Polynomials over Fields

Cunsheng Ding

HKUST, Hong Kong

November 18, 2015

Contents

The Objectives of This Lecture

The fields we learnt so far

- The prime fields $(\mathbb{Z}_p, \oplus_p, \otimes_p)$, where p is any prime.
- The field $(\mathbb{Q}, +, \cdot)$ of rational numbers.
- The field $(\mathbb{R}, +, \cdot)$ of real numbers.
- The field $(\mathbb{C}, +, \cdot)$ of complex numbers.

Let $(\mathbb{F}, +, \cdot)$ denote any of the fields above throughout this lecture.

Our objective

The objective of this lecture is to study polynomials over $\mathbb{F}$.

Polynomials over $\mathbb{F}$

Definition 1

A polynomial over $\mathbb{F}$ is an expression of the form

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

where n is a nonnegative integer, the coefficients a_i, $0 \leq i \leq n$, are elements of the field $\mathbb{F}$, and x is a symbol not belonging to $\mathbb{F}$, called an indeterminate over $\mathbb{F}$.

For any positive integer h, the polynomial $f(x)$ above may be given in the equivalent form

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

By convention, we usually do not write terms with 0 coefficients.

Polynomials over $\mathbb{F}$

Definition 2

$\mathbb{F}[x]$ denotes the set of all polynomials in indeterminate x over $\mathbb{F}$.

Let $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{F}[x]$ and $g(x) = \sum_{i=0}^{n} b_i x^i \in \mathbb{F}[x]$.

Definition 3

Two polynomials $f(x)$ and $g(x)$ are considered equal if and only if their coefficients are equal, i.e., $a_i = b_i$ for all $0 \leq i \leq n$.

Polynomials over $\mathbb{F}$

Let $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{F}[x]$ and $g(x) = \sum_{i=0}^{n} b_i x^i \in \mathbb{F}[x]$.

Definition 4

The sum (or addition) of $f(x)$ and $g(x)$ is defined by

$$f(x) + g(x) = \sum_{i=0}^{n} (a_i + b_i) x^i \in \mathbb{F}[x].$$

Proposition 5

$(\mathbb{F}[x], +)$ is an abelian group with identity 0, called the zero polynomial, whose all coefficients are zero.

Proof.

Note that $\mathbb{F}$ is a field. The proof is trivial and left as an exercise. $\square$

Polynomials over $\mathbb{F}$

Let $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{F}[x]$ and $g(x) = \sum_{i=0}^{m} b_i x^i \in \mathbb{F}[x]$.

Definition 6

The product (or multiplication) of $f(x)$ and $g(x)$ is defined by

$$f(x) \cdot g(x) = \sum_{i=0}^{n+m} c_k x^k \in \mathbb{F}[x],$$

where

$$c_k = \sum_{\substack{i+j=k \\ 0 \le i \le n,\, 0 \le j \le m}} a_i b_j.$$

Remark

This is the polynomial multiplication we learnt in school, except that the computation of each c_k is over $\mathbb{F}$.

Polynomials over $\mathbb{F}$

Proposition 7

$(\mathbb{F}[x], +, \cdot)$ *is a commutative ring with identity* 1.

Proof.

- The binary operation $\cdot$ is associative, as the multiplication $\cdot$ in $\mathbb{F}$ is so.
- The distribution laws hold as $\mathbb{F}$ is a field.
- The binary operation $\cdot$ for polynomials is commutative, as $\mathbb{F}$ is commutative.
- $1 \cdot f = f \cdot 1 = f$ for all $f \in \mathbb{F}[x]$. Hence, 1 is the identity.

The desired conclusion then follows from Proposition 5. □

Polynomials over $\mathbb{F}$

Definition 8

Let $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{F}[x]$ and $f \neq 0$. Suppose that $a_n \neq 0$. Then a_n is called the leading coefficient of $f(x)$ and a_0 the constant term, while n is called the degree of $f(x)$, and denoted by $\deg(f)$.

We define $\deg(0) = -\infty$.

Polynomials of degree ≤ 0 are called constant polynomials.

A polynomial over $\mathbb{F}$ is called monic if its leading coefficient is 1.

Polynomials over $\mathbb{F}$

Proposition 9

Let $f, g \in \mathbb{F}[x]$. *Then*

$$\begin{aligned} \deg(f+g) &\le \max(\deg(f), \deg(g)), \\ \deg(fg) &= \deg(f) + \deg(g). \end{aligned}$$

Proof.

The proof is trivial and omitted. $\square$

Polynomial Ring $\mathbb{F}[x]$ over $\mathbb{F}$

Proposition 10

$(\mathbb{F}[x], +, \cdot)$ *is an integral domain.*

Proof.

