Finite Field Extensions: Uniqueness and Existence

Mathematics Seminar at Kyiv School of Economics

Dmytro Zakharov

Abstract

This small lecture is devoted to a quick glance at the structure of finite fields, primarly based on [IR90, Chapter 7]. One obvious well-known example of the finite field is $\mathbb{Z}/p\mathbb{Z}$, but is this the only possible finite field? We first show the explicit construction of the finite field of order p^n for prime p and build the intuition of how elements of such fields look like. We then show that *(i)* p^n is the only possible such a finite field order, *(ii)* always possible regardless of the chosen characteristic p, and *(iii)* such construction is unique (up to an isomorphism).

Contents

1 Introduction

In this section, we *informally* introduce finite field extensions and specify how to think of them. We will demonstrate how to build quadratic field extensions and show how one constructs higher-degree field extensions.

1.1 Basic Notions

For the sake of completeness, we recall what is a field and introduce some basic notation.

Definition 1.1 (Finite Field). Recall that K is a **field** if:

- $(K, +)$ and $(K \setminus \{0\}, \times)$ form abelian groups. We denote the latter group simply by $K^\times$.
- Distributive law holds: $a(b+c) = ab + ac$ for arbitrary $a, b, c \in K$.

Field K is **finite** if it contains the finite number of elements q. In such case, one commonly denotes such a field by $\mathbb{F}_q$ or even $\mathrm{GF}(q)$ (latter is more common in Computer Science).

The most basic example of such a field is the **prime field** $\mathbb{Z}/p\mathbb{Z}$ or simply $\mathbb{F}_p$. For instance, for $p = 5$, one can perform operations over $\mathbb{F}_5$ as follows:

$$2 + 4 = 1, \quad 3 \cdot 4 = 2, \quad 3^{-1} = 2 \quad (\textit{all over } \mathbb{F}_5)$$

Motivating Question. Is this the only form of a finite field?

1.2 Quadratic Field Extensions

Of course the answer is negative. Let us give the example of the field with p^2 elements.

Example. Suppose it so happens that $p \equiv 3 \pmod 4$. Then, the following quotient ring

$$\mathbb{F}_{p^2} \cong \mathbb{F}_p[x]/\langle x^2 + 1\rangle$$

is a finite field with p^2 elements.

Proof. Recall that $K[x]/\langle f(x)\rangle$ is a field iff $f(x) \in K[x]$ is irreducible over field K. Thus it suffices to show that x^2+1 is irreducible over $\mathbb{F}_p$ for $p \equiv 3 \pmod 4$. This reduces down to showing that -1 is not a quadratic residue in $\mathbb{F}_p$. Accoring to Euler's criterion, one has $\left(\frac{-1}{p}\right) \equiv (-1)^{(p-1)/2} \pmod p$. Since $p = 4m + 3$, we obtain $\left(\frac{-1}{p}\right) = (-1)^{2m+1} = -1$, so -1 is a quadratic non-residue. This proves that $\mathbb{F}_p[x]/\langle x^2 + 1\rangle$ is a field. Since such field consists of linear polynomials $\alpha + \beta x$ with $\alpha, \beta \in \mathbb{F}_p$, we conclude that such finite field indeed consists of p^2 elements. □

Example. In fact, $\mathbb{F}_{p^2}$ greatly resembles complex numbers $\mathbb{C}$ (especially if we use i to denote the variable x). For instance, letting $p = 19$, operations in $\mathbb{F}_{361} \cong \mathbb{F}_{19}(i)$ look as follows:

$$\begin{aligned} \textbf{Addition:} \quad & (1 + 10i) + (18 + 15i) = 19 + 25i = 6i \\ \textbf{Multiplication:} \quad & (5 + 6i)(6 + 7i) = 30 + 71i + 42i^2 = 7 + 14i. \end{aligned}$$

Remark. In fact, for other primes $p > 2$ (such that $p \equiv 1 \pmod 4$) one might use the similar construction: $\mathbb{F}_{p^2} \cong \mathbb{F}_p[x]/\langle x^2 + \alpha\rangle$ for quadratic non-residue α. It is well-known that for every $p > 2$ we can find at least one quadratic non-residue (moreover, there are exactly $\frac{p-1}{2}$ of them).

