afcs
ALGEBRAIC FOUNDATIONS
of COMPUTER SCIENCE
lectures by Ferucio Laurentiu Tiplea

Rings and Fields

Part II

Prof.dr. Ferucio Laurențiu Țiplea

Spring 2022

Department of Computer Science
"Alexandru Ioan Cuza" University of Iași
Iași 700506, Romania

e-mail: ferucio.tiplea@uaic.ro

Outline

Prime fields

The additive structure of a finite field

Polynomials

The multiplicative structure of a finite field

Polynomial representation of finite fields

Reading and exercise guide

Prime fields

Prime fields

Definition 1

A prime field is a field that does not possesses proper subfields.

Example 2

$\mathbb{Z}_p$, where p is a prime, is a prime field of characteristic p, while $\mathbb{Q}$ is a prime field of characteristic 0.

Remark 3

Any field R includes a unique prime subfield, namely the intersection of all subfieds. This is usually denoted R_P. Therefore,

$$R_P = \bigcap_{K \leq R} K$$

Characteristic of a ring: basic properties

Theorem 4

Let R be a field.

1. *If R has characteristic a prime p, then $R_P \cong \mathbb{Z}_p$.*
2. *If R has characteristic 0, then $R_P \cong \mathbb{Q}$.*

Proof.

See textbook [1], page 329. □

Summarizing,

- Every field of characteristic a prime p is either a prime field isomorphic to $\mathbb{Z}_p$ or includes a prime subfield isomorphic to $\mathbb{Z}_p$;
- Every field of characteristic 0 is either a prime field isomorphic to $\mathbb{Q}$ or includes a prime subfield isomorphic to $\mathbb{Q}$.

The additive structure of a finite field

Linear combinations over a subfield

Let K and R be fields such that $K \leq R$.

1. If $a \in R$ can be written as $a = k_1 a_1 + \cdots + k_n a_n$, where $a_1, \ldots, a_n \in R$ and $k_1, \ldots, k_n \in K$, then we say that a is a linear combination of $a_1, \ldots, a_n \in R$ with coefficients in K;
2. $a_1, \ldots, a_n \in R$ are called linearly independent over K if, for any $k_1, \ldots, k_n \in K$,

$$k_1 a_1 + \cdots + k_n a_n \quad \Rightarrow \quad k_1 = \cdots = k_n = 0$$

3. $a_1, \ldots, a_n \in R$ are called linearly dependent over K if they are not linearly independent over K.

Prove that no element in R can have distinct representations as linear combinations of the same linearly independent elements $a_1, \ldots, a_n \in R$ over K!

Basis over a subfield

Let K and R be fields such that $K \leq R$. A subset $B = \{a_1, \ldots, a_n\} \subseteq R$ is a basis of R over K if:

1. $a_1, \ldots, a_n \in R$ are linearly independent over K;
2. Each element $a \in R$ is a linear combination of $a_1, \ldots, a_n$ with coefficients in K.

We consider here only finite basis!

Proposition 5

If K and R be fields such that $K \leq R$ and B_1 and B_2 are basis of R over K, then $|B_1| = |B_2|$.

Proof.

This result will be proven later in a more general framework. □

Basis over a subfield

Definition 6

Let K and R be fields such that $K \leq R$. If $B = \{a_1, \ldots, a_n\} \subseteq R$ is a basis of R over K, then n is called the dimension of R over K.

The dimension of R over K is usually denoted by $[R : K]$.

A basis of R over K ensures that any element in R is written uniquely as a linear combination of the basis' elements with coefficients in K. As any linear combination of basis' elements with coefficients in K is in R, we obtain the following significant result.

Theorem 7

Let K and R be fields such that $K \leq R$. If there exists a basis B of R over K, then $|R| = |K|^n$, where $n = |B| = [R : K]$.

Prove that if $K \leq L \leq R$, $[R : L] = n$, and $[L : K] = m$, then $[R : K] = mn$.

Existence of bases for finite fields and consequences

Theorem 8

Let K and R be fields such that $K \leq R$. If R is finite then there exists a basis of R over K.

