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

$$a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0, \quad a_i \in R, i \in \{0, \ldots, n\}$$

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

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

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

Obs: Ra

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

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

$$\begin{aligned}&(a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0) + (b_nX^n + b_{n-1}X^{n-1} + \cdots + b_1X + b_0)\\ =&(a_n + b_n)X^n + (a_{n-1} + b_{n-1})X^{n_1} + \cdots + (a_1 + b_1)X + (a_0 + b_0)\end{aligned}$$

(ii) Closure under multiplication

$$\begin{aligned}&(a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0) \cdot (b_nX^n + b_{n-1}X^{n-1} + \cdots + b_1X + b_0)\\ &= (a_0 \cdot b_0) + (a_1 \cdot b_0 + a_0 \cdot b_1)X + (a_2 \cdot b_0 + a_1 \cdot b_1 + a_0 \cdot b_2)X^2\\ &\qquad + \cdots + \sum_{k=0}^{l} a_k \cdot b_{l-k}X^l + \cdots + (a_n \cdot b_m)X^{n+m}\end{aligned}$$

■

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

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

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

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) $f(a \bullet_R b) = f(a) \bullet_S f(b)$

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

$$\ker f \coloneqq f^{-1}(0_S) \subset R$$

Proposition 3.2

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

(i)