MAT4006: Introduction to Coding Theory

Lecture 05: Rings of Polynomials and Construction of Fields

Instructor: Zitan Chen
Scribe: Siqi Yao

Spring 2025

1 The Ring of Polynomials

Definition 1.1 (Ring of Polynomials)

Let F be a field. The set

$$F[x] := \left\{ \sum_{i=0}^{n} a_i x^i \mid a_i \in F, n \geq 0 \right\} \tag{1}$$

is called the ring of polynomials. An element $f(x) = \sum_{i=0}^{n} a_i x^i$ in $F[x]$ is called a polynomial over F.

Remarks

1. If $a_n \neq 0$, the integer n is called the degree of f, denoted by $\deg(f)$. More precisely,

$$\deg(f) = \max \{ i \mid 0 \leq i \leq n, a_i \neq 0 \} \tag{2}$$

   For convenience, define

$$\deg(0) = -\infty. \tag{3}$$

2. A nonzero polynomial $f(x)$ of degree n is said to be monic if $a_n = 1$.

Definition 1.2 (Reducibility)

A polynomial $f \in F[x]$ with $\deg(f) > 0$ is said to be reducible (similar to composite number) over F if there exist two polynomials $g, h \in F[x]$ such that:

$$\deg(g) < \deg(f), \quad \deg(h) < \deg(f), \quad \text{and} \quad f = gh. \tag{4}$$

Otherwise, f is said to be irreducible over F.

Example

1. Let $f(x) = x^4 + 2x^6 \in \mathbb{Z}_3[x]$. $\deg(f) = 6$. f is not monic. $f(x) = x^4(1 + 2x^2)$
2. Let $g(x) = 1+x+x^2 \in \mathbb{Z}_2[x]$. $\deg(g) = 2$. g is monic. Since $\mathbb{Z}_2 = \{0, 1\}$, if g is reducible, it can only be reduced into product of $1+x$ and x. However, $g(1) = 1, g(0) = 1$, meaning that g has no linear factors over $\mathbb{Z}_2$, so g is irreducible. Recall the Factor theorem: Exists root $\alpha \Leftrightarrow$ has factor $x - \alpha$.

2 Roots of Polynomials

Definition 2.1 (Subfields)

Let E, F be two fields and $F \subseteq E$. The field F is called a subfield of E if the addition and multiplication of E, when restricted to F, are the same as in F. E is also called an extension field of F.

Example

1. $\mathbb{Q}$ is a subfield of $\mathbb{R}$.
2. $\mathbb{C}$ is a extension field of $\mathbb{R}$.
3. $\mathbb{Z}_p$ can be viewed as a subfield of any finite field with characteristic p. Important note: Same multiplication and addition rule.

Definition 2.2 (Roots)

Let F be a field and E be an extension field of F. An element $\beta \in E$ is a root of $f(x) \in F[x]$ if the equality $f(\beta) = 0$ holds in E.

Example

Consider $f(x) = 1 + x^2 \in \mathbb{R}[x]$. f is irreducible over $\mathbb{R}$. Let β be the imaginary unit in $\mathbb{C}$. $f(\beta) = 1 + \beta^2 = 0$. So β is a root of $f(x)$ in $\mathbb{C}$.

3 Construction of Fields

The ring $F[x]$ is a "generalization" of $\mathbb{Z}$. We can define congruence in $F[x]$ similarly as in $\mathbb{Z}$. Let $f(x) \in F[x]$, $\deg(f) = n \geq 1$. Then for any $g(x) \in F[x]$, there exist a unique pair of polynomials $(s(x), r(x))$ with $\deg(r) < \deg(f)$ such that:

$$g(x) = s(x)f(x) + r(x). \tag{5}$$

$s(x)$ corresponds to q and $r(x)$ corresponds to b in $a = qm + b$, respectively. The polynomial $r(x)$ is called the remainder of $g(x)$ divided by $f(x)$, denoted by $g(x) \pmod{f(x)}$.

Example

Let $f(x) = 1 + x^2 \in \mathbb{Z}_3[x], g(x) = x + 2x^4 \in \mathbb{Z}_3[x]$. Use long division to find that $g(x) \bmod f(x) = x + 2$.

Analogies between $\mathbb{Z}$ and $F[x]$

$\mathbb{Z}$	$F[x]$
integer m	polynomials $f(x)$
prime	irreducible

Recall the ring $\mathbb{Z}_m$ of integers modulo m. We can construct a set $F[x]/(f(x))$ for a given polynomial $f(x)$ of degree $n \geq 1$:

$\mathbb{Z}_m$	$F[x]/(f(x))$
$\{0, 1, \ldots, m-1\}$	$\left\{\sum_{i=0}^{n-1} a_i x^i \mid a_i \in F\right\}$
$a + b = (a + b \mod m)$	$g(x) + h(x) = (g(x) + h(x) \mod f(x))$
$a \cdot b = (a \cdot b \mod m)$	$g(x) \cdot h(x) = (g(x) \cdot h(x) \mod f(x))$
$\mathbb{Z}_m$ is a ring	?
$\mathbb{Z}_m$ is a field iff m is prime	?

Theorem 3.1

The set $F[x]/(f(x))$ together with the addition $+$ and multiplication $\cdot$ defined above forms a ring. $F[x]/(f(x))$ is a field iff $f(x)$ is irreducible.

Size of Field

If $F = \mathbb{Z}_p$, p is prime (this guarantees that F is a field), and f is irreducible over $\mathbb{Z}_p$ (this guarantees that $\mathbb{F}[x]/(f(x))$ is a field) with $\deg(f) = n \geq 1$, then there are p^n elements in the field $\mathbb{F}[x]/(f(x))$, since there are n coefficients and p choices for each coefficient. This implies that $\mathrm{char}(\mathbb{F}[x]/(f(x))) = p$. Also, the elements in a field can be viewed as polynomials.

Example

1. Is $\mathbb{Z}_2[x]/(1 + x^2)$ a field? No.

   Need to check whether $1 + x^2$ is irreducible over $\mathbb{Z}_2$. $f(x) = 1 + x^2$. $f(1) = 0$ so 1 is a root of $1 + x^2 : (1 + x) \mid f(x)$. Actually $f(x) = (1 + x)^2 = 1 + 2x + x^2 = 1 + x^2$.

2. What about $\mathbb{Z}_2[x]/(1 + x + x^2)$?

   Let $f(x) = 1 + x + x^2 . f(0) = 1, f(1) = 1$, so $f(x)$ has no linear factors, $f(x)$ is irreducible over $\mathbb{Z}_2$. $\mathbb{Z}_2[x]/(1 + x + x^2) = \{0, 1, x, 1 + x\}$.

   Note: these 2 sets actually contain the same elements.