Finite Fields

https://iuk.one/1033-1010

Clemens H. **Cap**
ORCID: 0000-0003-3958-6136

Department of Computer Science
University of **Rostock**
Rostock, Germany
clemens.cap@uni-rostock.de

Version 4

Overview

1. Some Algebra Basics
2. Polynomials
3. Galois Fields
4. Lagrange Interpolation

1. Some Algebra Basics

Let us review some algebra.

Group

A **group** is a pair $(\mathbb{G}, \star)$ consisting of

1. a non-empty **set** $\mathbb{G}$ and
2. a **binary operation** $\star\colon \mathbb{G} \times \mathbb{G} \to \mathbb{G}$

such that the following **axioms** are fulfilled:

1. $\star$ is **associative**: $\forall a, b, c \in \mathbb{G} : a \star (b \star c) = (a \star b) \star c$
2. $\star$ has a **neutral element**: $\exists n_\star \in \mathbb{G} : \forall a \in \mathbb{G} : a \star n_\star = n_\star \star a = a$
3. $\star$ has **inverse elements**: $\forall a \in \mathbb{G} : \exists b \in \mathbb{G} : a \star b = b \star a = n_\star$

A group is called **commutative** or **Abelian**, iff $\forall a, b \in \mathbb{G} : a \star b = b \star a$.

Examples: $(\mathbb{R}, +)$, $(\mathbb{R} \setminus \{0\}, \cdot)$

Field

A **field** is a triple $(\mathbb{F}, +, \cdot)$ consisting of

1. a **set** $\mathbb{F}$ consisting of at least two elements
2. a binary operation $+ \colon \mathbb{F} \times \mathbb{F} \to \mathbb{F}$, which is called **addition**, and
3. a binary operation $\cdot \colon \mathbb{F} \times \mathbb{F} \to \mathbb{F}$, which is called **multiplication**

such that the following **axioms** are fulfilled:

1. $(\mathbb{F}, +)$ is an **Abelian group**.
2. $(\mathbb{F} \setminus \{n_+\}, \cdot)$ is an **Abelian group**.
3. **Multiplication distributes** over addition: $\forall a, b, c \in \mathbb{F} : a \cdot (b + c) = (a \cdot b) + (a \cdot c)$

Common notation: $0 = n_+$ and $1 = n.$ and $\mathbb{F}^* = \mathbb{F} \setminus \{n_+\}$

Examples: $(\mathbb{R}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$

Ring

A **(commutative, unitary) ring** is *nearly* a field $(\mathbb{E}, +, \cdot)$. The *only* thing which is missing is that we do *not* require the multiplicative structure to have inverse elements.

More formally, a **commutative, unitary ring** requires a structure $(\mathbb{E}, +, \cdot)$ to fulfill the following **axioms**:

1. $(\mathbb{E}, +)$ is an **Abelian group**.
2. $(\mathbb{E}, \cdot)$ is a **commutative monoid** (**Associative** and having a **neutral element**).
3. **Multiplication distributes** over addition: $\forall a, b, c \in \mathbb{E} : a \cdot (b + c) = (a \cdot b) + (a \cdot c)$

Commutative indicates that the multiplication is commutative.
This is not always guaranteed: Matrices are the prominent counterexample.

Unitary indicates that the multiplication has a neutral element.

Modulo Operations as Example for Rings and Fields

Let $n \in \mathbb{Z}^+$ be a positive integer, a, b range over $\mathbb{Z}$.
Denote by $\sim_n$ the **equivalence relation** modulo n: $a \sim_n b$ iff $\exists k \in \mathbb{Z} : (a - b) = k \cdot n$
Denote by $\mathbb{Z}_n$ the set of all **equivalence classes** $[x]_n$ modulo n.

For example for $n = 3$ we get:
$$[0]_3 = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$$
$$[1]_3 = \{\ldots, -5, -2, 1, 4, 7, \ldots\}$$
$$[2]_3 = \{\ldots, -4, -1, 2, 5, 8 \ldots\}$$

Define on $\mathbb{Z}_n$ **operations** $[a]_n +_n [b]_n := [a + b]_n$ and $[a]_n \cdot_n [b_n] := [a \cdot b]_n$.
For example $[3]_7 +_7 [2]_7 = [5]_7$ and $[4]_7 +_7 [5]_7 = [9]_7 = [2]_7$.

$\mathbb{Z}_n$ with the operations $+_n$ and $\cdot_n$ is a **ring**.

If n is a prime number, it even is a **field**.

Bezout Identity

Bezout Identity

The **greatest common divisor** $g = \mathbf{gcd}(a, b)$ of two integers a, b can be written **as integer linear combination** $g = \alpha \cdot a + \beta \cdot b$ of these two numbers.

Algorithm:

1. **Input:** a and b in $\mathbb{Z}^+$.
2. Use the **Euclidean algorithm** for calculating the **gcd**.
3. Run the algorithm **backwards** from the result.
4. **Output:** α and β in $\mathbb{Z}$ such that $\mathbf{gcd}(a, b) = \alpha \cdot a + \beta \cdot b$

Example: Bezout Identity

Calculate the Bezout Identity for **gcd** (228 , 174). We use the Euclidean algorithm:

$$228 = 1 \cdot 174 + 54 \quad (1)$$

$$174 = 3 \cdot 54 + 12 \quad (2)$$

$$54 = 4 \cdot 12 + 6 \quad (3)$$

$$12 = 2 \cdot 6 + 0 \quad \text{the gcd is } 6 \quad (4)$$

$6 = 1 \cdot 54 - 4 \cdot \underline{12}$ from (3) we get from (2) $12 = 1 \cdot 174 - 3 \cdot 54$

$6 = -4 \cdot 174 + 13 \cdot \underline{54}$ we get from (1) $54 = 1 \cdot 228 - 1 \cdot 174$

$6 = 13 \cdot 228 - 17 \cdot 174$ Done!

