Chapter 1

Finite Fields

1.1 Introduction

Finite fields are one of the essential building blocks in coding theory and cryptography and thus appear in many areas in IT security. This section introduces finite fields systematically stating for which orders finite fields exist, shows how to construct them and how to compute in them efficiently.
For applications 3 types of fields are particularly interesting – fields with a prime number of elements, extension fields of the minimal field $\{0, 1\}$ and optimal extension fields. We met *prime fields*, the first kind of fields, already in Chapter **??** as $\mathbb{Z}/p\mathbb{Z}$, the second one appeared as an example of a vector space and we also defined some multiplicative structure on it which lead to a ring but not to a field. Here were show how one constructs a *binary field*. These fields are particularly suitable for hardware implementations as the arithmetic involves basic bit operations. If, however, software implementations are the focus then it might be interesting to go for yet another construction in which the size of the elements is tailored to the word size of the processor, such fields are called *optimal extension fields*.
References for this chapter are:

- T. Høholdt and J. Justesen, "A Course In Error-Correcting Codes", Springer Verlag. Contains details for binary fields.
- R. Lidl and H. Niederreiter, "Finite Fields, Encyclopedia of Mathematics and its Applications 20", Addison-Wesley.
- R. Lidl and H. Niederreiter, "Introduction to finite fields and their applications", Cambridge University Press.
- A. Menezes, "Applications of Finite Fields", Kluwer.
- T. Murphy, "Finite Fields", Script online at `http://www.maths.tcd.ie/pub/Maths/Courseware/FiniteFields/FiniteFields.pdf`
- V. Shoup, "A Computational Introduction to Number Theory and Algebra", Cambridge University Press. This book is also available online for download at `http://www.shoup.net/ntb/ntb-b5.pdf`

In this chapter we first assume that finite fields exist and study their properties. We show that for any prime p and for any natural number n there exists a field with p^n elements. We then detail constructions of finite fields and go into the arithmetic properties.

1.2 First definitions

Definition 1 (Finite field) *A field with finitely many elements is called a* finite field. *We denote a finite field with q elements by $\mathbb{F}_q$.*

Finite fields are also called *Galois fields*, named after Évariste Galois, and several books and scientific papers thus use $GF(q)$ to denote a finite field with q elements.

Definition 2 (Characteristic) *Let K be a field. The smallest natural number $n > 0$ such that*

$$n \cdot 1 = \underbrace{1 + 1 + \ldots + 1}_{n\ -times} = 0$$

is called the characteristic of K, *denoted by* $\mathrm{char}(K) = n$.
If no such n exists one puts $\mathrm{char}(K) = 0$.

We have already encountered the following example in the previous chapter but state it again here as the first example of a finite field.

Example 3 *The ring $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ is a finite field of characteristic p. Obviously $\mathbb{F}_p$ has exactly p elements and is thus finite, we have seen that it is a field and every element vanishes under multiplication by p, thus the characteristic is p.*

The following lemma gives useful properties of the characteristic.

Lemma 4 *Let K be a field.*

1. *If the characteristic of K is positive,* $\mathrm{char}(K)$ *is prime.*
2. *Finite fields have* $\mathrm{char}(K) > 0$. *By the first part of this lemma we even have that a finite field has prime characteristic.*

Proof.

1. Assume on the contrary that there exists a nontrivial factorization $\mathrm{char}(K) = n = p \cdot q$. Then

   $$0 = n \cdot 1 = (p \cdot q) \cdot 1 = p \cdot (q \cdot 1) = (p \cdot 1) \cdot (q \cdot 1) = \underbrace{(1 + 1 + \cdots + 1)}_{p\text{ -times}} \cdot \underbrace{(1 + 1 + \cdots + 1)}_{q\text{ -times}}.$$

   We encountered earlier that fields have no zero divisors, that means that one of the terms in the product must be zero which contradicts the minimality of the characteristic.

2. In a *finite* field not all of $1, 2 \cdot 1, 3 \cdot 1, \ldots$ can be distinct, e.g. $r \cdot 1 = s \cdot 1$ for some $s > r$. Then $\Rightarrow (s - r) \cdot 1 = 0$ and so $\mathrm{char}(K) | s - r > 0$

□

Lemma 5 *Let K be a field. Then there exists a smallest subfield of K.*

Proof. Let F_1, F_2 be subfields of K, then their intersection $F_1 \cap F_2$ is also a subfield of K.
This holds for arbitrary many subfields, thus also for the intersection of all subfields of K. Obviously, the resulting intersection is the smallest subfield of K. □

This smallest subfield is an important concept and thus deserves a name.

Definition 6 (Prime subfield)
The smallest subfield of a field K is called the prime subfield *or short* prime field *of K.*

Depending on K the prime subfield can be finite or infinite. If the characteristic of the field is zero one finds a copy isomorphic to $\mathbb{Q}$ the rational numbers by observing that all "integer" multiples of 1 must be in the field and that the field must be closed under division. For finite fields – and generally for fields of positive characteristic – one can always find a subfield of the type encountered in Example 3.

Lemma 7 *Let K be a finite field of characteristic p. The prime subfield of K is isomorphic to $\mathbb{F}_p$, the finite field with p elements.*

Proof. We represent $\mathbb{F}_p$ as $\{0, 1, 2, \ldots, p-1\}$ and define a map into K as

$$\varphi : \mathbb{F}_p \mapsto K, r \mapsto r \cdot 1 = \underbrace{1 + \ldots + 1}_{r \text{ -times}}$$

where 1 is the multiplicative unit in K and + denotes addition in K.
One easily checks that φ is additive and multiplicative, thus a field homomorphism. To show that the field $\mathbb{F}_p$ is embedded into K it remains to show that the map is injective. Assume on the contrary that for some $p > r > s \geq 0$ we have $\varphi(r) = \varphi(s)$. Put $c = r - s > 0$. By the definitions of r and s one can consider c as an element of $\mathbb{F}_p^*$ and thus it has a multiplicative inverse c^{-1} in $\mathbb{F}_p$. We obtain

$$\varphi(1) = \varphi\left(c \cdot c^{-1}\right) = \varphi(c) \cdot \varphi\left(c^{-1}\right) = (\varphi(r) - \varphi(s)) \cdot \varphi\left(c^{-1}\right) = 0.$$

However, by the definition of φ one has $\varphi(1) = 1 \neq 0$ since K is a field. Because of this contradiction, φ is an isomorphism between $\mathbb{F}_p$ and the image of the homomorphism $\mathrm{Im}(\varphi) \subset K$.
This isomorphism proves that $\mathrm{Im}(\varphi)$ is a subfield of K (the image contains 0 and 1 and the field operations are inherited). Since $\mathbb{F}_p$ has no non-trivial subfield, it is its own prime subfield and the argument carries over to $\mathrm{Im}(\varphi)$. So $\mathrm{Im}(\varphi)$ is the prime field of K. □

We already used the notation $\mathbb{F}_p$ as if this would be a unique field. Indeed this holds true up to isomorphism.

Corollary 8 *Let p be a prime. Up to isomorphism there is only one finite field with p elements, denoted by $\mathbb{F}_p$.*

The proof follows from Lemma 7 by observing that $\mathbb{F}_p$ is isomorphic to its own prime subfield.
Finite fields with a prime number of elements are often referred to as *prime fields*.

Exercise 9 *Let K be a field of characteristic p, where p is prime. Show that for any integer n one has*

$$(a+b)^{p^n} = a^{p^n} + b^{p^n}$$

for all $a, b \in K$.

1.3 The additive structure of finite fields

So far we do not know whether fields other than $\mathbb{F}_p$ exist but we can find criteria a more general finite field has to satisfy. That reduces the search space and actually gives rise to a construction method.
In the Section **??** we considered extension fields as vector spaces over their subfield. This approach helps to determine the additive structure of finite fields and limits the possible sizes for which finite fields can exist.
Let K be a finite field of characteristic $\mathrm{char}(K) = p, |K| > p$. By Lemma 7 there exists a subfield of K isomorphic to $\mathbb{F}_p$. For ease of notation we identify this field with $\mathbb{F}_p$.
K is a vector space over $\mathbb{F}_p$ and so there must exist a basis of linearly independent elements $a_1, \ldots, a_n$ for some dimension n. This is the main observation leading to the proof of the following lemma.