In fact, $\mathbb{F}_{p^2}$ is a *field extension* of $\mathbb{F}_p$. We will not define field extensions rigorously nor rely on Galois theory extenstively, but we will need the following fact: if L/K is a field extension (roughly speaking, L is a field containing smaller field K), then L is a K-vector space. We further denote the dimensionality of L (viewed as a K-vector space) as $[L : K]$.

As an example, $\mathbb{F}_{p^2}$ constructed above is a field extension of $\mathbb{F}_p$ since *(i)* $\mathbb{F}_p \subset \mathbb{F}_{p^2}$ and *(ii)* $\mathbb{F}_{p^2}$ is a field. Therefore, it is a linear space with scalars from $\mathbb{F}_p$. Specifically, the basis is given by $\{1, i\}$. In Proposition 3.3, we will formalize this intuition more systematically and formally.

1.3 Explicit Construction for $\mathbb{F}_{p^n}$

Now we notice that extending the previous construction to the n-degree extension should be straightforward. Indeed, fix some polynomial $f \in \mathbb{F}_p[x]$ that is irreducible over $\mathbb{F}_p$ and such that $\deg f = n$. Then, the finite field extension $\mathbb{F}_{p^n}$ is defined as:

$$\mathbb{F}_{p^n} \cong \mathbb{F}_p[x]/\langle f(x)\rangle,$$

so elements of $\mathbb{F}_{p^n}$ are polynomials $\sum_{j=0}^{n-1} \alpha_j x^j$ with $\alpha_j \in \mathbb{F}_p$ and arithmetic is done "modulo $f(x)$".

The core three questions here are:

Q1 Can we find any other finite fields of order other than p^n?

Q2 Does such f always exist?

Q3 Can we construct another field K of order p^n such that $K \ncong \mathbb{F}_p[x]/\langle f(x)\rangle$?

All questions are in fact crucial. For instance, in the informal discussion above, we were quite sketchy with the notation $\mathbb{F}_{p^n}$. Suppose we had two finite fields, say, K_0 and K_1, of order p^n such that $K_0 \ncong K_1$. In such case, it would be unclear what we denote by $\mathbb{F}_{p^n}$: should it be the field K_0, the field K_1, or some class of such fields?

Since we give the positive answer to **Q2** and negative to **Q3**, such an issue with the definition does not arise. Specifically, we prove both facts in Section 3. But first, we need more fundamental mathematical preliminaries on finite fields, which we specify in Section 2.

2 Basic Properties of Finite Fields

In this section, we analyze finite fields more systematically and rigorously. Further always assume $K = \mathbb{F}_q$ is a finite field with order q. We shall first prove that $q = p^n$ for some prime p and natural n. Additionally, we analyze the structure of multiplicative and additive groups of K.

Lemma 2.1. For any finite field K of order q one has:

$$x^q - x = \prod_{\alpha \in K} (x - \alpha)$$

Proof. Notice that every $\alpha \in K$ is a root of $x^q - x$. Indeed, if $\alpha = 0$, the result is obvious. Otherwise, $\alpha^q - \alpha = \alpha(\alpha^{q-1} - 1)$ and since $K^\times$ is of order $q - 1$, this equates to zero as well. Thus, $\prod_{\alpha \in K}(x - \alpha)$ divides $x^q - x$. Since both polynomials are of degree q and the leading coefficient of both expressions is 1, we obtain the equality, as required. □

This result is fundamental for our further discussion. In particular, we provide the following two important corollaries.

Proposition 2.2. The following holds:

(i) Let L/K be the field extension. An element $\alpha \in K$ iff $\alpha^q = \alpha$.

(ii) For $f \in K[x]$, let $f(x) \mid (x^q - x)$ and $d := \deg f$. Then, f has d distinct roots.

Proof.

Part (i). $\alpha^q = \alpha$ iff it is a root of $x^q - x$. Since all roots of $x^q - x$ are exactly elements of K from Lemma 2.1, the result follows.

