Fields and Finite Fields

Reinhard Lüftenegger

Mathematical Background of Cryptography – WT 2019/20

Evariste Galois

Overview

Fields

Algebraic Cheat Sheet

Groups $+ , -$

Rings $+ , - , \times$

Fields $+ , - , \times , \div$

“A system with a certain completeness, fullness and self-containedness; a naturally unified organic whole.”

“A system of [...] numbers, which is complete and self-contained, such that addition, subtraction, multiplication and division of any two of these numbers bring forth a number of the same system.”

Fields

Roughly speaking, the field axioms are a means to enable elementary arithmetic with more general objects (not just $\mathbb{Q}, \mathbb{R}, \mathbb{C}$).

Definition

A set F together with two functions $+ : F \times F \to F$ and $\cdot : F \times F \to F$ is called a field, if

- $(F, +)$ is an abelian group (with identity element 0),
- $(F \setminus \{0\}, \cdot)$ is an abelian group and
- it holds $(a + b) \cdot c = ac + bc$, for every $a, b, c \in F$.

Examples: For which $n \in \mathbb{N}$ is the ring of congruence classes $\mathbb{Z}/n\mathbb{Z}$ a field? What about the set of all real multiples of the identity matrix, i.e. all matrices of the form $a \cdot I_n$ for $a \in \mathbb{R}$?

Homomorphisms

Homomorphisms link algebraic structures (e.g. vector spaces, groups, rings, fields) with "compatible" structure.

Definition

A field homomorphism is a map $\varphi : E \to F$ between two fields E and F such that φ is a homomorphism of rings, i.e. such that

- $\varphi(a + b) = \varphi(a) + \varphi(b)$ and
- $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$, for every $a, b \in E$.

Examples: Complex conjugation $\varphi : \mathbb{C} \to \mathbb{C}$, $\varphi(a + ib) = a - ib$, is a field homomorphism (try to check!). Is the function $\varphi : \mathbb{R} \to \mathbb{R}$ with $\varphi(x) = x^2$ a field homomorphism? What about $\varphi(x) = x^d$ (with $d \in \mathbb{N}$)?

Subfields and Extension Fields

Definition

A field E is called a subfield of a field F, if there is a field homomorphism $\iota : E \to F$. In this case, the field F is also called an extension field of E.

Remark: We write $F \supseteq E$ (or $E \subseteq F$) to indicate that F is an extension field of E (or E is a subfield of F).

Examples: Let $\mathbb{C} := \mathbb{R} \times \mathbb{R}$ be the set of all real 2-tuples with canonical addition and multiplication that makes it a field. Then the function $\iota : \mathbb{R} \to \mathbb{C}$ with $\iota(a) := (a, 0)$ is a field homomorphism (why?). Another example: let $p < q$ be two primes. Is there a field homomorphism from $\mathbb{Z}_p$ to $\mathbb{Z}_q$?

Characteristic of a Field

Remember: The smallest subring of a ring is either isomorphic to $\mathbb{Z}$ or $\mathbb{Z}_n$, for $n \in \mathbb{N}$.

Question: What about the smallest subfield of a field?

Answer: The smallest subfield of a field is either isomorphic to $\mathbb{Q}$ or $\mathbb{Z}_p$, for p prime.

Proposition (Characteristic of a Field)

The characteristic of a field is either zero or a prime number.

Nota Bene: Knowing about the characteristic (of a ring or field) is important because it tells us how to do arithmetic (see e.g. Freshman's Dream).

Field Theory and Linear Algebra

Remember: Vector spaces are algebraic structures where we can add objects and multiply objects with a scalar from a field.

Lemma (Field Extensions as Vector Spaces)

Every field extension $F \supseteq E$ can be regarded as an E-vector space.

Sketch of the proof

Vector addition is addition in F. Scalar multiplication is multiplication in F (this is meaningful since $F \supseteq E$ is a field extension).