Lemma 10 *Let K be a finite field of $\mathrm{char}(K) = p$. There exists an integer $n \geq 1$ so that $|K| = p^n$.*

Proof. Consider K as vector space over $\mathbb{F}_p$. Let $\dim_{\mathbb{F}_p}(K : \mathbb{F}_p) = n$ and let $\{\xi_1, \ldots, \xi_n\}$ be a basis.
Then every element $a \in K$ can be represented via a linear combination of the basis elements with coefficients in $\mathbb{F}_p$. So there exist $c_1, \ldots, c_n \in \mathbb{F}_p$ satisfying $a = c_1\xi_1 + \cdots + c_n\xi_n$.
Each c_i can have p different values, since we consider linear combinations over a basis all these p^n elements in K are distinct. Again by the property of a basis each element of K can be represented as linear combination this way. Thus $|K| = p^n$. □

So for any finite field the number of elements must be a prime or a prime power. E.g. there exists no finite field with 6 elements since 6 is not a prime or prime power. In the following q denotes a prime power $q = p^n$.
We also get conditions on the relative sizes of subfields.

Lemma 11 *Let L be a finite field with $|L| = p^n$ and let K be a subfield of L.*
There exists an integer $n > 1$ so that $|K| = p^m$ and $m|n$.
The extension degree of L over K is $[L : K] = n/m$.

Proof. Left to the reader (given as homework at the end of this section). □

We know have a necessary condition on the number of elements in a finite field. The following example studies one finite field which is not a prime field.

Example 12 *The number 4 is a prime power, so there could be a finite field with 4 elements. What would $\mathbb{F}_4 = \mathbb{F}_{2^2}$ look like? For the moment let us assume that $\mathbb{F}_4$ exists (we will later see that this is indeed the case).*
Let 0 be the additive and 1 be the multiplicative neutral element. Let a be one of the other two elements. Since $\mathbb{F}_4$ is closed under addition the other element must equal $a+1$, so $\mathbb{F}_4 = \{0, 1, a, a+1\}$. We now give the addition table which follows easily from the fact that the characteristic is 2, thus $x + x = 0$ for any $x \in \mathbb{F}_4$. Since every element must appear in each row and each column of the table we obtain $a \cdot a = a+1$ and consequently $a \cdot (a+1) = 1$.

$+$	*0*	*1*	a	$a+1$
0	*0*	*1*	a	$a+1$
1	*1*	*0*	$a+1$	a
a	a	$a+1$	*0*	*1*
$a+1$	$a+1$	a	*1*	*0*

$\cdot$	*0*	*1*	a	$a+1$
0	*0*	*0*	*0*	*0*
1	*0*	*1*	a	$a+1$
a	*0*	a	$a+1$	*1*
$a+1$	*0*	$a+1$	*1*	a

We were able to fill the tables completely using just necessary conditions. We note that a basis of $\mathbb{F}_4$ over $\mathbb{F}_2$ could be given by $\{1, a\}$ or likewise by $\{1, a+1\}$.
But: do these tables actually form a field? To answer this we need to check associativity of $+$ and $\cdot$ and prove that the distributive laws hold. Since the number of elements is very small we could check these by explicitly considering all possible cases. The next section provides us with a better understanding of finite fields and their multiplicative structure so that we skip this tedious work here.

Let $\xi_1, \xi_2, \ldots, \xi_n$ be a basis of the finite field K with $|K| = p^n$ over $\mathbb{F}_p$. We can state K as a set as

$$K = \{a_1\xi_1 + a_2\xi_2 + \cdots + c_n\xi_n | a_i \in \mathbb{F}_p \text{ for } 1 \leq i \leq n\}.$$

It is very easy to add two field elements by using the vector space structure:
Let $a = \sum_{i=1}^n a_i\xi_i$ and $b = \sum_{i=1}^n b_i\xi_i$ be elements of K. Their sum is given by

$$a + b = \sum_{i=1}^{n} (a_i + b_i)\xi_i,$$

where $a_i + b_i$ is computed as an element of $\mathbb{F}_p$, i.e. modulo p.

However, we are not able to multiply in this representation unless we know the value of $\xi_i \cdot \xi_j$ expressed in this basis for all $1 \leq i, j \leq n$. Apparently one can store all $n(n+1)/2$ results of the multiplication of the basis vectors and perform multiplications with table lookups but that seems rather tedious. The following section suggests a representation which is particularly suitable for multiplications and Section 1.6 gives the representation which we will use for most applications.

Exercise 13 *Prove Lemma 11. Hint: consider L as vector space over K and follow the proof of Lemma 10.*

1.4 The multiplicative structure of finite fields

The previous section gave us insight in the number of elements of a finite field and determined the additive structure. Given a basis of a finite field K over its prime subfield we are able to perform additions. We now turn our attention to the study of K^*, the multiplicative group of K.

Lemma 14 *Let K be a finite field with $|K| = p^n$. The multiplicative group $K^* = K \setminus \{0\}$ is cyclic.*

Proof. For ease of notation put $q = p^n$. Since K is a field, K^* consists of all elements of K but 0. So $|K^*| = q - 1$.
According to the Lagrange Theorem for each $a \in K$ we have $a^{q-1} = 1$ and $\mathrm{ord}(a)|q-1$.
If K^* is cyclic then there must exist at least one element g with $\mathrm{ord}(g) = q - 1$.
Let e be the exponent of K^*. By the definition of e the order of every element divides e, i.e. $a^e = 1$ for all $a \in K^*$. This implies that all $a \in K^*$ are roots of $F(x) = x^e - 1$. Thus $F(x)$ is a non-zero polynomial of degree e which has at least $q - 1$ different roots which implies $q - 1 \leq e$ by Corollary **??**.
Since the exponent of a group divides its order we have $e|q-1$ and thus $e \leq q - 1$.
Together this gives $e = q - 1$, i.e. the exponent is the full group order which implies that there is at least one element of order $q - 1$. □

Definition 15 (Primitive element)
Let K be a finite field. A generator of K^* is called primitive element.

An obvious consequence of Lemma 14 is the following:

Corollary 16 *Every finite field contains at least one primitive element.*
More precisely there are exactly $\varphi(q-1)$ primitive elements.

This gives a second possibility of representing finite fields. Let g be a primitive element of K then

$$K = \{0, 1, g, g^2, \ldots, g^{q-2}\} = \{0\} \cup \langle g \rangle.$$

In this representation it is very easy to multiply two elements $a = g^i$ and $b = g^j$ as

$$a \cdot b = g^i \cdot g^j = g^{i+j},$$

where the exponent $i + j$ is taken modulo $q - 1$. However, we don't know how to add a and b. Assume $j \leq i$. We observe that

$$a + b = g^i + g^j = g^j(g^{i-j} + 1)$$

and so it would be enough to tabulate all $q - 1$ values of $g^k + 1, 1 \leq k \leq q - 2$ expressed as a power of g to be able to add in this representation.
The lemma also allows to obtain properties of power maps and find possible orders.

Corollary 17 *Let K be a finite field with $|K| = q$ elements. There exist elements of order k if and only if $k|(q-1)$.*
The power map $\tau : K \to K; a \mapsto a^k$ is a bijection if and only if $\gcd(k, q-1) = 1$.

The following section deals with polynomials over finite fields. We obtain necessary knowledge to find a representation of finite fields that allows to perform addition and multiplication without keeping a big table.

Exercise 18 *a) Corollary 16 also holds for the prime fields $\mathbb{F}_p$. Find primitive elements of $\mathbb{F}_5, \mathbb{F}_7, \mathbb{F}_{11}, \mathbb{F}_{13}$ and $\mathbb{F}_{17}$.*

b) State all primitive elements of $\mathbb{F}_7$.

c) Let $\mathbb{F}_{16}^* = \langle g \rangle$. State all primitive elements in terms of g.

d) Prove Corollary 16.

1.5 Polynomials over finite fields

This section studies polynomials over finite fields. In Section **??** we introduced many properties of polynomials over a field. We refer to that section for general background and concentrate here on the case that the coefficients come from a finite field.
We recall the definition of an irreducible polynomial (Definition **??**). A polynomial $f(x) \in K[x]$ is *irreducible* if it cannot be written as a product of polynomials of lower degree over the same field, i.e. $u(x)|f(x)$ implies u is constant or $u(x) = f(x)$. Otherwise it is called *reducible*.

Example 19 *Consider the following polynomials in $\mathbb{F}_2[x]$: $f_1(x) = x$, $f_2(x) = x^2 + 1$, $f_3(x) = x^2 + x + 1$, and $f_4(x) = x^4 + x^2 + 1$.*

a) Apparently f_1 is irreducible.

b) A non-trivial factor of f_2 must be linear, one sees that $(x+1)|f_2(x)$, actually $f_2(x) = (x+1)^2$.

c) There are only two linear polynomials, x and $x+1$, over $\mathbb{F}_2$. One easily checks that none of them divides f_3, so f_3 is irreducible.

d) The last polynomial is not divisible by a linear factor. However, it is not irreducible since $f_4(x) = (x^2 + x + 1)^2 = f_3^2(x)$. which cannot be factored further since f_3 is irreducible.