Part (ii). Suppose $f(x)g(x) = x^q - x$ with $\deg g = q - d$. If f had less than d distinct roots, then $f(x)g(x)$ would have fewer than q roots, which is not the case since $x^q - x$ has q roots. □

2.1 Properties of Multiplicative Subgroup

Now we shall discuss the properties of $K^\times$. We first prove the following fact.

Theorem 2.3. The multiplicative group of a finite field $K^\times$ is *cyclic*.

Proof. Fix $d \mid (q-1)$ and let K_d denote the set of elements of $K^\times$ of order d. Suppose $K_d \neq \emptyset$, so there exists some $\beta \in K_d$. Clearly, $\langle\beta\rangle \subseteq \{\alpha \in K^\times : \alpha^d = 1\}$ (since for any $\beta^i \in \langle\beta\rangle$, one has $(\beta^i)^d = (\beta^d)^i = 1$). But notice that $\langle\beta\rangle$ has a cardinality d, so $\langle\beta\rangle = \{\alpha \in K^\times : \alpha^d = 1\}$. Thus, K_d is a set of generators of $\langle\beta\rangle$ of order d, so $\#K_d = \varphi(d)$, where φ is the Euler totient function.

So we have proven that either $\#K_d = 0$ or $\#K_d = \varphi(d)$. So we shall prove that the latter is true for any $d \mid (q-1)$. Notice that we can count the number of elements in $K^\times$ as $\#K^\times = \sum_{d|(q-1)} \#K_d$. On the other hand, $\sum_{d|(q-1)} \#K_d \leq \sum_{d|(q-1)} \varphi(d) = q - 1$. Thus, $\#K_d = \varphi(d)$. In particular, by letting $d := q - 1$, one has $\#K_{q-1} = \varphi(q-1) > 0$, so the generator of $K^\times$ is any $\omega \in K_{q-1}$. □

Definition 2.4. The generators of $K^\times$ are called **primitive elements**.

Two important consequences of this fact are the following.

Proposition 2.5. If $d \mid (q-1)$, then there is a cyclic subgroup $G \leq K^\times$ of order d. If ω is the primitive element of K, the generator of G is $\omega^{(q-1)/d}$.

Proposition 2.6. Let $\alpha \in K^\times$. Then equation $x^n = \alpha$ has solutions iff $\alpha^{(q-1)/d} = 1$, where $d = \gcd(n, q-1)$. If there are solutions, then there are exactly d solutions.

Proof. Since $K^\times$ is cyclic, let $\langle\omega\rangle = K^\times$. Then, $\alpha = \omega^a$ for some a. Since $x = 0$ is clearly not a solution, then $x \in K^\times$, so let $x = \omega^y$. Thus, we have an equation $\omega^{ny} = \omega^a$ with respect to y. This clearly reduces down to equation $ny \equiv a \pmod{q-1}$. It is then well-known that this equation is solvable iff $d = \gcd(n, q-1) \mid a$ and the number of solutions is d. But $d \mid a$ iff $\alpha^{(q-1)/d} = 1$. □

We have investigated the structure of $K^\times$. Let us now turn our attention of the additive subgroup of K which would give us information on the possible values of $\#K$.

2.2 Properties of Additive Subgroup

Lemma 2.7. Let K be a finite field. Denote by $\langle e\rangle_+$ the set, additively generated by identity e of $K^\times$. Then, $\langle e\rangle_+$ is a subfield of K, isomorphic to $\mathbb{Z}/p\mathbb{Z}$ for some prime number p.