Done: We obtained the **gcd** 6 as linear combination of 228 and 174 :

$$6 = 13 \cdot 228 - 17 \cdot 174$$

Modulo-Division

Proposition: Modulo-Division

Let the non-zero integers x and n be relatively prime. Then there exists an integer y such that $x \cdot y \equiv 1 \mod n$. The integer y is called the **inverse** to x **modulo** n.

Note: $a \sim_n b$ often also is written $a \equiv b \mod n$

Proof:
Let x and n be relatively prime. Then $\mathbf{gcd}(x, n) = 1$
According to the Bezout Lemma there exist α, β that $1 = \alpha \cdot x + \beta \cdot n$
Looking at this equation modulo n we get $1 \equiv \alpha \cdot x + 0 \mod n \equiv \alpha \cdot x$
Thus: α is the multiplicative inverse of x mod n.

Consequence: We just demonstrated that $(\mathbb{Z}_p, +_p, \cdot_p)$ is a field when p is prime.

Task: Revise Prime Fields

Tasks::

- Calculate the inverse of 5 modulo 9.
- Is there an inverse for 6 modulo 9?
- $(\mathbb{Z}_6, +_6, \cdot_6)$ is not a field. Why? Give a precise counterexample!
- $(\mathbb{Z}_4, +_4, \cdot_4)$ is not a field. Why? Give a precise counterexample!

Show: When there is an inverse to x modulo n, then x and n must be relatively prime.

2. Polynomials

Expressions with variables
...well, in a certain sense.

What is a polynomial?

A polynomial is an "expression of the form" $3X^2 + 2X + 4$ where we "calculate with" the X "as if it were a number".

Evaluation:

- Provides an intuition and motivation.
- As a definition, it is *complete garbage*.

A definition **must** be capable of answering all questions on the defined object via precise, systematic methods.

The above definition does not provide this.

Some mathematical definitions may look a bit awkward, to live up to that expectation.

Polynomials (1)

Let $(\mathbb{F}, +, \cdot)$ be a field. A polynomial of degree d with coefficients in $\mathbb{F}$ is an **expression of the form** $a_d \cdot \mathbb{X}^d + a_{d-1} \cdot \mathbb{X}^{d-1} + \ldots + a_0 \cdot \mathbb{X}^0$ where $d \in \mathbb{N}_0$ $a_0, a_1, \ldots, a_d \in \mathbb{F}$ and $\mathbb{X}$ a symbol.

Definition of a Polynomial

A polynomial over $\mathbb{F}$ is a $d+1$ tuple $(a_d, a_{d-1}, \ldots, a_1, a_0)$ of values in $\mathbb{F}$.

Notation: $a_d \cdot \mathbb{X}^d + a_{d-1} \cdot \mathbb{X}^{d-1} + \ldots + a_1 \cdot \mathbb{X}^1 + a_0 \cdot \mathbb{X}^0$

Denote by $\mathbb{F}[\mathbb{X}]_d$ the set of all polynomials of degree d.

Denote by $\mathbb{F}[\mathbb{X}]$ the set of all polynomials as union $\mathbb{F}[\mathbb{X}] = \bigcup_{d \in \mathbb{N}_0} \mathbb{F}[\mathbb{X}]_d$

We can define operations $+$ and $\cdot$:

$+ \colon \mathbb{F}[\mathbb{X}]_d \times \mathbb{F}[\mathbb{X}]_d \to \mathbb{F}[\mathbb{X}]_d$ and $\cdot \colon \mathbb{F}[\mathbb{X}]_e \times \mathbb{F}[\mathbb{X}]_f \to \mathbb{F}[\mathbb{X}]_{e+f}$

Polynomials (2)

$(a_d, a_{d-1}, \ldots, a_1, a_0) + (b_d, b_{d-1}, \ldots, b_1, b_0) := (a_d + b_d, a_{d-1} + b_{d-1}, \ldots, a_1 + b_1, a_0 + b_0)$

Observe: Polynomials form a vector space!

$(a_e, a_{e-1}, \ldots, a_1, a_0) \cdot (b_f, b_{f-1}, \ldots, b_1, b_0) :=$
$(a_e \cdot b_f, a_{e-1} b_f + a_e b_{f-1}, \ldots, a_1 b_0 + a_0 b_1, a_0 + b_0)$

Note: ... here is particularly imprecise – let us make it more precise:

Number at position k is $\sum_{i,j \in \mathbb{N}_0, i+j=k} a_i b_j$

Now: Understanding the precise definition we fall back to intuitive notations.

$$\left(\sum_{i=0}^{e} a_i \mathbb{X}^i \right) \cdot \left(\sum_{j=0}^{f} b_j \mathbb{X}^j \right) = \sum_{k=0}^{e+f} \sum_{i,j \in \mathbb{N}_0, i+j=k} a_i b_j \mathbb{X}^k$$

Observe: Polynomials form a ring!

Substitution into a Polynomial

Substitution Homomorphism:

- Let R be a commutative, unitary ring.
- Let S be another commutative, unitary ring.
- Let $h\colon R \to S$ be a ring homomorphism, let $s \in S$.