For functions over the reals, the derivative gives information about the slope of the tangent in a point. In the discrete setting of finite fields we lose this interpretation but we can still define the derivative of a polynomial.

Definition 20 *Let K be a field and $f(x) = \sum_{i=0}^{n} f_i x^i \in K[x]$ be a polynomial. The* derivative f' of f *is given by*

$$f'(x) = \sum_{i=1}^{n} i \cdot f_i x^{i-1}.$$

Note that if K has characteristic p then the derivative of all terms x^{mp} vanishes.
One can show that for this derivative the usual rules hold.

Corollary 21 *Let $f, g \in K[x]$. One has*

$$(f+g)' = f' + g', \tag{1.1}$$
$$(f \cdot g)' = f' \cdot g + f \cdot g', \tag{1.2}$$
$$(f^a)' = af^{a-1} \cdot f'. \tag{1.3}$$

Exercise 22 *a) Let $f(x) = x^{17} + 3x^{15} - 2x^{12} + x^{11} - x^{10} - 2x^8 + x^5 + 3x^2 + 2 \in \mathbb{F}_5[x]$. Compute the derivative f' of f.*

b) Let $f \in K[x]$ be a polynomial. Show that if α is a multiple root of f then $(x - \alpha) | \gcd(f, f')$.

c) Let $f \in K[x]$ be a polynomial. Show that $\gcd(f, f') \in K^*$ if and only if f has no multiple roots in K or any of its extension fields.

1.6 Polynomial representation of finite fields

In this section we show how to construct finite fields with p^n, $n > 1$, elements by using an irreducible polynomial of degree n over $\mathbb{F}_p$. The same considerations can be used to construct an extension field of K with $|K| = p^m$ in which case the polynomial must be irreducible over K.
We start by investigating relations between a finite field and a subfield of it.

Lemma 23 *Let K, L be finite fields with $K \subset L$, $|K| = q$, $|L| = q^n$.*
Every element $\alpha \in L$ is a root of a uniquely defined monic polynomial $m_\alpha \in K[x]$, $\deg m_\alpha \leq n$. This polynomial m_α satisfies that if α is a root of some polynomial $f \in K[x]$ then $m_\alpha | f$.

Proof. We start by considering L as a vector space over K. Since the dimension $\dim_K(L : K)$ is n, any $n + 1$ or more elements are linearly dependent.
So the elements $1, \alpha, \alpha^2, \ldots, \alpha^n$ are linearly dependent and there exist coefficients $c_0, \ldots, c_n \in K$ so that $c_0 + c_1\alpha + c_2\alpha^2 + \cdots + c_n\alpha^n = 0$.
We just constructed a polynomial $f(x) = \sum_{i=0}^{n} c_i x^i \in K[x]$ of degree n such that $f(\alpha) = 0$. This proves the existence part of the lemma.
Now that we know that there is at least one polynomial of degree $\leq n$ over K which has α as root and since we can make each polynomial monic as K is a field, let m_α be the monic polynomial of minimal degree so that $m_\alpha(\alpha) = 0$. From the first part we know $\deg(m_\alpha) \leq \deg(f) \leq n$.
We first note that m_α must be irreducible because if it would split as $m_\alpha = a \cdot b$ with $\deg(a), \deg(b) > 1$ would give $0 = m_\alpha(\alpha) = a(\alpha) \cdot b(\alpha)$ and because there are no zero divisors either $a(\alpha) = 0$ or $b(\alpha) = 0$ which contradicts the minimality of the degree of m_α.
Let $f(\alpha) = 0$, and let $r(x), \deg(r) < \deg(m_\alpha)$ be the remainder of f by division by m_α, i.e. $f(x) = q(x)m_\alpha(x) + r(x)$. Evaluating both sides at α gives the identity

$$0 = f(\alpha) = q(\alpha)m_\alpha(\alpha) + r(\alpha) = q(\alpha) \cdot 0 + r(\alpha) = r(\alpha),$$

so $r(\alpha) = 0$. Again by the minimality of $\deg(m_\alpha)$ we obtain $r(x) = 0$ which means $m_\alpha | f$. □

Definition 24 (Minimal polynomial)
Let K be a field, L be a finite extension field of K and $\alpha \in L$. The polynomial $m_\alpha \in K[x]$ constructed in Lemma 23 is called the minimal polynomial of α over K.

The prime fields $\mathbb{F}_p$ are constructed as residue classes of the integers modulo a prime p. We have seen that the ring of polynomials over a field shares many similarities with the ring of integers and so we consider the polynomial ring modulo an irreducible polynomial.

Theorem 25 *Let K be a finite field and let $L = K[x]/fK[x]$ be the residue classes modulo a polynomial $f \in L[x]$.*
L is a field if and only if f is irreducible.

Proof. In Example **??** we considered the case $K = \mathbb{F}_2$ and $f(x) = x^n + 1$ in detail and showed that $\mathbb{F}_2[x]/(x^n + 1)\mathbb{F}_2$ is a commutative ring with unity. The same proof works for any field K and any polynomial f.
Let $\deg(f) = n$. Like in the example we represent each residue class in L by the polynomial of smallest degree in it $L = \{a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1}x^{n-1} \mid a_i \in K\}$. Given that L is a commutative ring with unity for any field K and any polynomial f it remains to show the equivalence

$$L \text{ is a field } \iff f \text{ is irreducible.}$$

Let f be irreducible and let $0 \neq a(x) \in K[x]$ be a polynomial of degree $\deg(a) < n$. In $K[x]$ we have $\gcd(a(x), f(x)) = 1$ and Bézout's identity **??** leads to a representation

$$1 = a(x)u(x) + f(x)v(x), \text{ with } \deg(u) < n.$$

This implies $(a(x))^{-1} \equiv u(x) \bmod f(x)$ and because of the degrees, a and u are both representatives of classes in L and we obtain the identity of classes $(a(x))^{-1} = u(x)$.
To prove the other implication assume on the contrary that f splits as $f(x) = g(x) \cdot h(x)$, with $1 \leq \deg(g), \deg(h) < n$. Because of the degrees, g and h are representatives of their respective classes in L and they both do not represent the class of 0. However, we have $g \cdot h = f \equiv 0 \bmod f$ and thus $g \cdot h = 0$ in L which contradicts that fields do not have zero divisors. □

This theorem is the most important tool to construct finite fields of cardinality p^n with $n > 1$. All we need is to find is an irreducible polynomial of degree n over $\mathbb{F}_p$. Let us first consider some examples.

Example 26 *Let $K = \mathbb{F}_2$.*

a) The polynomial $f(x) = x$ is obviously irreducible but the residue class field $\mathbb{F}_2[x]/x\mathbb{F}_2[x] \cong \{a_0 \in \mathbb{F}_2\}$ is isomorphic to the field $\mathbb{F}_2$ itself.

b) Consider $f(x) = x^2 + 1$. We know from Example 19 that $f(x) = (x+1)^2$ is not irreducible. Consider the addition and multiplication tables modulo f.

$+$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

$\cdot$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	1	$x+1$
$x+1$	0	$x+1$	$x+1$	0

Since $(x+1)\cdot(x+1) = 0$ this is not a field but only a ring.

c) Let $f(x) = x^2 + x + 1$; f is irreducible. By the previous lemma, $\mathbb{F}_2[x]/f\mathbb{F}_2$ is a field. Given that the number of elements in

$$L = \mathbb{F}_2[x]/(x^2+x+1)\mathbb{F}_2 = \{a_0 + a_1 x | a_i \in \mathbb{F}_2, 0 \leq i \leq 1\}$$

is 4 we have that L is a finite field with 4 elements. In Example 12 we investigated what the field $\mathbb{F}_4$ would look like. Note that the addition and multiplication tables we presented there apply directly to L with a representing the class of x and so we have now established that they define addition and multiplication in $\mathbb{F}_4$.

Exercise 27 *a) Show that $h(x) = (x^3 + x + 1) \in \mathbb{F}_2[x]$ defines a field with 8 elements. Give addition and multiplication tables of $\mathbb{F}_8 \cong \mathbb{F}_2[x]/h\mathbb{F}_2[x]$.*

b) Let $\mathbb{F}_4$ be defined using the irreducible polynomial $f(x) = x^2 + x + 1$. Show by direct inspection that $k(y) = (y^3 + y + 1)$ has no roots over $\mathbb{F}_4$.