Proof.

In class. □

Prove the following two important corollaries!

Corollary 9

If R is a finite field of characteristic p, then $|R| = p^n$, where $n = [R : R_P]$.

Corollary 10

If R is a finite field of characteristic p, $|R| = p^n$, and $K \leq R$, then there exists m such that $|K| = p^m$ and $m|n$.

Computations in the additive representation

Assume R is a finite field of characteristic p, $n = [R : R_P]$, and $B = \{b_1, \ldots, b_n\}$ is a basis of R over R_P.

1. It is very easy to add two elements $a = \sum_{i=1}^{n} \alpha_i b_i$ and $b = \sum_{i=1}^{n} \beta_i b_i$ in R:

$$a + b = \sum_{i=1}^{n} (\alpha_i + \beta_i) b_i$$

2. It is not that easy to multiply a and b in this representation unless we know the value of $b_i \cdot b_j$, for all $1 \leq i \leq j \leq n$!
   One may try to compute all the $n(n+1)/2$ values and perform multiplication with table lookups, but that seems rather tedious.

The additive group of a finite field

Assume R is a finite field of characteristic p, $n = [R : R_P]$, and $B = \{b_1, \ldots, b_n\}$ is a basis of R over R_P.

1. If $n = 1$, then the additive commutative group $R^+ = (R, +, -, 0)$ of R is cyclic generated by e. Clearly, it is isomorphic to the group $\mathbb{Z}_p^+ = (\mathbb{Z}_p, +, -, 0)$ (prove it!);
2. If $n > 1$, the additive commutative group $R^+ = (R, +, -, 0)$ of R is isomorphic to the direct product of the group $\mathbb{Z}_p^+$ with itself n times, $\mathbb{Z}_p^+ \times \cdots \times \mathbb{Z}_p^+$. The binary operation in this group is the component-wise addition.

   Prove that $\mathbb{Z}_p^+ \times \cdots \times \mathbb{Z}_p^+$ is a commutative group and prove also the isomorphism!

Polynomials

Polynomials

This is an individual study section. You should recall some basic concepts about polynomials you already studied in high school, such as operations with polynomials, divisibility, irreducible polynomial, and polynomial roots. The textbook covers this topic from pages 331 to 336.

The multiplicative structure of a finite field

The multiplicative group of a finite field

Assume R is a finite field of characteristic p, and $n = [R : R_P]$. Therefore, $|R| = p^n$.

The multiplicative group of R, usually denoted $R^\times$ or R^*, has order $p^n - 1$. It also has a special structure.

Theorem 11

The multiplicative group of a finite field R is cyclic of order $|R| - 1$.

Proof.

In class. □

A generator of R^* is called a primitive element of the field R. Clearly, there are $\phi(|R| - 1)$ primitive elements.

Prove that there are elements of order $k \geq 1$ in R if and only if $k||R| - 1$!

Computations in the multiplicative representation

Assume R is a finite field of characteristic p, and $n = [R : R_P]$. Therefore, $|R| = p^n$.

Given a primitive element g of R, we may write

$$R = \{0, e = g^0, g = g^1, g^2, \ldots, g^{p^n-2}\} = \{0\} \cup \langle g \rangle$$

Given two elements $a = g^i$ and $b = g^j$:

1. It is easy to multiply them, $a \cdot b = g^{i+j}$;
2. It is not that easy to add them unless we pre-compute all values $g^k + 1$ as powers of g. This is because $a + b = g^j(g^{i-j} + 1)$, assuming $j \leq i$.

Polynomial representation of finite fields

The multiplicative group and polynomial roots

Assume R is a finite field of order $q = p^n$, where p is a prime and $n \geq 1$. As the order of any $a \in R^*$ divides the group order, we have $a^{q-1} = 1$. That is, a is a root of the polynomial $f(x) = x^{q-1} - 1$. More generally:

Proposition 12

Let R is a finite field of order $q = p^n$, where p is a prime and $n \geq 1$. Then, the following properties hold:

1. $\prod_{a \in R^*}(x - a) = x^{q-1} - 1$;
2. $\prod_{i=0}^{q-2}(x - g^i) = x^{q-1} - 1$, *for any primitive element $g \in R^*$.*

Complete the proof of the proposition above!