Field of Fractions I

Idea: We have a (certain) ring and want to construct the smallest field in which it can be embedded.

Example: Construction of the rationals $\mathbb{Q}$ via the integers $\mathbb{Z}$

- Typically, a rational number is written in the form $\frac{m}{n}$, for $m, n \in \mathbb{Z}$, $n \neq 0$, and thus can be described by the 2-tuple $(m, n) \in \mathbb{Z} \times \mathbb{Z}$.
- Two fractions $\frac{m_1}{n_1}$ and $\frac{m_2}{n_2}$ represent the same rational number, if and only if $m_1 \cdot n_2 = m_2 \cdot n_1$.

Observation: Roughly speaking, by adding multiplicative inverses to the integers we get the rationals.

We abstract these principles and introduce a generalised version of this construction.

Field of Fractions II

Definition

Let $(R, +, \cdot)$ be a commutative ring with identity that doesn't contain zero divisors. Then the following construction on top of $R \times R \setminus \{0\}$

$$\mathrm{Frac}(R) := \{[(m,n)]_\sim : m, n \in R, n \neq 0\},$$

where for $(m_1, n_1), (m_2, n_2) \in R \times R \setminus \{0\}$ we define the equivalence relation

$$(m_1, n_1) \sim (m_2, n_2) :\Leftrightarrow m_1 \cdot n_2 = m_2 \cdot n_1,$$

is called the field of fractions of R. Instead of $[(m,n)]_\sim$ we also write $\frac{m}{n}$.

Remark: Together with canonical addition and multiplication this is indeed a field (try to check!).

Finite Fields

Finite Fields

Definition

A finite field is a field that comprises finitely many elements.

Remark: We also write $\mathbb{F}_q$ to denote a finite field with q elements.

Most basic example: Ring of congruence classes $\mathbb{Z}_p$ (or $\mathbb{F}_p$) modulo a prime number p.

Application: Finite fields are a fundamental algebraic structure to do calculations within a block cipher (e.g. the AES operates in $\mathbb{F}_{2^8}$ or one instance of MiMC in $\mathbb{F}_{2^{129}}$), to define elliptic curves (e.g. Curve25519 over $\mathbb{F}_p$ with $p = 2^255 - 19$) or to implement Shamir's Secret Sharing (e.g. over $\mathbb{F}_{2^{128}}$).

Structure of Finite Fields

Nota Bene: For finite fields, the smallest subfield is isomorphic to $\mathbb{Z}_p$ for some prime p.

Theorem (Existence and Uniqueness of Finite Fields)

The number of elements in a finite field $\mathbb{F}_q$ is a prime power, i.e. $q = p^n$, for some $n \in \mathbb{N}$ and some prime p. Conversely, for every $n \in \mathbb{N}$ and every prime p there is a finite field with p^n elements, which is unique up to isomorphism.

Lagrange's theorem helps us to classify all subfields of a finite field.

Theorem (Subfield Criterion for Finite Fields)

A field $\mathbb{F}_{p^m}$ is a subfield of $\mathbb{F}_{q^n}$ if and only if $p = q$ and m divides n.

Prime vs. Irreducible I

Remember: A natural number p greater than one and whose only divisors are 1 and p itself is called a prime number. In other words

$$p = a \cdot b \Rightarrow a = 1 \text{ or } b = 1.$$

This aspect of primality leads us to the concept of irreducibility.

Definition

Let R be a commutative ring with identity that doesn't contain zero divisors. An element $r \in R$ which is not a unit is called irreducible, if

$$r = a \cdot b \Rightarrow a \sim 1 \text{ or } b \sim 1.$$

Prime vs. Irreducible II

Remember: A fundamental property of a prime number $p \in \mathbb{N}$ is

$$p \mid a \cdot b \Rightarrow p \mid a \text{ or } p \mid b$$

This aspect of being prime motivates a more general definition of primality.