1.7 Existence and uniqueness of finite fields

We have now obtained a way of constructing finite fields by using irreducible polynomials over prime fields and mentioned that the same construction can also be used for an arbitrary base field. This raises the need to question whether the constructed fields are the same and whether we can always find an irreducible polynomial of the desired degree. This section is rather technical in nature but establishes a major result towards proving the existence and uniqueness of finite fields of prime power order.
The following definition and lemma hold in the context of arbitrary fields.

Definition 28 (Splitting field)
Let K be a field and let $f(x) \in K[x]$ be a polynomial. The splitting field of f *is the smallest field extension L of K so that f splits into linear factors in $L[x]$.*

We state the following lemma without proof. It is an important piece in the construction of finite fields but its proof is rather technical.

Lemma 29 *Let K be a field and let $f(x) \in K[x]$ be a polynomial. The splitting field of f exists and is unique up to isomorphism.*

Example 30 *a) The splitting field of $f(x) = x + 1 \in \mathbb{F}_2[x]$ is $\mathbb{F}_2$ itself since f is linear.*

b) The splitting field of $g(x) = x^2 + x + 1$ *is* $\mathbb{F}_4$ *– by construction the class of* x *in* $L = \mathbb{F}_2[x]/g\mathbb{F}_2[x]$ *is a root of* g*. To see this consider* $g(y) = y^2 + y + 1$ *as polynomial in* $L[y]$ *and note that we compute modulo* $x^2 + x + 1$ *in* L

$$(y + x)(y + x + 1) = y^2 + (x + x + 1)y + x^2 + x = y^2 + y + 1 = g(y).$$

c) Put $h(x) = (x^3 + x + 1) \in \mathbb{F}_2[x]$*. This polynomial is irreducible over* $\mathbb{F}_2$ *and it thus allows to define a field with 8 elements as* $\mathbb{F}_8 \cong \mathbb{F}_2[x]/h\mathbb{F}_2[x]$*. By the same considerations as above the splitting field of* h *is* $\mathbb{F}_8$*.*

d) Put $j(x) = (x^2 + x + 1)(x^3 + x + 1) \in \mathbb{F}_2[x]$*. Over* $\mathbb{F}_2$ *the polynomial splits but not into linear factors. As seen right before the first factor splits in* $\mathbb{F}_4$ *while the second one splits only in* $\mathbb{F}_8$*. We know from Lemma 11 that* $\mathbb{F}_4$ *is not a subfield of* $\mathbb{F}_8$ *as* $2 \nmid 3$ *and so the splitting field of* j *must be* $\mathbb{F}_{2^6}$*, the smallest extension field of* $\mathbb{F}_2$ *containing both* $\mathbb{F}_{2^2}$ *and* $\mathbb{F}_{2^3}$*.*

We now provide a *reducible* polynomial which is very important for the existence proof of finite fields.

Lemma 31 *Let* $f(x) = x^{p^n} - x \in \mathbb{F}_p[x]$ *for some integer* n*. The splitting field of* f *is a finite field* K *with* $|K| = p^n$ *elements and* f *splits as*

$$x^{p^n} - x = \prod_{a \in K} (x - a).$$

Proof. We use the result of Exercise 22 c that a polynomial f has no multiple roots if and only if $\gcd(f, f') = 1$ when made monic. Here $f'(x) = p^n x^{p^n - 1} - 1 = -1$ since we are working in a field of characteristic p and thus $\gcd(f, f') = 1$. Put $q = p^n$.
The splitting field K of f exists by Lemma 29 and it contains the set $S = \{a \in K | a^q = a\}$. We just showed $|S| = q = p^n$. We now show that S is a subfield of K and by the minimality of the splitting field we obtain that $S = K$ is the splitting field of f.
The elements 0 and 1 are in S since they are roots of f.
Let $a, b \in S$. By Exercise 9 we have

$$(a - b)^q = a^q + (-b)^q = a^q - b^q = a - b \text{ and thus } (a - b) \in S,$$

where the second equality holds apparently in odd characteristic while in characteristic 2 there is no difference between $+$ and $-$. The third equality uses that $a, b \in S$.
The respective considerations for the multiplicative group are even easier. Let $a, b \in S$ then

$$\left(\frac{a}{b}\right)^q = \frac{a^q}{b^q} = \frac{a}{b} \text{ and thus } \frac{a}{b} \in S$$

and so indeed S is a subfield of K. □

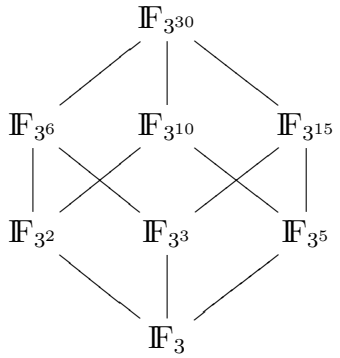
We now have all the knowledge needed to prove that finite fields of any prime power order q exist and that they are unique up to isomorphisms.

Theorem 32 (Existence and uniqueness of finite fields)
For any prime p *and any natural number* n *there exists a finite field with* p^n *elements. Every field with* p^n *elements is isomorphic to the splitting field of* $f(x) = x^{p^n} - x$ *over* $\mathbb{F}_p$*.*

Proof. We start by noticing that for $n = 1$ the theorem is true as $\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$ exists and is unique up to isomorphism by Corollary 7.
Obviously the polynomial $f(x) = x^{p^n} - x \in \mathbb{F}_p[x]$ can be stated for any prime p and integer n. The existence and uniqueness of a field with p^n elements follows from the uniqueness of the splitting field of a polynomial, Lemma 29, and Lemma 31 showing that the splitting field of $f(x)$ is a finite field with p^n elements. □

It is also easy to give the complete list of subfields of a finite field $\mathbb{F}_q$ and the relations between the subfields by using Lemma 11. This is best done in a Hasse-diagram in which the largest field, in this case $\mathbb{F}_q$, is situated in the top row. The next row contains the direct subfields of $\mathbb{F}_q$, each of then connected with a line to $\mathbb{F}_q$ etc. The bottom level contains only the prime subfield $\mathbb{F}_q$.

Example 33 *Consider the finite field $\mathbb{F}_{3^{30}}$. By Lemma 11 any subfield $\mathbb{F}_{3^m}$ must satisfy $m|30$ and thus there are only the following subfields: $\mathbb{F}_3, \mathbb{F}_{3^2}, \mathbb{F}_{3^3}, \mathbb{F}_{3^5}, \mathbb{F}_{3^6}, \mathbb{F}_{3^{10}}$ and $\mathbb{F}_{3^{15}}$. This leads to the following Hasse-diagram:*



This easily allows to read off that $\mathbb{F}_{3^5}$ is a subfield of $\mathbb{F}_{3^{10}}, \mathbb{F}_{3^{15}}$ and $\mathbb{F}_{3^{30}}$ but not of $\mathbb{F}_{3^6}$ or any field on the same or a lower level.

Exercise 34 *State all subfields of $\mathbb{F}_{2^{24}}$ and their relations in a Hasse-diagram.*

1.8 Construction of finite fields

We have obtained that for any prime p and any natural number n there exists a finite field with p^n elements. We have a description of this field as splitting field of $x^{p^n} - x$; we also learned how to define a field as the ring of polynomials modulo an irreducible polynomial; and starting from an extension field we defined the minimal polynomial of an element – which is an irreducible polynomial. This section highlights the connections between these approaches.

Definition 35 *Let K be a field, let L be an extension field of K, and let $\theta \in L$. The smallest extension field of K containing θ is denoted by $K(\theta)$. It is called the* field obtained by adjoining θ to K.

Example 36 *a) The first example does not deal with finite fields but shows that we know the concept of adjoining elements to fields from other contexts.*

$$\mathbb{R}(i) = \{a + b \cdot i \mid a, b \in \mathbb{R}\} \cong \mathbb{C}.$$

b) Let α be a root of $j(x) = (x^2 + x + 1)(x^3 + x + 1)$ in $\mathbb{F}_{2^6}$. Depending on whether $\alpha^2 + \alpha + 1 = 0$ or $\alpha^3 + \alpha + 1 = 0$ we have $\mathbb{F}_2(\alpha) \cong \mathbb{F}_4$ or $\mathbb{F}_2(\alpha) \cong \mathbb{F}_8$.

We now highlight the connection between constructing fields by adjoining elements from extension fields and by using the ring of polynomials modulo an irreducible polynomial.

Lemma 37 *Let $\theta \in L$ and let $m_\theta(x)$ be the minimal polynomial of θ over K and $\deg(m_\theta) = m$. We have*

1. *$K(\theta) \cong K[x]/m_\theta K[x]$,*
2. *$\dim_K(L : K) = m$, a basis of $K(\theta)$ over K is given by $\{1, \theta, \theta^2, \ldots, \theta^{m-1}\}$,*
3. *For every $\alpha \in K(\theta)$ there exists a minimal polynomial $m_\alpha(x) \in K[x]$, with $\deg(m_\alpha)|m$.*

Proof.