Remark that the element 0 of the field R in the proposition above is avoided. It can be included if we consider the polynomial $x^q - x$.

Splitting field

Definition 13

Let K be a field and $f(x) \in K[x]$. The splitting field of $f(x)$ is the smallest field extension R of K (that is, $K \leq R$) such that $f(x)$ splits over R into linear factors.

Theorem 14

Let K be a field and $f(x) \in K[x]$. The splitting field of $f(x)$ exists and it is unique up to an isomorphism.

Proof.

See the textbook [1], pages 336-343. □

Example 15

The splitting field of $f(x) = x^{p^n} - x \in \mathbb{Z}_p[x]$ is a field R with p^n elements (the roots of $f(x)$) and

$$f(x) = x^{p^n} - x \in \mathbb{Z}_p[x] = \prod_{a \in R}(x - a)$$

Existence of finite fields

Theorem 16

For any prime p and $n \geq 1$, there exists a field with p^n elements. Moreover, any such field is isomorphic to the splitting field of $x^{p^n} - x \in \mathbb{Z}_p[x]$.

Corollary 17

Any two finite fields with the same number of elements are isomorphic.

The finite field with p^n elements, which is unique up to isomorphism, is denoted by $GF(p^n)$ or F_{p^n} and it is called the Galois field with p^n elements.

Construction of finite fields

Steps for constructing $GF(p^n)$ (p prime and $n \geq 1$):

- The set of all polynomials over $\mathbb{Z}_p$ of degree at most $n-1$ has exactly p^n elements. $GF(p^n)$ consists of all these polynomials;
- Let $f \in \mathbb{Z}_p[x]$ of degree n and irreducible. Define the following operations on $GF(p^n)$:
  - the addition of two polynomials in $GF(p^n)$ is the component-wise addition modulo p;
  - the multiplication of two polynomials in $GF(p^n)$ is performed modulo p for coefficients and modulo f for the entire result;
  - the zero element is the zero polynomial, and the unity of $GF(p^n)$ is the constant polynomial 1;
  - the additive (multiplicative) inverse exists for any polynomial (non-zero polynomial) in $GF(p^n)$.

Construction of finite fields

Constructing $GF(p^n)$ – Example

- $GF(2^8)$ consists of all polynomial of degree at most 7 with coefficients in $\mathbb{Z}_2 = \{0, 1\}$;
- Let $f(x) = x^8 + x^4 + x^3 + x + 1 \in \mathbb{Z}_2[x]$ be an irreducible polynomial of degree 8 over $\mathbb{Z}_2[x]$;
- Example of addition in $GF(2^8)$:

$$(x^6 + x^4 + x^2 + x + 1) + (x^7 + x + 1) = x^7 + x^6 + x^4 + x^2$$

- Example of multiplication in $GF(2^8)$:

$$(x^6 + x^4 + x^2 + x + 1)(x^7 + x + 1) = x^7 + x^6 + 1$$

Examples of irreducible polynomials

Example 18

- $f(x) = x^2 + x + 1$ is irreducible over $\mathbb{Z}_2[x]$. This polynomial can be used to define $GF(2^2)$;
- $f(x) = x^3 + x^2 + x + 2$ is irreducible over $\mathbb{Z}_3[x]$. This polynomial can be used to define $GF(3^3)$;
- $f(x) = x^8 + x^4 + x^3 + x + 1 \in \mathbb{Z}_2[x]$ is irreducible over $\mathbb{Z}_2[x]$. This polynomial is used by the cryptosystem Rijndael (AES) to define $GF(2^8)$.

Reading and exercise guide

Reading and exercise guide

It is highly recommended that you do all the exercises marked in red from the slides.

Course readings:

1. Pages 315-349 from textbook [1].

References

[1] Ferucio Laurențiu Țiplea. *Algebraic Foundations of Computer Science*. "Alexandru Ioan Cuza" University Publishing House, Iași, Romania, second edition, 2021.