Proof. Define morphism $\phi : \mathbb{Z} \to K, n \mapsto ne$. Note that $\langle e\rangle_+ = \mathrm{im}(\phi)$. We also notice that

ϕ is clearly a ring homomorphism. Therefore, $\mathrm{im}(\phi)$ forms a finite subring of K, so in particular, it is an integral domain. Recall that $\mathbb{Z}/\ker(\phi) \cong \mathrm{im}(\phi)$ due to first isomorphism theorem, so in particular $\mathbb{Z}/\ker(\phi)$ is an integral domain. Therefore, $\ker(\phi)$ is a prime ideal, so $\ker(\phi) = p\mathbb{Z}$ for some prime p. Thus we conclude $\langle e \rangle_+ = \mathrm{im}(\phi) \cong \mathbb{Z}/p\mathbb{Z}$. □

Definition 2.8. Let K be a finite field and e an identity of $K^\times$. The (prime) number p is called a **characteristic** of K (and denoted as $\mathrm{char}(K)$) if $\langle e \rangle_+ \cong \mathbb{Z}/p\mathbb{Z}$.

We shall finally prove the theorem on the number of elements in K.

Theorem 2.9. Let K be a finite field. Then, $\#K = p^n$ where p is a characteristic of K.

Proof. From Lemma 2.7, we know that $\mathbb{F}_p$ is a subfield of K for some prime p. Notice that K is a $\mathbb{F}_p$-vector space. Let $[K : \mathbb{F}_p] = n$. Then, there exists a basis, say, $\beta_1, \ldots, \beta_n \in K$, such that any $\beta \in K$ can be written as $\beta = \sum_{i=1}^{n} \alpha_i \beta_i$ with $\alpha_i \in \mathbb{F}_p$. There are clealy p^n elements in K. □

Proposition 2.10 (Freshman's Dream). Suppose K has a characteristic of p. Then, $(\alpha+\beta)^{p^d} = \alpha^{p^d} + \beta^{p^d}$ for any finite field elements $\alpha, \beta \in K$ and any positive integer d.

Proof. We prove this fact by induction. For $d = 1$, notice

$$(\alpha + \beta)^p = \sum_{j=0}^{p} \binom{p}{j} \alpha^j \beta^{p-j}.$$

Notice that for each $j \neq 0$ and $j \neq p$, one has $p \mid \binom{p}{j}$. Thus, all terms except for $j = 0$ and $j = p$ vanish, so we conclude $(\alpha + \beta)^p = \alpha^p + \beta^p$.

Now suppose this formula holds for d, that is $(\alpha + \beta)^{p^d} = \alpha^{p^d} + \beta^{p^d}$. Raise both sides by the power of p. In such case, left-hand side is exactly $(\alpha + \beta)^{p^{d+1}}$. The right-hand side, after applying the result from the induction base, one gets $\alpha^{p^{d+1}} + \beta^{p^{d+1}}$. □

3 Uniqueness and Existence

3.1 Preliminaries

Proposition 3.1. Let K be a field. Then, $(x^\ell - 1) \mid (x^m - 1)$ in $K[x]$ iff $\ell \mid m$.

Proof. We first show that $\ell \mid m$ implies $(x^\ell - 1) \mid (x^m - 1)$. If $\ell \mid m$, then $m = n\ell$ for some integer n. Then,

$$\frac{x^m - 1}{x^\ell - 1} = \frac{x^{n\ell} - 1}{x^\ell - 1} = \sum_{j=0}^{n-1} x^{j\ell} \in K[x]$$

Now we show the opposite direction. Suppose $m = n\ell + r$ with $0 \leq r < \ell$. Then we have

$$\frac{x^m - 1}{x^\ell - 1} = \frac{x^{n\ell+r} - 1}{x^\ell - 1} = \frac{x^{n\ell} x^r - 1}{x^\ell - 1} = x^r \cdot \frac{x^{n\ell} - 1}{x^\ell - 1} + \frac{x^r - 1}{x^\ell - 1}$$

As we have already shown, $(x^{n\ell} - 1)/(x^\ell - 1) \in K[x]$, so in order for the left-hand side to be a polynomial, $(x^r - 1)/(x^\ell - 1)$ must be a polynomial. Since degree of $x^r - 1$ is r, which is less than the degree in the denominator (which is ℓ), the only case when $(x^\ell - 1) \mid (x^r - 1)$ is $r = 0$. □

We shall finally show that for d, there is an in irreducible polynomial in $\mathbb{F}_p[x]$ of degree d. We first provide and show the more general fact.