1. The evaluation at θ map $\tau : K[x] \to K(\theta)$, $f \mapsto f(\theta)$ is a ring homomorphism. The kernel of this map $\mathrm{Ker}(\tau)$ consists of the elements mapped to 0 in $K(\theta)$

$$\mathrm{Ker}(\tau) = \{h(x) \in K[x] \mid h(\theta) = 0\} = (m_\theta(x)),$$

   where $(m_\theta(x))$ denotes the ideal generated by m_θ (that is all multiples of $m_\theta(x)$ in $K[x]$).

   According to Theorem **??** the image of τ is isomorphic to $K[x]/(\mathrm{Ker}(\tau)) \cong \mathrm{Im}(\tau)$. The set $\mathrm{Im}(\tau)$ contains θ (as image of $\tau(x) = \theta$). Therefore $K(\theta) = \mathrm{Im}(\tau)$.

2. From the first part we have that $\alpha \in K(\theta)$ is in the image of τ and can thus be represented as $f(\theta)$ for some $f \in K[x]$. Since all polynomials are reduced modulo m_θ it is enough to consider polynomials f with $\deg(f) < m$. So α equals a linear combination of $1, \theta, \ldots, \theta^{m-1}$ with coefficients from K and so each element is a linear combination of $1, \theta, \ldots, \theta^{m-1}$.

   To show that $1, \theta, \ldots, \theta^{m-1}$ form a basis we need to show that they are linearly independent over K. Assume on the contrary that there would be coefficients $a_i \in K$, not all $a_i = 0$ for $0 \leq i < m$ so that $a_0 + a_1\theta + \cdots + a_{m-1}\theta^{m-1} = 0$. The polynomial $h(x) = \sum_{i=0}^{m-1} a_i x^i$ would have θ as root and strictly lower degree than $m = \deg(m_\theta)$ which contradicts the definition of minimal polynomial.

3. According to Definition 24, α has a minimal polynomial over K. We have the following inclusion of finite extension fields $K \subseteq K(\alpha) \subseteq K(\theta)$. According to Lemma 11 the degrees of the extension fields divide each other leading to $\deg(m_\alpha)|\deg(m_\theta) = m$.

□

If we use an irreducible polynomial f of degree n to define an extension field there are n different roots of f over the splitting field which can be adjoined to the ground field. The following corollary which follows from the previous lemma shows that all choices are isomorphic.

Corollary 38 *Let $f(x) \in K[x]$ be irreducible and let L be the splitting field of f over K. Let α and β be roots of $f(x)$ over L.*
We have $K(\alpha) \cong K(\beta)$.

This shows that all m roots have the same effect on the splitting field. This is no surprise since we work modulo $f(x)$ and thus consider all m roots simultaneously.

Lemma 39 *Let $f(x) \in \mathbb{F}_q[x]$ be irreducible and let α be a root of $f(x)$ in some extension field $\mathbb{F}_{q^m}$. If a polynomial $h(x) \in \mathbb{F}_q[x]$ also has α as root, $h(\alpha) = 0$ then we have that $f(x)|h(x)$.*

Proof. According to Lemma 23 the minimal polynomial of α divides any polynomial $h(x)$ with $h(\alpha) = 0$. Let $LT(f) = a$ be the leading coefficient of f. The polynomial $a^{-1} \cdot f$ is monic and irreducible with root α and thus equals the minimal polynomial of α. □

Lemma 40 *Let $f(x) \in \mathbb{F}_q[x]$ be irreducible over $\mathbb{F}_q$ of $\deg(f) = m$. Then $f(x)$ divides $x^{q^n} - x$ if and only if $m|n$.*

Proof. Let $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_m$ be the roots of $f(x)$ in the splitting field $L \cong \mathbb{F}_{q^m}$ of f over $\mathbb{F}_q$.
If $f(x) \mid x^{q^n} - x$ then $\alpha^{q^n} = \alpha$, and so L is a subfield of $\mathbb{F}_{q^n}$.
Since $[L : \mathbb{F}_q] = m$ and $[\mathbb{F}_{q^n} : \mathbb{F}_q] = n$ one must have $m|n$ by Lemma **??**.
If $m|n$ then $\mathbb{F}_{q^m} \subseteq \mathbb{F}_{q^n}$ and so $\alpha \in \mathbb{F}_{q^n}$ and satisfies $\alpha^{q^n} = \alpha$ which implies $x^{q^n} \equiv x \bmod (x - \alpha)$. This holds not only for α but for all roots $\alpha_i, 1 \leq i \leq m$ of f. By the Chinese Remainder Theorem **??** it also holds modulo the product $f(x) = \prod_{i=1}^{m}(x - \alpha_i)$ and thus $f(x) \,|x^{q^n} - x$. □

We already know that an irreducible polynomial f of degree m over $\mathbb{F}_q$ can be used to construct $\mathbb{F}_{q^m}$. Since $\mathbb{F}_{q^m}$ is the splitting field of $x^{q^m} - x$ we now know that all roots of f are contained in $\mathbb{F}_{q^m}$.

Corollary 41 *Let $f \in \mathbb{F}_q[x]$ be irreducible of $\deg(f) = m$. Then $\mathbb{F}_{q^m}$ is the splitting field of f.*

The previous lemma is very useful as it states that every irreducible polynomial over $\mathbb{F}_p$ of degree n is a factor of $x^{p^n} - x$.
Even more is true:

Lemma 42 *The polynomial $f(x) = x^{q^n} - x$ is product of all monic, irreducible polynomials over $\mathbb{F}_q$ of degree dividing n.*

Proof. This lemma holds as each irreducible polynomial of degree m with $m|n$ divides f by Lemma 40, the polynomials are co-prime, and every irreducible polynomial of degree $m|n$ constructs a subfield of $\mathbb{F}_{q^n}$ and so its roots must satisfy f. $\square$
However, the degree of this polynomial grows very quickly so that it is not possible to obtain irreducible polynomials by factoring it.
We know already that for any degree m and any finite field $\mathbb{F}_q$ there exists at least one irreducible polynomial over $\mathbb{F}_q$ since the finite field $\mathbb{F}_{q^m}$ exists and has dimension m over $\mathbb{F}_q$. Now we can compute the number of irreducible polynomials of a given degree.

Corollary 43 *Let $N_q(d)$ be the number of irreducible polynomials over $\mathbb{F}_q$ of degree d. Then*

$$q^n = \sum_{d|n} dN_q(d).$$

In particular for all d and q we have $N_q(d) > 0$.

Corollary 38 shows that all roots (over some extension field) of a fixed irreducible polynomial give rise to the same field if adjoined to the ground field. Since for each order there is only one field up to isomorphism the resulting field is even independent of the choice of the polynomial.

Corollary 44 *Let $f, g \in \mathbb{F}_q[x]$ be irreducible, of the same degree $\deg(f) = \deg(g)$. Then their splitting fields are isomorphic.*

Exercise 45 *a) Find all irreducible polynomials of degree 1 and 2 over $\mathbb{F}_3$ and verify directly Lemma 42.*

b) Verify directly Lemma 42 for $n = 3$ and $q = 2$.

1.9 Conjugates, trace and norm

This section investigates connections between the roots of an irreducible polynomial and defines two important maps, the trace and the norm.

Lemma 46 *Let $f \in \mathbb{F}_q[x]$ be irreducible of degree m. Then f has a root α in $\mathbb{F}_{q^m}$ and all roots of f in $\mathbb{F}_{q^m}$ are different and given by*

$$\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}} \in \mathbb{F}_{q^m}.$$

Proof. By Corollary 41 f splits completely over $\mathbb{F}_{q^m}$ and it has m roots. Let β be some root of f, we now show that then also $f(\beta^q) = 0$. Let $f(x) = \sum_{i=0}^m a_i x^i$.

$$\begin{aligned} f(\beta^q) &= a_0 + a_1\beta^q + a_2(\beta^q)^2 + \ldots + a_m(\beta^q)^m,\ a_i \in \mathbb{F}_q \Rightarrow a_i^q = a_i \\ &= a_0^q + a_1^q\beta^q + a_2^q(\beta^2)^q + \ldots + a_m^q(\beta^m)^q \\ &= \left(a_0 + a_1\beta + a_2\beta^2 + \ldots + a_m\beta^m\right)^q \\ &= (f(\beta))^q = 0^q = 0. \end{aligned}$$

This shows that with α also α^q is a root and thus also $\alpha^{q^2}, \ldots, \alpha^{q^{m-1}}$ are roots of $f(x)$.