Then there exists a unique ring homomorphism $H\colon R[\mathbb{X}] \to S$ such that $H(\mathbb{X}) = s$ and $\forall r \in R : H(r) = h(r)$.

Special Case: $R = S$ and $h = id$.

Example: Let $R = S = \mathbb{R}$, $s = 3$, $H(\mathbb{X}) = 3$, $\forall y \in \mathbb{R} : H(y) = y$. We get:
$H(\mathbb{X}^2 + 2\mathbb{X} + 4) = H(\mathbb{X}) \cdot H(\mathbb{X}) + H(2) \cdot H(\mathbb{X}) + H(4) = 3 \cdot 3 + 2 \cdot 3 + 4 = 19$

Non-mathematicians say: Substituting 3 for $\mathbb{X}$ in $\mathbb{X}^2 + 2\mathbb{X} + 4$ gives 19.

Ideal

Let $(\mathbb{E}, +, \cdot)$ be a commutative, unitary ring. A subset $I \subseteq \mathbb{E}$ is called an **ideal** iff

1. it is **closed under addition**: $\forall a, b \in I : a + b \in I$
2. it is **closed under multiplication from** $\mathbb{E}$: $\forall a \in \mathbb{E}, x \in I : a \cdot x \in I$

Example 1: Consider the ring $(\mathbb{Z}, +, \cdot)$.
All numbers congruent 0 mod 3 form an ideal:
$I = \{\ldots, -6, -3, 0, 3, 6, \ldots\} = \{\lambda \cdot 3 | \lambda \in \mathbb{Z}\}$
All numbers congruent 2 mod 3 form **no** ideal.
Not closed under multiplication with $0 \in \mathbb{Z}$.

Example 2: Consider the ring $(\mathbb{R}[\mathbb{X}], +, \cdot)$.
All real multiples of a polynomial, eg. $I = \{\lambda(\mathbb{X}^2 + 1) \mid \lambda \in \mathbb{R}\}$ form an ideal.

Quotient Ring

Let $(\mathbb{E}, +, \cdot)$ be a commutative, unitary ring and $I \subseteq \mathbb{E}$ an ideal. Define an equivalence relation $\sim \subseteq \mathbb{E} \times \mathbb{E}$ by $a \sim b \Leftrightarrow a - b \in I$. The **set of equivalence classes** of $\sim$ is written $\mathbb{E}/_I$. It can be given the structure of a ring.

Example 1: $(\mathbb{Z}, +, \cdot)$ is a ring.
$I = \{\ldots, -6, -3, 0, 3, 6, \ldots\} = \{\lambda \cdot 3 \mid \lambda \in \mathbb{Z}\}$ is an ideal.
$a \sim b \Leftrightarrow a - b \in I$ means $a \sim b$, iff $a - b$ is a multiple of 3.
$\mathbb{Z}/_I$ is $\{[0], [1], [2]\}$; of which we know it is a ring.
The construction of the ideal generalizes the modulo construction.

Example 2: $(\mathbb{R}[\mathbb{X}], +, \cdot)$ is a ring.
$I = \{\lambda(\mathbb{X}^2 + 1) \mid \lambda \in \mathbb{R}\}$ is an ideal.
What is $\mathbb{R}[\mathbb{X}]/_I$?
It contains all of $\mathbb{R}$, all of $r \cdot \mathbb{X}$ and all of $r \cdot \mathbb{X} + s$
We get $\mathbb{X} \cdot \mathbb{X} = -1$ since $\mathbb{X}^2 + 1 = 0$
$r \cdot \mathbb{X} + s$ corresponds to $r \cdot i + s$ and we just constructed the complex numbers.

Irreducible Polynomials

A polynomial $P \in \mathbb{F}[X]$ over a field is called **irreducible**, if the only divisors of P are $a \cdot P$ and b with some $a, b \in \mathbb{F}$.

For a field $\mathbb{F}$ and an **irreducible** polynomial P the quotient $\mathbb{F}[X]/I$ with $I = \{\lambda \cdot P \mid \lambda \in \mathbb{F}\}$ is a **field**.

Compare: When p is prime then the ring $\mathbb{Z}_p$ is a field.

3. Galois Fields

Galois fields and polynomials with coefficients in Galois fields play an important role in cryptography and in coding theory.

What are they and how do they work?

Characteristic, Order and Finite Fields

The **characteristic** of a field $(\mathbb{F}, +, \cdot)$ is the smallest number $c \in \mathbb{N}$ such that $\underbrace{n_\cdot + n_\cdot + \ldots + n_\cdot}_{c} = n_+$ which in different notation is $\underbrace{1 + 1 + \ldots + 1}_{c} = 0$.

Remark: The expression describing the characteristic sometimes is given as $c \star 1$ or $c \cdot 1$, without providing further information regarding the notation.

The first notation is bad, since it is not at all clear what $\star$ (or a similar symbol) is.

The second notation is bad, since $\cdot$ is defined $\mathbb{F} \times \mathbb{F} \to \mathbb{F}$ and not $\mathbb{N} \times \mathbb{F} \to \mathbb{Z}$.

Many then pretend they know what is meant.

In reality it is a disaster for those who want to understand what is meant.

If no such number exists, the field is said to have **characteristic 0**.

The **order** of a field $(\mathbb{F}, +, \cdot)$ is the number of elements of the set $\mathbb{F}$.

A field is called **finite** or a **Galois field**, iff it has finite order.