Proposition 3.2. Suppose K is a field and $f \in K[x]$ is irreducible over K. There exists some other field $L \supset K$ and an element $\alpha \in L$ such that $f(\alpha) = 0$.

Proof. Recall that $K[x]$ is a principal ideal domain. Therefore, $\langle f(x) \rangle$ is a maximal ideal and therefore $K[x]/\langle f(x) \rangle$ is a field. Let $K' := K[x]/\langle f(x) \rangle$ and let $\iota : K[x] \to K'$ be the natural homomorphism, mapping element from $K[x]$ to the representative in K'. We shall prove that indeed K is a subfield of K'. For that, we shall prove that $\iota|_K \cong K$. Indeed, suppose $\gamma \in K$. If $\iota(\gamma) = 0$, then $\gamma \in \langle f(x) \rangle$. In other words, $\gamma = f(x)h(x)$ for some $h \in K[x]$. Since $\deg f > 0$, the only possibility of this is when $\gamma = 0$. Therefore, $\iota|_K$ is one-to-one. Since it is obviously surjective, it is a bijection (and thus an isomorphism).

To finish the proof, we construct α. Take $\alpha := x + \langle f(x) \rangle$ in K'. Then, $f(\alpha) = f(x + \langle f(x) \rangle) = f(x) = 0$ in K'. Thus, we have proven the proposition. □

Further, denote by $K(\alpha)$ the polynomial K' constructed as in the proof above.

Proposition 3.3. The elements $1, \alpha, \ldots, \alpha^{n-1}$ form a basis for $K(\alpha)/K$ with $n = \deg f$.

Proof. First we show linear independence. Suppose that we have a linear combination that vanishes: $\sum_{j=0}^{n-1} c_j \alpha^j = 0$. Define polynomial $h(x) := \sum_{j=0}^{n-1} c_j x^j$. Then, we have $h(\alpha) = 0$. Then, either h is a multiple of f or 0. Since degree of f is n, we conclude that h is a zero polynomial, so the set is linearly independent.

This set spans $K(\alpha)$. Indeed, consider any element $g(x) + \langle f(x) \rangle \in K(\alpha)$. If $\deg g \geq n$, we can divide by $f(x)$, and the remainder $r(x)$ will be equal to this element. In such case, $r(x) = \sum_{j=0}^{n-1} r_j x^j$. Evaluate at α: $r(\alpha) = \sum_{j=0}^{n-1} r_j \alpha^j$. This is exactly the representation of g in $K(\alpha)$ using basis. □

3.2 Existence

Let $\Phi_d(x)$ be the product of all monic irreducible polynomials of degree d. Also let S be the set of all monic irreducible polynomials over $\mathbb{F}_p[x]$. We prove the following central theorem.

Theorem 3.4. The following holds:

$$x^{p^n} - x = \prod_{d|n} \Phi_d(x)$$

Proof. Recall that $\mathbb{F}_p[x]$ is a UFD, so we can factor $x^{p^n} - x$:

$$x^{p^n} - x = c \prod_{f \in S} f(x)^{e(f)}, \quad c \in \mathbb{F}_p^\times.$$

Note that $c = 1$ since $x^{p^n} - x$ is monic. So all we have to prove is the following:

(i) If $f(x)$ divides $x^{p^n} - x$, then $f(x)^2$ does not divide $x^{p^n} - x$. This way, $e(f)$ is either 1 or 0.

(ii) Irreducible polynomial $f(x)$ divides $x^{p^n} - x$ if and only if $d = \deg f$ divides n. This way, $e(f) = 0$ for $d \nmid n$.

These two facts imply that indeed $x^{p^n} - x = \prod_{d|n} \Phi_d(x)$.