Definition

Let R be a commutative ring with identity that doesn't contain zero divisors. An element $r \in R$ which is not a unit is called prime, if

$$r \mid a \cdot b \Rightarrow r \mid a \text{ or } r \mid b.$$

Note: In general, being prime is **not** equivalent to being irreducible, but in the polynomial ring $F[X]$ over a field F it is!

Construction of Finite Fields I

Remark: There are two different types of finite fields, prime fields ($\mathbb{F}_p$) and extension fields ($\mathbb{F}_{p^n}$).

Observation: Prime fields are constructed by taking the integers modulo a prime number p.

Question: Can we imitate this construction to get extension fields?

Answer: Yeah!

	Prime Fields	**Extension Fields**
Base structure	$\mathbb{Z}$	$\mathbb{F}_p[X]$
Modulus	prime number p	prime polynomial f
Resulting model	$\mathbb{Z}/(p) = \mathbb{F}_p$	$\mathbb{F}_p[X]/(f) = \mathbb{F}_{p^n}$

Construction of Finite Fields II

In $\mathbb{Z}_p$ elements are congruence classes (of integers) modulo some prime p. This is the reason why we write

$$\mathbb{F}_p = \{0, 1, \ldots, p-1\},$$

whereas on a technical level in $\mathbb{Z}_p$ the element i represents the set

$$i = \{i + kp : k \in \mathbb{Z}\} = \{\ldots, i-2p, i-p, i, i+p, i+2p, \ldots\}.$$

In $\mathbb{F}_{p^n}$ elements are congruence classes (of polynomials over $\mathbb{F}_p$) modulo some prime polynomial f of degree n, hence we write

$$\mathbb{F}_{p^n} = \{a_{n-1}X^{n-1} + a_{n-2}X^{n-2} + \cdots + a_1X + a_0 : a_i \in \mathbb{F}_p\},$$

again with the technicality that

$$a_{n-1}X^{n-1} + \cdots + a_0 = \{(a_{n-1}X^{n-1} + \cdots + a_0) + kf : k \in \mathbb{F}_p[X]\}.$$

Construction of Finite Fields III

More formally we have

Theorem (Construction of Extension Fields)

Let $\mathbb{F}_p$ be a field with p elements. If $f \in \mathbb{F}_p[X]$ is a prime polynomial of degree n, then the quotient ring $\mathbb{F}_p[X]/(f)$ is a finite field with p^n elements.

The justification is straightforward and mimics the proof for $\mathbb{F}_p$ over $\mathbb{Z}$. In essence, the only prerequisite is the following

Theorem (Extended Euclidean Algorithm)

For every two elements a, b in $\mathbb{Z}$ (or $\mathbb{F}_p[X]$) we can compute elements x, y in $\mathbb{Z}$ (or $\mathbb{F}_p[X]$) such that

$$a \cdot x + b \cdot y = \gcd(a, b).$$

Maps over Finite Fields

Remark: Every polynomial $f \in E[X]$ induces a polynomial function $f : E \to E, a \mapsto f(a)$.

Remember: Over the real numbers, for a data set of m points $(x_1, y_1), \ldots, (x_m, y_m)$ there is a unique polynomial p with degree at most $m-1$ that interpolates between these points, i.e. $p(x_i) = y_i$ for all i.

Theorem (Every Function over a Finite Field is a Polynomial Function)

Every map $\mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ can be uniquely described as a univariate polynomial with maximum degree $p^n - 1$.

Questions?

Questions for Self-Control

1. What are the main differences between a commutative ring (with identity) and a field?
2. Is there a field homomorphism between $\mathbb{F}_p$ and $\mathbb{F}_q$ for $p \neq q$?
3. Describe the construction of prime and extension fields and discuss the similarities/differences in the construction process.
4. Can every map over a finite field be described as a polynomial? Justify your answer.
5. What is the connection between linear algebra and field theory? Why is it beneficial?