Evariste Galois

Fig. 1: Evariste Galois (1811-1832), to the honor of whom finite fields are called Galois fields, died at the age of 20 years from the wounds of a duel. Despite his early death he is probably the most influential researcher in the field of algebra in his century.

Tasks: Familiarization with Characteristic

Show from the field axioms alone that $\forall a \in \mathbb{F} : n_+ \cdot a = n_+$.
(In more familiar notation this reads: $0 \cdot a = 0$)

Show: $\forall a, b \in \mathbb{F} : a \cdot b = n_+ \Leftrightarrow a = n_+ \vee b = n_+$

Show: If a field has characteristic 0 then it must have infinitely many elements.
Hint: Look at the elements $n.$, $n. + n.$, $n. + n. + n.$, ... Maybe these are the infinitely many elements! And what, if not?

Determine the characteristic of the field $(\mathbb{Z}_5, +, \cdot)$.

Show: If a field $\mathbb{F}$ has characteristic q then q must be a prime.
Hint: Indirect proof. Assume that $q = r \cdot s$. Then look at $\underbrace{n. + \ldots n.}_{r \cdot s}$ and use the distributive law.

Show: If a field $\mathbb{F}$ has characteristic p, then $\forall a, b \in \mathbb{F} : (a + b)^p = a^p + b^p$.
Hint: Use the binomial theorem and use the property that p is a prime.

Theorem of Moore

- **Order:** The **order** of a finite field is a **prime power** p^k
- **Existence:** For every prime power p^k there **exists** a field of order p^k.
- **Uniqueness:** All fields of order p^k are **isomorphic**.
- **Characteristic:** The **characteristic** of the finite field of order p^k is p.

Core Consequence and Notation of $GF(p^k)$

The **Galois Field** of order p^k is uniquely defined by the value of p^k.
It is written as $GF(p^k)$ and given by the set of $\{0, 1, \mathbb{X}^2, \mathbb{X}^3, \ldots, \mathbb{X}^{p^k-1}\}$ in $GF(p)[\mathbb{X}]/P$ where P is an arbitrary irreducible polynomial in $GF(p)[\mathbb{X}]$.

Proof: Requires the theory of finite dimensional vector spaces over a field.

Galois Field GF(2)

The **Galois Field** $GF(2)$ is given by the operations:

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

Observations:

- It is identical with the **prime field** $(\mathbb{Z}_2, +_2, \cdot_2)$.
- We know that $(\mathbb{Z}_2, +_2, \cdot_2)$ is a field.
- We know that finite fields are unique (Moore theorem).
- It is identical with the Boolean structure $(\{0,1\}, \oplus, \wedge)$ where $\oplus$ denotes **exclusive or**.

Galois Field GF(3)

The **Galois Field** $GF(3)$ is given by the operations:

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Observations:

- It is identical with the **prime field** $(\mathbb{Z}_3, +_3, \cdot_3)$.
- We know that $(\mathbb{Z}_3, +_3, \cdot_3)$ is a field.
- We know that finite fields are unique (Moore theorem).

Galois Field GF(4) Construction (1)

Watch out:

- $GF(4)$ is **not** identical to $(\mathbb{Z}_4, +_4, \cdot_4)$
- $(\mathbb{Z}_4, +_4, \cdot_4)$ is **not** a field!

Thus: Let's not write the elements as $\{0, 1, 2, 3\}$, this is confusing, but as $\{0, 1, a, b\}$.

From the laws of neutrality and from $0 \cdot x = 0$ we get:

$+$	0	1	a	b
0	0	1	a	b
1	1			
a	a			
b	b			

$\cdot$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a		
b	0	b		

The rest must follow in a unique way (by the **Theorem of Moore**).
More precisely: Unique up to **isomorphism** (i.e. renaming).

Galois Field GF(4) Construction (2)

Since $+$ is invertible, in every row and column we must find every value.

For $1+1$ we must chose 0 (we have characteristic 2).

Then $a+a = a\cdot(1+1) = a\cdot 0 = 0$ and $b+b=0$.

$+$	0	1	a	b
0	0	1	a	b
1	1	0		
a	a		0	
b	b			0

$+$	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

$a+1=a$ is false (would imply $1=0$) and $a+1=1$ is false (would imply $a=0$).

$a+1=0$ is false since $0=1+1$ due to the characteristic and then $a+1=0=1+1$ would imply $a=1$.

Leaves us with $a+1=b$ and thus also $1+a=b$.

We fill in remaining values to use every value in every column and row.

Galois Field GF(4) Construction (3)

Now let's do the multiplication table! what about $a \cdot a$?

$a \cdot a$ cannot be 0 since then $a = 0$.

$a \cdot a$ cannot be a since then $a = 1$

Leaves us with possibilities $a \cdot a = 1$ or $a \cdot a = b$.

Now we know $a + 1 = b$.

This means $(a + 1) \cdot (a + 1) = b \cdot b$.

But $(a + 1) \cdot (a + 1) = a \cdot a + a + a + 1 = a \cdot a + 1$.

If we assume $a \cdot a = 1$ we then get by above result $b \cdot b = 1 + 1 = 0$ and so $b = 0$, so this can be excluded. Leaves us with $a \cdot a = b$.

From $b = a + 1$ we get $b \cdot b = (a + 1) \cdot (a + 1)$ and this is $a \cdot a + 1$. With $a \cdot a = b$ we get $b \cdot b = a$.

Galois Field GF(4) Construction (4)

Filling these results in and again completing rows and columns by a similar argument as before, we get:

$\cdot$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

So: What have we learned thus far?