If any two of these powers would coincide, e.g. $\alpha^{q^i} = \alpha^{q^j}$ for some $0 \leq i < j \leq m-1$, then we would have $\alpha^{q^{m-j+i}} = \alpha^{q^m} = \alpha$ and α would satisfy a polynomial of degree $m - j + i < m$ which contradicts the definition of α as root of an irreducible polynomial of degree m. $\square$

The roots are thus q-th powers of one-another.

Definition 47 (Conjugates)
Let $\mathbb{F}_{q^m}$ be an extension field of $\mathbb{F}_q$ and let $\alpha \in \mathbb{F}_{q^m}$.
The elements $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}$ are called the conjugates of α.

We know the term "conjugates" from the complex numbers. Indeed there it refers to the same concept:

Example 48 *The field of complex numbers has degree $[\mathbb{C} : \mathbb{R}] = 2$ over the reals and we obtain $\mathbb{C}$ as $\mathbb{C} \cong \mathbb{R}[x]/(x^2+1)\mathbb{R}[x]$. The roots of x^2+1 are $i = \sqrt{-1}$ and $-i$. For $a_0 + a_1 i \in \mathbb{C}$ the conjugate is traditionally defined as $\overline{(a_0 + a_1 i)} = a_0 - a_1 i$. So the conjugate is obtained by changing the root of the irreducible polynomial.*

Example 49 *Let $[\mathbb{F}_{q^m} : \mathbb{F}_q] = m$ and let $f(x) \in \mathbb{F}_q[x]$ be irreducible of degree m and let the roots of $f(x)$ be $\beta, \beta^q, \ldots, \beta^{q^{m-1}}$. By Lemma 38 we have $\mathbb{F}_{q^m} \cong \mathbb{F}_q[x]/f\mathbb{F}_q[x] \cong \mathbb{F}_q(\beta)$. Let $\alpha = a_0 + a_1\beta + a_2\beta^2 + \cdots + a_{m-1}\beta^{m-1}$. The conjugate α^q of α is given by*

$$\begin{aligned} \alpha^q &= a_0^q + a_1^q\beta^q + a_2\beta^2 + \ldots + a_{m-1}^q \left(\beta^q\right)^{m-1},\ a_i \in \mathbb{F}_q \\ &= a_0 + a_1\beta^q + a_2 \left(\beta^q\right)^2 + \ldots + a_{m-1} \left(\beta^q\right)^{m-1} \end{aligned}$$

and so also in the case of finite fields the conjugates are obtained by changing the root in the representation.

We note that computing q-powers is a homomorphism of the field to itself. In the context of extension fields we need a more detailed definition.

Definition 50 (Automorphism of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$)
An automorphism of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ is an isomorphism of $\mathbb{F}_{q^m}$ that leaves every element of $\mathbb{F}_q$ invariant.

Note that it is not enough that the field $\mathbb{F}_q$ is kept invariant, each individual element must remain fixed.

Lemma 51 *The automorphisms of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ are exactly the maps $\sigma_0, \sigma_1, \ldots, \sigma_{m-1}$, where $\sigma_i(\alpha) = \alpha^{q^i}$ for $\alpha \in \mathbb{F}_{q^m}$ and $0 \leq i \leq m-1$.*

Proof. The maps σ_i are field homomorphisms by Exercise 9.
For any $0 \leq i \leq m-1$ one has that the only element α with $\sigma_i(\alpha) = \alpha^{q^i} = 0$ is $\alpha = 0$ and thus the maps are injective. Since they operate of finite sets of the same cardinality they are also surjective and thus they are isomorphisms.
The elements of $a \in \mathbb{F}_q$ are exactly those elements in $\mathbb{F}_{q^m}$ which satisfy $a^q = a$ and thus each σ_i leaves any element of $\mathbb{F}_q$ fix.
On a finite set every isomorphism can be described as a polynomial. The field $\mathbb{F}_q$ is defined as the set of roots of $x^q - x$ and so every automorphism of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ must be a power of σ. Since $\sigma_m = \sigma_0$ these are all possibilities. □

Definition 52 (Frobenius automorphism)
The automorphism $\sigma = \sigma_0$ is called the Frobenius automorphism. *It operates by raising each element to the q-th power.*

Definition 53 (Trace)
Let $\alpha \in \mathbb{F}_{q^m}$. The relative trace of α over $\mathbb{F}_q$ *denoted by* $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha)$ *is given by*

$$\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) = \alpha + \alpha^q + \cdots + \alpha^{q^{m-1}}.$$

If $\mathbb{F}_q = \mathbb{F}_p$ is a prime field then $\mathrm{Tr}_{\mathbb{F}_{p^m}/\mathbb{F}_p}$ is called the absolute trace *or just* trace. *In this case the index of* Tr *is often skipped.*

With the notation from above the trace $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha)$ of α is the sum of all conjugates of α over $\mathbb{F}_{q^m}$. We now define the multiplicative analogue.

Definition 54 (Norm)
Let $\alpha \in L = \mathbb{F}_{q^m}$ and put $K = \mathbb{F}_q$. The relative norm of α over $\mathbb{F}_q$ *of α over K denoted by $\mathrm{N}_{L/K}(\alpha)$ is given by*

$$N_{L/K}(\alpha) = \alpha \cdot \alpha^q \cdot \ldots \cdot \alpha^{q^{m-1}}.$$

Lemma 55 *The images of the relative trace map and of the relative norm map are contained in $\mathbb{F}_q$*

$$\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) \in \mathbb{F}_q,\ \mathrm{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) \in \mathbb{F}_q,$$

for all $\alpha \in \mathbb{F}_{q^m}$.

Proof. Let $m_\alpha(x) \in \mathbb{F}_q[x]$ be the minimal polynomial of α over $\mathbb{F}_q$ and let $m_\alpha(x) = \sum_{i=0}^{r} a_i x^i$ for some $r = [\mathbb{F}_q(\alpha) : \mathbb{F}_q]$. By Lemma 37 we have $r|m$ and m_α defines an extension field $\mathbb{F}_{q^r}$ of $\mathbb{F}_q$. Lemma 46 we have

$$\begin{aligned}
\prod_{i=0}^{m-1}\left(x - \alpha^{q^i}\right) &= \prod_{i=0}^{r-1}\left(x - \alpha^{q^i}\right) \cdot \prod_{i=0}^{r-1}\left(x - \alpha^{q^{i+r}}\right) \cdot \ldots \cdot \prod_{i=0}^{r-1}\left(x - \alpha^{q^{i+r(\frac{m}{r}-1)}}\right) \\
&= \underbrace{\prod_{i=0}^{r-1}\left(x - \alpha^{q^i}\right) \cdot \ldots \cdot \prod_{i=0}^{r-1}\left(x - \alpha^{q^i}\right)}_{\frac{m}{r} \text{ times}} \\
&= m_\alpha(x)^{\frac{m}{r}}
\end{aligned}$$

Since $m_\alpha \in \mathbb{F}_q[x]$ also its $\frac{m}{r}$-th power has all coefficients in $\mathbb{F}_q$. The coefficient of the second highest term equals $-(\alpha + \alpha^q + \cdots + \alpha^{q^{m-1}}) = -\mathrm{Tr}(\alpha)$ while the constant term equals the norm.
By comparison we obtain

$$r\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) = -ma_{m-1} \in \mathbb{F}_q$$

and

$$\mathrm{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) = a_0^{\frac{m}{r}} \in \mathbb{F}_q.$$

□

We note some properties of the trace.

Lemma 56 *Let L be a finite extension of K with $[L:K] = m$ and let $\alpha, \beta \in L, c \in K$. For the relative trace $\mathrm{Tr}_{L/K}$ we have:*

1. $\mathrm{Tr}_{L/K}(\alpha + \beta) = \mathrm{Tr}_{L/K}(\alpha) + \mathrm{Tr}_{L/K}(\beta)$,
2. $\mathrm{Tr}_{L/K}(c \cdot \alpha) = c \cdot \mathrm{Tr}_{L/K}(\alpha)$,
3. $\mathrm{Tr}_{L/K}(c) = m \cdot c$,
4. $\mathrm{Tr}_{L/K}(\alpha^q) = \mathrm{Tr}_{L/K}(\alpha)$.

Proof. Given below as homework. □

One also has the corresponding properties of the norm.