Part (i). Suppose $f(x) \mid (x^{p^n} - x)$. Then, $f(x)^2 \nmid (x^{p^n} - x)$. Indeed, suppose otherwise. Then,

$f(x)^2 g(x) = x^{p^n} - x$ for some $g \in \mathbb{F}_p[x]$. Take the formal derivative of both sides:

$$2f(x)f'(x)g(x) + f(x)^2 g'(x) = p^n x^{p^n-1} - 1 = -1 \quad \textit{(over } \mathbb{F}_p[x]\textit{)}$$

Thus, $f \mid 1$ which is not possible if $\deg f > 0$. Thus, $f(x)^2 \nmid (x^{p^n} - x)$.

Part (ii). So it remains to prove that if $f \in S$, then one has $f(x) \mid (x^{p^n} - x) \iff d \mid n$. To prove this, we construct $K := \mathbb{F}_p(\alpha)$ where α is a root of $f(x)$. By Proposition 3.3, $[K : \mathbb{F}_p] = d$, so $\#K = p^d$ and every element of K is a root of polynomial $x^{p^d} - x$.

($\Rightarrow$) Assume that $x^{p^n} - x = f(x)g(x)$. Substitute $x = \alpha$. Then one gets $\alpha^{p^n} = \alpha$. Consider any $\gamma := \sum_{j=0}^{d-1} b_j \alpha^j$ — an element of K, then $\gamma^{p^n} = \sum_{j=0}^{d-1} b_j (\alpha^{p^n})^j = \sum_{j=0}^{d-1} b_j \alpha^j = \gamma$ (here we use the fact that $\pi_{p^n} : x \mapsto x^{p^n}$ is a homomorphism). Hence, elements of K satisfy $x^{p^n} - x = 0$. It follows that $(x^{p^d} - x) \mid (x^{p^n} - x)$ and thus by Proposition 3.1, $d \mid n$.

($\Leftarrow$) Assume now that $d \mid n$. Since $\alpha^{p^d} = \alpha$ and $f(x)$ is the monic irreducible polynomial for α, we have $f(x) \mid (x^{p^d} - x)$. Since $d \mid n$, we have $(x^{p^d} - x) \mid (x^{p^n} - x)$ again by Proposition 3.1. Thus $f(x) \mid (x^{p^n} - x)$. □

Denote by N_d the number of monic irreducible polynomials of degree d in $\mathbb{F}_p[x]$. Notice that $\deg \Phi_d = d N_d$. In such case, equating degrees of Theorem 3.4, we obtain

Proposition 3.5. One has $p^n = \sum_{d|n} d N_d$. In particular, applying Möbius inversion formula, one obtains $N_n = n^{-1} \sum_{d|n} \mu(n/d) p^d$ where $\mu(n)$ is a Möbius function.

Theorem 3.6. For each $n \geq 1$, there exists an irreducible polynomial over $\mathbb{F}_p$ of degree n.

Proof. From Proposition 3.5, the number of such polynomials is $n^{-1}(p^n - \cdots + p\mu(n))$. Consider the sum in the parentheses:

$$S_n = p^n + R_n, \quad R_n := \sum_{j=1}^{n-1} b_j p^j, \quad b_j \in \{0, \pm 1\}.$$

We bound the expression for R_n:

$$|R_n| \leq \sum_{j=1}^{n-1} |b_j| p^j \leq \sum_{j=1}^{n-1} p^j \leq \frac{p^n - p}{p - 1} < p^n$$

Thus, $S_n > 0$, so $n^{-1} S_n > 0$, thus we are done. □

3.3 Uniqueness

Lemma 3.7. Let p be a prime and K be a finite field of order p^n. There exists an irreducible polynomial $f \in \mathbb{F}_p[x]$ such that $K \cong \mathbb{F}_p[x]/\langle f(x) \rangle$.