Galois Field GF(4)

$+$	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

$\cdot$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

We can write this with different symbols, which looks brain-damaged. Only 0 and 1 keep their meaning as neutral elements, the meaning of the others can be kept (partially) for addition but not for multiplication.

$+$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

Task: Division and Subtraction Tables

Task: Produce the tables for the division and the subtraction operations for $GF(2)$, $GF(3)$ and $GF(4)$.

Construction of General Galois Fields

Observations:

- $GF(p)$ is well understood as field $\mathbb{Z}_p$ for prime p
- $GF(4)$ could be constructed in a unique way.
- Other Galois Fields allow a variability in their construction.
- Thus, we first get several different $GF(p^k)$.
- Further analysis then shows that they are isomorphic.
- Isomorphic means: They are identical as structure after renaming.

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

iso to

$+$	a	x
a	a	x
x	x	a

$\cdot$	a	x
a	a	a
x	a	x

iso to

$+$	x	a
x	x	a
a	a	x

$\cdot$	x	a
x	x	x
a	x	a

Two fields $(\mathbb{F}_1, +_1, \cdot_1)$ and $(\mathbb{F}_2, +_2, \cdot_2)$ are called **isomorphic**, iff there exists a bijective function $f : \mathbb{F}_1 \to \mathbb{F}_2$ such that $f(x +_1 y) = f(x) +_2 f(y) \qquad f(x \cdot_1 y) = f(x) \cdot_2 f(y)$

General Construction Method

$GF(p^k)$

- Find an irreducible polynomial P of degree k.
- $GF(p^k)$ is the quotient $GF(p)[\mathbb{X}]/P$
- Find the set by looking at the 2^k elements $0, 1, \mathbb{X}^1, \mathbb{X}^2, \ldots, \mathbb{X}^{2^k-2}$
- Find the calculation rules by working with these representations and reducing modulo P where appropriate.

Good news: Since the coefficients are chosen from a finite set, irreducibility is decidable in finitely many steps.

Bad news: Doing so for humans might be a bit involved for the general case.

Good news: A bit of algebra often can help us speed this up.

Example: Let's do this for $GF(8)$.

Finding Irreducible Polynomials (1)

There are $8 = 2^3$ polynomials of degree 3. Find the irreducible ones!

First discard those, where we see a factoring.

$\mathbb{X}^3$	$\mathbb{X}^2 \cdot \mathbb{X}$	not irreducible due to factoring
$\mathbb{X}^3 + 1$		candidate – I see no factoring
$\mathbb{X}^3 + \mathbb{X}$	$\mathbb{X} \cdot (\mathbb{X}^2 + 1)$	not irreducible due to factoring
$\mathbb{X}^3 + \mathbb{X} + 1$		candidate – I see no factoring
$\mathbb{X}^3 + \mathbb{X}^2$	$\mathbb{X}^2 \cdot (\mathbb{X} + 1)$	not irreducible due to factoring
$\mathbb{X}^3 + \mathbb{X}^2 + 1$		candidate – I see no factoring
$\mathbb{X}^3 + \mathbb{X}^2 + \mathbb{X}$	$\mathbb{X} \cdot (\mathbb{X}^2 + \mathbb{X} + 1)$	not irreducible due to factoring
$\mathbb{X}^3 + \mathbb{X}^2 + \mathbb{X} + 1$		candidate – I see no factoring

Even when we do not see a factoring, still a factoring might exist!

Finding Irreducible Polynomials (2)

Factoring theorem

A polynomial $P \in \mathbb{F}[\mathbb{X}]$ over a field $\mathbb{F}$ **has a zero** at $a \in \mathbb{F}$ (this means $P(a) = 0$) if and only if $\mathbb{X} - a$ **is a factor** of P (this means there exists a $Q \in \mathbb{F}[\mathbb{X}]$ that P can be written as $P = (\mathbb{X} - a) \cdot Q$.

Example: $\mathbb{X}^3 + 1$ has a zero at $\mathbb{X} = 1$ since $1 + 1 = 0$ in $GF(2)$.
Polynomial division produces a factoring: $\mathbb{X}^3 + 1 = (\mathbb{X}^2 + \mathbb{X} + 1) \cdot (\mathbb{X} - 1)$.

Note: $\mathbb{X} - 1 = \mathbb{X} + 1$ since we are in $GF(2)$.

Task: Reducible and Irreducible Polynomials

Task 1: Show that $\mathbb{X}^3 + \mathbb{X}^2 + \mathbb{X} + 1$ is reducible.

- Even if you see a factoring with your "naked eye", use the factoring theorem!

Task 2: Show that $\mathbb{X}^3 + \mathbb{X} + 1$ and $\mathbb{X}^3 + \mathbb{X}^2 + 1$ are irreducible.

- Hint: Use factoring theorem and look at the degree of the polynomial.
- Why would we need to have a look at the degree?

Constructing GF(8)

$GF(2^3) \sim \{0, \mathbb{X}^0, \mathbb{X}^1, \mathbb{X}^2, \mathbb{X}^3, \mathbb{X}^4, \mathbb{X}^5, \mathbb{X}^6\}/P$

For doing calculations we need to fix an irreducible polynomial P in $GF(2)[\mathbb{X}]$.

We can take $\mathbb{X}^3 + \mathbb{X} + 1$ or $\mathbb{X}^3 + \mathbb{X}^2 + 1$.

We decide for $\mathbb{X}^3 + \mathbb{X} + 1$.