Lemma 57 *Let L be a finite extension of K with $[L:K] = m$ and let $\alpha, \beta \in L, c \in K$. For the relative norm $\mathrm{N}_{L/K}$ we have:*

1. $\mathrm{N}_{L/K}(\alpha \cdot \beta) = \mathrm{N}_{L/K}(\alpha) \cdot \mathrm{N}_{L/K}(\beta)$,
2. $\mathrm{Im}(\mathrm{N}_{L/K}) = K$ *and* $\mathrm{Im}(\mathrm{N}_{L/K|_{F^*}}) = K^*$
3. $\mathrm{N}_{L/K}(c) = c^m$,
4. $\mathrm{N}_{L/K}(\alpha^q) = \mathrm{N}_{L/K}(\alpha)$.

Proof. Given below as homework. □

Exercise 58 *a) Prove Lemma 56 by just using the definition.*

b) Prove Lemma 57 by just using the definition.

1.10 Irreducible polynomials

As stated before it is too expensive to factor $x^{q^m} - x$ over $\mathbb{F}_q$ to find an irreducible polynomial of degree m over $\mathbb{F}_q$ and to construct the extension field $\mathbb{F}_{q^m}$. A more careful analysis of the number $N_q(d)$ of irreducible polynomials of degree d over $\mathbb{F}_q$ given in Corollary 43 gives the probability that a randomly chosen polynomial of degree d is irreducible.
In this section we state a criterion to determine whether a given polynomial is irreducible. There is a vast literature on factorization of polynomials over finite fields and on constructing irreducible polynomials. We would like to refer the interested reader to a few books covering this topic.

- H. Cohen, "A Course in Computational Algebraic Number Theory", Springer
- J. von zur Gathen and J. Gerhard, "Modern Computer Algebra", Cambrigde University Press.
- M. Pohst and H. Zassenhaus, "Algorithmic Algebraic Number Theory", Cambridge University Press.

and the books by Lidl and Niederreiter and by Shoup mentioned in the introduction to this chapter.
We present here the *Rabin test* which allows to test whether a polynomial is irreducible.

Lemma 59 (Rabin test)
The polynomial $f(x) \in \mathbb{F}_q[x]$ of degree $\deg(f) = m$ is irreducible if and only if

$$f(x) \big| x^{q^m} - x$$

and for all divisors $d|m$ one has

$$\gcd(f(x), x^{q^d} - x) = 1.$$

Proof. We first note that all conditions hold for an irreducible polynomial of degree m. It remains to be shown that they are sufficient. Let f split into factors $f = f_1 \cdots f_r$ over $\mathbb{F}_q$, where $r \geq 1$.
By Lemma 42 $x^{q^m} - x$ is the product of all irreducible polynomials of degree dividing m. So if the first property holds we must have $\deg(f_i)|m$ for $1 \leq i \leq r$. If $r > 1$ the degree $\deg(f_1)$ equals one of the d in the second round of tests and $f_1 | x^{q^d} - x$ for this d. So f is only if also the second property holds.
Since any factor of f must lead to a non-trivial gcd for some d we also have that this condition is sufficient. □

For efficiency it might be interesting to note that one can release the second property to testing only that for all prime divisors $\ell|m$ one has

$$\gcd(f, x^{q^{m/\ell}} - x) = 1.$$

For a random polynomial it is likely that the condition $\gcd(f, x^{q^d} - x) = 1$ fails for some small d so that it is computationally more efficient to have an early abort after it. If, however, the candidate polynomial is likely to be irreducible and thus all checks are expected to be done anyway this observation saves running time.

Example 60 *Find an irreducible polynomial of the form $x^3 - a$ over $\mathbb{F}_7$. This can still be done by a naive approach since a polynomial of degree 3 is irreducible if and only if it does not have a root. In this case if $a \neq 0, 1, -1$. So $x^3 - 2$ is irreducible.*
Use of the Magma online calculator available at
`http://magma.maths.usyd.edu.au/calc/` *makes it easy to implement the Rabin test and it even comes with a built-in in function* `IsIrreducible`*.*

Irreducible polynomials with only two terms as considered in this example are interesting for constructing finite fields. In low weight polynomials have special names.

Definition 61 (Binomial, trinomial, pentanomial) *A polynomial of the form $x^n + a_0$ with two non-zero coefficients is called a* binomial.
A polynomial of the form $x^n + a_m x^m + a_0$ with three non-zero coefficients is called a trinomial.
A polynomial of the form $x^n + a_m x^m + a_l x^l + a_k x^k + a_0$ with five non-zero coefficients is called a pentanomial.

We first note that over $\mathbb{F}_2$ there cannot be an irreducible binomial as 0 or 1 would be a root. It is a bit more surprising that there cannot be an irreducible binomial of even degree over $\mathbb{F}_2^n$.
The following lemma considers irreducible binomials over arbitrary finite fields.

Lemma 62 *Let n be prime. An irreducible binomial $f(x) = x^n + a_0$ of degree n over $\mathbb{F}_q$ exists if and only if $n|q-1$.*

Proof. If $n \nmid q-1$ then the map $\tau : \mathbb{F}_q \to \mathbb{F}_q; a \mapsto a^n$ is a bijection by Corollary 17 and thus every element a_0 is an n-th power and any binomial of degree n has a linear factor over $\mathbb{F}_q$.
If, however, $n|q-1$ then τ has a non-trivial kernel and each element in the image has n pre-images. Choose $a_0 \notin \mathrm{Im}(\tau)$ and so f has no linear factor over $\mathbb{F}_q$. Then the last property of the Rabin test holds since n is prime.
For the first property note that $n|q-1$ implies that there is some integer k with $q = 1+kn$ and thus $q^n - 1 = (1+kn)^n - 1 = 1 + nkn + \binom{n}{2}(kn)^2 + \cdots (kn)^n - 1 = n^2 k\ell = n(q-1)\ell$ for some ℓ.To show that $f(x) = x^n + a_0$ divides $x^{q^n} - x$ note

$$x^{q^n} - x = x(x^{q^n-1} - 1) = x(x^{n(q-1)\ell} - 1) \equiv x(a_0^{(q-1)l} - 1) = x(1-1) = 0 \bmod x^n + a_0$$

using $a_0^{q-1} = 1$. □

1.11 Arithmetic in binary fields

In Section 1.6 we have seen that an extension field $\mathbb{F}_{q^n}$ of $\mathbb{F}_q$ can be represented using a polynomial basis. Let $f(x) \in \mathbb{F}_q[x]$ be an irreducible polynomial of degree n. Then we have by Lemma 37 that

$$\mathbb{F}_{q^n} \cong \mathbb{F}_q[x]/f(x)\mathbb{F}_q[x] = \left\{ \sum_{i=0}^{n-1} a_i x^i + f(x)\mathbb{F}_q[x] \middle| a_i \in \mathbb{F}_q \right\}.$$

In this section we consider the special case $q = 2$ which is very important for applications, particularly for hardware implementations. An advantage of such *binary fields* is that additions are `XOR`s and that in squarings no mixed terms need to be considered as by Exercise 9 we have $(a+b)^2 = a^2 + b^2$.
For multiplications and squarings it is necessary to reduce the resulting polynomial of degree $\geq n$ modulo the irreducible polynomial $f(x)$ to obtain the unique remainder modulo f of degree less than n.

Example 63 *The polynomial* $f(x) = x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1 \in \mathbb{F}_2[x]$ *is irreducible. To compute the product* $(x^9+x^7+x^4+x^2+1)\cdot(x^8+x^6+x^5+x^3+x^2)$ *in* $\mathbb{F}_{2^{10}}$ *we first compute the product in* $\mathbb{F}_2[x]$ *and then reduce the result modulo* $f(x)$*. The steps are as follows:*

$$
\begin{aligned}
&(x^9+x^7+x^4+x^2+1)\cdot(x^8+x^6+x^5+x^3+x^2) = \\
&x^{17}+x^{14}+x^{13}+x^{12}+x^{11}+x^{10}+x^4+x^3+x^2 = \\
&x^7\cdot x^{10}+x^{14}+x^{13}+x^{12}+x^{11}+x^{10}+x^4+x^3+x^2 = \\
&(x^{16}+x^{15}+x^{14}+x^{13}+x^{12}+x^{11}+x^{10}+x^9+ \\
&\qquad +x^8+x^7)+x^{14}+x^{13}+x^{12}+x^{11}+ \\
&\qquad +x^{10}+x^4+x^3+x^2 = \\
&x^{16}+x^{15}+x^9+x^8+x^7+x^4+x^3+x^2 = \\
&x^6\cdot x^{10}+x^{15}+x^9+x^8+x^7+x^4+x^3+x^2 = \\
&x^{14}+x^{13}+x^{12}+x^{11}+x^{10}+x^6+x^4+x^3+x^2 = \\
&x^4\cdot x^{10}+x^{13}+x^{12}+x^{11}+x^{10}+x^6+x^4+x^3+x^2 = \\
&= x^9+x^8+x^7+x^5+x^3+x^2.
\end{aligned}
$$