Let $f \in \mathbb{F}[x]$ and $g \in \mathbb{F}[x]$ be any two nonzero polynomials. Then

$$f(x) = \sum_{i=0}^{m} a_i x^i \text{ and } g(x) = \sum_{j=0}^{n} b_j x^j$$

where m and n are nonnegative integers such that $a_m \neq 0$ and $b_n \neq 0$. Then

$$f(x) \cdot g(x) \neq 0$$

as the leading coefficient of $f(x) \cdot g(x)$ is equal to $a_m b_n \neq 0$. The desired conclusion then follows from Proposition 7. □

Division Algorithm in $\mathbb{F}[x]$

Proposition 11

Let $g \neq 0$ be a polynomial in $\mathbb{F}[x]$. Then for any $f \in \mathbb{F}[x]$ there exist unique polynomials $q, r \in \mathbb{F}[x]$ such that

$$f = qg + r,$$

where either $r = 0$ or $\deg(r) < \deg(g)$.

Proof.

One can give a proof by induction. This is left as an assignment problem. $\square$

Definition 12

In the Division Algorithm, the polynomial q is called the quotient and r the remainder, in symbol we write $r = f \bmod g$.

Example for the Division Algorithm

Example 13

Let $f = x^3 + x^2 - 1 \in \mathbb{R}[x]$ and $g(x) = x - 1 \in \mathbb{R}[x]$. Find the quotient $q(x)$ and remainder $r(x)$ such that

$$f = qg + r,$$

where either $r = 0$ or $\deg(r) < \deg(g)$.

$$\begin{array}{rrrrr}
 & & x^2 & +2x & +2 \\
\cline{2-5}
x-1 \big) & x^3 & +x^2 & & -1 \\
 & -x^3 & +x^2 & & \\
\cline{2-3}
 & & 2x^2 & & \\
 & & -2x^2 & +2x & \\
\cline{3-4}
 & & & 2x & -1 \\
 & & & -2x & +2 \\
\cline{4-5}
 & & & & 1
\end{array}$$

Hence, $q(x) = x^2 + 2x + 2$ and $r(x) = 1$.

Euclidean Domain $(\mathbb{F}[x], +, \cdot, \deg)$

Theorem 14

$(\mathbb{F}[x], +, \cdot, \deg)$ *is a Euclidean domain.*

Proof.

It follows from Propositions 10 and 11. $\square$

Divisors and Divisibility in $\mathbb{F}[x]$

Definition 15

Let $f, g \neq 0$ be two polynomials in $\mathbb{F}[x]$. In the Division Algorithm, if the remainder $r = 0$, then g is called a divisor or factor of f. In this case, we say that g divides f and f is divisible by g.

Example 16

$x + 2 \in \mathrm{GF}(3)[x]$ is a divisor of $x^2 - 1 \in \mathrm{GF}(3)[x]$.

Common Divisors in $\mathbb{F}[x]$

Definition 17

A common divisor $h(x) \in \mathbb{F}[x]$ of $f \in \mathbb{F}[x]$ and $g \in \mathbb{F}[x]$ is a divisor of both f and g.

The greatest common divisor, denoted by $\gcd(f, g)$, of $f \in \mathbb{F}[x]$ and $g \in \mathbb{F}[x]$ is the common divisor of f and g with leading coefficient 1 and the largest degree.

The least common multiple, denoted by $\mathrm{lcm}(f, g)$, of f and g is the monic polynomial with the least degree that is a multiple of both f and g.

Greatest Common Divisor $\gcd(f, g)$

Remarks

- By definition, $\gcd(f, g)$ is unique.
- It can be computed with the Euclidean Algorithm for polynomials, which is similar to that for integers.

Problem 18

Let $f(x) = 2x^6 + x^3 + x^2 + 2 \in \mathrm{GF}(3)[x]$ *and* $g(x) = x^4 + x^2 + 2x \in \mathrm{GF}(3)[x]$*. Use the Euclidean algorithm to prove that* $\gcd(f, g) = 1$*.*

Greatest Common Divisor $\gcd(f, g)$

Definition 19

Two polynomials $f, g \in \mathbb{F}[x]$ are said to be coprime or relatively prime, if $\gcd(f, g) = 1$.

Example 20

Let $f(x) = x^2 + 1 \in \mathrm{GF}(2)[2]$ and $g(x) = x^2 + x + 1 \in \mathrm{GF}(2)[x]$. Then $\gcd(x^2 + 1, x^2 + x + 1) = 1$. Hence, they are coprime.

Greatest Common Divisor $\gcd(f, g)$

Theorem 21

Let $f \in \mathbb{F}[x]$ and $g \in \mathbb{F}[x]$, which are not zero at the same time. Then there exist two polynomials $u \in \mathbb{F}[x]$ and $v \in \mathbb{F}[x]$ such that

$$\gcd(f, g) = uf + vg.$$

Proof.