Question: What is $\mathbb{X}^7$?

- Want to know why this does not continue beyond $\mathbb{X}^6$?
- Want to know what $\mathbb{X}^3 \cdot \mathbb{X}^4$ is (or $\mathbb{X}^2 \cdot \mathbb{X}^5$).

Answer: For $\mathbb{X}^7$ we get: $\mathbb{X}^7 = 1 = \mathbb{X}^0$.

Constructing GF(8)

$$\mathbb{X}^7 \sim \mathbb{X}^7 - \mathbb{X}^4 \cdot (\mathbb{X}^3 + \mathbb{X} + 1) \quad \text{may subtract multiple of ideal generating polynomial}$$
$$= \mathbb{X}^7 - \mathbb{X}^7 - \mathbb{X}^5 - \mathbb{X}^4 = \mathbb{X}^5 + \mathbb{X}^4 \quad \text{algebra and specifics of GF(2)}$$
$$\sim \mathbb{X}^5 + \mathbb{X}^4 - \mathbb{X}^2 \cdot (\mathbb{X}^3 + \mathbb{X} + 1) \quad \text{may subtract multiple of ideal generating polynomial}$$
$$= \mathbb{X}^5 + \mathbb{X}^4 - \mathbb{X}^5 - \mathbb{X}^3 - \mathbb{X}^2 = \mathbb{X}^4 + \mathbb{X}^3 + \mathbb{X}^2 \quad \text{algebra and specifics of GF(2)}$$
$$\sim \mathbb{X}^4 + \mathbb{X}^3 + \mathbb{X}^2 - \mathbb{X} \cdot (\mathbb{X}^3 + \mathbb{X} + 1) \quad \text{may subtract multiple of ideal generating polynomial}$$
$$= \mathbb{X}^4 + \mathbb{X}^3 + \mathbb{X}^2 - \mathbb{X}^4 - \mathbb{X}^2 - \mathbb{X} = \mathbb{X}^3 - \mathbb{X} = \mathbb{X}^3 + \mathbb{X} \quad \text{algebra and specifics of GF(2)}$$
$$\sim \mathbb{X}^3 + \mathbb{X} - (\mathbb{X}^3 + \mathbb{X} + 1) = -1 = 1 \quad \text{algebra and specifics of GF(2)}$$

Providing an Encoding for GF(8)

We want our calculation rules in "nicer" encoding.
$\{0, 1, a, b, c, d, e, f\}$ works here and is fine.
$\{0, 1, 2, 3, 4, 5, 6, 7\}$ works for arbitrary large values and thus is preferred.

The elements then are as follows:

R	$R \bmod P$	Vec	**Bin**	Why?
0	0	$(0,0,0)$	0	Nothing to say
$\mathbb{X}^0$	1	$(0,0,1)$	1	"trivial"
$\mathbb{X}^1$	$\mathbb{X}^1$	$(0,1,0)$	2	Nothing to say
$\mathbb{X}^2$	$\mathbb{X}^2$	$(1,0,0)$	4	Nothing to say
$\mathbb{X}^3$	$\mathbb{X}+1$	$(0,1,1)$	3	$\mathbb{X}^3 \sim \mathbb{X}^3 - (\mathbb{X}^3 + \mathbb{X} + 1) = \mathbb{X} + 1$
$\mathbb{X}^4$	$\mathbb{X}^2 + \mathbb{X}$	$(1,1,0)$	6	Student task: Fill in!
$\mathbb{X}^5$	$\mathbb{X}^2 + \mathbb{X} + 1$	$(1,1,1)$	7	Student task: Fill in!
$\mathbb{X}^6$	$\mathbb{X}^2 + 1$	$(1,0,1)$	5	Student task: Fill in!

Deriving Calculation Rules in GF(8)

R	$R \bmod P$	**Bin**
0	0	0
$\mathbb{X}^0$	1	1
$\mathbb{X}^1$	$\mathbb{X}$	2
$\mathbb{X}^2$	$\mathbb{X}^2$	4
$\mathbb{X}^3$	$\mathbb{X}+1$	3
$\mathbb{X}^4$	$\mathbb{X}^2+\mathbb{X}$	6
$\mathbb{X}^5$	$\mathbb{X}^2+\mathbb{X}+1$	7
$\mathbb{X}^6$	$\mathbb{X}^2+1$	5

Watch out:
Do not confuse a 1 as element of the coefficient domain $GF(2) = \mathbb{Z}_2$
with a 1 which serves as an encoding of a polynomial in $GF(8)$.

The same warning applies for all other values!

$2 + 2 = \mathbb{X}^1 + \mathbb{X}^1 = 0$ true in GF(8), false in $\mathbb{N}$

$2 + 3 = \mathbb{X}^1 + (\mathbb{X}+1) = +1$ true in GF(8)

$2 \cdot 3 = \mathbb{X} \cdot (\mathbb{X}+1) = \mathbb{X}^2 + \mathbb{X} = 6$ true in GF(8) and coincidentally in $\mathbb{N}$

$3 \cdot 5 = 4$ true in GF(8), coincidentally false in $\mathbb{N}$

GF(8) Addition and Multiplication Table

$+$	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	0						
2	2		0	1				
3	3		1	0				
4	4				0			
5	5					0		
6	6						0	
7	7							0

$\cdot$	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0							
2	0			6				
3	0		6			4		
4	0							
5	0			4				
6	0							
7	0							

Task: Complete GF(8)

Task 1: Fill in the missing "Why?" fields in the encoding table above!