Proof. Let α be the generator of $K^\times$. Since $x^{p^n} - x = \prod_{d|n} \Phi_d(x)$, there is some irreducible polynomial $f \in \mathbb{F}_p[x]$ such that $f(\alpha) = 0$. But in such case, $\alpha^p, \alpha^{p^2}, \ldots, \alpha^{p^{n-1}}$ are its distinct roots (they are distinct because α has an order $p^n - 1$). Indeed, $f(\alpha)^p = \sum_{j=0}^{n} f_j^p \alpha^p = \sum_{j=0}^{n} f_j \alpha^p = f(\alpha^p)$. Thus, $f(\alpha^p) = 0$. By applying this repeatedly, we prove that the rest are also roots of f. Therefore, f is of degree n, thus $\mathbb{F}_p[x]/\langle f(x) \rangle$ is a field with p^n elements. Since both $\mathbb{F}_p[x]/\langle f(x) \rangle$ and K are n-dimensional vector spaces over $\mathbb{F}_p$, they are isomorphic. □

Theorem 3.8. Let p be a prime. If K_0 and K_1 are both finite fields of order p^n, then $K_0 \cong K_1$.

Proof. We know that $\mathbb{F}_p$ is a subfield of both K_0 and K_1. From Lemma 3.7, there exists an irreducible polynomial $f \in \mathbb{F}_p[x]$ of degree n such that $K_0 \cong \mathbb{F}_p[x]/\langle f(x)\rangle$. But since all elements of K_0 are roots of $x^{p^n} - x$, we have $f(x) \mid (x^{p^n} - x)$. But note that all elements in K_1 also satisfy $x^{p^n} - x$, so there is some $\beta \in K_1$ such that $f(\beta) = 0$. It follows that $K_1 = \mathbb{F}_p(\beta)$ is a vector space of dimensionality n, so $K_0 \cong K_1$. □

Example. Suppose $p \geq 5$. Then, there are at least 2 quadratic non-residues in $\mathbb{F}_p$: say, a and b. Define two quadratic extensions:

$$K_1 := \mathbb{F}_p[u]/\langle u^2 - a\rangle, \quad K_2 := \mathbb{F}_p[v]/\langle v^2 - b\rangle.$$

One easily checks these are two finite fields of order p^2. Let us build the concrete isomorphism $\phi : K_1 \to K_2$. We need to understand what u gets mapped to. So let $\phi : u \mapsto \alpha + \beta v$. Then:

$$\phi(u)^2 = (\alpha + \beta v)^2 = \alpha^2 + 2\alpha\beta v + \beta^2 v^2 = (\alpha^2 + b\beta^2) + 2\alpha\beta v = a$$

Thus, $\alpha\beta = 0$. If $\beta = 0$, then $\alpha^2 = a$, which has no solutions over $\mathbb{F}_p$. Thus, let $\alpha = 0$, then $b\beta^2 = a$, so $\beta = \sqrt{a/b}$. So the isomorphism is thus:

$$\phi : c_0 + c_1 u \mapsto c_0 + c_1\sqrt{a/b} \cdot v$$

3.4 Subfields & Applications

Important corollary which we have not yet mentioned explicitly is the following.

Lemma 3.9. Let K be a finite field of dimensionality n over $\mathbb{F}_p$. The subfields of K are in one-to-one correspondence with divisors n. In other words, if $d \mid n$, there exists a subfield $E \subseteq K$ of order p^d and it is unique.

Proof. Suppose E is a subfield of K of dimensionality d over $\mathbb{F}_p$. We shall show that $d \mid n$.

Since $E^\times$ contains $p^d - 1$ elements all satisfying $x^{p^d-1} - 1$, we have that $(x^{p^d-1} - 1) \mid (x^{p^n-1} - 1)$. By Proposition 3.1, we have $(p^d - 1) \mid (p^n - 1)$. Applying Proposition 3.1 once again, $d \mid n$.

Now, from the theory above, this field exists and it is unique up to an isomorphism. □

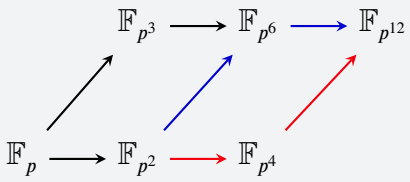
Lemma 3.9 plays a central role in various practical applications. For instance, in Cryptography, it is highly convenient and optimal to work with low-bit prime fields: for instance, over the Mersenne prime $p = 2^{31} - 1$. However, this field cannot be used in real-world applications, since it is too small (breaking the protocol with the effective brute-force size of 31 bits is trivial for modern computers). There are two natural ways to extend the number of elements: the first is to choose different p. However, another practical solution is to construct extension $\mathbb{F}_{p^d}$ for suitable d. For instance, for 31-bit Mersenne prime and $d = 4$, one can construct the 124-bit field extension $\mathbb{F}_{p^4}$, where the base field arithmetic is done very effectively.