Note, that $g(x) = x^{10}+x^3+1$ *is an irreducible polynomial of degree* 10 *over* $\mathbb{F}_2$*. Reducing modulo* g *has much easier iterations since* x^{10} *is replaced by only two terms* x^3+1*. Since* g *is sparse it also becomes useful to replace more than one power simultaneously.*

$$
\begin{aligned}
&(x^9+x^7+x^4+x^2+1)\cdot(x^8+x^6+x^5+x^3+x^2) = \\
&x^{17}+x^{14}+x^{13}+x^{12}+x^{11}+x^{10}+x^4+x^3+x^2 = \\
&x^7\cdot x^{10}+x^{14}+x^{13}+x^{12}+x^{11}+x^{10}+x^4+x^3+x^2 = \\
&(x^{10}+x^7)+x^{14}+x^{13}+x^{12}+x^{11}+x^{10}+x^4+x^3+x^2 = \\
&x^{14}+x^{13}+x^{12}+x^{11}+x^7+x^4+x^3+x^2 = \\
&(x^4+x^3+x^2+x)\cdot x^{10}+x^4+x^3+x^2 = \\
&x^6+x^5+x^4+x.
\end{aligned}
$$

We deduce from this example that it is useful to choose irreducible polynomials with as few terms as possible.

Lemma 64 *For all* $n, m \in \mathbb{N}, n > 1$ *the binomial* $x^n + x^m \in \mathbb{F}_2[x]$ *is not irreducible. More generally, there is no irreducible polynomial over* $\mathbb{F}_2$ *with an even number of nonzero terms.*

Proof. If $m > 0$ then $x^n + x^m$ is divisible by x^m and thus not irreducible. If $m = 0$ we see that 1 is a root of $x^n + 1$.
Consider $f(x) = \sum_{i=1}^{2m} x^{k_i}$, where $k_i < k_{i+1}$ for all $1 \leq i \leq 2m-1$. If $k_1 > 0$ we have that x^{k_0} divides $f(x)$ while otherwise 1 is a root of it since we are working in characteristic 2. □

As the example showed, there are extension degrees n for which there exists an irreducible polynomial of degree n with only 3 nonzero terms. Polynomials with 3 nonzero terms are called *trinomials*. To construct $\mathbb{F}_{2^n}$ for a given n, it is best to use an irreducible trinomial is one exists. Note that if an irreducible trinomial exists there is one $x^n + x^m + 1$ for which $m \leq n/2$.
By the lemma we know that there are no irreducible polynomials with 4 nonzero coefficients, so if no suitable trinomial exists one should search for an irreducible *pentanomial*. It is conjectured that for all binary fields for which there is no irreducible trinomial one can find an irreducible pentanomial. Even though this is not proven, all fields of cryptographic interest have been checked. So in applications we can always find an irreducible trinomial or pentanomial.
For a table of irreducible polynomials consult Gadiel Seroussi's paper "Table of Low-Weight Binary Irreducible Polynomials".

Remark 65 *For more details on the implementation of binary fields the reader is encouraged to check the literature for* normal basis *representations. A normal basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ is a basis of the form $\{\theta, \theta^2, \theta^{2^2}, \theta^{2^3}, \ldots, \theta^{2^{n-1}}\}$. Note that for most values $\alpha \in \mathbb{F}_{2^n}$ the conjugates of α do not form a basis, so* normal elements *are special.*
An advantage of normal bases is that they lead to very fast squarings:

$$\textit{If } a = \sum_{i=0}^{n-1} a_i \theta^{2^i} \textit{ then } a^2 = \sum_{i=0}^{n-1} a_{i-1} \theta^{2^i},$$

where the index i of a_i is considered modulo n. This means that a squaring can be implemented as a cyclic shift of the coordinates from $(a_0, a_1, \ldots, a_{n-1}, a_{n-2})$ to $(a_{n-1}, a_0, a_1, \ldots, a_{n-2})$. Likewise, squareroots can be implemented by a cyclic left-shift. On the downside, in software multiplications are usually less efficient than in a polynomial basis. So it depends on the application and in particular on the importance of squarings in it whether a normal basis or a polynomial basis representation should be chosen. In hardware implementation the situation is yet again different and normal bases can be the clear winner.

Exercise 66 *1. State all irreducible polynomials of degree 3 and of degree 4 over $\mathbb{F}_2$.*

2. *The polynomial $f(x) = x^{97} + x^6 + 1$ is irreducible over $\mathbb{F}_2$. We can use it to construct $\mathbb{F}_{2^{97}} \cong \mathbb{F}_2[x]/f(x)\mathbb{F}_2[x]$. Compute $(x^{86} + x^{25} + x^{13} + x^4 + x + x^2 + 1) \cdot (x^{83} + x^{31} + x^{17} + x^7 + x^3)$ modulo $f(x)$.*

3. *The polynomial $g(x) = x^{89} +^6 + x^5 + x^3 + 1$ is irreducible over $\mathbb{F}_2$. We can use it to construct $\mathbb{F}_{2^{89}} \cong \mathbb{F}_2[x]/g(x)\mathbb{F}_2[x]$. Compute $(x^{86} + x^{25} + x^{13} + x^4 + x + x^2 + 1) \cdot (x^{83} + x^{31} + x^{17} + x^7 + x^3)$ modulo $g(x)$. Compare the time you needed for the multiplication in this exercise and in the previous one. Note that the previous one deals with a larger finite field.*

1.12 Arithmetic in prime fields

There exists a vast amount of literature on fast implementations of prime fields. We do not go into the details here but comment that to speed up modular reductions it is useful to choose primes which are close to a power of 2, or even better close to a power of 2^w, where w is the word size, i.e. $p = (2^w)^k - c$, where $c \in \mathbb{N}$ is small. This approach is analogous to choosing irreducible trinomials in binary fields.

1.13 Arithmetic in optimal extension fields

Optimal extension fields (OEFs) are finite fields $\mathbb{F}_{q^n}$ where the base field $\mathbb{F}_q$ and the extension degree n are chosen such that arithmetic in $\mathbb{F}_q$ can be implemented particularly fast. A common choice for the base field is $\mathbb{F}_q = \mathbb{F}_p$, a prime field, such that p fits into the word size and is close to a power of two, i.e. $p = \texttt{PreviousPrime}(2^w)$, where w is the word-size. The extension degree n is often chosen to be prime, particularly in applications to elliptic curve cryptography – we will not go into the details here but mention that Weil descent attacks on elliptic curves may apply when the extension degree is not prime. As we have seen in the section on binary fields, it is interesting to work with irreducible polynomials with few nonzero coefficients. If q is odd we can hope for irreducible *binomials*.

Lemma 67 *Let n and p be primes such that $p \equiv 1 \bmod n$. The binomial $x^n - a$ is irreducible over $\mathbb{F}_p$ if and only if a is not an nth power in $\mathbb{F}_p$.*

Proof. If a is an nth power in $\mathbb{F}_p$, i.e. there exists a $b \in \mathbb{F}_p$ with $b^n = a$, then clearly $x^n - a$ is not irreducible since b is a root.
If a is not an nth power then there is no root of $f(x) = x^n - a$ over $\mathbb{F}_p$. The condition $n \equiv 1 \bmod p$ means that the nth roots of unity are in $\mathbb{F}_p$, i.e. there are n elements $u_i \in \mathbb{F}_p, 1 \leq i \leq n$ with $u_i^n = 1$. To fix notation let $u_1 = 1$. Let α be a root of $f(x)$ over some extension field $\mathbb{F}_{p^m}$. The multiples $u_i\alpha$ for $2 \leq i \leq n$ are distinct from α, are defined over the same extension field $\mathbb{F}_{p^m}$ and are also roots of $f(x)$ because

$$(u_i\alpha)^n = u_i^n\alpha^n = \alpha^n = a.$$

Since there are n of them they are exactly the roots of $f(x)$ and so they are the conjugates of α. This means that α is defined over a field of extension degree no less than n, and so α is defined exactly over $\mathbb{F}_{p^n}$. We have $\mathbb{F}_{p^n} \cong \mathbb{F}_p(\alpha) \cong \mathbb{F}_p[x]/(x^n - a)\mathbb{F}_p$. □

Following this lemma, optimal extension fields are finite fields $\mathbb{F}_{p^n}$ for which p is a prime closely related to the word-size, n satisfies $n \equiv 1 \bmod p$ and the extension field is constructed with an irreducible binomial $f(x) = x^n - a$.