Task 2: Fill in addition and multiplication table for $GF(8)$ with our encoding.

- **Hint:** You have to do thus once yourself to get a "feel" for this.
- **Hint:** Smartly exploiting algebraic properties & symmetries reduces your work load.

Task 3: Generate a table with a different encoding and show that it is isomorphic.

- For the **brave**: Take the path using the other irreducible polynomial.
- For the **timid**: Cheat: https://www.wolframalpha.com/input/?i=GF%288%29
- Only for those wanting to be the **best**: Take both paths and compare.
- Now find a suitable function $F\colon \{0,1,2,3,4,5,6,7\} \to \{0,1,a,b,c,d,e,f\}$ and demonstrate that it is an isomorphism.

4. Lagrange Interpolation

Interpolation constructs functions through points.

Lagrange interpolation does this for polynomials.

It works in arbitrary fields, thus also in Galois fields.

Joseph-Louis Lagrange

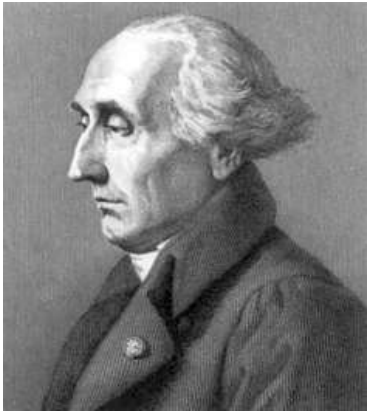

Fig. 2: Joseph-Louis Lagrange (1763 – 1813), Italian astronomer and mathematician, whose most important contributions were in the field of theoretical mechanics. When during the French revolution many of his peers in nobility were executed, he was specifically exempted. He commented the execution of his colleague, the chemist Antoine Lavoisier, with the bitter words: "*It took only a moment to cause this head to fall and a hundred years will not suffice to produce its like.*"

Theorem of Lagrange Interpolation

Let $(\mathbb{F}, +, \cdot)$ be a field, $n \in \mathbb{N}$ be a natural number.

Let $x_0, \ldots x_n$ be $n+1$ *pairwise different* values $x_i \in \mathbb{F}$ of the field and $y_0, \ldots, y_n$ be $n+1$ *arbitrary* values $y_i \in \mathbb{F}$ of the field.

Then there exists a polynomial $P \in \mathbb{F}[\mathbb{X}]$ with degree at most n such that

$$\forall i : P(x_i) = y_i$$

Above, $P(x_i)$ denotes the substitution of x_i for $\mathbb{X}$ in polynomial P.

Lagrange Basis Polynomials

For $n \in \mathbb{N}$ fixed and $j = 0, 1, \ldots, n$ define the **Lagrange basis polynomial** L_j as

$$L_j := \prod_{0 \le k \le n \quad k \neq j} \frac{\mathbb{X} - x_k}{x_j - x_k} \quad \text{which yields} \quad L_j(x_k) = \delta_{j,k} = \begin{cases} 0 & \Leftrightarrow \quad j \neq k \\ 1 & \Leftrightarrow \quad j = k \end{cases}$$

For $n = 2$ this is:

$$L_0 = \frac{\mathbb{X} - x_1}{x_0 - x_1} \cdot \frac{\mathbb{X} - x_2}{x_0 - x_2}$$

$$L_0(x_0) = \frac{x_0 - x_1}{x_0 - x_1} \cdot \frac{x_0 - x_2}{x_0 - x_2} = 1$$

$$L_0(x_1) = \frac{x_1 - x_1}{x_0 - x_1} \cdot \frac{x_1 - x_2}{x_0 - x_2} = 0$$

$$L_0(x_2) = \frac{x_2 - x_1}{x_0 - x_1} \cdot \frac{x_2 - x_2}{x_0 - x_2} = 0$$

$$L_1 = \frac{\mathbb{X} - x_0}{x_1 - x_0} \cdot \frac{\mathbb{X} - x_2}{x_1 - x_2}$$

$$L_1(x_0) = \frac{x_0 - x_0}{x_1 - x_0} \cdot \frac{x_0 - x_2}{x_1 - x_2} = 0$$

$$L_1(x_1) = \frac{x_1 - x_0}{x_1 - x_0} \cdot \frac{x_1 - x_2}{x_1 - x_2} = 1$$

$$L_1(x_2) = \frac{x_2 - x_0}{x_1 - x_0} \cdot \frac{x_2 - x_2}{x_1 - x_2} = 0$$

Pro Tip: Write this down for $n = 3$.

Lagrange Interpolation Polynomial

Finally we get the **Lagrange interpolation polynomial**

$$P = \sum_k y_k L_k = \sum_k y_k \prod_{0 \le k \le n \quad k \neq j} \frac{\mathbb{X} - x_k}{x_j - x_k}$$

Task: Find Largrange Interpolation Polynomials

Task 1: Over the field of the real numbers, find a polynomial passing through the points $(0,0),(1,1),(2,4)$.

- **Hint:** This is easily done with the "naked" eye. Do it with the Lagrange method!

Task 2: Over the field of the real numbers, find a polynomial passing through the points $(0,0),(1,1),(2,2)$.

- **Hint:** This is easily done with the "naked" eye. Do it with the Lagrange method!

Task 3: Over the field $GF(8)$, find a polynomial passing through the points $(0,1),(1,1),(2,4)$ where $0,1,2,4$ correspond to the encodings used above.

- **Hint:** Calculate using the encodings. Otherwise you have polynomials with polynomial coefficients.