Yet, sometimes dealing with the finite field extensions is the necessity. For instance, when implementing the bilinear pairing operation over elliptic curves, by construction one has to perform arithmetic over $\mathbb{F}_{p^k}$ where k, called an *embedding degree*, is the minimal integer such that $\mathbb{F}_{p^k}$ contains all r-th roots of unity (with r being the order of an elliptic curve). For suitable pairs (p, r),

the embedding degree is small enough to be efficiently implemented.

Still, for now we simply stated importance of finite field extensions. However, what is the use of Lemma 3.9? Suppose it so happens that $k = 12$. In such case, what is the most efficient way to implement arithmetic over $\mathbb{F}_{p^{12}}$? Obvious answer is to pick irreducible polynomial $f(x) \in \mathbb{F}_p[x]$ of degree 12 and conduct polynomial operations in the base polynomial ring $\mathbb{F}_p[x]$ modulo $f(x)$. However, this sounds highly suboptimal! The more efficient way of doing this is to exploit Lemma 3.9. We show this using a widely used prime field from [BN06].

Example (Barreto-Naehrig Field [BN06]). We consider the special case where the prime is parameterized as $p = 36x^4 + 36x^3 + 24x^2 + 6x + 1$ with $x = \mathsf{0x44E992B44A6909F1}$.
Turns out that for such prime p and suitable elliptic curve over $\mathbb{F}_p$ (also parameterized by x), the embedding degree $k = 12$. According to Lemma 3.9, we have the following lattice for $\mathbb{F}_{p^{12}}$:



This way, instead of directly building extension $\mathbb{F}_p \subset \mathbb{F}_{p^{12}}$, we can go in three different ways:

(i) $\mathbb{F}_p \subset \mathbb{F}_{p^3} \subset \mathbb{F}_{p^6} \subset \mathbb{F}_{p^{12}}$.

(ii) $\mathbb{F}_p \subset \mathbb{F}_{p^2} \subset \mathbb{F}_{p^6} \subset \mathbb{F}_{p^{12}}$ (marked in blue).

(iii) $\mathbb{F}_p \subset \mathbb{F}_{p^2} \subset \mathbb{F}_{p^4} \subset \mathbb{F}_{p^{12}}$ (marked in red).

Turns out (according, e.g., to [Hou23]) that the last two options are the most optimal: option *(i)* provides a better compression ratio while *(ii)* is slightly faster to implement. In particular, option *(ii)* is practically implemented using the following construction:

$$\begin{aligned}\mathbb{F}_{p^2} &= \mathbb{F}_p[u]/\langle u^2 + 1\rangle,\\ \mathbb{F}_{p^6} &= \mathbb{F}_{p^2}[v]/\langle v^3 - \xi\rangle,\\ \mathbb{F}_{p^{12}} &= \mathbb{F}_{p^6}[w]/\langle w^2 - v\rangle,\end{aligned}$$

where $\xi = 9 + u \in \mathbb{F}_{p^2}$.

References

[BN06] Paulo S. L. M. Barreto and Michael Naehrig. Pairing-friendly elliptic curves of prime order. In Bart Preneel and Stafford Tavares, editors, *Selected Areas in Cryptography*, pages 319–331, Berlin, Heidelberg, 2006. Springer Berlin Heidelberg.

[Hou23] Youssef El Housni. Pairings in rank-1 constraint systems. In *Applied Cryptography and Network Security*, pages 339–362, Cham, 2023. Springer Nature Switzerland. URL: https://eprint.iacr.org/2022/1162.

[IR90] K. Ireland and M.I. Rosen. *A Classical Introduction to Modern Number Theory*. Graduate Texts in Mathematics. Springer, 1990. URL: https://books.google.com.ua/books?id=jhAXHuP2y04C.