}[X] \to \mathbb{R}\\ &p(x) \mapsto p(1)\end{aligned}$$