Task 4: What is the largest number of points we can interpolate in a finite field?

- **Hint:** Can we find a polynomial over the field $GF(4)$ which passes through 6 points?

Appendix

Contents of Appendix

List of Figures

List of Rights

Fig. 2 Public Domain, Source: https://commons.wikimedia.org/w/index.php?curid=44110

Terms of Use (1)

Die hier angebotenen Inhalte unterliegen deutschem Urheberrecht. Inhalte Dritter werden unter Nennung der Rechtsgrundlage ihrer Nutzung und der geltenden Lizenzbestimmungen hier angeführt. Auf das Literaturverzeichnis wird verwiesen. Das Zitatrecht in dem für wissenschaftliche Werke üblichen Ausmaß wird beansprucht. Wenn Sie eine Urheberrechtsverletzung erkennen, so bitten wir um Hinweis an den auf der Titelseite genannten Autor und werden entsprechende Inhalte sofort entfernen oder fehlende Rechtsnennungen nachholen. Bei Produkt- und Firmennamen können Markenrechte Dritter bestehen. Verweise und Verlinkungen wurden zum Zeitpunkt des Setzens der Verweise überprüft; sie dienen der Information des Lesers. Der Autor macht sich die Inhalte, auch in der Form, wie sie zum Zeitpunkt des Setzens des Verweises vorlagen, nicht zu eigen und kann diese nicht laufend auf Veränderungen überprüfen.

Alle sonstigen, hier nicht angeführten Inhalte unterliegen dem Copyright des Autors, Prof. Dr. Clemens Cap, ©2020. Wenn Sie diese Inhalte nützlich finden, können Sie darauf verlinken oder sie zitieren. Jede weitere Verbreitung, Speicherung, Vervielfältigung oder sonstige Verwertung außerhalb der Grenzen des Urheberrechts bedarf der schriftlichen Zustimmung des Rechteinhabers. Dieses dient der Sicherung der Aktualität der Inhalte und soll dem Autor auch die Einhaltung urheberrechtlicher Einschränkungen wie beispielsweise Par 60a UrhG ermöglichen.

Die Bereitstellung der Inhalte erfolgt hier zur persönlichen Information des Lesers. Eine Haftung für mittelbare oder unmittelbare Schäden wird im maximal rechtlich zulässigen Ausmaß ausgeschlossen, mit Ausnahme von Vorsatz und grober Fahrlässigkeit. Eine Garantie für den Fortbestand dieses Informationsangebots wird nicht gegeben.

Die Anfertigung einer persönlichen Sicherungskopie für die private, nicht gewerbliche und nicht öffentliche Nutzung ist zulässig, sofern sie nicht von einer offensichtlich rechtswidrig hergestellten oder zugänglich gemachten Vorlage stammt.

Use of Logos and Trademark Symbols: The logos and trademark symbols used here are the property of their respective owners. The YouTube logo is used according to brand request 2-9753000030769 granted on November 30, 2020. The GitHub logo is property of GitHub Inc. and is used in accordance to the GitHub logo usage conditions https://github.com/logos to link to a GitHub account. The Tweedback logo is property of Tweedback GmbH and here is used in accordance to a cooperation contract.

Terms of Use (2)

Disclaimer: Die sich immer wieder ändernde Rechtslage für digitale Urheberrechte erzeugt für mich ein nicht unerhebliches Risiko bei der Einbindung von Materialien, deren Status ich nicht oder nur mit unverhältnismäßig hohem Aufwand abklären kann. Ebenso kann ich den Rechteinhabern nicht auf sinnvolle oder einfache Weise ein Honorar zukommen lassen, obwohl ich – und in letzter Konsequenz Sie als Leser – ihre Leistungen nutzen.

Daher binde ich gelegentlich Inhalte nur als Link und nicht durch Framing ein. Lt EuGH Urteil 13.02.2014, C-466/12 ist das unbedenklich, da die benutzten Links ohne Umgehung technischer Sperren auf im Internet frei verfügbare Inhalte verweisen.

Wenn Sie diese Rechtslage stört, dann setzen Sie sich für eine Modernisierung des völlig veralteten Vergütungssystems für urheberrechtliche Leistungen ein. Bis dahin klicken Sie bitte auf die angegebenen Links und denken Sie darüber nach, warum wir keine für das digitale Zeitalter sinnvoll angepaßte Vergütungssysteme digital erbrachter Leistungen haben.

Zu Risiken und Nebenwirkungen fragen Sie Ihren Rechtsanwalt oder Gesetzgeber.

Weitere Hinweise finden Sie im Netz hier und hier oder hier.

Citing This Document

If you use contents from this document or want to cite it,
please do so in the following manner:

Clemens H. Cap: Finite Fields. Electronic document. https://iuk.one/1033-1010 6. 6. 2021.

Bibtex Information: https://iuk.one/1033-1010.bib

```
@misc{doc:1033-1010,
   author       = {Clemens H. Cap},
   title        = {Finite Fields},
   year         = {2021},
   month        = {6},
   howpublished = {Electronic document},
   url          = {https://iuk.one/1033-1010}
}
```

Typographic Information:
Typeset on June 6, 2021
This is pdfTeX, Version 3.14159265-2.6-1.40.21 (TeX Live 2020) kpathsea version 6.3.2
This is pgf in version 3.1.5b
This is preamble-slides.tex myFormat©C.H.Cap

List of Slides

Legend:
- continuation slide
- slide without title header
- image slide