§1 Lecture 11-18

§1.1 Polynomial Rings

Definition 1.1. Let R be a commutative ring with 1.

Polyomial over R with indeterminate x.

$$f(x) = \sum_{i=0}^{n} a_i x^i = a_0 + a_1 x^1 + \cdots + a_n x^n$$

Usually assume that $a_n \neq 0$ so that a_n is a leading coefficient.

f is monic if $a_n = 1$. $a_0, \cdots, a_n$ are coefficients of f.

n is the degree of f. The degree of 0 polynomial is $-\infty$.

$R[x]$ is the set of all polynomials over R. It is a ring. Add component wise and multiply by combining like terms.

$$\sum_{i=0} a_i x_{i + \sum_{i=0} b_i x^i = \sum (a_i + b_i) x_i}$$

$$(\sum a_i x^i)(\sum b_j x^j) = \sum c_k x^k \qquad \text{where } c_k = \sum_{i+j=k} a_i b_j$$

Multiplication and addition are associative, distributive, etc.

Example 1.2

$\mathbb{Z}_2[x]$:

$$(1 + x^2 + x^4)(1 + x^2 + x^4) = 1 + x^4 + x^8$$
$$(1 + x + x^2 + x^3)(1 + x + x^2 + x^3) = (1 + x^2 + x^4 + x^6)$$

$\mathbb{Z}_4[x]$:

$$(1 + x + x^2 + x^3)(1 + x + x^2 + x^3) = (1 + 2x + 3x^2 + 3x^4 + 2x^5 + x^8)$$

$\mathbb{Z}_6[x]$:

$$(2x^2 + 4 + 2)(3x^2 + 3x) = 0$$

Proposition 1.3

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

Moreover, degree$(p \cdot q)$ = degree(p) + degree(q) for $p, q \in R[x]$.

$$\underbrace{(a_n x^n + \cdots + a_0)}_{p}\underbrace{(b_m x^m + \cdots + b_0)}_{q} = (a_n b_m x^{n+m} + \cdots + a_0 b_0)$$

Definition 1.4 (The evaluation homomorphism)**.** Let F be the set of functions $\{f : \mathbb{R} \to \mathbb{R}\}$. Define the following:

$$(f+g)(x) = f(x) + g(x)$$
$$(f \cdot g)(x) = f(x) \cdot g(x)$$

Associative, distributive, etc. F is a commutative ring with unity.

The evaluation homomorphism is defined as follows:

$$\varphi_a : F \to \mathbb{R}$$

Let $a \in \mathbb{R}$. Define $\varphi_a(f) = f(a)$. This is a homomorphism because:

$$\varphi_a(fg) = \varphi_a(f)\varphi_a(g)$$
$$\varphi_a(f+g) = \varphi_a(f) + \varphi_a(g)$$

Likewise: $\varphi_a : R[x] \to R$ defined by $\varphi_a(f) = f(a)$ is homomorphic (where $a \in R$). Let

$$f = b_n x^n + b_{n-1} x^{n-1} + \cdots + b_1 x^1 + b_0$$

Then

$$f(a) = b_n a^n + b_{n-1} a^{n-1} + \cdots + b_1 a^1 + b_0$$

You can check that φ_a is a homomorphism for each $a \in R$.

Example 1.5

1. $\varphi_0 : R[x] \to R$

$$\varphi_0(f) = \text{ the constant term of } f$$

2. $\varphi_1 : R[x] \to R$

$$\varphi_1(f) = \sum(\text{ coefficients of } f)$$

3. $\varphi_1 : \mathbb{Z}_2[x] \to \mathbb{Z}_2$

   The kernel of φ_1 is ideal of all polynomials with an even number of terms.

Theorem 1.6 (Division Algorithm)

Let $f, g \in \mathbb{F}[x]$ where $\mathbb{F}$ is a field. Suppose $g \neq 0$. Then there exists unique $q, r \in \mathbb{F}[x]$ such that $f = gq + r$ where $r = 0$ or $\deg(r) < \deg(g)$.

Proof by induction on $\deg(f) - \deg(g)$.

If $\deg(f) < \deg(g)$ we stop $f = g \cdot 0 + f$. Otherwise, let $f = a_n x^n + \cdots$ and let $g = b_m x^m + \cdots$ where $m < n$.

Now let $f' = f - \frac{a_n}{b_m} x^{n-m} g$. Then $\deg(f') < \deg(f)$.

So by induction, $f' = gq' + r$ where $\deg(r) < \deg(g)$. So

$$f = f' + \frac{a_n}{b_m} x^{n-m} g = g(\frac{a_n}{b_m} x^{n-m} + q') + r$$

$\square$

Example 1.7

Apply the division algorithm to $x^2 + 0x + 1$ in $\mathbb{Z}_3[x]$. Let $f = 2x^5 + x^4 + 1$ and $g = x^2 + 1$.

$$
\begin{array}{r|rrrrrr}
 & & & 2x^3 & +x^2 & -2x & -1 \\
\hline
x^2+1 & 2x^5 & +x^4 & & & & +1 \\
 & -2x^5 & & -2x^3 & & & \\
\hline
 & & x^4 & -2x^3 & & & \\
 & & -x^4 & & -x^2 & & \\
\hline
 & & & -2x^3 & -x^2 & & \\
 & & & 2x^3 & & +2x & \\
\hline
 & & & & -x^2 & +2x & +1 \\
 & & & & x^2 & & +1 \\
\hline
 & & & & & 2x & +2
\end{array}
$$