The Extended Euclidean Algorithm for polynomials, which is similar to that for integers, gives a constructive proof of this conclusion. $\square$

Problem 22

Let $f(x) = 2x^6 + x^3 + x^2 + 2 \in \mathrm{GF}(3)[x]$ and $g(x) = x^4 + x^2 + 2x \in \mathrm{GF}(3)[x]$. Use the Extended Euclidean Algorithm to find two polynomials u and v such that $\gcd(f, g) = uf + vg$.

Zeros of Polynomials in $\mathbb{F}$

Definition 23

Let $f \in \mathbb{F}[x]$. An element $a \in \mathbb{F}$ is called a zero or root of f if $f(a) = 0$.

Example 24

The polynomial $f(x) = x^2 + x + 2 \in \mathrm{GF}(3)[x]$ has no zero in $\mathrm{GF}(3)$, while $g = x^2 + x + 1$ has the zero 1.

Zeros of Polynomials in $\mathbb{F}$

An important connection between roots and divisibility is given by the following theorem.

Theorem 25

An element $b \in \mathbb{F}$ is a root of $f \in \mathbb{F}[x]$ if and only if $x - b$ divides $f(x)$, i.e., $x - b$ is a divisor of $f(x)$.

Proof.

By the Division Alroithm, we find $q \in \mathbb{F}[x]$ and $c \in \mathbb{F}$ such that $f(x) = q(x)(x-b) + c$. Substituting b for x, we obtain that $c = f(b)$. Hence, $f(x) = q(x)(x-b) + f(b)$. The desired conclusion then follows. $\square$

Irreducible Polynomials in $\mathbb{F}[x]$

Definition 26

A polynomial $f \in \mathbb{F}[x]$ is called irreducible over $\mathbb{F}$ (or in $\mathbb{F}[x]$) if f has positive degree and only nonzero constant divisors $a \in \mathbb{F}$ and af, where a is a nonzero element of $\mathbb{F}$.

Example 27

$f(x) = x^2 + x + 2 \in \mathrm{GF}(3)[x]$ is irreducible over $\mathrm{GF}(3)$.

Proof.

Since $f(a) \neq 0$ for all $a \in \mathrm{GF}(3)$, $f(x)$ cannot have a divisor of degree one in $\mathrm{GF}(3)[x]$. □

Remark

Irreducible polynomials In $\mathbb{F}[x]$ are similar as primes in $\mathbb{Z}$.

Unique Factorization in $\mathbb{F}[x]$

Theorem 28 (Canonical factorization)

Any polynomials $f \in \mathbb{F}[x]$ with positive degree can be written in the form

$$f = a p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k},$$

where $a \in \mathbb{F}$, $p_1, p_2, \ldots, p_k$ are distinct monic irreducible polynomials in $\mathbb{F}[x]$, $e_1, e_2, \ldots, e_k$ are positive integers. Moreover, this factorization is unique apart from the order in which the factors occur.

Proof.

An inductive proof on the degree of f is easily worked out and left as an exercise. $\square$

Example of the Canonical Factorization

Example 29

The canonical factorization of
$f(x) = x^9 + x^8 + 2x^7 + x^5 + 2x^4 + x^3 + 2x^2 + x + 1 \in \mathrm{GF}(3)[x]$ is

$$f(x) = (x^2 + x + 2)^3 (x + 2)(x + 1)^2.$$

Factorization of Polynomials in $\mathbb{F}[x]$

By Theorem 28, every polynomial $f \in \mathbb{F}[x]$ has a canonical factorization. However, we have the following question.

Question 1 (Factorization problem)

How do we factorize $f \in \mathbb{F}[x]$ into the canonical form?

There are techniques for solving this problem, which can be found in Chapter 4 of the following book:
R. Lidl and H. Niederreiter, Finite Fields, Cambridge University Press 1997.

Polynomial Congruence mod $m(x)$

Definition 30

Let $f(x), g(x)$, and $m(x)$ be polynomials in $\mathbb{F}[x]$. We say that $f(x)$ is congruent to $g(x)$ modulo $m(x)$, written as $f(x) \equiv g(x) \pmod{m(x)}$, if $f(x) - g(x)$ is divisible by $m(x)$.

Example 31

Let $f(x) = x^4 + x^2 + x \in \mathrm{GF}(2)[x]$, $g(x) = x^2 + x + 1 \in \mathrm{GF}(2)[x]$ and $m(x) = x^2 + 1 \in \mathrm{GF}(2)[x]$. Then $f(x) \equiv g(x) \pmod{m(x)}$.

Remark

Solving polynomial congruence equations is similar to solving integer congruence equations. Some of the assignment questions are of this type.